Città
metropolitana
di Milano

Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi della Città Metropolitana di Milano

Allegato n. 12

Sistema informatico

1. Sistema informatico

Il sistema di protocollo informatico in uso presso la Città metropolitana di Milano è il DocsPA di NTTDATA Italia S.p.A..
Il sistema è conforme alla normativa per i sistemi di protocollo informatico e gestione documentale (DPR 445/2000, CAD e DPCM 3 dicembre 2013), la conformità del sistema alle specifiche di cui sopra sono attestate dal fornitore con idonea documentazione come indicato nell'allegato n.1.
Al fornitore è affidata la manutenzione evolutiva e correttiva del sistema, in accordo con la normativa perla protezione dei dati personali, il fornitore è nominato responsabile per il trattamento dei dati.

2. Architettura del sistema informatico

Il sistema è composto da:

- DBMS Oracle (PAAS - platform as a service);
- repository documentale (IAAS - infrastructure as a service);
- due web application server (IAAS - infrastructure as a service);
- componenti software da installare sui client utente per funzionalità specifiche come:
    - firma digitale integrata;
    - acquisizione diretta dei documenti da scanner;
    - stampa etichette adesive per la segnatura;
    - importa ed esporta documenti.

In linea con le indicazioni della Strategia per la crescita digitale del Paese e con le previsioni del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019 – 2021, il sistema è strutturato utilizzando servizi di cloud computing erogati da Telecom Italia S.p.A. Cloud service provider (CSP) qualificato mediante l'adesione al contratto Quadro Consip SPC Cloud lotto 1.
I soggetti Cloud service provider qualificati della PA rispondono a una serie di requisiti organizzativi, di sicurezza e affidabilità, di performance e interoperabilità, fissati dalla circolare AGID n. 2 del 9 aprile 2018.
Le qualificazioni AGID assicurano che le infrastrutture siano sviluppate e fornite secondo criteri minimi di affidabilità e sicurezza considerati necessari per i servizi digitali pubblici.
Il backup del sistema è assicurato tramite servizi cloud BAAS backup as a service erogati da Telecom Italia S.p.A. Cloud service provider (CSP) qualificato mediante l'adesione al contratto Quadro Consip SPC Cloud lotto 1.
Con riferimento al trattamento dei dati personali relativamente ai servizi cloud si rimanda all'allegato n. 2.

In aggiunta al sistema in produzione, è disponibile un ambiente di test che replica l'ambiente di produzione con dati parziali e anonimizzati a tutela dei dati personali registrati.

3. Accesso al sistema

L'applicazione web è raggiungibile mediante link pubblicati all'interno del sito Intranet dell'Ente (rete interna).
Gli utenti interagiscono con l'applicazione tramite l'interfaccia utente alla quale è possibile accedere previa autenticazione con userid e password.
L'interfaccia utente viene generata in funzione delle autorizzazioni in possesso dell'utente connesso, funzionalità e dati ai quali l'utente non ha accesso non vengono resi disponibili.
Agli utenti abilitati all'accesso al sistema non è in alcun caso consentito:

- interagire direttamente con il database;
- interagire direttamente con il repository documentale;
- accedere direttamente ai server ai server siano essi fisici o virtuali.

Le suddette operazioni sono consentite esclusivamente ai soggetti autorizzati appartenenti all'Ente, o al fornitore in ragione del contratto di manutenzione, per lo svolgimento delle attività sistemistiche di amministrazione, aggiornamento e manutenzione delle componenti del sistema.
Nessuna componente del sistema è direttamente accessibile e fruibile dalla rete internet (rete esterna).

Tutte le Unità organizzative definite nell'organigramma dell'Ente sono operative nel sistema di protocollo informatico.
Il sistema consente la gestione di livelli di accesso differenziati riguardo alla registrazione e consultazione dei documenti.
L'accesso è consentito previa richiesta di abilitazione ed avviene mediante autenticazione con l'inserimento di userid e password.
L'autenticazione per l'accesso al sistema di protocollo informatico avviene con le credenziali di dominio.
Le abilitazioni per l'accesso al sistema sono rilasciate/revocate dal Responsabile della gestione documentale previa richiesta del Dirigente o del Responsabile di servizio competente e implementate con il supporto dei tecnici dei sistemi informativi.
La gestione delle utenze e dei ruoli avviene tramite un cruscotto di amministrazione cui hanno accesso esclusivamente il Responsabile della gestione documentale e i tecnici che operano in qualità di amministratori di sistema.

Il sistema prevede la disconnessione automatica dall'applicazione dopo 20 minuti di inattività. È impossibile accedere a sessioni multiple su postazioni differenti con la stessa userid.
Gli utenti interni autorizzati ad utilizzare il sistema devono operare nel rispetto del "Disciplinare per l'utilizzo dei servizi informatici e di comunicazione telematica" adottato dall'Ente.
Gli addetti autorizzati ad accedere al sistema di protocollo informatico e gestione documentale, sono formalmente incaricati con riferimento a quanto indicato nel Regolamento per la protezione dei dati personali adottato dall'Ente.

Il sistema espone inoltre una serie di servizi web (web services) per l'integrazione con altri applicativi e prodotti di terze parti e per consentire l'interoperabilità dei sistemi informatici.
In aggiunta alle utenze personali sono gestite utenze di servizio utilizzate per l'integrazione del sistema con altre applicazioni informatiche.

4. Profilazione delle utenze e visibilità di documenti e fascicoli

In fase di abilitazione ogni utente è inserito in uno o più ruoli collegati ad una Unità organizzativa, per ciascuno dei quali sono definite, in base alle competenze e ai compiti istituzionali, le specifiche funzioni che gli utenti possono svolgere nel sistema e il livello di visibilità sui documenti e sui fascicoli.
La visibilità di documenti e fascicoli è limitata alla struttura proprietaria ed alle strutture gerarchicamente superiori definite in organigramma.
L'estensione gerarchica della visibilità dei documenti può essere bloccata con la creazione di un protocollo "Privato".
La selezione della casella "Privato" è possibile solo al momento della creazione di un nuovo documento. Una volta che il documento è stato protocollato o salvato, non è permessa la modifica di questo attributo.
A differenza dei documenti principali, non è consentita la creazione di un documento allegato con la specifica "Privato" in considerazione del fatto che l'allegato non ha visibilità propria, ma è soggetto alla medesima visibilità del documento principale a cui è stato associato e da cui non può essere scisso.
Le registrazioni di protocollo effettuate con modalità "Privato", sono accessibili esclusivamente agli utenti appartenenti ai ruoli della Unità organizzativa che ha effettuato la registrazione.
La visibilità dei documenti può essere estesa con una trasmissione e con la fascicolazione.
Il criterio applicato dal sistema per la gestione della visibilità dei documenti vale anche per i fascicoli.

I ruoli definiti nel sistema sono:

- Responsabile

  E' il Dirigente dell'Unità organizzativa con accesso in sola consultazione, non può protocollare i documenti.
- Controllore ACL

  Gli utenti di questo ruolo possono limitare la visibilità di un documento per ragioni di riservatezza e tutela della privacy.

  E' possibile agire sulla lista di controllo degli accessi (ACL) del documento per rimuovere la visibilità dello stesso a ruoli ai quali ad esempio è stato trasmesso per errore o per gestire il c.d. protocollo riservato.
- Impiegato

  Gli utenti abilitati a questo ruolo non possono protocollare i documenti, hanno accesso in consultazione sui documenti/fascicoli di propria competenza.
- Protocollista

  Appartengono a questo ruolo gli utenti a cui è assegnato il compito di registrare i documenti.

Al ruolo di protocollista sono associate le seguenti funzionalità:

a. registrazione documenti arrivo, partenza, interni;
b. classificazione e fascicolazione;
c. protocollazione in emergenza (solo per le postazioni dedicate);
d. modifica oggetto e mittente/destinatario;
e. aggiornamento anagrafica mittente/destinatario.

- Fascicolatore

Appartengono a questo ruolo gli utenti abilitati alla creazione dei fascicoli.

L'ordine di elencazione dei ruoli segue l'ordine gerarchico con cui gli stessi sono definiti, ciò significa che i documenti e i fascicoli trasmessi ad esempio ad un protocollista sono automaticamente visibili all'impiegato ed al responsabile in quanto ruoli gerarchicamente superiori.
Ai ruoli sopra elencati si aggiungono quelli del Servizio Gestione e conservazione documentale:

- Responsabile;
- Conservazione;
- Presidio caselle di posta elettronica istituzionale;
- Lettore.

Con specifiche funzionalità è possibile restringere ulteriormente l'accesso ai singoli documenti considerati riservati per tutelare dati personali o per questioni di riservatezza ed opportunità.
Ciascuna Unità organizzativa valuta il livello di riservatezza di ciascun documento ed opera ad eventuali restrizioni in aggiunta ai criteri generali applicati dal sistema per la gestione dei documenti riservati.

La descrizione funzionale e operativa dettagliata del software è illustrata nel manuale d'uso dell'applicativo di cui all'allegato n. 3.

NTT DATA

Global IT Innovator

Analisi del sistema DOCSPA in relazione alla normativa vigente

Documento analisi

Codice: DOCSPA-2015_001_01

Data emissione/ultima modifica: 30-12-2015

Distribuzione: CLIENTI DOCSPA

EVOLUZIONE DEL DOCUMENTO

Versione	Descrizione
01	Prima emissione

INDICE

1 INTRODUZIONE

1.1 Premessa

Il sistema DocsPA è stato realizzato in base ai requisiti richiesti dal Testo Unico in materia di documentazione amministrativa (DPR 445/2000) e alla precedente normativa sul protocollo informatico, il DPR 428/1998 e relative regole tecniche, poi sostituiti dal TUDA che raccoglie le disposizioni legislative e regolamentari contenute nel DLG 28 dicembre 2000, n. 443 e nel DPR 28 dicembre 2000, n. 444. In seguito il Codice dell'Amministrazione Digitale è diventato il principale testo normativo di riferimento (D. Lgs 82/2005). L'introduzione delle nuove funzionalità e le evoluzioni del sistema nel corso degli anni hanno tenuto conto dei nuovi standard e delle nuove Regole Tecniche introdotte nei Decreti del Presidente del Consiglio dei Ministri per l'applicazione del Codice dell'Amministrazione Digitale.

Le ultime Regole Tecniche sulla conservazione e sul protocollo informatico risalgono al DPCM del 3 dicembre 2013 e sono state pubblicate sulla Gazzetta Ufficiale il 12 marzo 2014. Le pubbliche amministrazioni devono adeguare i propri sistemi di gestione informatica dei documenti entro e non oltre 18 mesi dall'entrata in vigore del decreto e pertanto entro e non oltre il 12 ottobre 2015. Sulla Gazzetta Ufficiale del 12 gennaio 2015 sono state pubblicate invece le ultime Regole Tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di conservazione dei documenti informatici delle pubbliche amministrazioni (DPCM 13 Novembre 2014) alle quali le Pubbliche amministrazioni dovranno adeguarsi ancora entro e non oltre diciotto mesi dall'entrata in vigore del decreto e cioè entro e non oltre il 12 agosto del 2016. In uno scenario internazionale invece il Regolamento (UE) n.910/2014 del Parlamento Europeo e del Consiglio del 23 Luglio 2014 pone requisiti in materia di firma elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno che vanno ad abrogare la direttiva 1999/93/CE. Tale regolamento stabilisce le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e le regole comuni, oltre che per le firme elettroniche, anche per l'autenticazione web. Tale regolamento si applica a decorrere dal 1° luglio 2016.

1.2 Scopo e area di applicazione

Con il presente documento si intende descrivere le funzionalità del sistema DocsPA rispetto alle indicazioni ed ai requisiti di cui alle norme citate in precedenza tra le quali, in particolare il Codice dell'Amministrazione Digitale (CAD) e il Testo Unico in materia di documentazione amministrativa (DPR 445/2000).

2 RISPOSTA DEL SISTEMA DOCSPA ALLA NORMATIVA VIGENTE

2.1 Protocollo informatico

Il DPCM del 3 dicembre 2013 richiede nel dettaglio un adeguamento alle norme in materia di **Protocollo informatico**. Nello specifico alcuni articoli sono riservati al tema delle funzionalità minime di un sistema informatico, altri presentano i requisiti minimi di sicurezza dei sistemi di protocollo informatico e altri ancora pongono le regole per l'annullamento informatico delle registrazioni in forma immodificabile. Attenzione particolare viene poi posta sul formato della

segnatura di protocollo. Analizziamo di seguito le funzionalità del sistema DocsPA rispetto ai requisiti previsti dalla normativa sopra citata.

2.1.1 Requisiti minimi di sicurezza dei sistemi di protocollo informatico

Per quanto riguarda i requisiti minimi di sicurezza il sistema DocsPA permette:

- l'univoca identificazione ed autenticazione degli utenti come richiesto dall' Art.7 c.1 lett. a) permettendo infatti nel modulo di amministrazione di censire gli utenti che hanno accesso al sistema e di associare ad ogni utente un codice proprio ed una password propria che lo identifica univocamente.
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri come previsto dall' Art.7 c.1 lett b), consentendo ad un utente amministratore di gestire i dati e le informazioni relative ai singoli utenti.
- l'accesso alle risorse esclusivamente agli utenti abilitati secondo l' Art.7 c.1 lett c). Nel modulo di amministrazione è possibile abilitare ogni singolo utente a determinate funzioni attraverso la configurazione nell'organigramma di un ruolo di appartenenza e l'amministratore può abilitare o meno l'utente all'accesso nel sistema.
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione (Art.7 c.1 lett d)). Nel modulo di amministrazione del sistema è possibile tener traccia delle azioni di ogni utente attraverso l'abilitazione dei Log. Si può decidere nello specifico di quali azioni tener traccia o meno.

Il sistema DocsPA, in base a quanto richiesto dall' Art.7 c.2, assolve alla funzione di controllo differenziato dell'accesso alle risorse per ciascun utente o gruppo di utenti. Ogni utente può infatti accedere soltanto a determinate risorse in funzione del gruppo di appartenenza.

DocsPA inoltre consente il tracciamento degli eventi di modifica delle informazioni trattate e l'individuazione del suo autore (Art.7 c.3).

La modifica delle informazioni è consentita esclusivamente agli utenti espressamente autorizzati (Art. 7 c.4)

Il sistema DocsPA non consente la modifica del registro giornaliero di protocollo. Inoltre ne può consentire la trasmissione, entro la giornata lavorativa successiva alla sua generazione, ad un sistema di conservazione (Art.7 c.5). DocsPA infatti può facilmente integrarsi tramite WS con sistemi di conservazione (già esistenti o sviluppati *ad hoc*) che gestiscono tale processo, oltre a disporre esso stesso di uno specifico modulo software già integrato per la gestione del processo di conservazione con opportune impostazioni.

Il sistema DocsPA ha implementato funzionalità che prendono in considerazione le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, come richiesto dall'Art.7 c.6 del DPCM. Si precisa al riguardo che il rispetto di tali misure di sicurezza è legato anche alla sussistenza di fattori e requisiti di sistema e di infrastruttura estranei al sistema DocsPA medesimo e con il quale quest'ultimo potrebbe interfacciarsi (ad es. alcuni requisiti riguardanti l'infrastruttura sulla quale viene installato il sistema DocsPA).

Secondo quanto richiesto nell'Art.34 c.1 del Codice in Materia di Protezione dei Dati Personali, il trattamento dei dati personali effettuato con DocsPA prevede:

- L'autenticazione informatica;

- L'adozione di procedure di gestione delle credenziali di autenticazione (sono gestite, nello specifico, la scadenza della password, il formato della password, l'annullamento della password con necessità di cambiamento al primo accesso. Inoltre la password viene memorizzata sul DB in forma cifrata);

Il sistema DocsPA consente di attribuire un determinata configurazione di riservatezza a particolari tipologie di documenti che sono così accessibili esclusivamente alle persone designate al loro trattamento. Inoltre il sistema DocsPA dispone di un insieme di regole che permettono il controllo sull'accessibilità dei documenti e dati in esso gestiti da parte degli utenti stessi del sistema. Pertanto tutti i dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari possono in tal modo essere preservati dalla visibilità di utenti non autorizzati (Art.34 c.1 lett h).

Relativamente all'Allegato B al codice in Materia di Protezione dei Dati Personali ovvero il disciplinare tecnico in materia di misure minime di sicurezza DocsPA consente quanto segue:

- configurare dei particolari ruoli per gli utenti riservati al trattamento di dati personali dotando gli incaricati di credenziali che consentono il superamento di una procedura di autenticazione relativa ad uno specifico trattamento..
- fornire credenziali di autenticazione che consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato
- assegnare o associare ad ogni incaricato individualmente una o più credenziali per l'autenticazione. impostare l'obbligo di utilizzare una parola chiave, composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; la parola chiave viene impostata per il primo accesso dall'amministratore e obbligatoriamente dovrà essere modificata dall'incaricato al primo utilizzo. Il sistema DocsPA consente di impostare regole per la composizione della parola chiave. L'intervallo temporale oltre il quale è necessario modificare la password si può impostare indipendentemente dalla tipologia del dato trattato.
- Un codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Il sistema DocsPA impedisce l'uso dello stesso codice identificativo per utenti differenti e, nel caso in cui più Amministrazioni utilizzino la stessa istanza del sistema, permette di verificare, quando una Amministrazione registra un nuovo utente se questo sia già registrato come utente di un'altra Amministrazione. In questo caso il sistema chiede conferma della volontà di creare un utente comune ad entrambe le Amministrazioni.
- DocsPA, consente di disattivare le credenziali di autenticazione non utilizzate per un periodo che l'amministrazione configurerà di volta in volta, potendo fare eccezione per quelle preventivamente autorizzate per soli scopi di gestione tecnica. Il sistema DocsPA consente di disattivare le credenziali anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. Il sistema DocsPA, nel caso in cui un utente perda il suo ruolo e quindi le sue funzionalità e le sue autorizzazioni, consente di mantenere l'utente censito ma disabilitato all'accesso.
- Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione. Il sistema DocsPA può essere integrato con sistemi esterni di autenticazione e gestione delle identità e degli accessi (IAM, Shibboleth, ecc…). Inoltre il sistema DocsPA consente di associare ad uno stesso utente profili di autorizzazione differenti, ovvero uno o più ruoli, ciascuno con un proprio specifico profilo funzionale e propri diritti di visibilità sui documenti.

- I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Un utente può accedere al sistema DocsPA solo se precedentemente è stato associato ad uno specifico ruolo in organigramma (non è sufficiente il suo censimento come utente); dalla posizione in organigramma e dal profilo funzionale del ruolo deriva il "profilo di autorizzazione" dell'utente sia in termini di funzionalità che è abilitato ad utilizzare, sia in termini di documenti a cui può avere accesso.
- Per quanto riguarda la frequenza degli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti anche in caso di trattamento di dati sensibili o giudiziari il requisito è legato alla gestione dell'infrastruttura del sistema.
- La protezione dall'accesso abusivo a dati sensibili o giudiziari di cui all'art. 615-ter del codice penale, può essere garantita mediante l'utilizzo di idonei strumenti elettronici di supporto che debbono essere messi a diposizione dalle piattaforme su cui viene istallato DOCSPA. Attraverso le funzioni di tipizzazione dei documenti è possibile separare particolari dati sensibili o giudiziari da altre tipologie di informazioni.

2.1.2 Annullamento delle informazioni registrate in forma immodificabile

Passiamo ad analizzare la risposta del sistema a quanto richiesto dalla normativa in materia dell'annullamento delle informazioni registrate in forma immodificabile.

Nel sistema DocsPA:

- l'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile è possibile solo con il contestuale annullamento dell'intera registrazione di protocollo come richiesto dall' Art.8 c.1 del DPCM del 3 dicembre 2013.
- L'annullamento anche di un solo campo delle altre informazioni registrate in forma immodificabile, necessario per correggere errori intercorsi in sede di immissione di dati delle altre informazioni, comporta la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica. La disposizione di cui al primo periodo si applica per lo stesso campo, od ogni altro, risultato successivamente errato. (Art.8 c.2 del DPCM del 3 dicembre 2013).
- Le informazioni originarie, successivamente annullate, vengono memorizzate secondo le modalità specificate nell'art. 54 del testo unico [DPR 445 del 28 dicembre 2000], come richiesto dall'Art.8 c.3 del DPCM del 3 dicembre 2013, ovvero il numero di protocollo del documento, la data di registrazione di protocollo, il mittente per i documenti ricevuti, il destinatario o i destinatari per i documenti spediti, l'oggetto del documento, la data e il protocollo del documento ricevuto e l'impronta del documento sono annullabili e le informazioni annullate sono memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura. La procedura per indicare l'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione.

2.1.3 Formato della segnatura di protocollo

Per quanto richiesto sul formato della segnatura di protocollo, in DocsPA

- Le informazioni apposte o associate ai documenti informatici, registrati nel registro di protocollo, negli altri registri di cui all'art. 53, comma 5, del testo unico, nei repertori e negli archivi, nonché negli albi, negli elenchi e in ogni raccolta di dati concernente stati, qualità personali e fatti con le modalità descritte nel manuale di gestione, mediante l'operazione di segnatura di cui all'art. 55 del testo unico che ne garantisce l'identificazione univoca e certa, sono espresse nel seguente formato:
  - Codice identificativo dell'amministrazione;
  - Codice identificativo del registro;
  - Data di protocollo;
  - Progressivo di protocollo costituito da almeno sette cifre numeriche. La numerazione è rinnovata ogni anno solare.
  - Codice identificativo dell'area organizzativa omogenea.

  Il sistema DocsPA consente la configurazione del formato della segnatura. L'amministratore del sistema può selezionare i valori da inserire nella segnatura tra quelli elencati, l'anno di protocollazione, l'ora di protocollazione e il tipo di registrazione. La rispondenza della segnatura a quanto previsto dalla normativa dipende pertanto da come viene configurata dall'Amministrazione; in particolare, in DocsPA il codice identificativo dell'area organizzativa omogenea è legato al Registro, è cioè presente se viene utilizzato come codice del registro il codice dell'AOO.

2.2 Formato e modalita' di trasmissione dei documenti informatici tra pubbliche amministrazioni

Il sistema DocsPA permette alle pubbliche amministrazioni di comunicare attraverso la funzione di interoperabilità rispondendo ai requisiti richiesti dall'articolo 10 c.2 del DPCM del 3 dicembre 2013.

Le pubbliche amministrazioni che mediante proprie applicazioni informatiche accedono al sistema, adottano le modalità di interconnessione stabilite nell'ambito delle norme e dei criteri tecnici emanati per la realizzazione della rete unitaria delle pubbliche amministrazioni. (Art.60 c.1 DPR 445 del 28 dicembre 2000).

Le pubbliche amministrazioni che accedono al sistema grazie all'interoperabilità, secondo quanto richiesto dall'Art.60 c.2 del DPR445/2000, possono ottenere le seguenti informazioni:

a) numero e data di registrazione di protocollo dei documenti, ottenuti attraverso l'indicazione alternativa o congiunta dell'oggetto, della data di spedizione, del mittente, del destinatario;

b) numero e data di registrazione di protocollo del documento ricevuto, ottenuti attraverso l'indicazione della data e del numero di protocollo attribuiti dall'amministrazione al documento spedito.

Il codice identificativo dell'amministrazione, assegnato automaticamente dall'indice IPA in fase di accreditamento, è riportato nei dati della segnatura di protocollo (Art.13 c.1 DPCM 3 dicembre 2013) se viene riportato come codice di AOO.

2.2.1 Modalita' di trasmissione dei documenti informatici mediante l'utilizzo della posta elettronica e in cooperazione applicativa

Lo scambio dei documenti soggetti alla registrazione di protocollo nel sistema DocsPA è effettuato mediante messaggi di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC821-822, RFC 2045 e 2049 e successive modificazioni. (Art.16 c.1)

Il Codice dell'Amministrazione Digitale nell'Art.47 stabilisce le norme riguardo alla trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni. Esso richiede che le comunicazioni di documenti tra le pubbliche amministrazioni avvengano mediante l'utilizzo della posta elettronica o in cooperazione applicativa; tali comunicazioni sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. DocsPA realizza proprio l'interoperabilità tra sistemi di protocollo di amministrazioni differenti mediante il canale della PEC.

Il sistema DocsPA, nella comunicazione tra le pubbliche amministrazioni, supporta l'accertamento della provenienza dei documenti informatici ricevuti per via telematica, secondo quanto previsto dall'Art. 47 c.2 del CAD,

- consentendo l'integrazione con specifici servizi di verifica di validità delle firme digitali o realizzando un'analoga verifica con propri strumenti,

- elaborando automaticamente la segnatura xml dei documenti ricevuti per interoperabilità e mantenendo associato al documento e visibile dall'utente il file xml della segnatura,

- - valorizzando automaticamente il mittente del documento con l'indirizzo mail di provenienza o i dati del corrispondente censito nell'anagrafica del sistema che ha associato tale indirizzo.

2.2.2 Modalita' di registrazione dei documenti informatici

Il sistema DocsPA ad ogni messaggio ricevuto o spedito da un'area organizzativa omogenea di una pubblica amministrazione fa corrispondere un'unica operazione di registrazione di protocollo (Art.18 c.1), con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, permettendo il completamento dell'intera operazione di modifica o registrazione dei dati come richiesto dal DPR 445/2000 nell'Art.53 c.3.

La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni (Art.53 c.1 DPR 445/2000):

- il numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

DocsPA consente la produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno come richiesto dal DPR 445/2000 nell'Art.53 c.2.

I documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici sono registrati nel sistema DocsPA (Art.53 c.5 DPR 445/2000). Sono comprese le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica (semplice o certificata).

L'eventuale indicazione dell'ufficio utente, ovvero del soggetto, destinatario del documento, è riportata nella segnatura di protocollo e cioè nel file .xml della segnatura come chiesto nell' Art. 53 c.5 del DPR 445/2000 e come vedremo meglio in seguito.

2.2.3 Impronta del documento informatico

Nell'effettuare l'operazione di registrazione di protocollo dei documenti informatici il sistema DocsPA calcola l'impronta per ciascun documento informatico associato alla registrazione di protocollo utilizzando la funzione crittografica di hash definita nella deliberazione CNIPA 45/2009, recante le regole per il riconoscimento e la verifica del documento informatico, secondo quanto emanato nell' Art.19 del DPCM in materia del protocollo informatico del 3 dicembre 2013.

2.2.4 Segnatura di protocollo dei documenti trasmessi

Nel sistema DocsPA i dati relativi alla segnatura di protocollo di un documento trasmesso da un'area organizzativa omogenea sono associati al documento stesso e contenuti, nel messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition). Nelle attività di manutenzione sono realizzati gli aggiornamenti necessari relativamente agli standard, alle modalità di trasmissione, ai formati e alle definizioni dei tipi di informazioni scambiate tra le amministrazioni pubbliche e associate ai documenti protocollati come richiesto nell' Art.20 del DPCM del 3 dicembre 2013.

Il file .xml contenente i dati relativi alla segnatura di protocollo racchiude inoltre le seguenti informazioni:

- l'oggetto
- il mittente
- il destinatario o i destinatari

come richiesto nell' Art.21 c.1 del DPCM del 3 dicembre 2013.

Nella segnatura di un documento protocollato in uscita da un'Amministrazione possono essere specificate inoltre una o più delle seguenti informazioni incluse anch'esse nello stesso file:

- indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento; e/o
- l'indice di classificazione; e/o
- l'identificazione degli allegati,

come indicato nell'art.21 c.2 del DPCM del 3 dicembre 2013, ma non sono gestiti dal sistema dati specifici sull'iter amministrativo a cui è soggetto il documento. Vengono gestiti soltanto i dati legati alla classificazione e alla fascicolazione del documento, se tali operazioni sono state effettuate nel sistema DocsPA.

È possibile estendere il file .xml della segnatura di protocollo di un documento informatico se due o più amministrazioni stabiliscono di scambiarsi informazioni non previste tra quelle indicate nell'Art.21 c.2 ed elencate precedentemente, includendo informazioni specifiche stabilite di comune accordo, nel rispetto delle indicazioni tecniche stabilite dall'Agid (Art.21 c.3 DPCM del 3 dicembre 2013).

2.2.5 Comunicazioni tra imprese e amministrazioni pubbliche

Il sistema DocsPA si integra con i canali si comunicazione telematica (posta elettronica semplice e posta elettronica certificata) consentendo di gestire direttamente a partire dal sistema le operazioni di ricezione, registrazione e spedizione dei messaggi/documenti scambiati dall'amministrazione con soggetti esterni pubblici e privati come indicato nell' Art.5 bis del Codice di Amministrazione Digitale.

2.3 Documento informatico

2.3.1 Segnatura di protocollo

Il sistema DocsPA permette di associare all'originale del documento la segnatura di protocollo e di apporla sul documento anche attraverso un timbro. Tale apposizione o associazione viene effettuata in forma permanente non modificabile delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile. La segnatura di protocollo contiene le seguenti informazioni previste dal D.P.R. 445/2000 nell'Art.55 c.1:

- Il progressivo di protocollo
- La data di protocollo
- L'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa omogenea.

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo come richiesto sempre dal D.P.R 445/2000 nell'Art.55 c.2.

Mediante una opportuna configurazione del sistema DocsPA è possibile includere nell'operazione di segnatura il codice identificativo dell'ufficio cui il documento è assegnato o il codice dell'ufficio che ha prodotto il documento, l'indice di classificazione del documento e ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo (D.P.R 445/2000 Art.55 c.3).

Con la segnatura in formato .xml è possibile includere tutte le informazioni di registrazione del documento che sono state selezionate dall'Amministrazione all'atto della configurazione. Quando il documento è indirizzato ad altre amministrazioni ed è formato e trasmesso con strumenti informatici, l'amministrazione che riceve il documento informatico può utilizzare le informazioni di registrazione del documento per automatizzare le operazioni di registrazione di protocollo del documento ricevuto (D.P.R. 445/2000 Art.55 c.4)

Il formato e la struttura delle informazioni associate al documento informatico tengono conto di quanto stabilito al c4 del D.P.R. 445/2000.

2.4 Operazioni ed informazioni minime del sistema di gestione informatica dei documenti

Il sistema DocsPA consente di gestire la protocollazione e la fascicolazione, operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni (D.P.R. 445/2000 Art.56 c.1).

2.4.1 Formazione del documento amministrativo informatico

Il documento amministrativo informatico è identificato e trattato nel sistema comprensivo del registro di protocollo e degli altri registri, dei repertori e degli archivi, nonchè degli albi, degli elenchi e di ogni raccolta di dati concernente stati, qualità personali e fatti già realizzati dalle amministrazioni su supporto informatico, in luogo dei registri cartacei con le modalità descritte nel manuale gestione (DPCM 14 novembre 2014, Art.9 c.3)

In DocsPA il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema come richiesto nella normativa nell'art.9 c.5 del DPCM DEL 14 novembre 2014.

In DocsPA è possibile andare incontro alle diverse esigenze delle pubbliche amministrazioni riguardanti i diversi formati da utilizzare. È possibile alle pubbliche amministrazioni utilizzare diversi formati in relazione agli specifici contesti operativi che devono essere esplicitati, motivati e riportati nel manuale di gestione (DPCM 14 novembre 2014, Art.9 c.6).

Al documento amministrativo informatico sono associati, oltre all'insieme minimo, eventuali ulteriori metadati rilevanti ai fini amministrativi, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce (DPCM 14 novembre 2014, Art.9 c.8).

2.4.2 Copie su supporto informatico di documenti amministrativi analogici

Il sistema DocsPA consente di inserire nel documento informatico contenente la copia informatica di un documento amministrativo analogico, formato dalla pubblica amministrazione, ovvero da essa detenuto, l'attestazione di conformità della copia stessa. Il documento informatico così formato può essere sottoscritto con firma digitale o firma elettronica qualificata del funzionario delegato grazie alle funzionalità di firma presenti nel sistema (DPCM 14 novembre 2014, Art.10 c.1).

Il sistema DocsPA consente di produrre l'attestazione di conformità, anche nel caso di uno o più documenti amministrativi informatici. Tale attestazione viene effettuata mediante un'operazione di raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche finalizzate ad accertare la corrispondenza del contenuto dell'originale e della copia, come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia. Il sistema DocsPA consente ove richiesto la sottoscrizione del documento informatico prodotto, con firma digitale o con firma elettronica qualificata del funzionario delegato. (DPCM 14 novembre 2014, Art.10 c.2).

2.5 Procedimento e fascicolo informatico

2.5.1 Procedimento e fascicolo informatico

La normativa richiede che la pubblica amministrazione titolare del procedimento raccolga in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati

(CAD Art.41 c.2). Il sistema DocsPA consente la creazione e la gestione di fascicoli elettronici, legati al piano di classificazione dell'archivio, e l'aggregazione in essi di documenti protocollati (prodotti o ricevuti dall'amministrazione) e non protocollati ma comunque registrati nel sistema.

Il fascicolo nel sistema DocsPA è accessibile soltanto ad utenti dell'amministrazione titolare del procedimento.. L'accesso selettivo ai contenuti del fascicolo da parte di altri eventuali soggetti individuati dall'Amministrazione titolare può avvenire tramite interfacce specifiche, quali portali o altri sistemi, e può essere realizzato attraverso apposite API già offerte dal sistema o personalizzate *ad hoc* in funzione del tipo di accesso che deve essere consentito. I documenti aggregati nel fascicolo sono gestiti nella loro formazione, conservazione, trasmissione secondo quanto dettato dalle regole tecniche analizzate nel presente documento. (CAD Art.41 c.2-bis)

Ciascun fascicolo creato e gestito nel sistema è sempre riconducibile alla specifica amministrazione che lo ha creato e che ne cura la gestione, essendo possibile l'utilizzo del sistema solamente a seguito della configurazione di determinati parametri che individuano e descrivono l'ente utilizzatore e gli enti del sistema. (CAD Art.41 c.2-ter lett.a) Ogni fascicolo creato nel sistema ha inoltre associati determinati metadati che ne costituiscono il "profilo standard", tra questi figurano come obbligatori l'oggetto del procedimento (espresso come descrizione del fascicolo), i dati identificativi del fascicolo (espresso come codice del fascicolo il cui formato è configurabile). Nel sistema DocsPA è possibile associare un fascicolo ad una tipologia documentale. Questo consente di assegnare al fascicolo ulteriori dati e tra questi quelli relativi alle amministrazioni partecipanti al procedimento (trattandosi di oggetto concepito come interno al sistema) e quelli relativi al responsabile del procedimento (che, a seconda delle regole organizzative dell'ente, potrebbe o meno coincidere con l'utente che forma il fascicolo nel sistema e di cui è tenuta traccia). In aggiunta ai metadati indicati, il fascicolo ha associati i documenti che ne fanno parte, visualizzabili come elenco di oggetti contenuti nel fascicolo e da qui direttamente accessibili (CAD Art.41 c.2-ter lett. b, c, d, e, e-bis).

I contenuti del fascicolo possono essere distribuiti in più sottofascicoli i quali possono a loro volta essere organizzati in una gerarchia a più livelli. La visibilità su tali sottofascicoli da parte degli utenti interni al sistema, ovvero appartenenti all'Amministrazione titolare del trattamento del fascicolo, segue quella del fascicolo padre. Tuttavia l'accesso selettivo ai contenuti del fascicolo da parte di altri eventuali soggetti individuati dall'Amministrazione titolare può avvenire tramite interfacce specifiche, quali portali o altri sistemi, e può essere realizzato attraverso apposite API già offerte dal sistema o personalizzate *ad hoc* in funzione del tipo di accesso che deve essere consentito. L'organizzazione dei contenuti in sottofascicoli, garantisce comunque che tutti i documenti di un dato procedimento, aggregati in un fascicolo, siano tra loro collegati grazie a tale aggregazione, accessibili a partire dal fascicolo stesso (CAD Art.41 c.2-quater).

I fascicoli fanno parte del sistema di gestione informatica dei documenti e contengono l' insieme minimo dei metadati indicato nel CAD Art.41 c.2-ter. La classificazione è determinata autonomamente dalle amministrazioni che definiscono adeguati piani per tutti i documenti, compresi quelli non soggetti a registrazioni di protocollo (DPCM 14 novembre 2014 Art.13 c.1).

Attraverso la gestione del fascicolo il sistema DocsPA permette di gestire eventuali aggregazioni documentali informatiche individuate da una chiave di aggregazione come richiesto nell'Art.13 c.2 del DPCM del 14 novembre 2014; ulteriori aggregazioni possono essere realizzate attraverso il salvataggio di ricerche documentali o attraverso particolari funzionalità.

2.5.2 Trasferimento in conservazione

Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale può generare, in DOCSPA a fronte di opportune integrazioni con sistemi esterni di

conservazione per uno o più fascicoli, un pacchetto di versamento che contiene i riferimenti che identificano univocamente i documenti informatici appartenenti al fascicolo con modalità differenti a seconda del servizio di conservazione con cui si integra (DPCM 14 novembre 2014 Art.15 c.1).

2.6 Registri e repertori informatici

2.6.1 Formazione dei registri e repertori informatici

I registri di protocollo e gli altri registri, i repertori, gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti realizzati dalle amministrazioni su supporto informatico in luogo dei registri cartacei sono formati da una generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica (Art.14 c.1 DPCM 14 novembre 2014). Per i repertori in particolare dipende dalla gestione degli enti.

Le pubbliche amministrazioni in DocsPA possono gestire registri particolari informatici, espressamente previsti da norme o regolamenti interni, generati dal concorso di più aree organizzative omogenee con le modalità previste ed espressamente descritte nel manuale di gestione, individuando un'area organizzativa omogenea responsabile (DPCM 14 novembre 2014 Art.14 c.2).

2.6.2 Trasferimento in conservazione dei registri e repertori informatici

Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale può generare in DOCSPA a fronte di opportune integrazioni con sistemi esterni di conservazione, per uno o più registri o repertori informatici, un pacchetto di versamento che contenga i riferimenti che identificano univocamente i documenti informatici appartenenti all'aggregazione documentale informatica con modalità differenti a seconda del servizio di conservazione con cui si integra (DPCM 14 novembre 2014 Art.15 c.1). DocsPA infatti può facilmente integrarsi tramite WS con sistemi esterni di conservazione (già esistenti o sviluppati *ad hoc*) che gestiscono tale processo, oltre a disporre esso stesso di uno specifico modulo software già integrato per la gestione del processo di conservazione con opportune impostazioni.

DOCUMENTO PROGRAMMATICO DI GESTIONE DELLA SICUREZZA DEI SERVIZI CLOUD TIM SPC

Gestione	Funzione	Riferimento
REDATTO:	CR.MB.ECC.C	Dario Piccirilli (ULS)
	CR.MB.ECC.C	Mauro Vittorini (ULS)
VERIFICATO:	CR.MB.ECC.C	Salvatore Brocca (ULS)
	CR.MTP.POS	Filippo Dall'Olio
	CR.MTP.SPAC	Massimiliano Materazzi
	CR.MB.ECC.A	Orazio Fichera, Giustiniano De Francesco, Vessela Tchechankova
	CR.MTP.POS	Maria Vittoria Tirone
	CR.MB.ECC.I	Marco Sbrega
	CR.MB.ECC.U	Fabrizio Seri
	CR.MB.ECC.I	Antonio Maiello
	CR.CD.R.PM.I	Massimo Dessi
	CR.CD.R/CS.S	Pierluigi Grasso
	CR.CD.R.PM.D	Paolo Bello
APPROVATO:	CR.CD.R	Antonio Barone
	CR.MTP.SPAC	Giovanni Santocchia
	CR.MB.ECC	Fabrizio Broccolini
N° allegati:		

Il presente documento è stato redatto in coerenza con il Codice Etico e di Condotta ed il Modello Organizzativo 231 del Gruppo TIM

INDICE

INDICE DELLE FIGURE

INDICE DELLE TABELLE

1 REVISIONI

REVISIONE	DATA	COMMENTO
1	01/03/2017	Prima emissione
2	24/07/2018	Seconda emissione che include il sito di Pomezia, i servizi managed e gli adempimenti necessari all'adeguamento al nuovo Regolamento UE n. 679/2016 in materia di protezione dei dati personali (General Data Protection Regulation, GDPR) ed alle misure minime AgID
3	03/08/2018	Eliminate le clausole di nomina a Responsabile del trattamento proposte da TIM
4	01/10/2018	Estensione del perimetro del Centro Servizi TIM ai 5 Data Center TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli – Cesano Maderno (MI).
5	28/12/2018	Inseriti i servizi di Cloud Enabling e tabella 19 con elenco subfornitori TIM
6	20/01/2020	• Aggiornate le sigle delle strutture aziendali TIM coinvolte nei servizi. • Inseriti i servizi IaaS e PaaS basati sulle nuove tecnologie Cisco-Canonical Openstack • Aggiornati i documenti che costituiscono i Profili di Sicurezza dei servizi IaaS e PaaS • Referenziati i documenti che costituiscono i Profili di Sicurezza delle PaaS con RDBMS Oracle basate su tecnologia Oracle OCM e Oracle-Hitachi • Inserito il servizio di *Conservazione a norma* di TI Trust Technologies Srl

2 RIFERIMENTI

2.1 Contratto quadro e documentazione di riscontro

Nel seguito vengono elencati i riferimenti relativi al contratto quadro ed ai documenti di riscontro utilizzati nel documento.

[CQ1]	Allegato 4A - Schema Contratto Quadro - Lotto1
[CQ2]	Capitolato Tecnico - parte generale
[CQ3]	Relazione Tecnica Lotto 1
[CQ4]	PDS CLOUD SPC Lotto 1
[CQ5]	Evoluzione piattaforma OpenStack SPC Cloud - Solution Guide

2.2 Documentazione interna

Nel seguito vengono elencati i riferimenti relativi alla documentazione interna TIM, generalmente classificata ad “Uso Interno – Telecom Italia”.

[RI1]	BU1600003 - Piano di Sicurezza dei Centri Servizi e Centri Servizi Ausiliari del Gruppo TIM
[RI2]	BU1600009 - Valutazione dei rischi in ambito SPC Cloud computing – Lotto 1
[RI3]	BU1600010 - Analisi dei rischi 2016 in ambito SPC Cloud - Lotto 1
[RI4]	Profilo di sicurezza del servizio di SPC1-HOS, per i servizi IaaS e PaaS unmanaged basati sulla tecnologia HP Helion Openstack
[RI5]	Profilo di sicurezza del servizio di SPC1-COMMVAULT, per il servizio BaaS (Backup as a Service)
[RI6]	Profilo di sicurezza del servizio di SPC1-LIFERAY-PORTAL-EE, per i servizi SaaS di Produttività individuale, SaaS di Collaborazione: File Sharing e SaaS di Collaborazione: Enterprise Social Network
[RI7]	Profilo di sicurezza del servizio di tipo SPC1-VOISMART, per il servizio SaaS di Comunicazione Unificata
[RI8]	Profilo di sicurezza del servizio di tipo SPC1-E-LEARNING, per il servizio SaaS di Collaborazione: Learning Management System
[RI9]	Template per richiesta nomina-revoca AdS_ambito sistemi di utilizzo gene....xlsx
[RI10]	Profilo di sicurezza del servizio di tipo SPC1-IAAS-PAAS-MANAGED, per i servizi IaaS e PaaS managed basati sulla tecnologia HP Helion Openstack
[RI11]	Profilo di sicurezza del servizio di tipo SPC1-DISASTER-RECOVERY-DRAAS, per il servizio DRaaS (Disaster Recovery as a Service)
[RI12]	Profilo di sicurezza del servizio di tipo SPC1-ECAAS, per il servizio ECaaS/CCaaS (Enterprise Container as a Service / Community Container as a Service)
[RI13]	Processo di gestione degli eventi di violazione dei dati personali ai sensi del Regolamento (UE) 2016/679 del 27/04/2016
[RI14]	Profilo di Sicurezza del servizio SPC-CCOS, unmanaged e managed e DRaaS su tecnologia Cisco-Canonical OpenStack
[RI15]	Profilo di Sicurezza del servizio SPC1-PAAS-ORACLE, per i servizi PaaS Oracle unmanaged e managed basati sulla tecnologia Oracle-Hitachi
[RI16]	Profilo di Sicurezza del servizio SPC1-OCM, per i servizi PaaS Oracle unmanaged e managed basati sulla tecnologia Oracle OCM
[RI17]	Documento Programmatico della Sicurezza (DPS) dei servizi SPC Cloud erogati da TITT (EVOCST01.TT.DPDT19009.00)

2.3 Riferimenti normativi

Nel seguito vengono elencati i riferimenti normativi che disciplinano gli aspetti di interesse in merito alla sicurezza dei servizi erogati.

[RN1]	Regolamento EU n. 679/2016 in materia di protezione dei dati personali (General Data Protection Regulation, GDPR)

[RN2] Provvedimento in materia dell'Autorità Garante italiana sugli Amministratori di Sistema del 25/11/2008 (e s.m.i. del 25/9/2009)

[RN3] MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI (GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA Serie generale - n. 79)

3 DEFINIZIONE ED ACRONIMI

ACRONIMO	SIGNIFICATO
BAAS	Backup As A Service
DPS	Documento programmatico sulla sicurezza
DRAAS	Disaster Recovery As A Service
KPI	Key Performance Indicator
ECAAS/CCAAS	Enterprise Container As A Service/Community Container As A Service
IAAS	Infrastructure As A Service
ICT	Information and Communication Tecnology
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NOC	Network Operation Center
PAAS	Platform As A Service
PDS	Profilo di Sicurezza
PDR	Piano di Rientro
RFS	Requisito Funzionale di Sicurezza
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAAS	Software As A Service
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività
SPOC	Single Point of Contact
TDB	To Be Defined
ULS	Unità Locale di Sicurezza
VCI	Valutazione della Criticità Intrinseca del sistema
VPN	Virtual Private Network

4 SCOPO DEL DOCUMENTO

Obiettivo del documento è descrivere le procedure e gli strumenti adottati da TIM SpA per garantire la sicurezza, in termini di Riservatezza, Integrità e Disponibilità, dei dati personali trattati nell'ambito dei *Servizi di Cloud Computing per le Pubbliche Amministrazioni* (*Lotto 1 della procedura ristretta, suddivisa in 4, lotti per l'affidamento dei servizi di cloud computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le pubbliche amministrazioni - id sigef 1403*) coerentemente ai requisiti del contratto quadro ed alla documentazione di riscontro (Rif. 2.1) ed i nuovi servizi che si aggiungono ed integrano quelli già previsti e richiesti dalla procedura di Gara, nel seguito di questo documento più sinteticamente denominati ***SPC Lotto 1***.

Pertanto nel documento saranno illustrati l'analisi dei rischi su tutti i servizi IaaS/PaaS unmanaged, IaaS/PaaS managed, BaaS, SaaS, DRaaS, ECaaS/CCaaS, Cloud Enabling e per ogni servizio:

- l'elenco dei trattamenti di dati personali e la tipologia dati
- il personale coinvolto nel trattamento dei dati: gli amministratori di sistema, il responsabile TIM dei trattamenti e gli incaricati
- attività affidate a terzi che comportano il trattamento di dati
- il piano degli interventi formativi previsto per gli incaricati alla responsabilità del trattamento dati e per tutte le risorse identificate come addetti alla sicurezza e alla gestione
- le banche dati (siano esse data base o archivi informatici), con le relative applicazioni, in cui sono contenuti i dati
- il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano gli elaboratori sui cui dischi sono memorizzati i dati (in quale sede, centrale o periferica, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile;
- la tipologia di dispositivi di accesso, cioè l'elenco e la relazione sintetica degli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.;
- la tipologia di interconnessione, cioè la descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.;
- le misure di sicurezza realizzate a protezione dei dati personali.

5 ADEGUAMENTO AL NUOVO REGOLAMENTO EU N. 679/2016 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (GDPR)

Il presente documento è stato aggiornato al fine di recepire il nuovo Regolamento EU N. 679/2016 in materia di protezione dei dati personali (GDPR) [RN1]. Continuano a rimanere in vigore alcuni Provvedimenti del Garante Italiano come il Provvedimento sugli Amministratori di Sistema [RN2].

Il nuovo regolamento armonizza la precedente normativa privacy, con regole comuni a tutti gli Stati UE cambiando però l'impostazione nella protezione dei dati personali, essendo maggiormente focalizzato sulla responsabilizzazione delle imprese, che da un lato devono garantire effettivamente la tutela dei dati personali, secondo un *approccio risk-based*, dall'altro essere in grado di dimostrare, secondo un *principio di accountability*, la conformità alle disposizioni in termini di valutazioni fatte e di efficacia delle misure adottate a protezione dei dati personali.

Il nuovo regolamento inoltre, rafforza le tutele delle persone, prevedendo l'applicabilità delle norme europee anche ai soggetti extra-UE che trattano i dati di persone che si trovano in UE al fine di offrire loro beni o servizi o di monitorarne i comportamenti.

Più in dettaglio, il nuovo regolamento:

- introduce l'obbligo di tenuta *di registri*, sia da parte del titolare (il *Data Controller*) sia da parte del responsabile (il *Data Processor*), tramite cui sono documentate tutte le attività di trattamento, che sostituiscono la notificazione dei trattamenti al Garante Privacy;
- prevede l'adozione di misure tecniche ed organizzative di sicurezza adeguate (*privacy by design* e *privacy by default*), che devono essere realizzate tenendo conto dello stato dell'arte e dei costi di attuazione e del rischio, in termini di probabilità e gravità per i diritti degli interessati; cioè non è più previsto un insieme di misure minime obbligatorie da implementare, come nel Codice Privacy;
- introduce, in caso di trattamenti di dati personali con rischio elevato per i clienti, esempio utilizzo di nuove tecnologie, *profilazione* e trattamento su larga scala di dati personali particolari (*sensibili*), biometrici o giudiziari, la redazione di una *Privacy Impact Assessment* (PIA);
- estende a tutti i settori di attività gli adempimenti in caso di eventi di *violazione dei dati personali* (*data breach*), attualmente previsti solo per i servizi comunicazioni elettroniche accessibili al pubblico, anche se l'obbligo di notifica all'Autorità ed alle persone interessate è prevista solo se nel caso di violazione sussistono rischi reali per gli individui c ui i dati personali si riferiscono (interessati);
- introduce il concetto di *pseudonimizzazione* dei dati, intesa come misura di sicurezza;
- semplifica le modalità di raccolta del consenso per i dati *personali particolari*, per i quali non è più richiesta necessariamente la forma scritta;
- rafforza i diritti degli interessati, con l'introduzione nuovi diritti *all'oblio* ed alla *portabilità* dei dati personali;
- aumenta la rilevanza economica delle sanzioni, che, in funzione delle violazioni, possono arrivare fino a 20 milioni di euro o per le imprese fino al 4% del fatturato mondiale totale;
- introduce la figura di *Data Protection Officer* (DPO), quale responsabile della protezione dei dati personali.

Un' altra importante novità introdotta dal GDPR, Art. 28 del Regolamento, prevede che il responsabile possa trattare i dati personali tramite istruzioni documentate da parte del titolare specificate in un contratto o altro atto giuridico tra le due parti.

Nelle istruzioni occorre:

- stabilire le condizioni per ricorrere ad un altro Responsabile del trattamento
- stabilire la natura del trattamento;
- definire la tipologia dei dati trattati;
- condividere le misure di sicurezza adottate a protezione dei dati personali;

➢ In merito agli ultimi due punti, **Tipologia Dato e Misure di Misure di Sicurezza**, si precisa che:

- i **servizi SaaS** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; è responsabilità delle singole Amministrazioni verificare la tipologia dei dati trattati dal servizio richiesto e, in caso di dati la cui tipologia richieda meccanismi di sicurezza superiori a quanto previsto, richiederne a TIM la fattibilità e una valutazione a progetto.
- I **servizi infrastrutturali IaaS/PaaS managed/unmanaged, BaaS, DraaS e ECaaS/CCaaS** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purché venga attuata la matrice di responsabilità cliente PA/fornitore TIM sulle misure specifiche. Questo aspetto è trattato all' interno di ogni servizio nel paragrafo "Misure di sicurezza a protezione dei dati personali".

6 Misure minime di sicurezza ICT per le Pubbliche Amministrazioni (Misure Minime AGID)

La Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, sollecita tutte le Amministrazioni e gli Organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici. A fine di agevolare tale processo l'Agenzia per l'Italia Digitale è stata impegnata a rendere prontamente disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

A tale scopo ad aprile 2017 AgiD ha pubblicato nella Gazzetta Ufficiale (GuRI) le Misure Minime di Sicurezza per la PA, un documento che contiene le *Misure minime di sicurezza ICT per le Pubbliche Amministrazioni* le quali costituiscono parte integrante delle *Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni* [RN3].

Le checklist dei controlli ABSC (Agid Basic Security Controll) a cui ogni PA deve rispondere, sono assolutamente coerenti al Regolamento EU (GDPR).

AgiD ha fatto riferimento ai controlli del SANS 20 (CCSC - "CIS Critical Security Controls for Effective Cyber Defense") mettendolo in relazione al "FNSC" (Framework Nazionale di Sicurezza Cibernetica).

Rispetto ai 20 ambiti di controllo del CCSC orientati prevalentemente alla Cybersecurity, AgiD ha voluto dare maggior peso agli eventi di sicurezza dovuti a casualità quali guasti ed eventi naturali. Le Misure Minime AgiD pongono l'accento sopra gli aspetti di prevenzione piuttosto che su quelli di risposta e ripristino.

Nel presente documento, in appendice (Rif. 19.3) sono riportate le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni soddisfatte dai servizi previsti nel Contratto Quadro.

7 ANALISI DEI RISCHI

L'analisi del livello di sicurezza associato ai servizi erogati nell'ambito della gara, risulta determinante nel processo di valutazione dei rischi connessi al trattamento delle informazioni gestite dalla singola Amministrazione.
Si illustra nel seguito la metodologia di analisi dei rischi adottata da TIM per presidiare la sicurezza delle informazioni ed i risultati ottenuti rimandando per i dettagli sulle modalità di analisi e calcolo ai documenti specifici [RI2] ed [RI3].

7.1 Metodologia

La metodologia di analisi dei rischi utilizzata fa riferimento allo standard ISO/IEC 27005:2011 (*Information Technology – Security Techniques - Information Security Risk Management*) ed è basata su un approccio per processi di tipo top-down.
È in grado di sviluppare un *framework* concettuale per la valutazione della sicurezza informatica e delle potenziali conseguenze e perdite dovute a violazioni di requisiti di sicurezza.
I parametri di valutazione utilizzati dall'analisi per definire il livello di criticità e sensibilità degli asset aziendali sono direttamente legati alle tre caratteristiche universalmente accettate per definire il livello di sicurezza di un servizio/applicazione: *Riservatezza, Integrità e Disponibilità*.
La metodologia utilizzata prevede le seguenti attività:

- identificazione del perimetro di riferimento, costituito dall'insieme degli asset attraverso cui vengono erogati i servizi.
- specializzazione dell'analisi, ovvero personalizzazione della metodologia di analisi del rischio al particolare contesto analizzato.
- modellizzazione, ovvero creazione del modello su cui effettuare l'analisi.
- valutazione, ovvero compilazione dei questionari proposti dalla metodologia.
- reporting, ovvero raccolta e presentazione dei risultati finali di livelli di rischio ottenuti.
- condivisione dei risultati raggiunti col cliente.
- creazione del documento finale che racchiude l'analisi effettuata.

L'attività di analisi del rischio è di tipo top-down, e a partire dai processi aziendali punta a far emergere prima le informazioni coinvolte poi tutte le risorse (asset) da cui è possibile accedere direttamente o indirettamente ad esse, al fine di valutare il rischio in funzione:

- delle **minacce**: probabilità di accadimento di incidenti di sicurezza (perdita di RID delle Informazioni aziendali);
- delle **vulnerabilità**: grado di esposizione alle minacce delle risorse aziendali (associate direttamente o indirettamente alle informazioni);
- dell'**impatto** che si potrebbe generare da una indisponibilità delle stesse.

L'analisi del rischio è condotta secondo il seguente flusso operativo:

- **modellizzazione delle risorse aziendali:** analisi top-down che a partire dai processi di business punta a far emergere prima le informazioni coinvolte, poi tutte le risorse (o asset) aziendali da cui è possibile accedere direttamente o indirettamente ad esse.
  Le figure seguenti riportano, a titolo esemplificativo, i passaggi logici utili alla fase di creazione del modello di analisi e un esempio di asset model

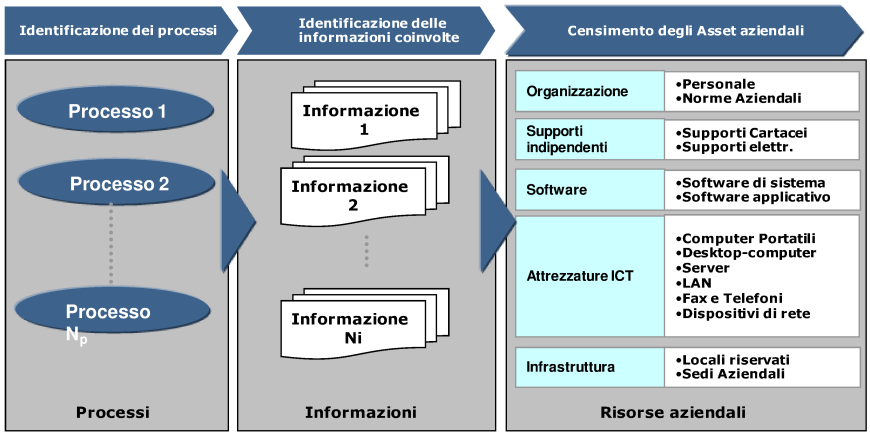


Figura 1- Modellizzazione delle risorse aziendali

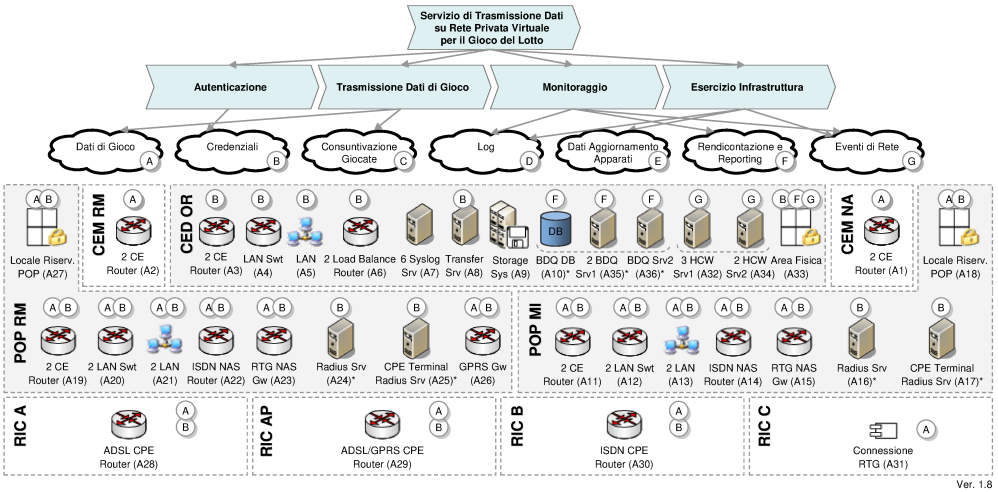


Figura 2 - Esempio di asset model

- **valutazione della criticità delle informazioni**: stima qualitativa degli impatti sui processi aziendali dovuti a incidenti di sicurezza che causano la rivelazione, alterazione o l'indisponibilità delle informazioni associate.
- **valutazione delle minacce:** valutazione della probabilità di accadimento delle minacce (associate alle risorse aziendali), che possono provocare incidenti di sicurezza delle informazioni. Le minacce (selezionate ed adattate da ISO/IEC TR13335) sono valutate considerando la frequenza storica di accadimento dell'evento e la condizione attuale della causa da cui scaturisce. Le vulnerabilità sono invece valutate considerando il grado di sviluppo ed il grado di rilevanza delle misure di protezione in atto (intrinseche o esterne all'asset), individuate sulla base dei controlli di sicurezza ISO 27001.
- **valutazione della vulnerabilità**: individuazione e valutazione delle vulnerabilità (debolezze) delle risorse aziendali, che possono essere sfruttate da una o più minacce causando incidenti di sicurezza.
  La valutazione delle minacce e delle vulnerabilità segue un percorso bottom-up (cfr. figura 3) in modo tale da associare al singolo asset le minacce appropriate, valutarne il livello di vulnerabilità e individuare in modo puntuale il livello di rischio associato.

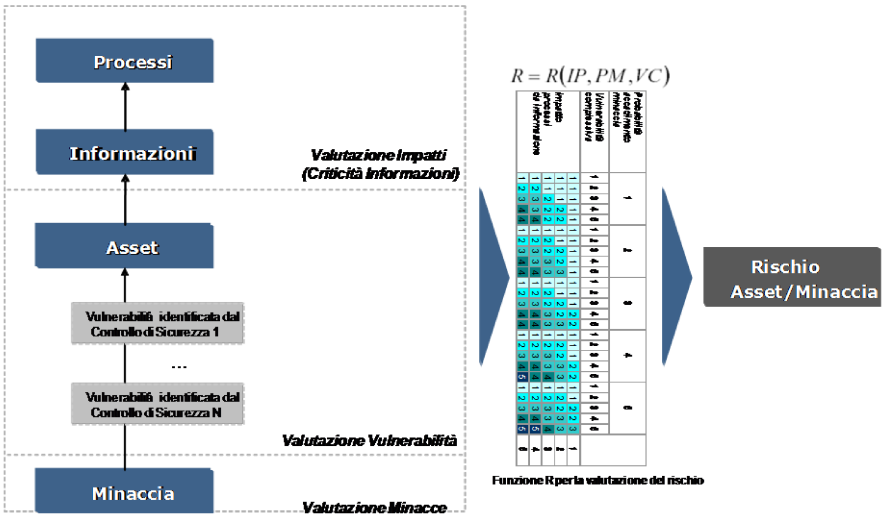


Figura 3 - Valutazione minacce e vulnerabilità

- impostato il modello di analisi e associate agli asset le opportune minacce, la **valutazione delle vulnerabilità** attraverso:
  - incontri (concordati e pianificati) per reperire informazioni relativamente alla struttura organizzativa, ai processi interni, alle prassi per la conduzione delle attività, alle location ed ai sistemi/piattaforme tecnologiche presenti all'interno dell'ambito di applicazione dell'assessment;
  - acquisizione della documentazione relativa a policy/procedure esistenti;
  - individuazione delle aree e delle attività regolamentate/proceduralizzate in modo tale da individuare eventuali vincoli, interfacce e riferimenti da tenere in considerazione nel corso delle attività di security assessment;
  - interviste con i Referenti individuati al fine di reperire informazioni relative:
    - alle informazioni di carattere tecnico/tecnologico, con riferimento ai principali Asset IT funzionali all'erogazione dei servizi;
    - alle informazioni di carattere organizzativo quali ruoli/responsabilità, organigrammi aziendali;
  - analisi dei vincoli normativi e regolatori. Analisi di tutti i vincoli regolatori, leggi dello Stato e Normative/Codici di settore rilevanti per lo specifico contesto operativo e organizzativo e che necessitano di essere indirizzati dal futuro Sistema di Gestione della Sicurezza;
- **elaborazione della mappa dei rischi**: in base ai valori degli impatti, delle minacce e delle vulnerabilità viene elaborata la mappa complessiva dei rischi a cui sono esposte le risorse aziendali. La mappa dei rischi viene utilizzata per l'identificazione dei requisiti di sicurezza e per la scelta delle opzioni di trattamento del rischio.

  La figura seguente riporta un esempio di mappa dei rischi:
  - sulle righe sono riportati le risorse aziendali che compongono l'asset model;
  - sulle colonne le minacce;
  - le celle riportato il livello di rischio associato alla coppia asset-minaccia calcolato in relazione alle vulnerabilità presenti;

- i box laterali riportano una breve descrizione della problematica evidenziata.

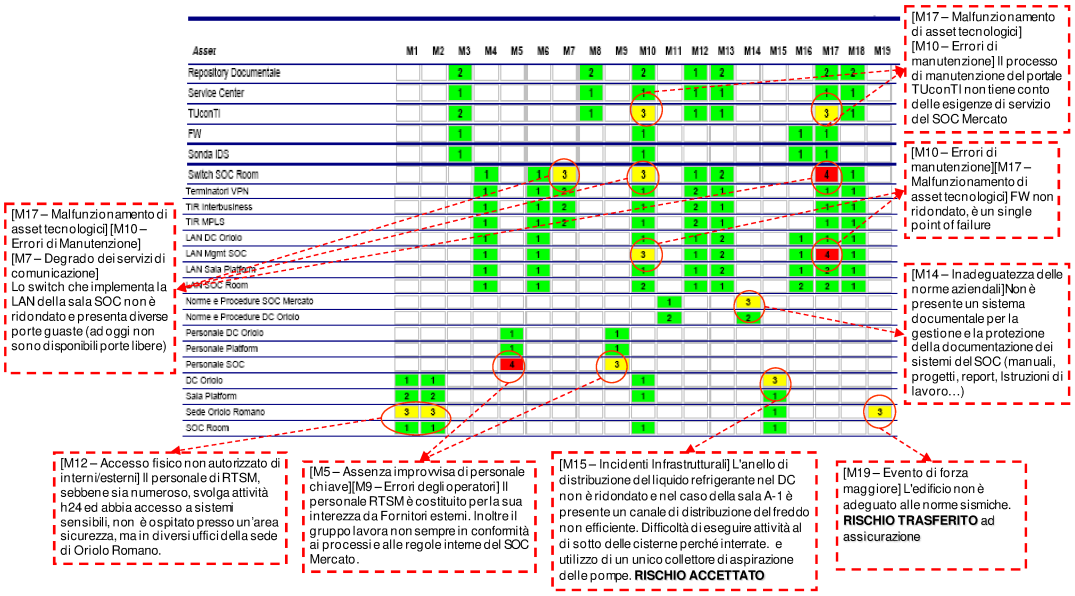


Figura 4 - Esempio di mappa dei rischi

- **definizione piano di trattamento**: al termine dell'analisi sono individuate le eventuali contromisure da implementare/migliorare utili alla definizione e formalizzazione del Piano di Trattamento del Rischio.
- **definizione delle metriche di valutazione della gestione della sicurezza.**

Per i dettagli sulle modalità di analisi, calcolo e risultati si rimanda ai documenti specifici [RI2] ed [RI3].[1]

[1] Il documento [RI3], così come il framework documentale relativo allo SGSI SCP Cloud, è in corso di aggiornamento per recepire i nuovi servizi Iaas/Paas managed, DRaaS e ECaaS/CCaaS. Vengono comunque garantite le misure di sicurezza descritte nei capitoli "Misure di sicurezza a protezione dei dati personali" di ogni singolo servizio.

8 SERVIZI DI INFRASTRUCTURE AS A SERVICE (IAAS) E DI PLATFORMS AS A SERVICE (PAAS) UNMANAGED

I servizi *SPC Cloud lotto 1 di tipo IaaS* sono attualmente forniti per mezzo di due distinte tecnologie, entrambe basate sulla piattaforma software open source Openstack sviluppata per la creazione di Private e Public Infrastructure as a Service.

- la HP Helion Openstack, in via di dismissione
- la Cisco-Canonical Openstack, su cui verrano migrati i servizi infrastrutturali attualmente erogati tramite la HP Helion Openstack, secondo il piano riportato al Rif. [CQ5]

La tecnologia Cisco-Canonical permette di aumentare l'affidabilità dei servizi e di migliorare la continuità operativa, poiché i servizi La modalità multi-Region tramite cui si servizi sono erogati, supporta sia servizi *legacy multi-tier* che servizi *cloud native*, e si avvale di due Region distribuite su due diverse aree geografiche: nord e centro.
Tale modalità consente inoltre la reingegnerizzazione ed evoluzione del *disaster recovery*, che per le applicazioni *legacy* non è più basato sull'intera piattaforma ma scalabile a livello del singolo tenant del cliente tramite una funzionalità di *fast recovery* pienamente equivalente.
Per le applicazioni *cloud native* i clienti possono invece avvalersi della continuità operativa dei propri servizi implementando autonomamente il bilanciamento geografico dei propri IP pubblici (Internet e Infranet) sulle due region, tramite una funzionalità di *always on* equivalente alla *business continuity*.

Le nuova tecnologia fornisce una user experience identica alla precedente, ed è utilizzata anche per l'erogazione dei servizi di tipo *Platform as a Service* (*PaaS*).

Le PaaS che includono lo RDBMS Oracle, possono essere erogate anche utilizzando piattaforme diverse dalla Openstack, potendo essere di tipo Oracle OCM e di tipo Oracle-Hitachi.

Per i servizi IaaS e PaaS la sicurezza delle istanze di Virtual Machine (VM)/ Virtual Data Center (VDC) è demandata alle singole Amministrazioni che, nell'ottica di acquisto di servizi *unmanaged*, hanno la possibilità di configurare in autonomia le proprie policy di sicurezza (Access & Security).
TIM pertanto, nell'erogazione dei servizi di competenza, svolge solo trattamenti di conservazione e gestione sistemistica infrastrutturale e non gestisce le singole VM.
In relazione ai trattamenti indicati, deve essere prevista la nomina di TIM e fornitori a Responsabile del trattamento da parte della Pubblica Amministrazione che sottoscrive il servizio, tramite specifica clausola contrattuale, così come previsto dall'Art. 28 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.

- I **servizi infrastrutturali IaaS/PaaS unmanaged** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM" sulle misure specifiche proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte sulle singole macchine virtuali da parte del cliente stesso oppure attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione.

8.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento e responsabilità:

- storage e gestione sistemistica infrastrutturale: responsabile TIM[2];

[2] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

- nel caso del servizio *PaaS Oracle su tecnologia Oracle OCM* storage e gestione sistemistica infrastrutturale responsabile il fornitore Oracle Italia.

Nomina di TIM e Fornitore a responsabile del trattamento: necessaria per i trattamenti su indicati
Tipologia dei dati trattati: dati personali e categorie particolari di dati
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

8.2 Personale coinvolto nel trattamento dei dati

Responsabile del trattamento dei dati: TIM.
Incaricati del trattamento dei dati: settore CR.CD.R (vedi rif. [RI9]) per l'elenco completo degli Amministratori di Sistema)

Riguardo gli incaricati della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (*password injection*) mediante l'interfaccia di RAMSES denominata Keepass.

8.3 Attività affidate a terzi che comportano il trattamento di dati

Oracle svolge attività di storage e gestione infrastrutturale, relativamente ai soli servizi PaaS Oracle erogati su infrastruttura Oracle OCM.

8.4 Piano degli interventi formativi

Piano formativo degli incaricati al trattamento dei dati:

- formazione nell'ambito dei perimetri di certificazione ISO 27001.

Piano formativo degli incaricati al trattamento dei dati amministratori di sistema:

- formazione nell'ambito dei perimetri di certificazione ISO 27001;
- formazione tecnica attraverso corsi col fornitore delle tecnologie (HP e Cisco-Canonical);

8.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

I servizi IaaS e PaaS, e le piattaforme attraverso cui sono erogati, sono ospitati presso i centri servizi riportati nella seguente tabella:

DATA CENTER	REGION/UTILIZZO
Rozzano, sito in Viale Toscana 3 (MI)	2
Pomezia, sito in Via Pontina Km. 29.1000 (RM),	1
Oriolo, sito in Via Oriolo Romano 257 (RM)	attuale sito di DR per la tecnologia HP Helion Openstack
Acilia, sito in Via di Macchia Palocco 243	1

Cesano Maderno, sito in Via Martinelli - Cesano Maderno (MI).	utilizzato per l'implementazione di progetti legacy che richiedono particolari personalizzazioni

Il servizio utilizza un RDBMS Oracle MySql per la memorizzazione delle utenze di sistema delle virtual machine e di accesso alla dashboard di configurazione Openstack Horizon.

8.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM, sono le sedi di:
Bari, sita in Via Dioguardi 1 e Taranto, sita in Via Campania 11.

8.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e le basi di dati

Le tipologie di interconnessione sono le seguenti:

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali
- tramite Internet (protocollo https), nel caso di accesso diretto alla dashboard di configurazione Openstack Horizon

Le tipologie di backup dei dati sono le seguenti:

- backup incrementale giornaliero e backup full settimanale, per i dati di configurazione dell'infrastruttura
- backup incrementale giornaliero e backup full settimanale, per le virtual machine
- backup ogni 30 minuti di tutta l'infrastruttura, incluse le virtual machine, presso il sito secondario di DR di Roma Oriolo Romano

I tempi di backup e restore rientrano nelle tempistiche contrattuali che prevedono:

- RTO <= di 4h e RPO <= 1 h

I luoghi dove vengono conservati i dati sono:

- Centro Servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI)

La struttura incaricata delle attività di backup e restore è il settore CR.CD.R.

8.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.
Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).
Inoltre i servizi sono sviluppati ed eserciti nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

- I **servizi infrastrutturali IaaS/PaaS unmanaged** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM" sulle misure specifiche proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte sulle singole macchine virtuali da parte del cliente stesso oppure attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione.

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione
- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione
- data retention
- documentazione
- hardening
- patching
- procedurale
- protezione log
- separazione ambienti

- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale è riportato in appendice par. 19.2.

Per quanto riguarda la sicurezza delle categorie particolari di dati personali sono riportate di seguito le misure minime che TIM adotta e le misure minime che restano in capo al cliente PA. La X indica chi ha la responsabilità di garantire la misura di sicurezza. Le misure di responsabilità cliente possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

8.8.1 Misure aggiuntive per il trattamento dei dati sensibili/giudiziari

Il trattamento di dati sensibili/giudiziari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di dati personali.

Categoria misura	Misura di protezione	Responsabilità TIM Oracle sulla PaaS OMC	Responsabilità cliente PA
Back-up	E' prevista la redazione di procedure documentate di ripristino/restore dei dati. Tali procedure di ripristino dell'accesso ai dati garantiscono tempi non superiori a sette giorni qualora tutti i dati utilizzati dal sistema andassero persi.		X
Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma.	X Sulle componenti infrastrutturali	X Sulle singole Virtual Machine
Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di DBMS necessari a correggere difetti e prevenire vulnerabilità della piattaforma.		X Sulle singole Virtual Machine
Riservatezza	Nella piattaforma è prevista soluzioni (es. cifratura o altre) che, considerato il numero e la natura dei dati trattati, rendano i dati sensibili o giudiziari temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità.		X[3]
Supporti di memorizzazione	E' prevista la definizione e l'attuazione di procedure di cancellazione fisica (ad es. tramite Wiping o Degaussing) a seguito della dismissione o della diversa assegnazione d'uso (ad es. utilizzo da parte di un Cliente differente) di elaboratori o supporti utilizzati, al fine di garantire l'inaccessibilità "assoluta" agli stessi.	X	

Tabella 1 – Servizi IaaS/PaaS Unmanaged, Misure a protezione dei dati personali sensibili/giudiziari

8.8.2 Misure aggiuntive per il trattamento dei dati sanitari

Il trattamento di Dati Sanitari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali e sensibili. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

[3] Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo

Categoria misura	Misura di protezione	Responsabilità TIM Oracle sulla PaaS omonima	Responsabilità cliente PA
Riservatezza	Nella piattaforma è prevista, al fine di garantire la riservatezza dei dati sanitari conservati (data-at-rest), la cifratura degli stessi o l'utilizzo di codici identificativi o di altre soluzioni che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. In caso di trasmissione dei dati sanitari è garantita in ogni caso la cifratura dei dati		X[4]

Tabella 2 – Servizi IaaS/PaaS Unmanaged, Misure a protezione dei dati personali sanitari

8.8.3 Misure aggiuntive per il trattamento dei dati sanitari tramite FSE / Dossier Sanitario

Il trattamento di dati sanitari tramite Fascicolo Sanitario Elettronico / Dossier Sanitario comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali, Sensibili e Sanitari. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

Categoria misura	Misura di protezione	Responsabilità TIM Oracle sulla PaaS omonima	Responsabilità cliente PA
Riservatezza	L'applicativo è costruito in maniera tale da permettere l'oscuramento (revocabile nel tempo) di taluni dati o documenti sanitari a seguito di richieste dell'interessato. Le informazioni oscurate sono in ogni caso rese disponibili al professionista sanitario o alla struttura interna titolare che li ha raccolti o elaborati. L'oscuramento dell'evento clinico avviene con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta.		X
Riservatezza	L'applicativo deve essere costruito in maniera tale da permettere la gestione del consenso al trattamento da parte dell'interessato. L'applicativo consente di raccogliere le informazioni e renderle disponibili e visualizzabili esclusivamente a un sottoinsieme di utenze definito dal Cliente Business. In caso di revoca dello stesso il Dossier/Fse non è ulteriormente implementato. Le informazioni sanitarie già presenti restano disponibili e visualizzabili esclusivamente alla funzione interna del Cliente che le ha raccolte (non sono più condivise con i professionisti di altri reparti).		X

Tabella 3 – Servizi IaaS/PaaS Unmanaged, Misure a protezione dei dati personali sanitari tramite FSE/Dossier Sanitario

L'elenco completo delle misure di sicurezza implementate da TIM sui servizi *SPC Cloud lotto 1 di tipo IaaS e PaaS*, incluse quelle derivanti dall' adozione delle policy aziendali, sono descritte in dettaglio ed in funzione dell'applicazione o della tecnologia utilizzata, nei documenti ad uso interno:

- *Profilo di Sicurezza del servizio SPC1-HOS* [RI4], per i servizi IaaS e PaaS unmanaged basati sulla tecnologia HP Helion Openstack;
- *Profilo di Sicurezza del servizio SPC1-CCOS* [RI14], per i servizi IaaS e PaaS unmanaged e managed e DRaaS basati sull'applicazione Cisco-Canonical Openstack.
- *Profilo di Sicurezza del servizio SPC1-PAAS-ORACLE* [RI15], per i servizi PaaS Oracle unmanaged e managed basati sulla tecnologia Oracle-Hitachi
- *Profilo di Sicurezza del servizio SPC1-OCM* [RI16], per i servizi PaaS Oracle unmanaged e managed basati sulla tecnologia Oracle OCM

[4] Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo.

9 SERVIZI DI INFRASTRUCTURE AS A SERVICE (IAAS) E DI PLATFORMS AS A SERVICE (PAAS) MANAGED

I servizi *IaaS ePaaS managed*, sono servizi aggiuntivi applicabili alle immagini standard di tipo IaaS e PaaS già presenti nel catalogo *SPC Cloud lotto 1*.
In particolare i servizi aggiuntivi sono applicabili a due scenari in cui si può trovare l'Amministrazione:

- nuovo progetto di attivazione IaaS/PaaS sul cloud SPC finalizzato all'esercizio direttamente in modalità *managed*;
- ambiente IaaS/PaaS già in esercizio sul Cloud SPC del RTI in modalità *unmanaged* e per il quale l'Amministrazione ha l'esigenza di trasformare l'erogazione del servizio alla modalità *managed*.

I servizi managed prevedono da parte di TIM, oltre a quelle di storage e gestione sistemistica infrastrutturale comunque già presenti per gli analoghi servizi *unmanaged,* le attività di:

- gestione sistemistica, per i servizi IaaS
- gestione sistemistica e gestione middleware, per i servizi PaaS,

In ogni caso non prevedono la gestione dell'ambiente applicativo che rimane in carico all'Amministrazione direttamente o per il tramite di un suo manutentore SW o per il tramite del Vendor applicativo.
In relazione ai trattamenti indicati, deve essere prevista la nomina di TIM e fornitori a *Responsabile del trattamento* da parte della Pubblica Amministrazione che sottoscrive il servizio, tramite specifica clausola contrattuale, così come previsto dall'Art. 28 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.

- I **servizi infrastrutturali IaaS/PaaS managed** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM" sulle misure specifiche proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte sulle singole macchine virtuali da parte del cliente stesso oppure attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione.

9.1 Elenco dei trattamenti di dati personali

Tipo di trattamento: Per il trattamento dei dati personali si ha nello specifico:

- IaaS managed: storage e gestione sistemistica infrastrutturale; gestione sistemistica delle virtual machine,
- PaaS managed: storage e gestione sistemistica infrastrutturale; gestione sistemistica e gestione middleware delle virtual machine, backup

Nomina di TIM e fornitori a responsabile del trattamento: necessaria la nomina di TIM[5] per i trattamenti su indicati.
Per le PaaS Oracle necessaria la nomina di Oracle Srl per i trattamenti PaaS managed ovvero storage e gestione sistemistica infrastrutturale; gestione sistemistica e gestione middleware delle virtual machine, backup.
Tipologia dei dati trattati: dati personali e categorie particolari di dati.
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

9.2 Personale coinvolto nel trattamento dei dati

Responsabile del trattamento dei dati: TIM, Oracle Srl

[5] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

Incaricati del trattamento dei dati ed Amministratori di Sistema:

- storage e gestione sistemistica infrastrutturale settore CR.CD.R ((vedi rif. [RI9]) per l'elenco completo degli Amministratori di Sistema)
- gestione sistemistica, gestione middleware, backup: settore CR.CD.R (vedi rif. [RI9]) per l'elenco completo degli Amministratori di Sistema)
- storage e gestione sistemistica infrastrutturale, gestione sistemistica e gestione middleware delle virtual machine, backup per la piattaforma PaaS Oracle: Oracle Srl

Riguardo gli incaricati della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (*password injection*) mediante l'interfaccia di RAMSES denominata Keepass.

9.3 Attività affidate a terzi che comportano il trattamento di dati

Fornitore a supporto di TIM.
Fornitore ORACLE nel caso dei servizi PaaS Oracle su tecnologia Oracle OCM per cui effettua gestione storage, gestione sistemistica infrastrutturale, gestione del sistema operativo e del middleware sulle virtual machine, backup.

9.4 Piano degli interventi formativi

Piano formativo degli incaricati al trattamento dei dati:

- formazione nell'ambito dei perimetri di certificazione ISO 27001.

Piano formativo degli incaricati al trattamento dei dati amministratori di sistema:

- formazione nell'ambito dei perimetri di certificazione ISO 27001;
- formazione tecnica attraverso corsi col fornitore delle tecnologie (HP e Cisco-Canonical);

9.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

I servizi IaaS e PaaS managed, e le piattaforme attraverso cui sono erogati, sono ospitati presso i centri servizi TIM riportati nella seguente tabella:

DATA CENTER	REGION/UTILIZZO
Rozzano, sito in Viale Toscana 3 (MI)	2
Pomezia, sito in Via Pontina Km. 29.1000 (RM),	1
Oriolo, sito in Via Oriolo Romano 257 (RM)	attuale sito di DR per la tecnologia HP Helion Openstack
Acilia, sito in Via di Macchia Palocco 243	1

Cesano Maderno, sito in Via Martinelli - Cesano Maderno (MI).	utilizzato per l'implementazione di progetti legacy che richiedono particolari personalizzazioni

Il servizio utilizza un RDBMS Oracle MySql per la memorizzazione delle utenze di sistema delle virtual machine e di accesso alla dashboard HP Helion OpenStack di configurazione.

9.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM, sono le sedi di:
Bari, sita in Via Dioguardi 1 e Taranto, sita in Via Campania 11 e Acilia Roma, Via di Macchia Palocco 243

9.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e le basi di dati

Le tipologie di interconnessione sono le seguenti:

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali
- tramite Internet (protocollo https), nel caso di accesso diretto alla alla dashboard di configurazione Openstack Horizon

Le tipologie di backup dei dati sono le seguenti:

- backup incrementale giornaliero e backup full settimanale, per i dati di configurazione dell'infrastruttura
- backup incrementale giornaliero e backup full settimanale, per le virtual machine
- backup ogni 30 minuti di tutta l'infrastruttura, incluse le virtual machine, presso il sito secondario di DR di Roma Oriolo Romano

I tempi di backup e restore rientrano nelle tempistiche contrattuali che prevedono:

- RTO <= di 4h e RPO <= 1 h

I luoghi dove vengono conservati i dati sono:

- I Centri servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

La struttura incaricata delle attività di backup e restore per i servizi infrastrutturali e per i servizi managed è il settore CR.CD.R.

9.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.
Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).

Inoltre i servizi sono sviluppati ed eserciti nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

- I **servizi infrastrutturali IaaS/PaaS managed** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM" sulle misure specifiche proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte sulle singole macchine virtuali da parte del cliente stesso oppure attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione
- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione
- data retention
- documentazione
- hardening
- patching
- procedurale

- protezione log
- separazione ambienti
- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale è riportato in appendice par. 19.2.

Per quanto riguarda la sicurezza delle categorie particolari di dati personali sono riportate di seguito le misure minime che TIM adotta e le misure minime che restano in capo al cliente PA. La X indica chi ha la responsabilità di garantire la misura di sicurezza. Le misure di responsabilità cliente possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

9.8.1 Misure aggiuntive per il trattamento dei dati sensibili/giudiziari

Il trattamento di dati sensibili/giudiziari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di dati personali.

Categoria misura	Misura di protezione	Responsabilità TIM Oracle per la PaaS Oracle	Responsabilità cliente PA
Back-up	E' prevista la redazione di procedure documentate di ripristino/restore dei dati. Tali procedure di ripristino dell'accesso ai dati garantiscono tempi non superiori a sette giorni qualora tutti i dati utilizzati dal sistema andassero persi.	X Se presente la gestione middleware	
Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma.	X	
Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di DBMS necessari a correggere difetti e prevenire vulnerabilità della piattaforma.	X Se presente la gestione middleware	
Riservatezza	Nella piattaforma sono previste soluzioni (es. cifratura o altre) che, considerato il numero e la natura dei dati trattati, rendano i dati sensibili o giudiziari temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità.		X[6]
Supporti di memorizzazione	E' prevista la definizione e l'attuazione di procedure di cancellazione fisica (ad es. tramite Wiping o Degaussing) a seguito della dismissione o della diversa assegnazione d'uso (ad es. utilizzo da parte di un Cliente differente) di elaboratori o supporti utilizzati, al fine di garantire l'inaccessibilità "assoluta" agli stessi.	X	

Tabella 4 – Servizi IaaS/PaaS Managed, Misure a protezione dei dati personali sensibili/giudiziari

9.8.2 Misure aggiuntive per il trattamento dei dati sanitari

Il trattamento di Dati Sanitari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali e sensibili. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

6 Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo.

Categoria misura	Misura di protezione	Responsabilità TIM Oracle per la PaaS Oracle	Responsabilità cliente PA
Riservatezza	Nella piattaforma è prevista, al fine di garantire la riservatezza dei dati sanitari conservati (data-at-rest), la cifratura degli stessi o l'utilizzo di codici identificativi o di altre soluzioni che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. In caso di trasmissione dei dati sanitari è garantita in ogni caso la cifratura dei dati		X[7]

Tabella 5 – Servizi IaaS/PaaS Managed, Misure a protezione dei dati personali sanitari

9.8.3 Misure aggiuntive per il trattamento dei dati sanitari tramite FSE / Dossier Sanitario

Il trattamento di dati sanitari tramite Fascicolo Sanitario Elettronico / Dossier Sanitario comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali, Sensibili e Sanitari. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

Categoria misura	Misura di protezione	Responsabilità TIM Oracle per la PaaS Oracle	Responsabilità cliente PA
Riservatezza	L'applicativo è costruito in maniera tale da permettere l'oscuramento (revocabile nel tempo) di taluni dati o documenti sanitari a seguito di richieste dell'interessato. Le informazioni oscurate sono in ogni caso rese disponibili al professionista sanitario o alla struttura interna titolare che li ha raccolti o elaborati. L'oscuramento dell'evento clinico avviene con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta.		X
Riservatezza	L'applicativo deve essere costruito in maniera tale da permettere la gestione del consenso al trattamento da parte dell'interessato. L'applicativo consente di raccogliere le informazioni e renderle disponibili e visualizzabili esclusivamente a un sottoinsieme di utenze definito dal Cliente Business. In caso di revoca dello stesso il Dossier/Fse non è ulteriormente implementato. Le informazioni sanitarie già presenti restano disponibili e visualizzabili esclusivamente alla funzione interna del Cliente che le ha raccolte (non sono più condivise con i professionisti di altri reparti).		X

Tabella 6 – Servizi IaaS/PaaS Managed, Misure a protezione dei dati personali sanitari tramite FSE / Dossier Sanitario

L'elenco completo delle misure di sicurezza implementate da TIM sui servizi *SPC Cloud lotto 1 di tipo IaaS e PaaS managed*, incluse quelle derivanti dall' adozione delle policy aziendali, sono descritte in dettaglio ed in funzione dell'applicazione o tecnologia utilizzata, nei documenti ad uso interno:

- *Profilo di Sicurezza del servizio SPC1-IAAS-PAAS-MANAGED* [RI10], per i servizi IaaS e PaaS managed basati sulla tecnologia HP Helion Openstack;
- *Profilo di Sicurezza del servizio SPC1-CCOS* [RI14], per i servizi IaaS e PaaS unmanaged e managed e DRaaS basati sull'applicazione Cisco-Canonical Openstack.
- *Profilo di Sicurezza del servizio SPC1-PAAS-ORACLE* [RI15], per i servizi PaaS Oracle unmanaged e managed basati sulla tecnologia Oracle-Hitachi
- *Profilo di Sicurezza del servizio SPC1-OCM* [RI16], per i servizi PaaS Oracle unmanaged e managed basati sulla tecnologia Oracle OCM;

[7] Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo.

10 SERVIZIO DI BACKUP AS A SERVICE (BAAS)

TIM, nell'erogazione del servizio *SPC Cloud lotto 1 di tipo BaaS*, svolge solo trattamenti di conservazione e gestione sistemistica infrastrutturale e non gestisce le politiche di backup.
Pertanto la sicurezza dei dati oggetto di backup è demandata alle singole Amministrazioni che hanno la possibilità di configurare in autonomia le proprie politiche incluso la funzionalità avanzata di cifratura.
In relazione ai trattamenti indicati, deve essere prevista la nomina di TIM a *Responsabile del trattamento* da parte della Pubblica Amministrazione che sottoscrive il servizio, tramite specifica clausola contrattuale, così come previsto dall'Art. 28 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.

- I **servizi infrastrutturali BaaS** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM" sulle misure specifiche proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte attraverso le funzionaltà avanzate di cifratura del servizio oppure attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione.

10.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento: storage e gestione sistemistica infrastrutturale
Nomina di TIM[8] a responsabile del trattamento: necessaria per i trattamenti su indicati.
Tipologia dei dati trattati: dati personali e categorie particolari di dati
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

10.2 Personale coinvolto nel trattamento dei dati

Responsabile del trattamento dei dati: TIM.
Incaricati del trattamento dei dati: settore CR.CD.R (vedi rif. [RI9] per l'elenco completo degli Amministratori di Sistema).

Riguardo gli incaricati della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (password injection) mediante l'interfaccia di RAMSES denominata Keepass.

10.3 Attività affidate a terzi che comportano il trattamento di dati

10.4 Piano degli interventi formativi

Piano formativo degli incaricati al trattamento dei dati:

[8] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

- formazione nell'ambito dei perimetri di certificazione ISO 27001.

Piano formativo degli incaricati al trattamento dei dati amministratori di sistema:

- formazione nell'ambito dei perimetri di certificazione ISO 27001;

10.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

Il servizio BaaS, e le piattaforme attraverso cui è erogato, sono ospitati presso i centri servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

Il servizio utilizza una base date Microsoft SQL Server per la memorizzazione delle utenze di accesso alla dashboard Commvault di configurazione delle policy di backup del cliente.

10.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM, sono le sedi di:
Bari, sita in Via Dioguardi 1 e Taranto, sita in Via Campania 11.

10.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e i dati

Le tipologie di interconnessione sono le seguenti:

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali

tramite Internet (protocollo https), nel caso di accesso diretto alla alla dashboard di configurazione Openstack Horizon
Le tipologie di backup dei dati sono le seguenti:

- backup incrementale giornaliero e backup full settimanale, per i dati di configurazione dell'infrastruttura
- backup incrementale giornaliero e backup full settimanale, per le virtual machine dell'infrastruttura
  L'allineamento dei dati di backup tra i datacenter primario e secondario (di DR) viene effettuato in maniera asincrona attraverso una replica applicativa dei dati

I tempi di backup e restore rientrano nelle tempistiche contrattuali che prevedono:

- RTO <= 4h e RPO <= 1h

I luoghi dove vengono conservati i dati sono:

- I Centri Servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

La struttura incaricata delle attività di backup e restore è il settore CR.CD.R.PM.I (Resp. Dessi Massimo).

10.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.
Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità

e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).
Inoltre i servizi sono sviluppati ed eserciti nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

- I **servizi infrastrutturali BaaS** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM" sulle misure specifiche proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte attraverso le funzionalità avanzate di cifratura del servizio oppure attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione.

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione
- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione
- data retention
- documentazione

- hardening
- patching
- procedurale
- protezione log
- separazione ambienti
- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale è riportato in appendice par. 19.2.

Per quanto riguarda la sicurezza delle categorie particolari di dati personali sono riportate di seguito le misure minime che TIM adotta e le misure minime che restano in capo al cliente PA. La X indica chi ha la responsabilità di garantire la misura di sicurezza. Le misure di responsabilità cliente possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

10.8.1 Misure aggiuntive per il trattamento dei dati sensibili/giudiziari

Il trattamento di dati sensibili/giudiziari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di dati personali.

Categoria misura	Misura di protezione	Responsabilità TIM	Responsabilità cliente PA
Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma.	X sull' infrastruttura	
Riservatezza	Nella piattaforma sono previste soluzioni (es. cifratura o altre) che, considerato il numero e la natura dei dati trattati, rendano i dati sensibili o giudiziari temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità.		X[9]
Supporti di memorizzazione	E' prevista la definizione e l'attuazione di procedure di cancellazione fisica (ad es. tramite Wiping o Degaussing) a seguito della dismissione o della diversa assegnazione d'uso (ad es. utilizzo da parte di un Cliente differente) di elaboratori o supporti utilizzati, al fine di garantire l'inaccessibilità "assoluta" agli stessi.	X	

Tabella 7 – Servizio BaaS, Misure a protezione dei dati personali sensibili/giudiziari

10.8.2 Misure aggiuntive per il trattamento dei dati sanitari

Il trattamento di Dati Sanitari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali e sensibili. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

Categoria misura	Misura di protezione	Responsabilità TIM	Responsabilità cliente PA
Riservatezza	Nella piattaforma è prevista, al fine di garantire la riservatezza dei dati sanitari conservati (data-at-rest), la cifratura degli stessi o l'utilizzo di codici identificativi o di altre soluzioni che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. In caso di trasmissione dei dati sanitari è garantita in ogni caso la cifratura dei dati		X[10]

Tabella 8 – Servizio BaaS, Misure a protezione dei dati personali sanitari

[9] Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo.

[10] Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo.

10.8.3 Misure aggiuntive per il trattamento dei dati sanitari tramite FSE / Dossier Sanitario

Il trattamento di dati sanitari tramite Fascicolo Sanitario Elettronico / Dossier Sanitario comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali, Sensibili e Sanitari. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

Categoria misura	Misura di protezione	Responsabilità TIM	Responsabilità cliente PA
Riservatezza	L'applicativo è costruito in maniera tale da permettere l'oscuramento (revocabile nel tempo) di taluni dati o documenti sanitari a seguito di richieste dell'interessato. Le informazioni oscurate sono in ogni caso rese disponibili al professionista sanitario o alla struttura interna titolare che li ha raccolti o elaborati. L'oscuramento dell'evento clinico avviene con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta.		X
Riservatezza	L'applicativo deve essere costruito in maniera tale da permettere la gestione del consenso al trattamento da parte dell'interessato. L'applicativo consente di raccogliere le informazioni e renderle disponibili e visualizzabili esclusivamente a un sottoinsieme di utenze definito dal Cliente Business. In caso di revoca dello stesso il Dossier/Fse non è ulteriormente implementato. Le informazioni sanitarie già presenti restano disponibili e visualizzabili esclusivamente alla funzione interna del Cliente che le ha raccolte (non sono più condivise con i professionisti di altri reparti).		X

Tabella 9 – Servizio BaaS, Misure a protezione dei dati personali sanitari tramite FSE / Dossier Sanitario

L'elenco completo delle misure di sicurezza implementate da TIM sul servizio *SPC Cloud lotto 1 di tipo BaaS*, incluse quelle derivanti dall'adozione delle policy aziendali, sono descritte in dettaglio nel documento ad uso interno *Profilo di sicurezza del servizio di SPC1-COMMVAULT* [RI5].

11 SERVIZIO DI SOFTWARE AS A SERVICE (SAAS) PRODUTTIVITÀ INDIVIDUALE

Per il servizio *SPC Cloud lotto 1 di tipo SaaS Produttività Individuale* le misure di sicurezza implementate sono atte a garantire la conformità di trattamento per la tipologia di dato personale comune.

- È responsabilità delle singole Amministrazioni verificare la tipologia di dati trattati dal servizio richiesto e, in caso di dati la cui tipologia richieda meccanismi di sicurezza superiori a quanto previsto, richiederne a TIM la fattibilità e una valutazione a progetto al di fuori del contratto quadro. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del *Documento Programmatico di Sicurezza* (questo documento) della singola Amministrazione.

11.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento: gestione sistemistica, gestione middleware (TIM), gestione applicativa (fornitore SMC S.r.l di Treviso).
Nomina di TIM[11] e Fornitori a responsabile del trattamento: necessaria per i trattamenti su indicati
Tipologia dei dati trattati: dato personale.
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

11.2 Personale coinvolto nel trattamento dei dati

Per la gestione sistemistica e gestione middleware:
Responsabile del trattamento dei dati: TIM.
Incaricati del trattamento dei dati: settore CR.CD.R (vedi rif. [RI9] per l'elenco completo degli Amministratori di Sistema)

Per la gestione applicativa:
Responsabile del trattamento dei dati: SMC S.r.l di Treviso (coordinamento TIM da parte del settore CR.CD.R);
Incaricati del trattamento dei dati per le attività di provisioning e configurazione delle utenze: settore CR.CD.R di TIM (vedi rif. [RI9] per l'elenco completo degli Amministratori di Sistema)

Riguardo gli incaricati della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (password injection) mediante l'interfaccia di RAMSES denominata Keepass.

11.3 Attività affidate a terzi che comportano il trattamento di dati

La gestione applicativa è affidata al fornitore SMC S.r.l di Treviso.

[11] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

11.4 Piano degli interventi formativi

Il Piano formativo degli incaricati al trattamento dei dati amministratori di sistema è nell'ambito dei perimetri di certificazione ISO 27001.

11.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

Il servizio *SaaS di Produttività Individuale*, e le piattaforme attraverso cui è erogato, sono ospitate presso i centri servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

Il servizio si basa su un database *liferay* e un database *onlyoffice*, realizzati tramite *RDBMS PostgreSQL*.

11.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM, sono le sedi di:

- Roma –Acilia Via di Macchia Palocco 243, per quanto concerne la gestione sistemistica e la gestione middleware;
- Roma – Acilia Via di Macchia Palocco 243, e di Taranto sita in Via Campania 11- Taranto, per quanto concerne la gestione applicativa;

11.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e i dati

Le tipologie di interconnessione sono le seguenti, per tutte le tipologie di trattamento dati (gestione sistemistica, gestione middleware e gestione applicativa):

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali

Le tipologie di backup dei dati sono le seguenti:

- backup incrementale giornaliero e backup full settimanale, per i dati di configurazione e dei data base
- backup incrementale giornaliero e backup full settimanale, per le *cartelle*

I tempi di backup e restore rientrano nelle tempistiche contrattuali che prevedono:

- RTO <= di 4h e RPO <= 1 h

I luoghi dove vengono conservati i dati sono:

- I Centri Servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

Le strutture incaricate delle attività di backup e restore sono il settore CR.CD.R.PM.I (Resp. Fornaro Franco).

11.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.
Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità

e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).
Inoltre i servizi sono sviluppati ed eserciti nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione
- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione
- data retention
- documentazione
- hardening
- patching
- procedurale
- protezione log
- separazione ambienti
- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale è riportato in appendice par. 19.2.

L'elenco completo delle misure di sicurezza implementate da TIM sul servizio *SPC Cloud lotto 1 di tipo SaaS Produttività Individuale*, incluse quelle derivanti dall'adozione delle policy aziendali, sono descritte in dettaglio nel documento ad uso interno *Profilo di sicurezza del servizio di SPC1-LIFERAY-PORTAL-EE* [RI6].

12 SERVIZIO DI SOFTWARE AS A SERVICE (SAAS) COMUNICAZIONE UNIFICATA

Per il servizio *SPC Cloud lotto 1 di tipo SaaS Comunicazione Unificata* le misure di sicurezza implementate sono atte a garantire la conformità di trattamento per la tipologia di dato personale comune.

- È responsabilità delle singole Amministrazioni verificare la tipologia di dati trattati dal servizio richiesto e, in caso di dati la cui tipologia richieda meccanismi di sicurezza superiori a quanto previsto, richiederne a TIM la fattibilità e una valutazione a progetto al di fuori del contratto quadro. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del *Documento Programmatico di Sicurezza* (questo documento) della singola Amministrazione.

12.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento: gestione sistemistica e gestione middleware, gestione applicativa (TIM e fornitore Voicesmart).
Nomina di TIM[12] e Fornitore a responsabile del trattamento: necessaria per i trattamenti su indicati.
Tipologia dei dati trattati: dati personali.
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

12.2 Personale coinvolto nel trattamento dei dati

Per la gestione sistemistica e la gestione middleware:
Responsabile del trattamento dei dati: TIM.
Incaricati del trattamento dei dati: settore CR.CD.R (vedi rif. [RI9] per l'elenco completo degli Amministratori di Sistema).

Per la gestione applicativa:
Responsabile del trattamento dei dati: Voicesmart (coordinamento TIM da parte del settore CR.CD.R);
Incaricati del trattamento dei dati per le attività di provisioning e configurazione delle utenze: settore CR.CD.R di TIM (vedi rif. [RI9]) per l'elenco completo degli Amministratori di Sistema)

Riguardo gli incaricati della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (password injection) mediante l'interfaccia di RAMSES denominata Keepass.

12.3 Attività affidate a terzi che comportano il trattamento di dati

La gestione applicativa è affidata al fornitore Voicesmart.

[12] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

12.4 Piano degli interventi formativi

Piano formativo degli incaricati al trattamento dei dati:

- formazione nell'ambito dei perimetri di certificazione ISO 27001.

Piano formativo degli incaricati al trattamento dei dati amministratori di sistema:

- formazione nell'ambito dei perimetri di certificazione ISO 27001;

12.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

Il servizio *SaaS di Comunicazione Unificata* e le piattaforme attraverso le quali è erogato, sono ospitate presso i centri servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).
Il servizio fa uso di RDBMS NoSQL ed SQL, che sono dedicati alla memorizzazione dei dati delle registrazioni audio/video nonché quelli relativi ai Clienti (profili, licenze, log, ecc.).

12.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle, per le attività di gestione sistemistica e gestione middleware;
- pc, tablet e smartphone, per le attività di gestione applicativa.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM e del fornitore, sono le sedi di:

- Bari, sita in Via Dioguardi 1 e Taranto, sita in Via Campania 11 per quanto concerne la gestione sistemistica e la gestione middleware;
- del fornitore Voicesmart, per quanto concerne la gestione applicativa;

12.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e i dati

Le tipologie di interconnessione sono le seguenti:

per la gestione sistemistica e la gestione middleware:

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali

mentre per la gestione applicativa affidata ai fornitori:

- tramite VPN dedicate

Le tipologie di backup dei dati sono le seguenti:

- backup incrementale giornaliero e backup full settimanale, per i dati di configurazione e dei data base

I tempi di backup e restore rientrano nelle tempistiche contrattuali che prevedono:

- RTO <= di 4h e RPO <= 1 h

I luoghi dove vengono conservati i dati sono:

- I Centri Servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

La struttura incaricata delle attività di backup e restore delle componenti sistemistiche e di middleware è il settore CR.CD.R.

12.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.
Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).
Inoltre i servizi sono sviluppati ed eserciti nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione
- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione

- data retention
- documentazione
- hardening
- patching
- procedurale
- protezione log
- separazione ambienti
- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale è riportato in appendice par. 19.2.
L'elenco completo delle misure di sicurezza implementate da TIM sul servizio *SPC Cloud lotto 1 di tipo Comunicazione Unificata*, incluse quelle derivanti dall'adozione delle policy aziendali, sono descritte in dettaglio nel documento ad uso interno *Profilo di Sicurezza del servizio SPC1-VOISMART* [RI7].

13 SERVIZIO DI SOFTWARE AS A SERVICE (SAAS) COLLABORAZIONE FILE SHARING

Per il servizio *SPC Cloud lotto 1 di tipo SaaS Collaborazione File Sharing*, le misure di sicurezza implementate sono atte a garantire la conformità di trattamento per la tipologia di dato personale comune.

- È responsabilità delle singole Amministrazioni verificare la tipologia di dati trattati dal servizio richiesto e, in caso di dati la cui tipologia richieda meccanismi di sicurezza superiori a quanto previsto, richiederne a TIM la fattibilità e una valutazione a progetto al di fuori del contratto quadro. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del *Documento Programmatico di Sicurezza* (questo documento) della singola Amministrazione.

13.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento: gestione sistemistica, gestione middleware (TIM), gestione applicativa (TIM e fornitore SMC S.r.l di Treviso).
Nomina di TIM[13] **e Fornitore a responsabile del trattamento**: necessaria per i trattamenti su indicati.
Tipologia dei dati trattati: dati personali.
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

13.2 Personale coinvolto nel trattamento dei dati

Per la gestione sistemistica e gestione middleware:
Responsabile del trattamento dei dati: TIM.
Incaricati del trattamento dei dati: settore CR.CD.R (vedi rif. [RI9] per l'elenco completo degli Amministratori di Sistema)

Per la gestione applicativa:
Responsabile del trattamento dei dati: SMC S.r.l di Treviso (coordinamento TIM da parte del settore CR.CD.R);
Incaricati del trattamento dei dati per le attività di provisioning e configurazione delle utenze: settore CR.CD.R di TIM. (vedi rif. [RI9]) per l'elenco completo degli Amministratori di Sistema)

Riguardo gli incaricati della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (password injection) mediante l'interfaccia di RAMSES denominata Keepass.

13.3 Attività affidate a terzi che comportano il trattamento di dati

La gestione applicativa è affidata a SMC S.r.l di Treviso.

[13] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

13.4 Piano degli interventi formativi

Il Piano formativo degli incaricati al trattamento dei dati amministratori di sistema è nell'ambito dei perimetri di certificazione ISO 27001.

13.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

Il servizio *SaaS di Collaborazione File Sharing* e le piattaforme attraverso le quali è erogato, sono ospitate presso i centri servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

Il servizio si basa su un database *liferay* e un database *onlyoffice*, realizzati tramite *RDBMS PostgreSQL*.

13.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM, sono le sedi di:

- Roma – Viale Parco de Medici 61, e di Taranto sita in Via Campania 11- Taranto, per quanto concerne la gestione sistemistica, la gestione middleware e la gestione applicativa.

13.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e i dati

Le tipologie di interconnessione sono le seguenti, per tutte le tipologie di trattamento dati (gestione sistemistica, gestione middleware e gestione applicativa):

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali

Le tipologie di backup dei dati sono le seguenti:

- backup incrementale giornaliero e backup full settimanale, per i dati di configurazione e dei data base
- backup incrementale giornaliero e backup full settimanale, per le cartelle

I tempi di backup e restore rientrano nelle tempistiche contrattuali che prevedono:

- RTO <= di 4h e RPO <= 1 h

I luoghi dove vengono conservati i dati sono:

- TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

Le strutture incaricate delle attività di backup e restore sono il settore CR.CD.R.

13.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.
Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità

e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).
Inoltre i servizi sono sviluppati ed esercitati nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione
- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione
- data retention
- documentazione
- hardening
- patching
- procedurale
- protezione log
- separazione ambienti
- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale è riportato in appendice par. 19.2.

L'elenco completo delle misure di sicurezza implementate da TIM sul servizio *SPC Cloud lotto 1 di tipo Collaborazione File Sharing*, incluse quelle derivanti dall'adozione delle policy aziendali, sono descritte in dettaglio nel documento ad uso interno *Profilo di sicurezza del servizio di SPC1-LIFERAY-PORTAL-EE* [RI6].

14 SERVIZIO DI SOFTWARE AS A SERVICE (SAAS) COLLABORAZIONE ENTERPRISE SOCIAL NETWORK

Per il servizio *SPC Cloud lotto 1 di tipo SaaS Collaborazione Enterprise Social Network*, le misure di sicurezza implementate sono atte a garantire la conformità di trattamento per la tipologia di dato personale comune.

- È responsabilità delle singole Amministrazioni verificare la tipologia di dati trattati dal servizio richiesto e, in caso di dati la cui tipologia richieda meccanismi di sicurezza superiori a quanto previsto, richiederne a TIM la fattibilità e una valutazione a progetto al di fuori del contratto quadro. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del *Documento Programmatico di Sicurezza* (questo documento) della singola Amministrazione.

14.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento: gestione sistemistica e gestione middleware (TIM), gestione applicativa (TIM e fornitore SMC S.r.l di Treviso).
Nomina di TIM[14] e Fornitore a responsabile del trattamento: necessaria per i trattamenti su indicati.
Tipologia dei dati trattati: dati personali.
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

14.2 Personale coinvolto nel trattamento dei dati

Per la gestione sistemistica e gestione middleware:
Responsabile del trattamento dei dati: TIM.
Incaricati del trattamento dei dati: settore CR.CD.R (vedi rif. [RI9] per l'elenco completo degli Amministratori di Sistema)

Per la gestione applicativa:
Responsabile del trattamento dei dati: SMC S.r.l di Treviso (coordinamento TIM da parte del settore CR.CD.R);
Incaricati del trattamento dei dati per le attività di provisioning e configurazione delle utenze: settore CR.CD.R di TIM (vedi rif. [RI9]) per l'elenco completo degli Amministratori di Sistema)

Riguardo gli incaricati della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (password injection) mediante l'interfaccia di RAMSES denominata Keepass.

14.3 Attività affidate a terzi che comportano il trattamento di dati

La gestione applicativa è affidata a SMC S.r.l di Treviso.

[14] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

14.4 Piano degli interventi formativi

Il Piano formativo degli incaricati al trattamento dei dati amministratori di sistema è nell'ambito dei perimetri di certificazione ISO 27001.

14.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

Il servizio *SaaS di Collaborazione Enterprise Social Network* e le piattaforme attraverso cui è erogato, sono ospitate presso i centri servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

Il servizio si basa su un database *liferay* e un database *onlyoffice*, realizzati tramite *RDBMS PostgreSQL*.

14.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM, sono le sedi di:

- Roma – Acilia Via di Macchia Palocco 243, e di Taranto sita in Via Campania 11- Taranto, per quanto concerne la gestione sistemistica, la gestione middleware e la gestione applicativa.

14.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e i dati

Le tipologie di interconnessione sono le seguenti, per tutte le tipologie di trattamento dati (gestione sistemistica, gestione middleware e gestione applicativa):

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali

Le tipologie di backup dei dati sono le seguenti:

- backup incrementale giornaliero e backup full settimanale, per i dati di configurazione e dei data base
- backup incrementale giornaliero e backup full settimanale, per le *cartelle*

I tempi di backup e restore rientrano nelle tempistiche contrattuali che prevedono:

- RTO <= di 4h e RPO <= 1 h

I luoghi dove vengono conservati i dati sono:

- I Centri Servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

Le strutture incaricate delle attività di backup e restore sono il settore CR.CD.R.

14.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.
Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità

e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).
Inoltre i servizi sono sviluppati ed eserciti nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione
- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione
- data retention
- documentazione
- hardening
- patching
- procedurale
- protezione log
- separazione ambienti
- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale è riportato in appendice par. 19.2.

L'elenco completo delle misure di sicurezza implementate da TIM sul servizio *SPC Cloud lotto 1 di tipo Collaborazione Enterprise Social Network*, incluse quelle derivanti dall'adozione delle policy aziendali, sono descritte in dettaglio nel documento ad uso interno *Profilo di sicurezza del servizio di SPC1-LIFERAY-PORTAL-EE* [RI6].

15 SERVIZIO DI SOFTWARE AS A SERVICE (SAAS) COLLABORAZIONE LEARNING MANAGEMENT SYSTEM

Per il servizio *SPC Cloud lotto 1 di tipo SaaS Collaborazione Learning Management System*, le misure di sicurezza implementate sono atte a garantire la conformità di trattamento per la tipologia di dato personale comune.

- È responsabilità delle singole Amministrazioni verificare la tipologia di dati trattati dal servizio richiesto e, in caso di dati la cui tipologia richieda meccanismi di sicurezza superiori a quanto previsto, richiederne a TIM la fattibilità e una valutazione a progetto al di fuori del contratto quadro. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del *Documento Programmatico di Sicurezza* (questo documento) della singola Amministrazione

15.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento: gestione sistemistica (TIM), gestione middleware OilProject Srl e applicativa (TIM e fornitori OilProject Srl di Milano e A.di.co.m. Group Srl).).
Nomina di TIM[15] e Fornitori a responsabile del trattamento: necessaria per i trattamenti su indicati.
Tipologia dei dati trattati: dati personali.
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

15.2 Personale coinvolto nel trattamento dei dati

Per la gestione sistemistica:
Responsabile del trattamento dei dati: TIM.
Incaricati del trattamento dei dati: settore CR.CD.R (vedi rif. [RI9] per l'elenco completo degli Amministratori di Sistema)

Per la gestione middleware e applicativa:
Responsabile del trattamento dei dati: OilProject Srl di Milano (coordinamento TIM da parte del settore CR.CD.R.) e A.di.co.m. Group Srl per la sola componente di Virtual Class Room.
Incaricati del trattamento dei dati per le attività di provisioning e configurazione delle utenze: settore CR.CD.R di TIM (vedi rif. [RI9]) per l'elenco completo degli Amministratori di Sistema)

Riguardo gli incaricati della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (password injection) mediante l'interfaccia di RAMSES denominata Keepass.

15.3 Attività affidate a terzi che comportano il trattamento di dati

La gestione middleware e applicativa è affidata a Oilproject Srl di Milano e a A.di.co.m. Group Srl per la componente di Virtual Class Room.

[15] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

15.4 Piano degli interventi formativi

Il Piano formativo degli incaricati al trattamento dei dati amministratori di sistema è nell'ambito dei perimetri di certificazione ISO 27001.

15.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

Il servizio *SaaS di Collaborazione Learning Management System* e le piattaforme attraverso cui è erogato, sono ospitate presso i centri servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

Il servizio si basa su due database realizzati tramite *RDBMS MySQL* e un database realizzato tramite *RDBMS MongoDB.*

15.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM, sono le sedi di:

- Roma – Viale Parco de Medici 61, e di Taranto sita in Via Campania 11- Taranto, per quanto concerne la gestione sistemistica, la gestione middleware e la gestione applicativa.

15.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e i dati

Le tipologie di interconnessione sono le seguenti, per tutte le tipologie di trattamento dati (gestione sistemistica, gestione middleware e gestione applicativa):

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali

Le tipologie di backup dei dati sono le seguenti:

- backup incrementale giornaliero e backup full settimanale, per i dati di configurazione e dei data base
- backup incrementale giornaliero e backup full settimanale, per le *cartelle*

I tempi di backup e restore rientrano nelle tempistiche contrattuali che prevedono:

- RTO <= di 4h e RPO <= 1 h

I luoghi dove vengono conservati i dati sono:

- I Centri Servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

Le strutture incaricate delle attività di backup e restore sono il settore CR.CD.R.

15.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.

Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).
Inoltre i servizi sono sviluppati ed esercitati nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione
- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione
- data retention
- documentazione
- hardening
- patching
- procedurale
- protezione log
- separazione ambienti
- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale è riportato in appendice par. 19.2.
L'elenco completo delle misure di sicurezza implementate da TIM sul servizio *SPC Cloud lotto 1 di tipo Collaborazione Learning Management System*, incluse quelle derivanti dall'adozione delle policy aziendali, sono descritte in dettaglio nel documento ad uso interno *Profilo di sicurezza del servizio di tipo SPC1-E-LEARNING* [RI8].

16 SERVIZIO DI DISASTER RECOVERY AS A SERVICE (DRAAS)

Il servizio *di tipo DRaaS*, si prefigge di estendere gli scenari implementativi di continuità operativa già in parte erogati dal servizio di BackUp as a Service, anche esso facente parte dei servizi *SPC Cloud lotto 1*, ma in modo da poter garantire parametri di RTO e RPO più stringenti secondo le necessità delle singole Pubbliche Amministrazioni.

Il servizio si ispira alle "*Linee Guida per il Disaster Recovery delle pubbliche amministrazioni*" pubblicate da *AgID* e consente di implementare soluzioni di Disaster Recovery classificate in base ai livelli di RTO ed RPO richiesti, dove:

- *RPO* (*Recovery Point Objective*), indica la perdita dati tollerata; rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto;
- *RTO* (*Recovery Time Objective*), indica il tempo di ripristino del servizio; è la durata di tempo entro il quale un business process, ovvero il sistema informativo primario, deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili;

In particolare sono disponibili 2 *Classi di Servizio*:

- *Classe 2*: RPO=4-8-24 ore ed RTO=24 ore, 3 giorni
- *Classe 3:* RPO<4-8-24 ore ed RTO=4-8-24 ore

Da un punto di vista architetturale il servizio consente di implementare un disaster recovery tra il sito primario di una Pubblica Amministrazione ed un sito secondario realizzato sull'infrastruttura SCP Cloud tramite piattaforma OpenStack.
La copia dei dati dall'ambiente di produzione all'ambiente di disaster recovery avviene in modalità asincrona sia per la Classe 2 sia per Classe 3 e può essere effettuata sia con collegamento dedicato (in questo caso si garantiscono RTO e RPO) sia con collegamento Internet (RPO e RTO non sono soggetti a SLA). Il dimensionamento del collegamento è in funzione della "Classe di servizio " scelta.
Il servizio prevede l'utilizzo di software specifici per la replica dei dati di configurazione e dei dati applicativi, che permettono di proteggere interi server o specifiche porzioni di dati sia da server fisici, sia da server virtuali, su server anche differenti, in dimensionamento e versione di sistema operativo, da quello del sito primario.
In relazione ai trattamenti indicati, deve essere prevista la nomina di TIM a *Responsabile del trattamento* da parte della Pubblica Amministrazione che sottoscrive il servizio, tramite specifica clausola contrattuale, così come previsto dall'Art. 28 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.

- I **servizi infrastrutturali DRaaS** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM" sulle misure specifiche proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione

16.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento: storage e gestione sistemistica infrastrutturale
Nomina TIM[16] a responsabile del trattamento: necessaria per i trattamenti su indicati
Tipologia dei dati trattati: dati personali e categorie particolari di dati.
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

[16] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

16.2 Personale coinvolto nel trattamento dei dati

Responsabile del trattamento dei dati: TIM.
Incaricati del trattamento dei dati: settore CR.CD.R (vedi rif. [RI9] per l'elenco completo degli Amministratori di Sistema).

Riguardo gli incaricati della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (password injection) mediante l'interfaccia di RAMSES denominata Keepass.

16.3 Attività affidate a terzi che comportano il trattamento di dati

16.4 Piano degli interventi formativi

Piano formativo degli incaricati al trattamento dei dati:

- formazione nell'ambito dei perimetri di certificazione ISO 27001.

Piano formativo degli incaricati al trattamento dei dati amministratori di sistema:

- formazione nell'ambito dei perimetri di certificazione ISO 27001;

16.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

Le basi dati sono nel sito TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

.

16.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM, sono le sedi di: Bari, sita in Via Dioguardi 1 e Taranto, sita in Via Campania 11 e Roma - Acilia Via di Macchia Palocco 243

16.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e i dati

Le tipologie di interconnessione sono le seguenti:

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali

16.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.
Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).
Inoltre i servizi sono sviluppati ed eserciti nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

- I **servizi infrastrutturali DRaaS** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM" sulle misure specifiche proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione

- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione
- data retention
- documentazione
- hardening
- patching
- procedurale
- protezione log
- separazione ambienti
- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale è riportato in appendice par. 19.2.

Per quanto riguarda la sicurezza delle categorie particolari di dati personali sono riportate di seguito le misure minime che TIM adotta e le misure minime che restano in capo al cliente PA. La X indica chi ha la responsabilità di garantire la misura di sicurezza. Le misure di responsabilità cliente possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

16.8.1 Misure aggiuntive per il trattamento dei dati sensibili/giudiziari

Il trattamento di dati sensibili/giudiziari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di dati personali.

Categoria misura	Misura di protezione	Responsabilità TIM	Responsabilità cliente PA
Back-up	E' prevista la redazione di procedure documentate di ripristino/restore dei dati (e di configurazione se previsto dal contratto). Tali procedure di ripristino dell'accesso ai dati garantiscono tempi non superiori a sette giorni qualora tutti i dati utilizzati dal sistema andassero persi.		X
Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma.	X Sulle componenti infrastrutturali	X Sulle singole Virtual Machine
Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di DBMS necessari a correggere difetti e prevenire vulnerabilità della piattaforma.	X Sulle componenti infrastrutturali	X Sulle singole Virtual Machine
Riservatezza	Nella piattaforma sono previste soluzioni (es. cifratura o altre) che, considerato il numero e la natura dei dati trattati, rendano i dati sensibili o giudiziari temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità.		X[17]
Supporti di memorizzazione	E' prevista la definizione e l'attuazione di procedure di cancellazione fisica (ad es. tramite Wiping o Degaussing) a seguito della dismissione o della diversa assegnazione d'uso (ad es. utilizzo da parte di un Cliente differente) di elaboratori o supporti utilizzati, al fine di garantire l'inaccessibilità "assoluta" agli stessi.	X	

Tabella 10 – Servizio DRaaS, Misure a protezione dei dati personali sensibili/giudiziari

[17] Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo.

16.8.2 Misure aggiuntive per il trattamento dei dati sanitari

Il trattamento di Dati Sanitari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali e sensibili. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

Categoria misura	Misura di protezione	Responsabilità TIM	Responsabilità cliente PA
Riservatezza	Nella piattaforma è prevista, al fine di garantire la riservatezza dei dati sanitari conservati (data-at-rest), la cifratura degli stessi o l'utilizzo di codici identificativi o di altre soluzioni che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. In caso di trasmissione dei dati sanitari è garantita in ogni caso la cifratura dei dati		X[18]

Tabella 11 – Servizio DRaaS, Misure a protezione dei dati personali sanitari

16.8.3 Misure aggiuntive per il trattamento dei dati sanitari tramite FSE / Dossier Sanitario

Il trattamento di dati sanitari tramite Fascicolo Sanitario Elettronico / Dossier Sanitario comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali, Sensibili e Sanitari. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

Categoria misura	Misura di protezione	Responsabilità TIM	Responsabilità cliente PA
Riservatezza	L'applicativo è costruito in maniera tale da permettere l'oscuramento (revocabile nel tempo) di taluni dati o documenti sanitari a seguito di richieste dell'interessato. Le informazioni oscurate sono in ogni caso rese disponibili al professionista sanitario o alla struttura interna titolare che li ha raccolti o elaborati. L'oscuramento dell'evento clinico avviene con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta.		X
Riservatezza	L'applicativo deve essere costruito in maniera tale da permettere la gestione del consenso al trattamento da parte dell'interessato. L'applicativo consente di raccogliere le informazioni e renderle disponibili e visualizzabili esclusivamente a un sottoinsieme di utenze definito dal Cliente Business. In caso di revoca dello stesso il Dossier/Fse non è ulteriormente implementato. Le informazioni sanitarie già presenti restano disponibili e visualizzabili esclusivamente alla funzione interna del Cliente che le ha raccolte (non sono più condivise con i professionisti di altri reparti).		X

Tabella 12 – Servizio DRaaS, Misure a protezione dei dati personali sanitari tramite FSE / Dossier Sanitario

L'elenco completo delle misure di sicurezza implementate da TIM sul servizio *SPC Cloud lotto 1 di tipo DRaaS*, incluse quelle derivanti dall'adozione delle policy aziendali, sono descritte in dettaglio nei documenti ad uso interno:

- *Profilo di Sicurezza del servizio SPC1-DISASTER-RECOVERY-DRAAS* [RI11], per i servizi basati sulla tecnologia HP Helion Openstack
- *Profilo di Sicurezza del servizio SPC-CCOS* [RI14], per i servizi basati sulla tecnologia Cisco-Canonical OpenStack

[18] Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo.

17 SERVIZIO DI ENTERPRISE CONTAINER AS A SERVICE (ECAAS) E DI COMMUNITY CONTAINER AS A SERVICE (CCAAS)

Nell'ambito del Contratto Quadro SPC Cloud Lotto 1 è proposto un servizio in grado di fornire una piattaforma ECaaS/CCaaS, basata su tecnologia *Container Docker*.
Il servizio è erogato usando una piattaforma, istanziata per ogni specifico cliente e basata su un'architettura che è funzionalmente suddivisa in tre livelli (planes) che supportano il classico modello Supply/Delivery/Demand delle piattaforme Cloud: *back plane, core plane e front plane*.
In particolare:

- il *back plane* fornisce le risorse infrastrutturali (IaaS) necessarie ad ogni istanza ECaaS/CCaaS e di fatto coincide con la piattaforma Cloud SPC, basata su OpenStack.
- il *core plane* implementa le funzionalità fondamentali che erogano i servizi basati su tecnologia Containers (*Containers Orchestration*), la loro gestione (*Delivery Management*) e la connessione con funzioni per lo sviluppo di servizi applicativi basati su incapsulamento a Containers (*CI/CD pipeline instances*).
- il *front plane* permette agli utenti finali di accedere e fruire i servizi offerti dalla piattaforma, tramite una console (dashboard) sia in modalità diretta (utente) che programmatica (a mezzo di funzioni API).

I vari moduli architetturali sono costituiti da diversi prodotti/soluzioni software, pressoché basati su progetti open source, integrati tra loro opportunamente usando chiamate API.
Tutti questi moduli sono incapsulati in Containers, per cui la stessa piattaforma ECaaS/CCaaS è di fatto realizzata usando la stessa tecnologia offerta per i servizi erogati.

Poiché la soluzione ECaaS/CCaaS è realizzata sfruttando le risorse infrastrutturali della piattaforma SPC Cloud OpenStack di fatto ne eredita le caratteristiche intrinseche di sicurezza e affidabilità. Inoltre un'istanza ECaaS/CCaaS e dedicata ad un singolo cliente garantendo quindi un elevato livello di separazione logica dei servizi da essa erogati.
In relazione ai trattamenti indicati, deve essere prevista la nomina di TIM a *Responsabile del trattamento* da parte della Pubblica Amministrazione che sottoscrive il servizio, tramite specifica clausola contrattuale, così come previsto dall'Art. 28 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.

- I **servizi infrastrutturali ECaaS/CCaaS** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM/fornitore DxC" sulle misure specifiche proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte sulle singole macchine virtuali da parte del cliente stesso oppure attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione

17.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento:
storage e gestione sistemistica infrastrutturale (creazione VdC): responsabile TIM;
backup delle VM: responsabile DxC
Nomina TIM[19] e Fornitori a responsabile del trattamento: necessaria per i trattamenti su indicati.
Tipologia dei dati trattati: dati personali e particolari;
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

[19] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

17.2 Personale coinvolto nel trattamento dei dati

Responsabile del trattamento dei dati: TIM.
Incaricati del trattamento dei dati: settore CR.CD.R (vedi rif. [RI9] per l'elenco completo degli Amministratori di Sistema).

Responsabile del trattamento dei dati: DxC
Incaricati del trattamento dei dati: l'elenco completo degli Amministratori di Sistema DXC è conservato sullo SharePoint aziendale di progetto.

Riguardo gli incaricaTIM della custodia delle credenziali di autenticazione, il servizio fa uso di una piattaforma centralizzata di controllo accessi chiamata RAMSES (*Remote Access Mediation Strategic Enterprise Security*) utilizzata dagli amministratori di sistema TIM, che dispone di una cassaforte elettronica integrata di tipo *Lieberman ERPM*, in cui custodisce le credenziali di autenticazione.
In particolare *Lieberman ERPM* offre un sistema di gestione delle credenziali privilegiate non personali su sistemi operativi e apparati di rete. L'applicazione gestisce in un archivio protetto le credenziali degli apparati e garantisce che le credenziali possano essere utilizzate solo dagli amministratori autorizzati. Durante l'uso le credenziali vengono assegnate univocamente agli amministratori e alla fine dell'utilizzo vengono modificate in modo automatico.
Le credenziali sono utilizzate dal singolo amministratore senza che questi ne venga a conoscenza (password injection) mediante l'interfaccia di RAMSES denominata Keepass.

17.3 Attività affidate a terzi che comportano il trattamento di dati

Le attività di backup delle VM sono affidate a DXC.

17.4 Piano degli interventi formativi

Piano formativo degli incaricaTIM al trattamento dei dati:

- formazione nell'ambito dei perimetri di certificazione ISO 27001.

Piano formativo degli incaricati al trattamento dei dati amministratori di sistema:

- formazione nell'ambito dei perimetri di certificazione ISO 27001;

Piano formativo degli incaricati DxC al trattamento dei dati:

- formazione al momento dell' assunzione
- formazione annuale WBL

17.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

Le basi dati sono nel Centro Servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

.

17.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli IncaricaTIM per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale TIM, sono le sedi di: Bari, sita in Via Dioguardi 1 e Taranto, sita in Via Campania 11 e Roma - Acilia Via di Macchia Palocco 243

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati DXC per effettuare il trattamento dei dati sono:

- pc e consolle

Il luogo in cui sono effettuati i trattamenti dati (Distruzione dei dati residui) da parte del personale DXC è la sede di Acilia Via di Macchia Palocco 243, mentre le sedi da dove si accede per la gestione del servizio sono: Inverno (PV) SP ex SS421 (incrocio SP 234) Basiglio (MI) Via Francesco Sforza 13 Pomezia (RM) Via Giamaica 7 Cernusco sul Naviglio (MI) Via Grandi 4.

17.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e i dati

Le tipologie di interconnessione TIM sono le seguenti:

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali

Le tipologie di backup dei dati svolte da TIM sono le seguenti:

- backup delle configurazioni

Le tipologie di interconnessione DXC sono le seguenti:

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale)

Le tipologie di backup dei dati svolte da DxC sono le seguenti:

- Non sono svolte attività di backup dei dati nell'ambito del servizio ECaaS.

I luoghi dove vengono conservati i dati sono:

- Centro Servizi TIM di Rozzano sito in Viale Toscana 3 (MI), Pomezia sito in Via Pontina Km. 29.1000 (RM), Oriolo sito in Via Oriolo Romano 257 – Roma, Acilia Via di Macchia Palocco 243 e Cesano Maderno sito in Via Martinelli - Cesano Maderno (MI).

17.8 Misure di sicurezza a protezione dei dati personali

I servizi ICT offerti da TIM alla propria clientela sono protetti mediante misure di carattere tecnico ed organizzativo, che tengono conto della criticità dei dati trattati e rispettano appieno i requisiti espressi dagli Articoli 22 e 32 del nuovo Regolamento EU n. 679/2016 in materia di protezione dei dati personali.
Secondo questi il titolare ed il responsabile del trattamento dei dati personali devono predisporre ed attuare delle misure tecniche ed organizzative idonee a garantire un livello di sicurezza dei dati personali adeguato al rischio, in termini di riservatezza, integrità e disponibilità dei dati e di resilienza dei servizi, ed essere in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso (*accountability*).
Inoltre i servizi sono sviluppati ed eserciti nel pieno rispetto di quanto espresso dall'Art. 25 del Regolamento, che riguarda la *protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* (*Data protection by design and by default*) tramite adeguate misure tecniche ed organizzative.

- I **servizi infrastrutturali ECaaS/CCaaS** hanno misure di sicurezza adeguate a garantire la sicurezza dei dati personali; queste piattaforme sono adeguate anche a trattare particolari categorie di dati personali (sensibili/giudiziari, sanitari, fse/ds) purchè venga attuata la matrice di responsabilità "cliente PA/fornitore TIM/fornitore DxC" sulle misure specifiche

proposte da TIM by design by default. Questo aspetto è trattato all' interno del paragrafo "Misure di sicurezza a protezione dei dati personali". Se il cliente ha esigenze particolari legate alla tipologia del dato queste devono essere risolte sulle singole macchine virtuali da parte del cliente stesso oppure attraverso valutazioni requisiti/soluzioni da richiedere al fornitore TIM con specifici atti integrativi al di fuori del CQ. Ogni personalizzazione dei requisiti/meccanismi di sicurezza aggiuntivi a quanto previsto dal contratto quadro, è declinata all'interno del Documento Programmatico di Sicurezza (questo documento) della singola Amministrazione

In particolare le misure di sicurezza attuate da TIM derivano da una valutazione condotta mediante una metodologia che assegna un valore di criticità ad ogni sistema/componente, calcolato considerando i seguenti contributi:

- la mappatura sui *processi* aziendali supportati dal sistema in esame e l'importanza che esso riveste per il loro funzionamento;
- la *Compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati trattati).

La criticità intrinseca di un sistema/piattaforma rappresenta un elemento fondamentale per:

- individuare il Profilo di Sicurezza (PdS) da applicare a protezione del sistema stesso;
- scegliere il tipo di analisi del rischio da effettuare sul sistema (di Baseline o di dettaglio);
- definire la priorità delle attività e degli interventi di sicurezza da realizzare.

La metodologia utilizza una *Libreria dei Requisiti di Sicurezza* che racchiude in se l'elenco di tutti i requisiti che la funzione tecnica di sicurezza ha individuato per:

- soddisfare vincoli normativi;
- soddisfare policy aziendali;
- realizzare la protezione dalle vulnerabilità note.

La *LRS* viene utilizzata nell'ambito del processo di *Risk Management* per individuare i requisiti di sicurezza da applicare sui singoli sistemi/componenti in base alle indicazioni derivanti dalla VCI, in particolare:

- il perimetro in cui il sistema/componente si colloca;
- la *compliance* dei dati trattati;
- gli *impatti di business* derivanti dall'eventuale perdita delle caratteristiche di sicurezza del sistema sulle informazioni da esso trattate (Riservatezza, Integrità e Disponibilità dei dati).
- la fascia di criticità in cui il sistema/componente si colloca.

Il risultato di questa analisi produce una lista di requisiti formalizzati nel documento *Profilo di Sicurezza* che e sono relativi ai seguenti ambiti:

- allarmistica
- alta affidabilità
- antivirus
- autenticazione
- autorizzazione
- back up
- cifratura flussi
- confinamento applicazione
- confinamento postazioni di amministrazione
- data retention
- documentazione
- hardening
- patching
- procedurale
- protezione log
- separazione ambienti
- sviluppo software
- tracciamento

Un elenco esaustivo delle misure di sicurezza adottate per il dato personale sia da TIM sia da DxC è riportato in appendice par. 19.2.

Per quanto riguarda la sicurezza delle categorie particolari di dati personali sono riportate di seguito le misure minime che TIM e DxC adottano e le misure minime che restano in capo al cliente PA. La X indica chi ha la responsabilità di garantire la misura di sicurezza. Le misure di responsabilità cliente possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

17.8.1 Misure aggiuntive per il trattamento dei dati sensibili/giudiziari

Il trattamento di dati sensibili/giudiziari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di dati personali.

Categoria misura	Misura di protezione	Responsabilità TIM	Responsabilità DxC	Responsabilità cliente PA
Back-up	E' prevista la redazione di procedure documentate di ripristino/restore dei dati. Tali procedure di ripristino dell'accesso ai dati garantiscono tempi non superiori a sette giorni qualora tutti i dati utilizzati dal sistema andassero persi.		SI' (Soltanto in caso di utilizzo del servizio BaaS da parte del Cliente)	
Back-up VM	Viene effettuato il backup dell'infrastruttura delle VM.		SI'	
Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma.	X Sull' infrastruttura	SI' (Limitatamente al patching del S.O. nell'ambito della gestione sistemistica)	
Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di DBMS necessari a correggere difetti e prevenire vulnerabilità della piattaforma.		SI' (Limitatamente al patching del middleware nell'ambito della gestione del middleware)	
Riservatezza	Nella piattaforma sono previste soluzioni (es. cifratura o altre) che, considerato il numero e la natura dei dati trattati, rendano i dati sensibili o giudiziari temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità.			X[20]
Supporti di memorizzazione	E' prevista la definizione e l'attuazione di procedure di cancellazione fisica (ad es. tramite Wiping o Degaussing) a seguito della dismissione o della diversa assegnazione d'uso (ad es. utilizzo da parte di un Cliente differente) di elaboratori o supporti utilizzati, al fine di garantire l'inaccessibilità "assoluta" agli stessi.		X	

Tabella 13 – Servizio ECaaS/CCaaS, Misure a protezione dei dati personali sensibili/giudiziari

17.8.2 Misure aggiuntive per il trattamento dei dati sanitari

Il trattamento di Dati Sanitari comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali e sensibili. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

[20] Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo.

Categoria misura	Misura di protezione	Responsabilità TIM /DxC	Responsabilità cliente PA
Riservatezza	Nella piattaforma è prevista, al fine di garantire la riservatezza dei dati sanitari conservati (data-at-rest), la cifratura degli stessi o l'utilizzo di codici identificativi o di altre soluzioni che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. In caso di trasmissione dei dati sanitari è garantita in ogni caso la cifratura dei dati		X[21]

Tabella 14 – Servizio ECaaS/CCaaS, Misure a protezione dei dati personali sanitari

17.8.3 Misure aggiuntive per il trattamento dei dati sanitari tramite FSE / Dossier Sanitario

Il trattamento di dati sanitari tramite Fascicolo Sanitario Elettronico / Dossier Sanitario comporta l'applicazione delle seguenti misure aggiuntive proposte da TIM by design by default rispetto alle misure applicate al trattamento di Dati Personali, Sensibili e Sanitari. Queste misure possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

Categoria misura	Misura di protezione	Responsabilità TIM /DxC	Responsabilità cliente PA
Riservatezza	L'applicativo è costruito in maniera tale da permettere l'oscuramento (revocabile nel tempo) di taluni dati o documenti sanitari a seguito di richieste dell'interessato. Le informazioni oscurate sono in ogni caso rese disponibili al professionista sanitario o alla struttura interna titolare che li ha raccolti o elaborati. L'oscuramento dell'evento clinico avviene con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta.		X
Riservatezza	L'applicativo deve essere costruito in maniera tale da permettere la gestione del consenso al trattamento da parte dell'interessato. L'applicativo consente di raccogliere le informazioni e renderle disponibili e visualizzabili esclusivamente a un sottoinsieme di utenze definito dal Cliente Business. In caso di revoca dello stesso il Dossier/Fse non è ulteriormente implementato. Le informazioni sanitarie già presenti restano disponibili e visualizzabili esclusivamente alla funzione interna del Cliente che le ha raccolte (non sono più condivise con i professionisti di altri reparti).		X

Tabella 15 – Servizio ECaaS/CCaaS, Misure a protezione dei dati personali sanitari tramite FSE / Dossier Sanitario

L'elenco completo delle misure di sicurezza implementate da TIM sul servizio *SPC Cloud lotto 1 di tipo ECaaS/CCaaS*, incluse quelle derivanti dall'adozione delle policy aziendali, sono descritte in dettaglio nel documento ad uso interno *Profilo di Sicurezza del servizio* SPC1-ECAAS [RI12].

21 Tipicamente le misure relative alla cifratura e/o separazione del dato sensibile dal dato anagrafico sono attuate a livello applicativo.

18 SERVIZI DI CLOUD ENABLING

I Servizi di Cloud Enabling sono servizi professionali finalizzati a supportare l'Amministrazione nei progetti di Cloud Transformation al fine di utilizzare le risorse ed i servizi previsti dal Contratto Quadro.
Il servizio è fornito attraverso l'impiego di specifiche figure professionali.
Di seguito alcune delle possibili finalità del servizio di Cloud Enabling:

- introduzione del paradigma cloud nell'ambito della loro infrastruttura tecnologica;
- virtualizzazione di infrastrutture fisiche nell'ambito dei CED privati delle Pubbliche Amministrazioni (migrazione Physical-to-Virtual);
- implementazione di progetti di natura "ibrida" utilizzando i CED delle Pubbliche Amministrazioni e le soluzioni infrastrutturali messe a disposizione dal Contratto Quadro (ad es.: soluzioni di Disaster Recovery):
- utilizzo di soluzioni infrastrutturali ed applicative "as a Service" e di implementazione di progetti complessi cloud nativi attraverso le soluzioni descritte nel Contratto Quadro;
- porting delle applicazioni delle Amministrazioni per l'utilizzo in ambienti Cloud

In particolare le principali attività sono di seguito elencate:

- analisi costi/benefici e fattibilità
- progettazione di virtual data center/ VM
- configurazione di virtual data center / VM
- supporto per la definizione e configurazione delle policy di backup/restore
- supporto per la progettazione di Virtual Private Cloud e di Virtual Data Center (comprensivo di progettazione di infrastrutture tecnologiche ad uso dei Poli regionali) tutorship.
- cloud compliancy della componente applicativa

18.1 Elenco dei trattamenti di dati personali

Tipo di trattamento: potrebbero essere svolti trattamenti di dati personali su ogni attività di cloud enabling

Nomina del fornitore[22] di Cloud Enabling a subresponsabile del trattamento: necessaria la nomina di TIM per i trattamenti su indicati. TIM nominerà subresponsabile il fornitore di cloud enabling
Tipologia dei dati trattati: dati personali e categorie particolari di dati.
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

18.2 Personale coinvolto nel trattamento dei dati

Responsabile del trattamento dei dati: TIM[23]

18.3 Attività affidate a terzi che comportano il trattamento di dati

Fornitore di Cloud Enabling

[22] L'elenco dei subfornitori TIM di Cloud Enabling è reperibile al seguente indirizzo www.cloudspc.it
[23] TIM nominerà subresposnabile al trattamento il fornitore di cloud enabling

18.4 Basi di dati e luoghi in cui risiedono fisicamente i dati

CED delle Pubbliche Amministrazioni e/o Data Center TIM.

18.5 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, cioè gli strumenti utilizzati dai Responsabili e dagli Incaricati per effettuare il trattamento dei dati sono:

- pc e consolle o qualsiasi altro strumento utilizzato dal fornitore necessario a svolgere le attività di Cloud Enabling

18.6 Misure di sicurezza a protezione dei dati personali

Le misure di sicurezza sono quelle previste per i servizi/piattaforme SPC Cloud situate nei DC TIM o servizi/piattaforme situate nei CED delle Pubbliche Amministrazioni coinvolti nelle attività di Cloud Enabling

19 SERVIZIO DI CONSERVAZIONE A NORMA

Il servizio di *Conservazione a norma* realizza il processo che permette di conservare dei documenti in formato digitale garantendone autenticità, integrità, affidabilità, leggibilità e reperibilità.
La validità legale del documento e del suo contenuto è garantita dall'apposizione sul documento di due "sigilli":

- firma digitale,
- marca temporale, un "timbro" che garantisce l'esistenza del documento in un momento temporalmente preciso.

La Conservazione Digitale a norma dei Documenti Informatici ha importanti Fondamenti Normativi, ovvero Leggi alle quali il Sistema di Conservazione deve essere conforme.
Il *Codice di Amministrazione Digitale*, emanato con decreto legislativo 7 marzo 2005 n. 82, e successivamente modificato ed aggiornato, definisce cosa è un 'Documento informatico' e ne definisce le condizioni di validità a termini di legge. In particolare, negli articoli 43, 44 e 44-bis vengono definiti i requisiti fondamentali per la sua gestione e conservazione.
Il Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, "*Regole tecniche in materia di sistema di conservazione*" stabilisce le regole tecniche che devono essere utilizzate per conservare i documenti informatici e garantire loro il valore legale. Questo decreto stabilisce in modo particolare due cose molto importanti:

- definisce che la Pubblica Amministrazione si può avvalere per la Conservazione a norma dei Documenti solo di Conservatori Accreditati;
- attribuisce ad AgID, Agenzia per l'Italia Digitale, il ruolo di Accreditare i Conservatori e garantirne la Vigilanza.

La Circolare AgID 10 aprile 2014, n. 65, "*Accreditamento e vigilanza conservatori*" dà finalmente attuazione alle Regole Tecniche stabilendo le modalità attraverso le quali un Conservatore si può accreditare e dunque diventa abilitato alla conservazione dei Documenti della Pubblica Amministrazione.

19.1 Elenco dei trattamenti di dati personali

Per il trattamento dei dati personali si ha nello specifico:
Tipo di trattamento: gestione sistemistica, gestione middleware, backup e gestione applicativa.
Nomina di TI Trust Technologies Srl a sub-responsabile del trattamento: necessaria per i trattamenti dei dati personali su indicati, di cui l'Amministrazione è Titolare per la fornitura del servizio.
In particolare, il responsabile del trattamento è l'Amministratore Delegato della società, che può a sua volta delegare tale ruolo al responsabile delle Direzione operativa.
Nomina di TIM a responsabile del trattamento: necessaria esclusivamente per il trattamento dei dati personali dei referenti della Pubblica Amministrazione sottoscrittrice del contratto

Tipologia dei dati trattati: dati personali, dati personali particolari
Tutti questi aspetti devono essere formalizzati nelle lettere di nomina.

19.2 Personale coinvolto nel trattamento dei dati

Per la gestione sistemistica, middleware e applicativa:
Responsabile del trattamento dei dati: TI Trust Technologies Srl.
Le risorse che ricoprono i ruoli indicati dalla normativa per le attività connesse all'operatività dei servizi soggetti ad accreditamento o ad attestazione della conformità normativa rispondano direttamente all'Amministratore Delegato.
Oltre ai ruoli specificamente definiti dalla normativa, i processi di erogazione dei detti servizi, richiedono lo svolgimento di altri ruoli caratteristici delle organizzazioni che erogano servizi di tipo informatico o del mondo ICT.
In TI Trust Technologies Srl questi ruoli sono organizzati per processo, ed essendo quindi trasversali rispetto alle funzioni organizzative non vengono riportati nel presente documento.

19.3 Attività affidate a terzi che comportano il trattamento di dati

Non sono presenti attività affidate a terzi che comportano il trattamento di dati.

19.4 Piano degli interventi formativi

TI Trust Technologies garantisce l'adeguatezza al ruolo del personale assegnato a tutti i livelli organizzativi, mediante:

- l'individuazione delle competenze necessarie per le risorse umane che svolgono attività che influenzano la conformità ai requisiti del servizio/sistema/prodotto;
- l'erogazione di formazione-addestramento alle risorse, poiché acquisiscano la necessaria competenza, realizzata attraverso il ricorso a docenti interni o ad Enti di formazione qualificati;
- la valutazione dell'efficacia della formazione-addestramento effettuata;
- la conservazione delle registrazioni.

Per il presidio di tale processo, TI Trust Technologies segue le modalità ed i metodi stabiliti dalla competente funzione di gestione del personale di TIM.
Tutti gli interventi di formazione-addestramento vengono registrati attraverso apposita documentazione; in tal modo è possibile avere evidenza delle date di svolgimento, dei contenuti e del personale che vi ha preso parte.

TI Trust Technologies è qualificata ed iscritta nei seguenti elenchi pubblici tenuti dall'autorità di vigilanza sui servizi da essa erogati:

- Qualified Trust Service Provider a norma del Regolamento eIDAS (n. 910/2014 dell'Unione Europea):
- dal novembre 2016 per i servizi di Validazione Elettronica Temporale
- dal maggio 2017, per i servizi di firma elettronica, sigillo elettronico e certificati di autenticazione di siti web;
- dal 2015, gestore dell'Identità Digitale in ambito SPID;
- dal 2014, elenco dei conservatori accreditati per il servizio di conservazione dei documenti informatici;
- dal 2005 (già come IT Telecom), elenco dei gestori del servizio di PEC (Posta Elettronica Certificata);
- dal 2000 (già come Saritel SpA, IT Telecom SpA, I.T. Telecom Srl e TI Trust Technologies Srl), elenco dei certificatori di firma qualificata.

Inoltre, dal novembre 2012 la società ha ottenuto e mantiene la Certificazione del proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI) rispetto alla normativa ISO 27001.
Infine, dal novembre 2019 la società ha ottenuto l'estensione della Certificazione del proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI) anche ai servizi SaaS con l'utilizzo delle linee guida ISO/IEC 27017:2015 e ISO 27018:2019.

19.5 Basi di dati e luoghi in cui risiedono fisicamente i dati

I dati del servizio *Conservazione a norma* risiedono presso la sede di TI Trust Technologies Srl, in S. R. 148 Pontina km. 29,100 - 00071 Pomezia (RM) e presso il sito di DR in Via Oriolo Romano 257 – 00189 Roma (RM).
I dati personali sono trattati dai dipendenti di TI Trust Technologies Srl, che sono stati autorizzati al trattamento dei dati personali ed hanno ricevuto, al riguardo, adeguate istruzioni operative.

19.6 Tipologia di dispositivi di accesso utilizzati per effettuare il trattamento dei dati

La tipologia di dispositivi di accesso, utilizzati dal personale di TI Trust Technologies per effettuare il trattamento dei dati sono:

- pc e consolle.

I luoghi in cui sono effettuati i trattamenti dati da parte del personale sono le sedi di TI Trust Technologies Srl, in S. R. 148 Pontina km. 29,100 - 00071 Pomezia (RM) e presso il sito di DR in Via Oriolo Romano 257 – 00189 Roma (RM).

19.7 Tipologia di interconnessione tra i dispositivi d'accesso utilizzati e i dati

Le tipologie di interconnessione sono le seguenti:

- tramite VPN di management, per i collegamenti effettuati dalle sedi aziendali (intranet aziendale);
- tramite NGVPN su Internet e successivo instradamento tramite VPN di management, per i collegamenti effettuati da sedi extra aziendali.

I dati e le informazioni contenuti nel sistema ICT di TI Trust Technologies sono soggetti a politiche di back up che si differenziano in funzione della tipologia dei dati e della loro riservatezza.
Le politiche di Back Up di base sono:

- back up incrementale giornaliero
- back up full settimanale
- retention dei dati di 1 mese

L'attività di ripristino totale o parziale prevede:

- identificazione del perimetro d'intervento, ovvero individuazione dei server sui quali deve essere eseguita l'attività di ripristino per rendere consistenti i dati;
- selezione dei dati di back-up in base all'identificativo temporale (giorno e ora);
- esecuzione del restore dei dati e verifica dell'esito positivo; nel caso in cui il restore non abbia esito positivo, viene effettuata un'operazione di roll-back.

I luoghi in cui sono effettuati i backup sono le sedi di TI Trust Technologies Srl, in S. R. 148 Pontina km. 29,100 - 00071 Pomezia (RM) e presso il sito di DR in Via Oriolo Romano 257 – 00189 Roma (RM).

19.8 Misure di sicurezza a protezione dei dati personali

Le misure adottate a protezione del Sistema ICT di TI Trust Technologies forniscono un livello elevato di protezione dei dati e del business dei Clienti e sono relative a:

- sicurezza fisica
- sicurezza logica
- sicurezza negli aspetti organizzativi
- gestione della continuità operativa

Per il dettaglio delle misure di sicurezza e compliance implementate a protezione dei dati personali trattati dal servizio di *Conservazione a norma* si veda il capitolo 9 di [RI17].

20 APPENDICE

20.1 Tabella riepilogativa delle tipologie dei dati e dei trattamenti previsti per i servizi SPC Cloud lotto 1

La seguente tabella riporta per ogni servizio *SPC Cloud lotto 1*, le informazioni relative al dato per cui il servizio è eventualmente *certificato*, la *tipologia dei dati* per cui il servizio, in termine di misure di sicurezza a protezione dei dati stessi, è conforme, i trattamenti dei dati previsti **e i responsabili del trattamento, siano essi TIM**[24] o suoi fornitori diretti.

Servizio	Tipologia dato certificato	Responsabile e trattamenti da prevedere nelle lettere di nomina
IAAS unmanaged (indifferentemente se su applicativo HP Helion OpenStack o applicativo Cisco-Canonical Openstack)	dati personali e particolari	**TIM:** a) gestione sistemistica infrastrutturale; b) storage.
PAAS unmanaged (indifferentemente se su applicativo HP Helion OpenStack o applicativo Cisco-Canonical Openstack)	dati personali e particolari	**TIM:** a) gestione sistemistica infrastrutturale; b) storage.
IAAS managed (indifferentemente se su applicativo HP Helion OpenStack o applicativo Cisco-Canonical Openstack)	dati personali e particolari	**TIM:** a) gestione sistemistica infrastrutturale; b) storage; c) gestione sistemistica.
PAAS managed (indifferentemente se su applicativo HP Helion OpenStack o applicativo Cisco-Canonical Openstack)	dati personali e particolari	**TIM:** a) gestione sistemistica infrastrutturale; b) storage; c) gestione sistemistica; d) gestione middleware e backup.
PAAS Oracle unmanaged su tecnologia Oracle OCM	dati personali e particolari	**Fornitore Oracle Italia:** a) gestione sistemistica infrastrutturale; b) storage.
PAAS Oracle managed su tecnologia Oracle OCM	dati personali e particolari	**Fornitore Oracle Italia:** a) gestione sistemistica infrastrutturale; b) storage; c) gestione sistemistica; d) gestione middleware e backup
PAAS Oracle unmanaged su tecnologia Oracle-Hitachi	dati personali e particolari	**TIM:** a) gestione sistemistica infrastrutturale; b) storage.
PAAS Oracle managed su tecnologia Oracle-Hitachi	dati personali e particolari	**TIM:** a) gestione sistemistica infrastrutturale; b) storage; c) gestione sistemistica; d) gestione middleware e backup.
BAAS	dati personali e particolari	**TIM:** a) gestione sistemistica infrastrutturale; b) storage.
SaaS di Produttività individuale	dati personali	**TIM:** a) gestione sistemistica[25] b) gestione middleware. **Fornitore Smc Treviso S.r.l:**

[24] TIM per svolgere le attività per le quali è nominata responsabile al trattamento dati personali potrebbe avvalersi di ulteriori soggetti terzi (subfornitori) il cui elenco aggiornato è reperibile al seguente indirizzo nell' area GDPR https://assistenza.timbusiness.it/

[25] L'attività di trattamento di *Gestione sistemistica* include per tale servizio anche quella di *Gestione backup dati*, effettuata a livello infrastrutturale

Servizio	Tipologia dato certificato	Responsabile e trattamenti da prevedere nelle lettere di nomina
		gestione applicativa
SaaS di Comunicazione Unificata	dati personali	**TIM:** a) gestione sistemistica[26]; b) gestione middleware. **Fornitore VoiSmart S.r.l:** gestione applicativa
SaaS di Collaborazione: File Sharing	dati personali	**TIM:** a) gestione sistemistica[27]; b) gestione middleware. **Fornitore Smc Treviso S.r.l:** gestione applicativa
SaaS di Collaborazione: Enterprise Social Network	dati personali	**TIM:** a) gestione sistemistica[28] b) gestione middleware. **Fornitore Smc Treviso S.r.l:** gestione applicativa
SaaS di Collaborazione: Learning Management System	dati personali	**TIM:** a) gestione sistemistica[29]; **Fornitore Oilproject S.r.l:** gestione middleware e applicativa **Fornitore A.di.co.m. Group S.r.l:** gestione applicativa (limitatamente alla componente Virtual Class Room)
DRAAS	dati personali e particolari	**TIM:** a) gestione sistemistica infrastrutturale; b) storage
ECAAS/CCaaS	dati personali e particolari	**TIM:** a) gestione sistemistica infrastrutturale; b) storage **Fornitore DXC:** a) backup delle virtual machine
Cloud Enabling	dati personali e particolari	**TIM**[30]**:** a) migrazione e/o cloud compliance;
Conservazione a norma	dati personali e particolari	**TIM:** a) gestione dei dati personali dei referenti della Pubblica Amministrazione sottoscrittrice del contratto **TI Trust Technologies:** a) gestione sistemistica; b) gestione middleware e backup; c) gestione applicativa.

Tabella 16– Tabella riepilogativa delle tipologie dei dati e dei trattamenti previsti per i servizi SPC Cloud lotto 1

[26] L'attività di trattamento di *Gestione sistemistica* include per tale servizio anche quella di *Gestione backup dati*, effettuata a livello infrastrutturale

[27] L'attività di trattamento di *Gestione sistemistica* include per tale servizio anche quella di *Gestione backup dati*, effettuata a livello infrastrutturale

[28] L'attività di trattamento di *Gestione sistemistica* include per tale servizio anche quella di *Gestione backup dati*, effettuata a livello infrastrutturale

[29] L'attività di trattamento di *Gestione sistemistica* include per tale servizio anche quella di *Gestione backup dati*, effettuata a livello infrastrutturale

[30] TIM per svolgere i trattamenti previsti nelle attività di Cloud Enabling si avvale dei subfornitori indicati nell'elenco presente su www.cloudspc.it

20.2 Misure di sicurezza definite da TIM a protezione dei dati personali

I servizi erogati al cliente in virtù dei contratti in corso sono stati acquisiti da terze parti soggette a stringenti vincoli contrattuali o sviluppati da TIM secondo metodologie già conformi al principio della **privacy by design** e **by default**. In particolare, tramite l'applicazione del processo di risk analysis e l'adozione di policy interne di sicurezza e compliance Privacy, TIM ha definito le misure di sicurezza adeguate per la protezione dei dati personali trattati nelle proprie piattaforme. Ad esse si aggiungono, ove applicabile e in relazione al servizio, le misure di sicurezza specifiche per rispondere alle esigenze del cliente e previste dai contratti in corso.
TIM tratta i dati personali di cui l'azienda cliente è titolare nei propri datacenter collocati sul territorio italiano. Solo nei casi previsti dal servizio contrattualizzato, a partire dal 25/5/2018 TIM applicherà le garanzie previste dal GDPR per il trasferimento extra-EU, previa autorizzazione all'azienda cliente, dei dati personali di cui l'azienda cliente stessa è titolare.

I riferimenti del Data Protection Officer del Gruppo TIM sono i seguenti:
recapito: Data Protection Officer, via Gaetano Negri, 1 - 20123 Milano
indirizzo email: dpo.clientibusiness.tim@telecomitalia.it

Per gli aspetti relativi alla sicurezza fisica, alle procedure generali ed all' organizzazione si rimanda al Piano della Sicurezza SPC Cloud lotto 1 [CQ4].
Di seguito sono riportate le misure di sicurezza logica definite da TIM a protezione dei dati personali.
Per le misure aggiuntive applicabili ai dati personali particolari si rimanda ai paragrafi relativi di ogni servizio.

Misure per il trattamento dei dati personali non particolari

Categoria misura	Misura di protezione
Log	La piattaforma tramite cui è effettuato il trattamento di Dati Personali, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da: - produrre la registrazione degli accessi logici (Access Log), compresi i tentativi falliti di accesso, effettuati da parte degli Amministratori di Sistema IT - conservare le registrazioni per un periodo di sei mesi.
Log	E' garantita la completezza, l'immodificabilità e la possibilità di verificare l'integrità delle registrazioni dei log di accesso degli Amministratori di Sistema IT.
Log	La piattaforma tramite cui è effettuato il trattamento di Dati Personali, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da prevedere tecnologie di sincronizzazione al fine di mantenere allineata la data e l'ora associata agli accessi registrati nei log.
Log	Le registrazioni dei log relativi agli accessi (access log) alla piattaforma degli Amministratori di Sistema IT includono le seguenti informazioni: - il sistema target e l'eventuale applicazione acceduta; - evento che ha generato il log (login, logout, failure login); - utenza, data e ora di inizio / fine connessione.
Back-up	Al fine di garantire la disponibilità e l'integrità dei dati è prevista la definizione e l'esecuzione di procedure di backup con cadenza almeno settimanale per i dati di configurazione e per i dati del Cliente.
Credenziali di autenticazione e controllo accessi	Tutti i profili di accesso e le politiche di gestione delle utenze degli Amministratori di Sistema IT (interni ed esterni) delle piattaforme rappresentate in specifiche matrici Profili/Funzioni sono verificati e aggiornati. Tale verifica avviene con frequenza almeno annuale o comunque a seguito di eventi significativi (es. cambi organizzativi, evoluzioni di sistema, etc.)
Credenziali di autenticazione e controllo accessi	Il Responsabile in ambito IT, o un suo delegato, autorizza gli Amministratori di Sistema IT all'accesso ai dati nella fase di creazione, modifica o monitoraggio (gestione credenziali di accesso).
Credenziali di autenticazione e controllo accessi	Gli Amministratori di Sistema sono stati formalmente nominati.

Categoria misura	Misura di protezione
Credenziali di autenticazione e controllo accessi	Per una gestione delle credenziali di autenticazione, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in modo tale da associare a ciascuna utenza dedicata agli Amministratori di Sistema IT credenziali di autenticazione individuali (costituite da una User-ID e un dispositivo di autenticazione - ad es. password). La piattaforma, inoltre, deve prevedere all'accesso meccanismi automatici di verifica delle stesse.
Credenziali di autenticazione e controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a impedire la riassegnazione di User-ID ad altri incaricati neppure in tempi diversi.
Credenziali di autenticazione e controllo accessi	La piattaforma è configurata in modo tale da garantire una soluzione tecnica o procedurale che consenta, in caso di cancellazione di utenze (assegnate ad Amministratori di Sistema IT), di risalire in maniera certa alla persona fisica assegnataria, in un dato periodo, dell'utenza in oggetto. Tali informazioni sono conservate per almeno un periodo di 60 mesi dalla cancellazione delle utenze.
Credenziali di autenticazione e controllo accessi	La piattaforma consente di associare le utenze degli Amministratori di Sistema IT ai profili rispettando i principi di "need to know" e "segregation of duties" secondo le regole fissate da specifiche matrici Profilo/Funzione.
Credenziali di autenticazione e controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, deve essere configurata in maniera tale da effettuare la verifica (almeno settimanale se eseguita tramite modalità automatiche o mensile per analisi procedurali), di tutte le utenze associate ad Amministratori di Sistema IT che hanno lasciato l'azienda al fine di cessare tempestivamente tutte le relative abilitazioni.
Credenziali di autenticazione e controllo accessi	Tutte le utenze degli Amministratori di Sistema IT sono sottoposte a rivalutazioni periodiche circa la sussistenza delle esigenze che ne hanno portato all'attivazione. In particolare le revisioni delle utenze devono essere previste con periodicità almeno annuale.
Credenziali di autenticazione e controllo accessi	L'applicativo è sviluppato in maniera tale da prevedere meccanismi in grado di consentire l'estrazione delle informazioni necessarie alla verifica della corretta attribuzione delle credenziali di autenticazione e dei relativi profili di autorizzazione degli utenti interni del Cliente Business.
Credenziali di autenticazione e controllo accessi	La piattaforma consente la sospensione delle utenze inattive degli utenti interni del Cliente Business a valle di periodi di inattività pari o maggiori a 6 mesi, salvo le utenze per le quali è stata preventivamente richiesta ed autorizzata una deroga sulla base di una necessità operativa.
Credenziali di autenticazione e controllo accessi	Il gruppo preposto alla creazione ed alla assegnazione delle credenziali di autenticazione agli Amministratori di Sistema IT richiedenti risulta essere nominato e costituito da un numero circoscritto di Amministratori di Sistema IT preventivamente individuati.
Credenziali di autenticazione e controllo accessi	E' precluso l'utilizzo di utenze di Sistema su processi automatici (ad esempio le utenze di Sistema non sono utilizzate come utenze Machine to Machine).
Credenziali di autenticazione e controllo accessi	E' precluso l'utilizzo di utenze di sistema e M2M da parte di persone fisiche, ad eccezione di attività saltuarie (es. gestione emergenze).
Credenziali di autenticazione e controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale che le utenze di sistema non nominali (comprese le M2M) siano comunque assegnate (in termini di responsabilità) ad una persona fisica, tipicamente un Responsabile in ambito IT o un suo delegato.
Credenziali di autenticazione e controllo accessi	Per una gestione delle modalità di accesso dedicate a ciascun Amministratore di Sistema IT interno ed esterno, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale che quando il sistema utilizza la password come dispositivo di autenticazione, essa effettui controlli automatici volti a garantire che la password risponda alle caratteristiche previste dalle vigenti policy aziendali
Credenziali di autenticazione e controllo accessi	La piattaforma consente la sospensione delle utenze inattive degli Amministratori di Sistema IT a valle di periodi di inattività pari o maggiori a 6 mesi, (salvo le utenze preventivamente autorizzate per soli scopi di gestione tecnica per le quali sia stata concessa una deroga da parte del Responsabile in ambito IT o suoi delegati). Nel caso di infattibilità tecnica il controllo può essere di tipo procedurale, con frequenza almeno mensile, garantendo comunque la sospensione trascorsi 6 mesi di inattività.

Categoria misura	Misura di protezione
Canali di comunicazione	E' prevista l'adozione di apparati hardware e software (ad es. firewall) in grado di contrastare tentativi di accesso non autorizzato da reti dati pubbliche (Internet) al fine di rispettare i livelli di isolamento e protezione dei dati trattati dalla piattaforma stessa.
Canali di comunicazione	Per tutti i sistemi in perimetro per i quali sia consentito l'accesso al sistema da parte di entità terze/esterne all'azienda (fornitori e non Clienti di TIM), è garantita, salvo diversa indicazione, la sicurezza dei dati scambiati verso l'esterno (es. canali con protocolli sicuri, meccanismi di cifratura).
Credenziali di autenticazione e controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a garantire i requisiti di robustezza delle credenziali di autenticazione. A tal fine deve essere prevista l'implementazione di controlli automatici volti a garantire che le credenziali di autenticazione (per es. password) rispondano alle caratteristiche previste dalla normativa di riferimento. In particolare la password deve prevedere: - lunghezza minima pari a 8 caratteri o al massimo permesso dal sistema; - complessità (la password deve essere costituita da caratteri diversi per tipologia quali lettere, numeri, simboli speciali)
Credenziali di autenticazione e controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione al primo accesso delle password temporanee inizialmente assegnate a ciascun Amministratore di Sistema IT.
Credenziali di autenticazione e controllo accessi	Per una gestione delle credenziali di autenticazione dedicate a ciascun Amministratore di Sistema IT, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione periodica della password almeno ogni 6 mesi nel caso di sistemi che trattano dati personali e almeno ogni 3 mesi in caso di trattamento di dati sensibili e giudiziari.
Credenziali di autenticazione e controllo accessi	Il sistema è costruito in modo da associare a ciascun Amministratore di Sistema IT un "profilo di autorizzazione" adeguato a garantire l'accesso ai soli dati che sono strettamente necessari per adempiere ai compiti affidati.
Documentazione	Viene garantita l'esistenza del Registro dei Trattamenti aggiornato degli eventuali Partner/Fornitori che concorrono all'erogazione del servizio. Tale documentazione deve riportare le seguenti informazioni: - identificativo della società esterna; - descrizione sintetica delle responsabilità affidate; - riferimento al contratto di fornitura.
Protezione degli elaboratori	La piattaforma prevede il corretto funzionamento e aggiornamento del software di protezione antivirus (prevenzione, rilevazione e rimozione virus e malicious code).
Protezione degli elaboratori	Al fine di minimizzare la vulnerabilità della piattaforma e garantire un livello minimo di protezione delle informazioni aziendali nelle piattaforme, sono installati, almeno annualmente, gli aggiornamenti del software applicativo (Patch Management).
Protezione degli elaboratori	Al fine di minimizzare la vulnerabilità della piattaforma e garantire un livello minimo di protezione delle informazioni aziendali nelle piattaforme, sono installati, almeno annualmente, gli aggiornamenti del software di sistema (Patch Management).
Protezione degli elaboratori	Sono state previste attività di configurazione che comportano la modifica delle impostazioni predefinite del fornitore (ad esempio password, community SNMP, ecc...), l'eliminazione di account e servizi non necessari e la risoluzione delle vulnerabilità di sicurezza note.
Protezione degli elaboratori	Tutti i terminali utilizzati per connettersi al sistema prevedono la funzionalità di screensaver con password o in alternativa il sistema abbatte la sessione secondo i criteri previsti dalla Policy per la costruzione, l'utilizzo e la gestione delle password.
Protezione degli elaboratori	Per i trattamenti che prevedono l'hosting fisico dei dati all'interno di siTIM, il sistema risiede all'interno di un Data Center, di un Service Center, di una Centrale o di un sito equivalente.
Riservatezza	E' prevista la stesura e la corretta implementazione di procedure atte a regolare il processo di cancellazione dei dati del Cliente a seguito della cessazione del contratto (ad es. cessazione di qualsiasi obbligazione derivante da accordi contrattuali oppure in applicazione di specifiche normative) assicurando che tali dati vengano cancellati in maniera definitiva e irreversibile al fine di impedire trattamenti non autorizzati degli stessi da parte di Amministratori di Sistema IT o di eventuali altri Clienti. Le tempistiche di cancellazione sono in linea con quanto previsto a livello contrattuale.

Categoria misura	Misura di protezione
Riservatezza	E' garantito l'isolamento logico dei dati relativi a clienti differenti su una medesima piattaforma. In particolare non deve essere possibile accedere/visualizzare i dati di un Cliente diverso da quello che ha acceduto alla piattaforma.
Riservatezza	E' prevista la separazione degli ambienti dedicati alle attività di sviluppo, test e collaudo dall'ambiente di esercizio della piattaforma. Per gli ambienti diversi da quello di produzione nel caso vengano utilizzati dati reali di esercizio, sono garantiti tutti i requisiti di compliance previsti.
Riservatezza	E' prevista la redazione formale di apposite procedure di estrazione o trasmissione dei dati trattati dalla piattaforma. Tali estrazioni/trasmissioni devono consentire la portabilità dei dati tramite l'esportazione degli stessi in formati standard in relazione alla tecnologia utilizzata (ad es. sistemi di tipo UNIX) e al layer di trattamento (ad es. DB).

Tabella 17 – Misure a protezione dei dati personali non particolari

20.3 Misure Minime di sicurezza AGID

Di seguito si riportano le misure minime AGID nel formato indicato in [RN3] che specificano il livello sotto il quale nessuna amministrazione può scendere: i controlli in essa indicati debbono riguardarsi come obbligatori.
Sono riportate di seguito le misure minime che TIM e suoi fornitori adottano e le misure minime che restano in capo al cliente PA. La X indica chi ha la responsabilità di garantire la misura di sicurezza. Le misure di responsabilità cliente possono essere adottate da TIM a fronte di valutazioni tecniche e specifici accordi contrattuali.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI							
Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso							
ABSC ID #			**Descrizione**	**FNSC**	**Min.**	**Responsabilità TIM**	**Responsabilità cliente PA**
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI						**Responsabilità TIM**	**Responsabilità cliente PA**

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione							
ABSC ID #			**Descrizione**	**FNSC**	**Min.**		
2	1	1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di si- stema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.	ID.AM-2	X	X	
	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autoriz- zato.	ID.AM-2	X		X
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER							
Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vul- nerabilità di servizi e configurazioni.							
ABSC_ID #			**Descrizione**	**FNSC**	**Min.**	**Responsabilità TIM**	**Responsabilità cliente PA**
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PR.IP-1	X	X	
	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di si- stemi usati dall'organizzazione.	PR.IP-1	X	X	
		2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzan- do la configurazione standard.	PR.IP-2 RC.RP-1	X	X	
	3	1	Le immagini d'installazione devono essere memorizzate offline.	PR.IP-2	X	X	

	4	1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	PR.AC-3 PR.MA-2	X	X	
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ							
Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.							
ABSC_ID #			**Descrizione**	**FNSC**	**Min.**	**Responsabilità TIM**	**Responsabilità cliente PA**
4	1	1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	ID.RA-1 DE.CM-8	X	X	
	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	DE.CM-8	X	X	
	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	PR.MA-1	X	X	
		2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli *air-gapped*, adottando misure adeguate al loro livello di criticità.	PR.MA-1	X		X
	7	1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure	PR.IP-12 RS.MI-3	X	X	

			oppure documentando e accettando un ragionevole rischio.				
	8	1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	ID.RA-4 ID.RA-5¶PR-IP.12	X	X	
		2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	PR.IP-12	X	X	
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE							
Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.							
ABSC_ID #			**Descrizione**	**FNSC**	**Min.**	**Responsabilità TIM**	**Responsabilità cliente PA**
5	1	1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	PR.AC-4 PR.PT-3	X	X	
		2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	PR.AC-4 PR.PT-3	X	X	
	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	ID.AM-6 PR.AT-2¶DE.CM-3	X	X	
	3	1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti	PR.IP-1	X	X	

			con quelli delle utenze amministrative in uso.				
	7	1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	PR.AC-1 PR.AT-2	X	X	
		3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (*password aging*).	PR.AC-1 PR.AT-2	X	X	
		4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo¶(*password history*).	PR.AC-1	X	X	
	10	1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	ID.AM-6	X	X	
		2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconduci- bili ad una sola persona.	ID.AM-6	X	X	
		3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	ID.AM-6 PR.AT-2	X	X	
	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	PR.AC-1 PR.AT-2	X	X	
		2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	PR.AC-1 PR.AC-2	X		X

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE							
Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.							
ABSC_ID¶¶#			**Descrizione**	**FNSC**	**Min.**	**Responsabilità TIM**	**Responsabilità cliente PA**
8	1	1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	DE.CM-4 DE.CM-5	X	X (solo sulle IaaS/PaaS Managed ed ECaaS)	
		2	Installare su tutti i dispositivi firewall ed IPS personali.	DE.CM-1	X		X
	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	PR.PT-3 DE.CM-7	X		X
	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	PR.PT-2	X		X
		2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	PR.AT-1 DE.CM-4	X		X
		3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	PR.AT-1 DE.CM-4	X		X
		4	Disattivare l'anteprima automatica dei contenuti dei file.	PR.AT-1 DE.CM-4	X		X
	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	PR.PT-2 DE.CM-4	X		X
	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	DE.CM-1 DE.CM-4	X		X
		2	Filtrare il contenuto del traffico web.	DE.CM-1 DE.CM-4	X		X

		3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	DE.CM-1 DE.CM-4	X		X
ABSC 10 (CSC 10): COPIE DI SICUREZZA							
Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.							
ABSC_ID #			**Descrizione**	**FNSC**	**Min.**	**Responsabilità TIM**	**Responsabilità cliente PA**
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	PR.IP-4	X	X	
	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.¶.	PR.DS-6	X	X	
	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	PR.AC-2 PR.IP-4¶PR.IP-5 PR.IP-9	X	X	
ABSC 13 (CSC 13): PROTEZIONE DEI DATI							
Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti							
ABSC ID #			**Descrizione**	**FNSC**	**Min.**	**Responsabilità TIM**	**Responsabilità cliente PA**
13	1	1	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali	ID.AM-5	X	X	

			va applicata la protezione crittografica				
	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	ID.-AM3 PR.DS-5¶DE.CM-1	X		X

Tabella 18 - Misure minime AGID

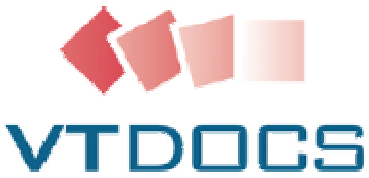
20.4 Elenco subfornitori di TIM

Di seguito i soggetti terzi (subfornitori/subresponsabili) che TIM utilizza per erogare i propri servizi:

Servizio	Subfornitori (Subresponsabili nominati da TIM)
IAAS e PaaS unmanaged (indifferentemente se su applicazione HP Helion OpenStack o su applicazione Cisco-Canonical OpenStack)	HP, Canonical e subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/*
IAAS e PaaS managed (indifferentemente se su applicazione HP Helion OpenStack o su applicazione Cisco-Canonical OpenStack)	HP, Canonical e subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/*
PAAS Oracle unmanaged e managed su tecnologia Oracle OCM	Oracle Italia e altri subfornitori indicati al seguente indirizzo nell'area GDPR *https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/*
PAAS Oracle unmanaged e managed su tecnologia Oracle-Hitachi	subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/*
BAAS	subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/*
SaaS di Produttività individuale	Smc Treviso S.r.l e altri subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/*
SaaS di Comunicazione Unificata	VoiSmart S.r.l e altri subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/*
SaaS di Collaborazione: File Sharing	Smc Treviso S.r.l e altri subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/*
SaaS di Collaborazione: Enterprise Social Network	Smc Treviso S.r.l e altri subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/*

Servizio	Subfornitori (Subresponsabili nominati da TIM)
SaaS di Collaborazione: Learning Management System	Oilproject S.r.l, A.di.co.m. Group S.r.l ed altri subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/*
DRAAS	subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/*
ECAAS/CCaaS	DXC e subfornitori indicati al seguente indirizzo nell'area GDPR: *https://assistenza.timbusiness.it/*
Cloud Enabling	I subfornitori di Cloud Enabling sono indicati nell'elenco presente su: *www.cloudspc.it*

Tabella 19 - Elenco subfornitori TIM



VTDOCS 3.30

Manuale utente

Data emissione/ultima modifica: 17/06/2013

EVOLUZIONE DEL DOCUMENTO

Di seguito le indicazioni relative alle modifiche apportare rispetto la versione precedente di VTDOCS.

Versione	Descrizione
3.30	o Par. 2.1 – Autenticazione utente multiamministrazione o Par. 2.5.2.3, 2.5.2.4 – Ricezione marca temporale o Par. 2.7.1.1, 3.1.1.2.1 – Evidenza contatore con azzeramento su intervallo personalizzato o Par. 2.7.2.2, 2.7.2.3 – Spedizione marca temporale o Par. 2.14.3 – Riconoscimento firma PAdES e visualizzazione marca temporale o Par. 2.14.7 – Creazione file TSD

INDICE GENERALE

INDICE DELLE FIGURE

1 INTRODUZIONE

1.1 Premessa

Il presente documento illustra i contenuti della release 3.30 di VTDOCS in termini di funzionalità.

1.2 Scopo e area di applicazione

Le indicazioni contenute nel presente documento hanno lo scopo di fornire all'utente, che utilizza il prodotto utile per la gestione informatizzata del protocollo, una guida di navigazione e di utilizzo delle funzionalità messe a disposizione dal prodotto VTDOCS nella versione 3.30.

1.3 Definizioni e abbreviazioni

Access Control List	Insieme di regole che definiscono i privilegi di accesso di utenti e gruppi a documenti e fascicoli.
Allegato	Documento (scritto) in maniera complementare ad un altro principale.
Applicativo di amministrazione	Applicazione messa a disposizione dell'amministratore del sistema VTDOCS per la gestione degli elementi di configurazione che caratterizzano ciascuna amministrazione.
Area di Lavoro	Area di memoria persistente e gestita dall'utente, nella quale ciasun utente può inserire documenti e fascicoli di particolare interesse o di utilizzo frequente. Rappresenta una sorta di scrivania virtuale in cui ciscun utente deposita i documenti e/o i fascicoli da tenere "in vista" senza di volta in volta doverli ricercare per poterli lavorare.
Area Organizzativa Omogenea	Insieme di Unità Organizzative dell'Amministrazione che usufruisce, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei flussi documentali. Una AOO offre, in particolare, il servizio di protocollazione dei documenti in entrata ed in uscita, utilizzando un unico registro di protocollo che eroga una sequenza numerica, rinnovata ad ogni anno solare.
Casella istituzionale	Indirizzo e-mail associato ad un AOO: è l'indirizzo utilizzato per l'interoperabilità.
Classificazione	Associazione ad un documento o fascicolo del codice nodo di titolario (titolo, classe o sottoclasse) cui il contenuto del documento/fascicolo fa riferimento
Codice a barre	Insieme di elementi grafici a contrasto elevato disposti in modo da poter essere facilmente letti da un sensore e decodificati tramite un apposito **circuito integrato**.
Completamento	Modalità di ricerca utile in particolare per documenti da protocollare, da assegnare, da classificare oppure ducumenti privi di immagine.

Conservazione sostitutiva	La conservazione sostitutiva è una procedura legale/informatica regolamentata dalla legge italiana, in grado di garantire nel tempo la validità legale di un documento informatico. Si intende per documento una rappresentazione di atti o fatti e dati su un supporto sia esso cartaceo o informatico (delibera CNIPA 11/2004). La conservazione sostitutiva equipara, sotto certe condizioni, i documenti cartacei con quelli elettronici. Conservare digitalmente significa pertanto sostituire i documenti cartacei, che per legge alcuni soggetti giuridici sono tenuti a conservare, con l'equivalente documento in formato digitale che viene “bloccato” nella forma, contenuto e tempo attraverso la firma digitale e la marca temporale.
Contatore	Meccanismo di attribuzione di un numero progressivo ad una particolare tipologia di documenti/fascicoli non soggetti a registrazione di protocollo.
Creatore e proprietario	Il creatore di un documento/fascicolo è l’utente/ruolo/UO che ha effettivamente creato il documento/fascicolo. Resta invariato per tutta la vita del documento/fascicolo stesso. L’utente/ruolo proprietario di un documento/fascicolo, inizalmente coincide con il creatore. Può successivamente cambiare a seguito di operazioni di cessione della proprietà.
Diagramma di stato	Insieme o sequenza degli stati che una tipologia di documento o fascicolo può assumere, a partire da uno stato iniziale per arrivare ad uno o più stati finali. Un diagramma di stato è identificato attraverso un nome. Attraverso l’applicazione di amministrazione è possibile creare e associare un diagramma di stato ad una tipologia di documento e/o ad una tipologia di fascicolo. Diverse tipologie di documento/fascicolo possono essere associate allo stesso diagramma.
Documento non protocollato	Documenti interni alla AOO che non necessitano della registrazione di protocollo. La gestione dei documenti non protocollati in VTDOCS differisce da quella relativa ai documenti protocollati unicamente per la mancanza dei dati di protocollo (segnatura, mittente/Destinatario) Al momento della creazione del documento VTDOCS assegna un identificativo e la data di creazione. Per un documento non protocollato sono possibili le stesse operazioni previste per i documenti protocollati, quali l’acquisizione, la classificazione, la gestione delle versioni, la creazione di allegati, la trasmissione, l’inserimento in uno o più fascicoli generali o procedimentali, ecc..
Documenti repertoriati	Serie di documenti di una stessa tipologia non soggetti a protocollazione cui è attribuita una specifica forma di numerazione attraverso un meccanismo denominato “contatore” che può essere automatico o manuale.
Etichetta	Foglietto adesivo su cui sono impresse le informazioni della segnatura del documento con la presenza di un codice a barre, univoco per ogni Amministrazione, che si applica sul documento cartaceo.

Fascicolazione	Azione di inserimento di un documento in un apposito fascicolo procedimentale.
Fascicolo generale	In VTDOCS ad ogni nodo di titolario (titolo, classe o sottoclasse) corrisponde un fascicolo generale, che ne assume codice e nome. Effettuare la classificazione equivale ad associare un documento od un fascicolo procedimentale ad un fascicolo generale. E' possibile associare lo stesso documento e fascicolo procedimentale a più fascicoli generali.
Fascicolo procedimentale	Fascicolo, collocato in un titolo e in una classe del titolario di classificaizone che contiene tutti i documenti relativi ad una pratica/procedimento. Pertanto in VTDOCS è possibile inserire un documento in un fascicolo procedimentale opportunamente creato. Lo stesso documento si può inserire in più fascicoli. La fascicolazione corrisponde quindi all'inserimento del documento ad una specifica istanza di fascicolo procedimentale. Il fascicolo procedimentale deve essere esplicitamente creato dall'utente attribuendogli una denominazione (oltre ad un codice classifica e ad un numero identificativo generato dal sistema). La denominazione dei fascicoli è libera.
File system	Meccanismo con il quale i file sono immagazzinati e organizzati su un dispositivo di archiviazione, come un disco fisso di un computer o un CD-ROM. Nella rappresentazione grafica è generalmente utilizzata la metafora delle cartelle che contengono documenti (i file) ed altre cartelle.
Firma digitale	Particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare, tramite la chiave privata, e al destinatario, tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Folder (Cartella)	Ad ogni fascicolo generale o procedimentale è associato una cartella principale alla quale è possibile associare altre cartelle per dare una organizzazione logica ai documenti contenuti nel fascicolo. Tali cartelle e sottocartelle nell'applicazione prendono il nome di sottofascicoli.
Home page	Pagina principale dell'applicazione. E' la prima pagina a cui si accede dopo aver inserito le credenziali di accesso (user Id e password).

Interoperabilità	L'interoperabilità è la capacità di un sistema o di un prodotto informatico di cooperare e di scambiare informazioni o servizi con altri sistemi o prodotti in maniera più o meno completa e priva di errori, con affidabilità e con ottimizzazione delle risorse. Obiettivo dell'interoperabilità è dunque facilitare l'interazione fra sistemi differenti, nonché lo scambio e il riutilizzo delle informazioni anche fra sistemi informativi non omogenei (sia per software che per hardware). VTDOCS implementa le regole di interoperabilità descritte dalla normativa in vigore consentendo la protocollazione semiautomatica (operazione con richiesta di conferma) per i documenti elettronici in arrivo sulla casella di posta istituzionale .
Iperfascicolo	Insieme dei fascicoli, anche di diversa tipologia, che si riferiscono ad un medesimo soggetto o oggetto aggregante. Un iperfascicolo rappresenta una aggregazione dinamica (una ricerca) di fascicoli, anche di tipo diverso, ottenuta specificando un valore per un campo riutilizzabile ed eventualmente altri criteri di selezione sugli attributi del profilo standard dei fascicoli.
Lista "Cose da fare"	Tutte le trasmissioni sia di documenti che di fascicoli, oltre a essere notificabili in modo asincrono ai destinatari attraverso il sistema di posta elettronica, alimentano una lista delle trasmissioni ricevute associata ad ogni utente nello svolgimento di un particolare ruolo. Tale lista denominata "Cose da fare" rappresenta una sorta di lista delle attività pendenti. Le trasmissioni effettuate verso un ruolo alimentano la lista delle cose da fare di tutti gli utenti che svolgono quel ruolo. La lista delle cose da fare appare nella pagina principale di VTDOCS in modo tale che, ad ogni connessione, il sistema propone automaticamente la lista delle trasmissioni ricevute.
Marca temporale	Una marca temporale (timestamp) è una sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato consistente, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione di tale marca temporale è detto timestamping.
Nodo di titolario	Singola voce del Titolario di classificazione utilizzato per classificare i documenti.
Numero documento (id doc)	Numero identificativo di un singolo documento.
Password	Parola d'ordine o anche parola d'accesso. E' una sequenza di **caratteri alfanumerici** utilizzata per accedere in modo esclusivo ad una **risorsa informatica**. Solitamente è associata ad uno specifico username (nome utente o identificatore utente) al fine di ottenere un'identificazione univoca da parte del sistema a cui si richiede l'accesso.

Portable Document Format	Comunemente abbreviato PDF, è un formato di file basato su un linguaggio di descrizione di pagina sviluppato da Adobe Systems per rappresentare documenti in modo indipendente dall'hardware e dal software utilizzati per generarli o per visualizzarli. Un file PDF può descrivere documenti che contengono testo e/o immagini a qualsiasi risoluzione. È un formato aperto, nel senso che chiunque può creare applicazioni che leggono e scrivono file PDF senza pagare i diritti (royalties) alla Adobe Systems.
Profilo	Sezione della scheda documento contenente le informazioni generali ad esso relative
PEC - Punto di accesso	È il punto che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione, di imbustamento del messaggio originale nella busta di trasporto.
PEC - Punto di ricezione	È il punto che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza/correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle busta di trasporto.
PEC - Punto di consegna	È il punto che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario. Verifica la provenienza/correttezza del messaggio, emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna.
PEC - Ricevuta di accettazione	È la ricevuta, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata. La ricevuta di accettazione è firmata con la chiave del gestore di posta elettronica certificata del mittente.
PEC - Avviso di non accettazione	E' l'avviso che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso. La motivazione per cui non è possibile accettare il messaggio è inserita all'interno del testo della ricevuta che esplicita inoltre che il messaggio non potrà essere consegnato al destinatario. L'avviso di non accettazione è firmato con la chiave del gestore di posta elettronica certificata del mittente.

PEC - Ricevuta di presa in carico	È emessa dal punto di ricezione verso il gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del dominio di posta elettronica certificata di destinazione. Nella ricevuta di presa in carico sono inseriti i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce. La ricevuta di presa in carico è firmata con la chiave del gestore di posta elettronica certificata del destinatario.
PEC - Ricevuta di avvenuta consegna	Il punto di consegna fornisce al mittente la ricevuta di avvenuta consegna nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario. È rilasciata una ricevuta di avvenuta consegna per ogni destinatario al quale il messaggio è consegnato. La ricevuta di avvenuta consegna è firmata con la chiave del gestore di posta elettronica certificata del destinatario. Al momento della spedizione il mittente può scegliere fra tre tipi di ricevuta: breve, completa o sintetica: • completa: contiene in allegato il Messaggio Originale e i Dati di Certificazione (daticert.xml) del gestore certificato del destinatario; • breve: contiene in allegato i Dati di Certificazione del gestore certificato del destinatario ed il testo del Messaggio Originale. Eventuali file allegati risulteranno 'sintetizzati' nei rispettivi Hash • sintetica: contiene in allegato soltanto i Dati di Certificazione del gestore certificato del destinatario del messaggio.
PEC - Avviso di mancata consegna	Nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario, il sistema emette un avviso di mancata consegna per indicare l'anomalia al mittente del messaggio originale.
Ragione di trasmissione	Insieme di attributi che caratterizzano una trasmissione e che ne influenzano la gestione. VTDOCS consente di definire liberamente le ragioni di trasmissione attraverso l'applicazione di amministrazione.
Registro di protocollo	Il Registro di protocollo è la fonte conoscitiva del giorno di arrivo o di spedizione di un dato documento, identificato obbligatoriamente da numero progressivo annuale, data, mittente, destinatario, sintesi del contenuto (oggetto); il registro può contenere molte altre informazioni non obbligatorie. Ogni AOO possiede un proprio registro di protocollo.
Responsabile AOO	Responsabile del Registro. In VTDOCS eredita automaticamente la visibilità (diritti di lettura e/o scrittura a seconda di come viene profilato dall'Amministratore del sistema) su ogni protocollo effettuato sul registro a prescindere da quale sia la posizione del suo Ruolo in UO all'interno dell'organigramma. È possibile definire un ruolo come responsabile di Registro al fine di ereditare tutti i protocolli e le stampe del registro. È inoltre possibile stabile se il ruolo deve ereditare i documenti in sola lettura.

Responsabile UO	Un Ruolo in UO può essere definito dall'Amministratore del sistema, al momento della definzione dell'organigramma dell'ente, come Ruolo Responsabile di UO. Questo attributo consente agli utenti del sistema di poter ottenere automaticamente, in caso di utilizzo di un modello di documento, il timbro con Nome, Congnome e Ruolo del Responsabile della UO in calce al documento.
Raggruppamento funzionale di ruoli in UO	Insieme di ruoli in UO, liberamente scelti dall'organigramma dell'amministrazione, che rappresenta tutti i ruoli che afferiscono ad una medesima funzione dell'ente. Il "Raggruppamento funzionale di Ruoli in UO" è una generalizzazione del concetto di AOO. Il Raggruppamento funzionale di ruoli in UO, analogamente alla AOO, ha un codice ed una descrizione. Analogamente alla AOO non è elemento nella rubrica ma è possibile associare corrispondenti esterni ad uno o più RF al fine di avere rubriche dei corrispondneti esterni sezionate per RF selezionato. Un RF ha una casella di posta per la ricezione sia dei messaggi interoperanti che non. Un RF è associato ad una AOO. Tale AOO è quella che verrà utilizzata per la registrazione dei documenti estratti dai messaggi di posta.
Rich Text Format	Abbreviato come RFT, è un formato per documenti multipiattaforma, sviluppato da Microsoft. La maggior parte degli editor di testo e dei word processor disponibili per Microsoft Windows, Mac OS e Linux sono in grado di leggere e scrivere documenti RTF.
Segnatura	Apposizione o associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni che consentono di identificare/individuare in modo inequivocabile il documento stesso. Le informazioni minime contenute sono: il progressivo di protocollo, la data di protocollazione e l'indentiifcativo in forma sintetica dell'amministrazione e dell'area organizzativa omogenea.
Smistamento	Attribuzione di responsabilità o invio per opportuna conoscenza di un documento, per una completa gestione del flusso documentale
Timbro	Riproduzione in formato elettronico del timbro che viene apposto sul documento cartaceo. La stampa del timbro sul documento protocollato e acquisito nel sistema VTDOCS riporta le seguenti informazioni: codice dell'Amministrazione, data della protocollazione, ora della protocollazione, protocollo in ingresso / uscita, numero di protocollo, codice AOO, numero degli allegati, classificazioni presenti.
Titolario	Il titolario, o piano di classificazione, si presenta come uno schema generale di voci logiche rispondenti ai bisogni funzionali del soggetto produttore e articolate tendenzialmente in modo gerarchico al fine di identificare, secondo uno schema logico che va dal generale al particolare, l'unità archivistica, cioè l'unità di aggregazione di base dei documenti all'interno dell'archivio (es. Il fascicolo) entro cui i documenti sono ordinati secondo le funzioni/attività/affari e/o materie di cui partecipano. In altre parole, il titolario d'archivio rappresenta l'insieme delle voci che rappresentano in modo sistematico le funzioni e le materie svolte e trattate dall'organizzazione.

Trasmissione	Operazione che consente di trasmettere, con diverse motivazioni (ragioni di trasmissione), documenti e fascicoli agli utenti del sistema (utente, ruolo, UO). La trasmissione di un documento agisce sulle Access Control List relative ai documenti e ai fascicoli attraverso le regole di visibilità gerarchica.
Unità Organizzativa	E' un ufficio associato ad una AOO e usufruisce dei servizi messi a disposizione dalla AOO stessa.
User Id	Nome utente. Identificativo associato a ciascun utente per l'accesso al sistema. E' sempre associato all'inserimento contestuale della password (parola d'ordine o parola d'accesso).
Workflow	In italiano "flusso di lavoro". In VTDOCS tale termine è utilizzato per indicare un attributo delle ragioni di trasmissione; le trasmissioni effettuate con una ragione con questo attributo sono caratterizzate dall'azione, da parte del destinatario della trasmissione, di accettazione / rifiuto della trasmissione ricevuta con notifica automatica dell'evento di rifiuto.
XLS	L'estensione .xls identifica la maggior parte dei fogli di calcolo o cartella di lavoro creati con Excel, foglio elettronico prodotto da Microsoft. È parte della suite di software di produttività personale Microsoft Office, ed è disponibile per i sistemi operativi Windows e Macintosh.
ACL	Access Control List
ADL	Area di Lavoro
AOO	Area Organizzativa Omogenea.
ASP	Application Service Provider. Con il termine ASP si intendono quegli operatori del settore dell'informatica e delle telecomunicazini che, disponendo di un'infrastruttura adeguata, rendono accessibile un applicativo software che viene condiviso da una molteplicità di utenti attraverso Internet o una rete privata virtuale.
CRN	Codice Riservato al Notaio
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
RF	Raggruppamento Funzionale di ruoli in UO.
RTF	Rich Text Format
UO	Documento (scritto) in maniera complementare a un altro principale

1.4Riferimenti

[1] Decreto legislativo 7 marzo 2005, n. 82, art. 1, lett. u), art. 17 lett. j), capo II sez. I, capo III e capo V sez. II - “Codice dell’amministrazione digitale.”

[2] Decreto legislativo 4 aprile 2006, n. 159 - “Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell’amministrazione digitale.”

[3] Deliberazione CNIPA 19 febbraio 2004, n. 11 - “Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.”

[4] Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 - “Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.”

[5] Direttiva del Ministro per l’innovazione e le tecnologie 9 dicembre 2002 - “Trasparenza dell’azione amministrativa e gestione elettronica dei flussi documentali.”

[6] Direttiva del Ministro per l’innovazione e le tecnologie 21 dicembre 2001, punto 3 - “Linee guida in materia di digitalizzazione dell’amministrazione.”

[7] Circolare AIPA 21 giugno 2001, n. 31 - "Art. 7, comma 6, del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, recante 'Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428'- Requisiti minimi di sicurezza dei sistemi operativi disponibili commercialmente."

[8] Circolare AIPA 7 maggio 2001, n. 28 - “Art. 18, comma 2, del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, recante regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati.”

[9] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, capo IV - “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo A).”

[10] Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - “Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.”

[11] Legge 15 marzo 1997, n. 59, art. 15, comma 2 - “Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa.”

[12] Decreto del Presidente del Consiglio dei Ministri 6 dicembre 1996, n. 694 - “Regolamento recante norme per la riproduzione sostitutiva dei documenti di archivio e di altri atti dei privati.”

[13] “Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata” – DigitPA - http://www.digitpa.gov.it/pec

2 PASSI OPERATIVI

Di seguito verranno esposti i passi operativi che consentono il corretto utilizzo dell'applicativo VTDOCS nella versione 3.30.

2.1Accesso al sistema e autenticazione

L'accesso al sistema si effettua a partire dalla schermata visualizzata nella Figura 1. L'utente seleziona , l'amministrazione con cui intende lavorare e digita la user id (nome utente) e la password (parola d'ordine) per l'accesso all'applicativo.

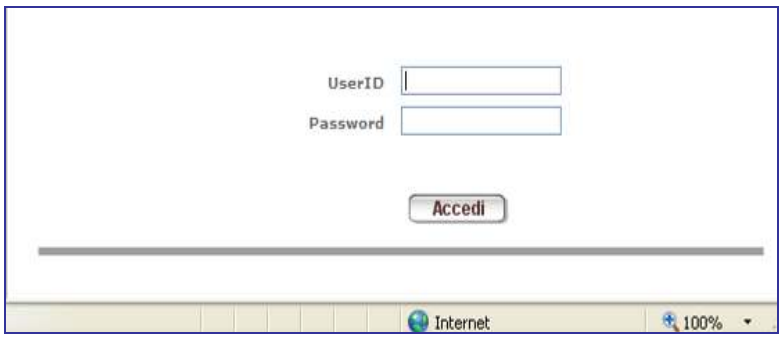


Figura 1 – Autenticazione

In fase di autenticazione il sistema verifica se la password dell'utente è ancora valida. Nel caso questa risulti scaduta, per accedere al sistema, viene richiesto all'utente di modificare la password, così come visualizzato nella Figura 2.

Figura 2 - Scadenza e modifica password

La nuova password deve rispettare i vincoli di lunghezza minima e presenza di caratteri speciali se definiti dall'amministratore. L'utente non può inserire una password uguale a quella scaduta.

Se l'utente è censito in più amministrazioni della stessa istanza, il sistema, dopo aver verificato la correttezza delle credenziali fornite, tramite opportuno menù a tendina, consentirà di scegliere a quale amministrazione accedere (Figura 3) fra quelle in cui l'utente risulta abilitato.

Figura 3 – Accesso utente multiamministrazione

2.2 Home page

Dopo aver effettuato l'accesso al sistema all'utente è proposto il pannello in Figura 4, nel quale sono presenti:

- il menù principale dell'applicativo;
- la sezione dedicata alla scelta del ruolo;
- l'elenco delle trasmissioni con la possibilità di applicare dei filtri di visualizzazione.

Inoltre, in alto a destra, si visualizza, per qualunque funzione si vada ad utilizzare nell'applicativo, il nome utente ed il ruolo con cui si sta lavorando nel sistema, la data e l'ora corrente.

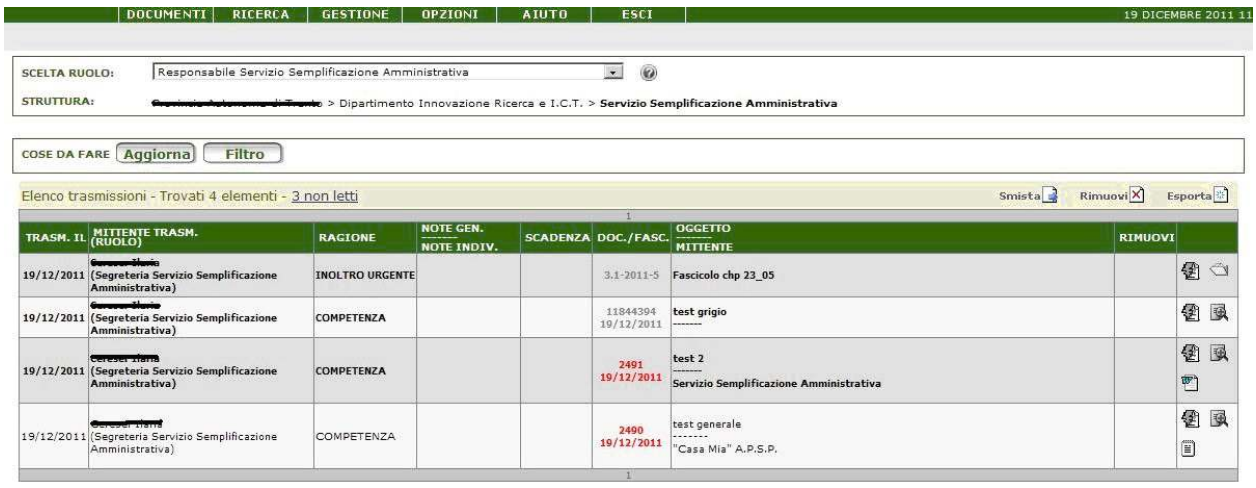


Figura 4 - Home page

2.3 Menù principale del sistema

Le voci del menù propongono le operazioni messe a disposizione dal sistema. La selezione di una delle voci visualizzerà i sottomenù utilizzabili dall'utente. La descrizione completa delle singole voci del menù e dei corrispondenti sottomenù è descritto nei capitoli successivi rispettivamente ai capitoli 2, 3, 4, 5, 6, 7.

2.4 Scelta del ruolo

La scelta del ruolo è un'operazione prevista per gli utenti ai quali sono associati più ruoli all'interno del sistema. L'amministratore di sistema imposta inizialmente un ruolo "principale" che si visualizza in automatico ogni qualvolta l'utente effettua l'accesso; per utilizzare l'applicativo con un altro ruolo è necessario selezionare dal menù a tendina "Scelta Ruolo" il ruolo con cui vuole operare all'interno dell'applicativo. Tale ruolo rimarrà selezionato fino a quando l'utente non deciderà di modificarlo. Per ogni ruolo, sotto il menù a tendina, è visualizzata la struttura gerarchica di appartenenza di quel ruolo all'interno della UO (campo "Struttura").

2.5 Cose da fare

L'elenco delle "cose da fare" è un elenco di documenti e di fascicoli trasmessi e/o inviati all'utente.

L'elenco si può visualizzare Automaticamente, ogni qualvolta l'utente accede all'interno del sistema laddove nella configurazione dell'applicazione sia stata prevista tale modalità automatica di visualizzazione. In caso di visualizzazione *automatica*, il sistema visualizza tutti i documenti/fascicoli contenuti nell'elenco delle cose da fare in corrispondenza del ruolo con cui l'utente deve lavorare.
Se la visualizzazione delle "cose da fare" *non è automatica*, c'è la possibilità di selezionare due differenti pulsanti, Cerca o Filtro.

Con Cerca l'utente ha la possibilità di vedere la lista completa delle trasmissioni che gli sono state effettuate; con Filtro, invece, è possibile visualizzare solo i documenti o i fascicoli filtrati in base ai seguenti parametri:

- **Tipo documento/fascicolo/Elementi non letti**: indica il tipo di documento che si vuole visualizzare, attraverso la selezione di pulsanti di controllo grafico che consentono all'utente di effettuare una scelta tra le varie opzioni:
  - Arrivo;
  - Partenza;
  - Interno;
  - Non Protocollato;
  - Tutti;
  - Documenti acquisiti;
  - Documenti firmati (P7M);
  - Documenti non firmati
- **In attesa di accettazione:** indica i documenti che sono in attesa di un'accettazione o di un rifiuto;
- **Ragione trasmissione:** indica la ragione con cui è stato trasmesso il documento o fascicolo;
- **Data Trasmissione:** indica il giorno in cui è stata effettuata la trasmissione. Per questo campo può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di protocollo. Inoltre, la data può essere inserita attraverso la selezione da calendario o semplicemente editandola**;**
- **Data scadenza:** indica il giorno entro cui si deve accettare o rifiutare il documento o fascicolo. Per questo campo può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali

inserire il valore minimo e massimo della data di protocollo. Inoltre, la data può essere inserita attraverso la selezione da calendario o semplicemente editandola;

- **Mittente trasmissione:** è possibile inserire il codice del mittente oppure selezionandolo dalla rubrica. Per la selezione da rubrica è necessario premere il pulsante associato al campo "mittente trasmissione". Nella finestra di dialogo che si apre a seguito della selezione dell'icona sono presenti i campi per la ricerca, e quindi per la successiva valorizzazione del campo mittente..
- **Oggetto:** è possibile inserire una parte del testo contenuta nell'oggetto del documento o nel dettaglio del fascicolo;
- **Ordinamento:** è possibile selezionare 4 differenti modalità di visualizzazione delle trasmissioni presenti nelle cose da fare. In particolare, attivando questo filtro è possibile scegliere tra i seguenti ordinamenti:
  - Data invio decrescente (valore impostato automaticamente);
  - Data invio crescente;
  - Data scadenza decrescente;
  - Data scadenza crescente.
- **Tipo file acquisito:** è possibile selezionare il formato con il quale è stato acquisito il documento trasmesso.

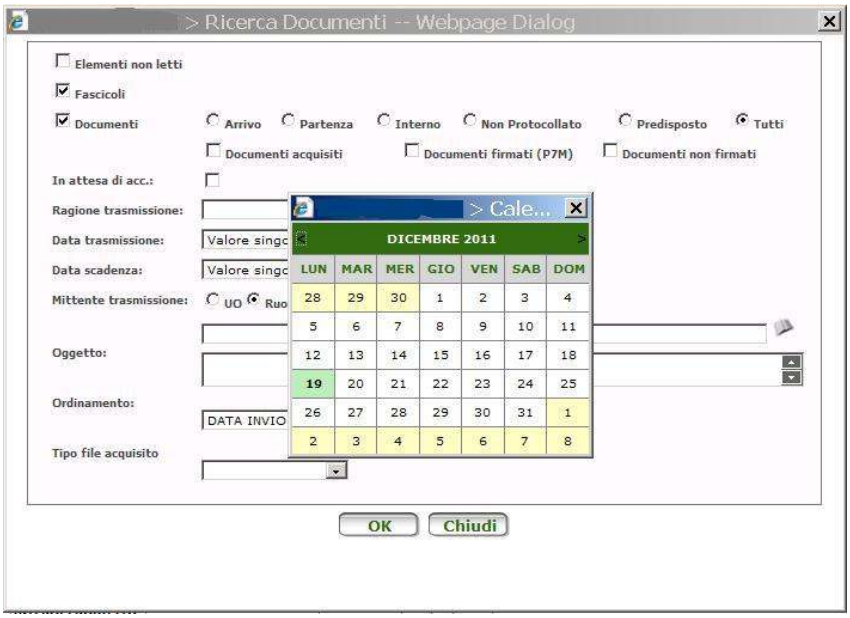


Figura 5 – Filtro nelle "cose da fare": dettaglio calendario

Una volta impostati i parametri di interesse, selezionando il pulsante "OK" viene attivata la ricerca per la visualizzazione dei relativi dati; se non si è più interessati a filtrare i documenti o i fascicoli si può selezionare il pulsante "Chiudi".
Un filtro attivato può essere ridefinito o rimosso attraverso il pulsante "Rimuovi filtro". Tale filtro viene comunque rimosso quando l'utente esce dall'applicazione dal sistema.

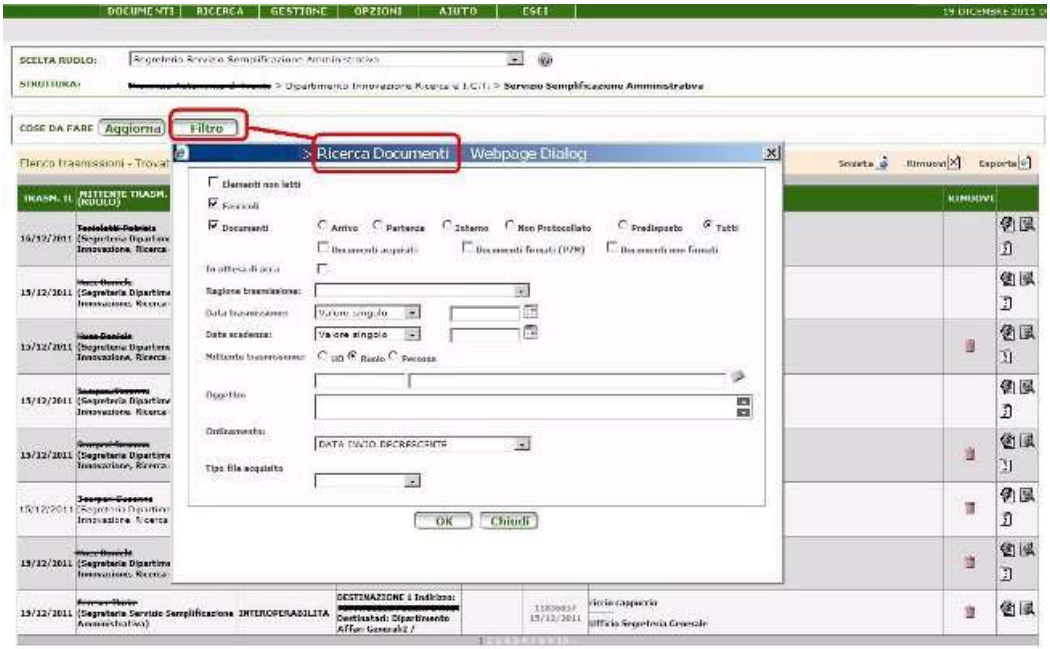


Figura 6 – Filtro nell'elenco delle "cose da fare"

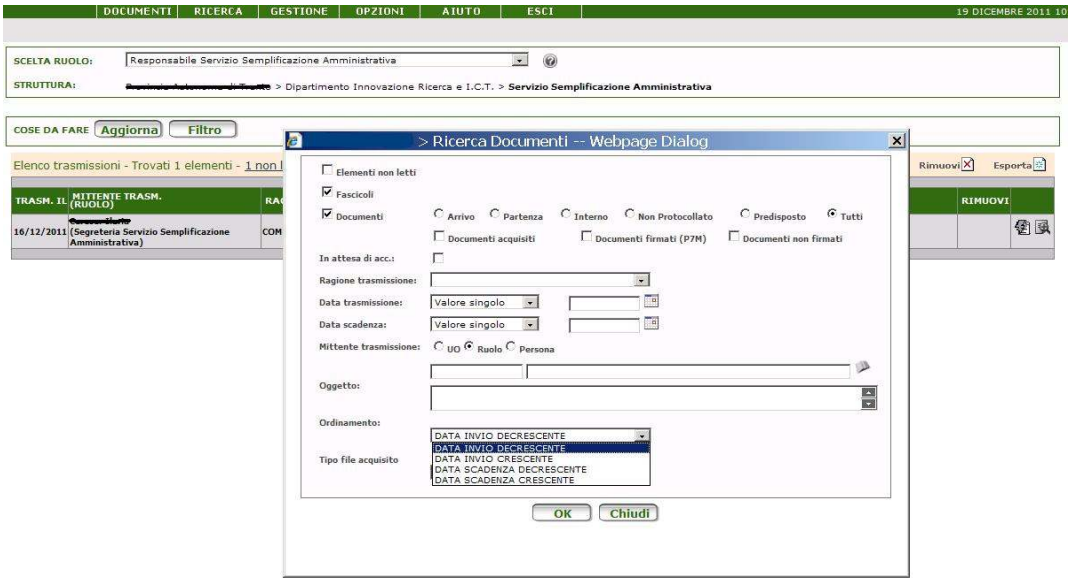
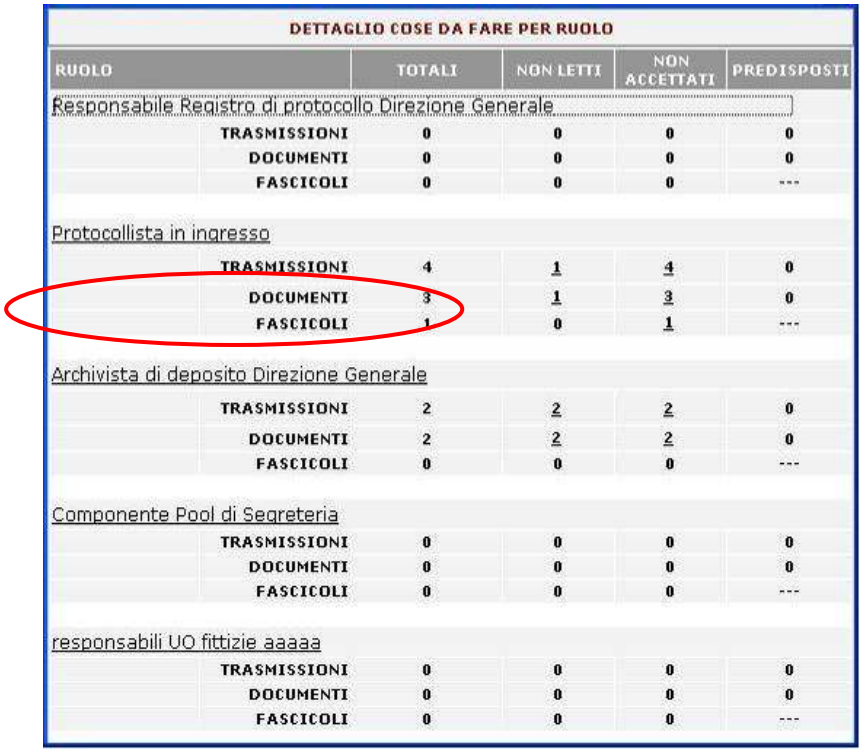


Figura 7 – Ordinamento dell'elenco delle "cose da fare"

Figura 8 – Lista delle cose da fare unificata

Attivando l'icona cerchiata in rosso,il sistema propone una finestra con la sintesi delle trasmissioni ricevute per ogni ruolo di appartenenza, con il particolare dei documenti e dei fascicoli.



DETTAGLIO COSE DA FARE PER RUOLO

RUOLO	TOTALI	NON LETTI	NON ACCETTATI	PREDISPOSTI
Responsabile Registro di protocollo Direzione Generale				
TRASMISSIONI	0	0	0	0
DOCUMENTI	0	0	0	0
FASCICOLI	0	0	0	---
Protocollista in ingresso				
TRASMISSIONI	4	1	4	0
DOCUMENTI	3	1	3	0
FASCICOLI	1	0	1	---
Archivista di deposito Direzione Generale				
TRASMISSIONI	2	2	2	0
DOCUMENTI	2	2	2	0
FASCICOLI	0	0	0	---
Componente Pool di Segreteria				
TRASMISSIONI	0	0	0	0
DOCUMENTI	0	0	0	0
FASCICOLI	0	0	0	---
responsabili UO fittizie aaaaa				
TRASMISSIONI	0	0	0	0
DOCUMENTI	0	0	0	0
FASCICOLI	0	0	0	---

Figura 9 – Dettaglio delle trasmissioni per ogni Ruolo di competenza dell'utente

Inoltre il sistema fornisce il dettaglio:

- degli elementi non letti;
- degli elementi non accettati, ad esempio elementi trasmessi per competenza solo visualizzati ma non accettati (come sarà spiegato in seguito);
- dei documenti predisposti alla protocollazione

Selezionando la descrizione del ruolo il sistema indirizza l'utente alla lista delle cose da fare relativa al ruolo corrispondente.

La lista delle cose da fare UNIFICATA mostra le trasmissioni di documenti protocollati, di documenti non protocollati (grigi) e di fascicoli utilizzando una grafica distinta per ogni tipologia di elemento, come mostrato nella figura sottostante.

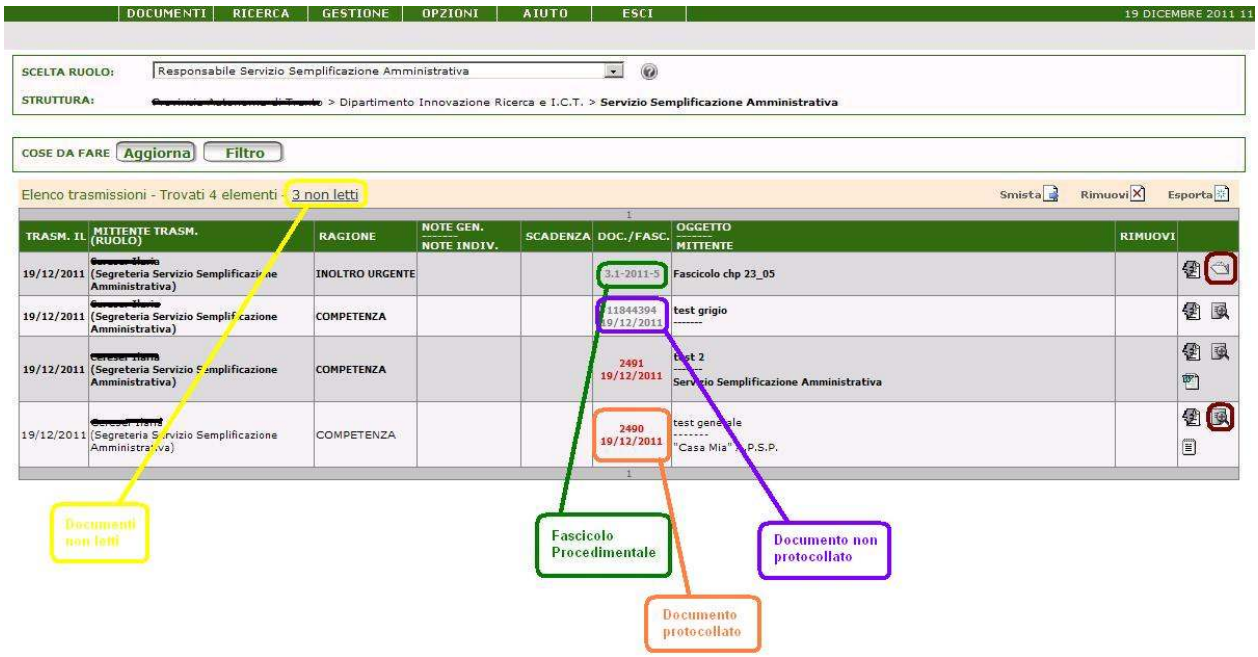


Figura 10 – Grafica differenziata per tipologia di documento trasmesso

Attivando l'icona evidenziata in blu si accede ai dettagli del documento/fascicolo.
I documenti/fascicoli non letti sono presentati con caratteri in grassetto mentre quelli già letti con caratteri non in grassetto. Il messaggio che indica il numero di documenti non letti è un collegamento. Selezionandolo, il sistema filtra le notifiche mostrando solo quelle relative agli elementi non letti.

Gli oggetti presentati nell'elenco delle trasmissioni sono di due tipi: documenti e fascicoli. Entrambi sono visibili in questa sezione fino a quando non sono visti, accettati, firmati, ecc., a seconda della ragione di trasmissione con cui sono inviati dal mittente.

Per i documenti/fascicoli presenti nell'elenco sono riportate le seguenti informazioni:

- **Trasm. il:** data in cui è stato effettuato l'invio;
- **Mittente trasm./(Ruolo):** il mittente della trasmissione ed il ruolo con cui è stata effettuata la trasmissione;
- **Ragione:** la ragione con cui è stato trasmesso il documento/fascicolo;
- **Note:** note generali relative alla trasmissione e note individuali visibili solo al ruolo destinatario al quale si riferiscono;
- **Scadenza:** data scadenza, ovvero data entro la quale il documento/fascicolo deve essere visionato;

- **Dett.:** dettaglio della trasmissione: selezionando l'icona viene visualizzato il dettaglio della trasmissione, ovvero le note generali ed individuali, le date in cui l'oggetto inviato è stato visto o accettato, la data di risposta; sono anche visualizzati i pulsanti che consentono di accettare/rifiutare la trasmissione, etc;
- **Doc.:** il numero del documento e la data di creazione;
- **Oggetto/Mittente:** oggetto del documento (o la descrizione del fascicolo) e, nel caso del documento, il mittente da cui è stato inviato;
- **Rimuovi:** Rimuove i documenti grigi o predisposti alla protocollazione direttamente dall'elenco delle "cose da fare". La cancellazione del documento avviene attraverso la selezione dell'icona ; l'applicativo mostra due finestre di dialogo differenti, in base all'utente che effettua l'operazione, così come descritto nel paragrafo 2.5.5.
- **L'ultima colonna permette di:**
  - Visualizzare i dettagli del documento attraverso la selezione dell'icona ;
  - Visualizzare i dettagli del fascicolo attraverso la selezione dell'icona ; ;
  - Visualizza i dettagli della trasmissione del documento/fascicolo
  - Visualizzare, attraverso la selezione dell'icona che rappresenta l'estensione del file, ogni documento di cui sia stata acquisita l'immagine o che sia associato a un documento elettronico attraverso la selezione dell'icona che rappresenta l'estensione del file.

2.5.1 Pulsanti di azione

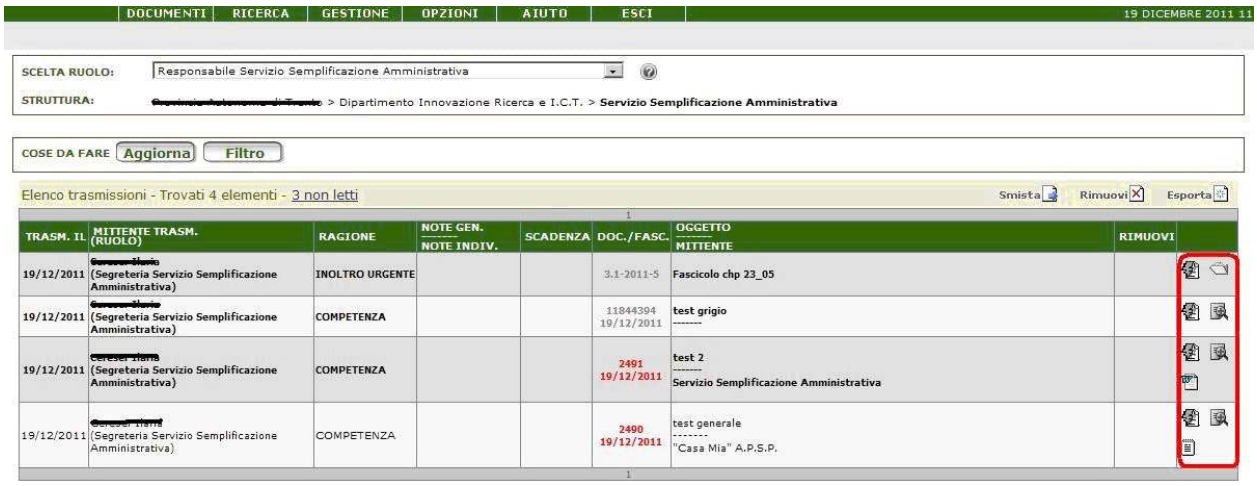


Figura 11 – Pulsanti di azione

I pulsanti di azione presenti nell'ultima colonna a destra permettono di:

(nelle versioni precedenti l'immagine era) : accedere al dettaglio della trasmissione

: mostrare l'estensione del file acquisito permettendo la visualizzazione del documento.

: accedere al dettaglio del documento (profilo, protocollo, classifica, allegati, versioni , trasmissioni).

 : accedere al dettaglio del fascicolo.

La stessa visualizzazione si ottiene anche come risultato di una ricerca:

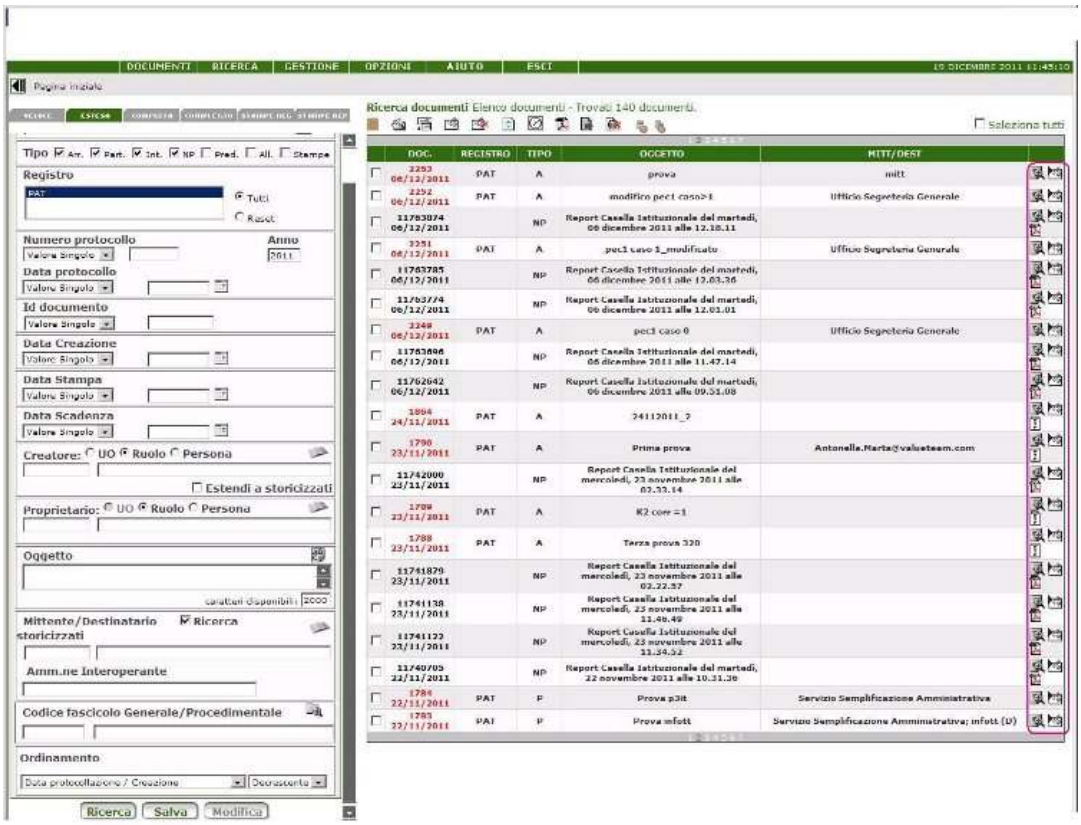


Figura 12 – Pulsanti di azione dal risultato di una ricerca

Se nell'elenco delle "cose da fare" sono presenti trasmissioni, è possibile effettuare le seguenti operazioni selezionando le rispettive icone:

- Smista  ;
- Rimuovi  ;
- Esporta  .

2.5.2 Dettaglio trasmissione

I documenti e i fascicoli ricevuti da un utente si differenziano a seconda delle "ragioni di trasmissioni" (vedi paragrafo 2.13.1) con cui vengono trasmessi. Ciascuna ragione di trasmissione, inoltre, può essere caratterizzata dall'attributo:

- **Con Workflow;**
- **Senza Workflow;**
- **Interoperabilità;**
- **Interoperabilità PI**

2.5.2.1 Con Workflow

Le trasmissioni con ragione caratterizzata da tale attributo richiedono al destinatario l'accettazione o il rifiuto (quest'ultimo motivato obbligatoriamente con una nota) del documento o del fascicolo trasmesso. Fino a quando l'utente non accetta o rifiuta la trasmissione, questa rimane all'interno della lista delle cose da fare. Se opportunamente configurato dall'amministratore inoltre, il sistema non estende la visibilità ai superiori gerarchici fino all'atto dell'accettazione (il documento/fascicolo in tal caso rimane in sola lettura fino all'accettazione esplicita da parte del destinatario). Per accettare/rifiutare una trasmissione si seleziona il pulsante "Dettagli" all'interno della tabella di presentazione dell'elenco delle cose da fare. Si visualizzano in tal modo le seguenti informazioni:

- **Note generali:** note generali relative alla trasmissione, visibili a tutti i destinatari della trasmissione;
- **Note individuali:** note individuali visibili solo ad uno specifico ruolo destinatario della trasmissione;
- **Vista il:** data in cui la trasmissione è stata vista, viene popolato in automatico dal sistema;
- **Risposto il:** valorizzato dal sistema a seguito di eventuale trasmissione in risposta alla trasmissione ricevuta;
- **Accettata il:** valorizzato dal sistema a seguito di eventuale accettazione;
- **Rifiutata il**: valorizzato dal sistema a seguito di eventuale rifiuto;
- **Note Acc/Rif**: valorizzato dal sistema a seguito di eventuale inserimento di note da parte dell'utente che accetta/rifiuta la trasmissione;
- **Rimossa da cose da fare:** valorizzato dal sistema a seguito di eventuale rimozione dalla lista delle cose da fare;
- "**Note di Accettazione/Rifiuto**" è un campo in cui si inserisce il motivo dell'eventuale accettazione/rifiuto.
- Per effettuare l'operazione desiderata si deve selezionare uno di questi tre pulsanti "**Accetta**", "**Accetta e AdL**", "**Rifiuta**" . E' possibile configurare il sistema affinché solamente l'effettiva accettazione di un documento/fascicolo permetta di acquisire i pieni diritti come destinatario della trasmissione; rifiutando la trasmissione, invece, i diritti vengono persi. .
  - Con "**Accetta**" si accetta il documento/fascicolo ricevuto e si prende in carico;
  - Con "**Accetta e AdL**" si accetta il documento/fascicolo ricevuto, si prende in carico ed al contempo si inserisce nell'Area di Lavoro;
  - Con "**Rifiuta**" non si prende in carico il documento/fascicolo ricevuto ed in questo caso è necessario indicare la motivazione nel campo "Note di Accettazione/Rifiuto".

Figura 13 – Trasmissione con ragione di tipo workflow

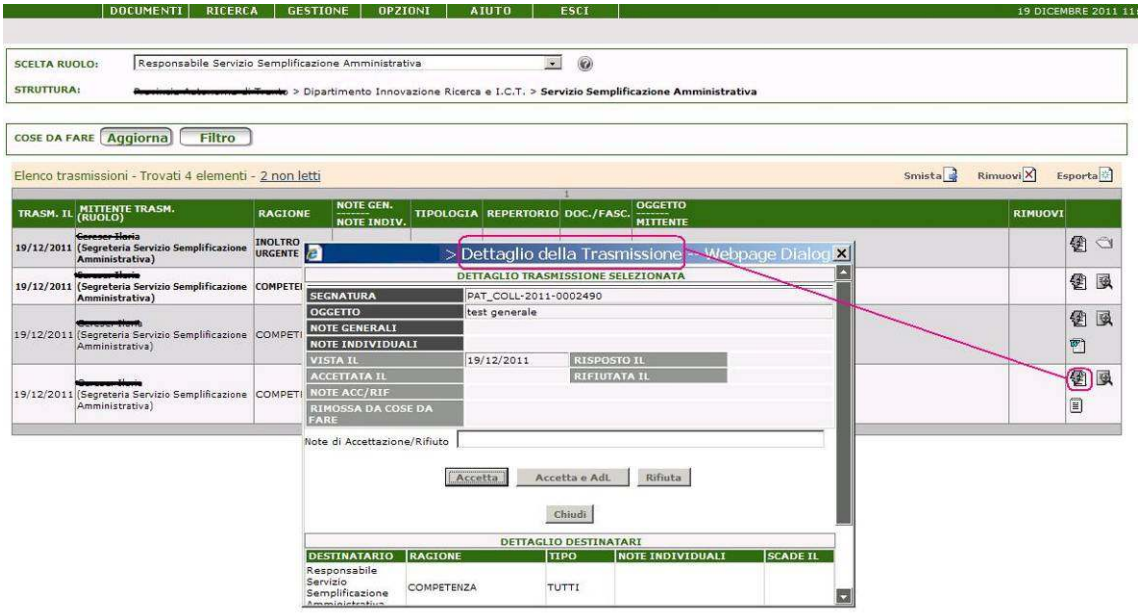


Figura 14 – Dettaglio trasmissione selezionata con ragione workflow

Il rifiuto di una trasmissione genera, in automatico, una nuova trasmissione di notifica verso il mittente con ragione "Rifiuto" e la seguente nota associata: "Trasmissione rifiutata da nome e cognome dell'utente che ha rifiutato" (con un'eventuale annotazione) è tornata al mittente".
All'atto dell'accettazione o del rifiuto la trasmissione selezionata viene eliminata automaticamente dall'elenco delle cose da fare.

2.5.2.2Senza Workflow

Le trasmissioni con ragione caratterizzata da tale attributo identificano i documenti ed i fascicoli trasmessi all'utente per conoscenza ed in visione. Tali ragioni non prevedono pertanto rifiuto o accettazione e quindi i documenti oggetto di una trasmissione con ragione senza workflow sono immediatamente visibili anche ai superiori gerarchici del destinatario. Se si tratta di un documento o di un fascicolo trasmesso in sola lettura, ad esempio con ragione "Sola lettura" (in base alle impostazioni definite dall'Amministratore del sistema), il destinatario non può modificare i dati. Nei documenti non si possono aggiungere allegati, né inserire nuove versioni. Nei fascicoli non si possono inserire nuovi documenti, né è possibile chiuderli. E' consentito effettuare una nuova trasmissione, ma con la stessa ragione con cui sono ricevuti (in sola lettura).
L'eliminazione delle trasmissioni dalle "cose da fare" è configurabile:
Il comportamento classico prevede che sia sufficiente vedere il documento/fascicolo (pagina di dettaglio) per eliminare la trasmissione dalla lista delle cose da fare ed il sistema registra la data in cui il documento/fascicolo è stato visto.
Il sistema può essere configurato in modo tale che la trasmissione rimanga nella lista fintanto che non si clicca sul pulsante "Visto" o "Visto e ADL" presente nella maschera di dettaglio della trasmissione.

Figura 15 – Dettaglio trasmissione selezionata con ragione senza workflow

2.5.2.3 Interoperabilità

Le trasmissioni con ragione caratterizzate da tale attributo sono previste nello scambio di documenti tra le diverse AOO di una stessa Amministrazione o tra Amministrazioni differenti. Selezionando una trasmissione ricevuta per interoperabilità nella lista delle cose da fare e accedendo alla scheda documento, il sistema presenta il documento con i campi obbligatori precompilati con i dati riportati dal mittente. Tale documento è predisposto alla protocollazione: si tratta cioè un documento grigio che può essere protocollato subito o lasciato grigio per poi essere ricercato tra i documenti in competamento e/o predisposti alla protocollazione.

Al momento della protocollazione del documento predisposto, il sistema presenta comportamenti differenti a seconda dell'esito della ricerca del mittente nelle anagrafiche visibili al ruolo a cui appartiene l'utente che ha effettuato l'interrogazione della casella. Tali comportamenti dipendono anche dall'attivazione o meno (a livello di amministrazione) di:
- controllo relativo al mittente interoperante
- controllo relativo ai corrispondenti con casella di posta elettronica identica.

In particolare:

1. se non esistono corrispondenti interoperanti con le stesse caratteristiche (mail o mail e descrizione), il sistema crea un nuovo corrispondente. Se è attivo il *controllo relativo al mittente interoperante* all'atto della protocollazione è disponibile per l'utente una finestra (Figura 16) in cui è possibile modificare il codice e la descrizione del corrispondente appena creato e integrare la registrazione mediante l'aggiunta di ulteriori dettagli.
2. se esiste già un solo corrispondente con le stesse caratteristiche del mittente, il sistema individua tale corrispondente e lo inserisce nel campo mittente del documento predisposto alla protocollazione. Se è attivo il *controllo relativo ai corrispondenti con casella di posta*

elettronica identica, all'atto della protocollazione è disponibile per l'utente un avviso in cui può confermare l'inserimento del corrispondente trovato o la creazione di uno nuovo che, a seconda della natura del corrispondente stesso, presenta unicamente lo stesso indirizzo mail o la stessa descrizione e lo stesso indirizzo mail del mittente;

3. se esistono più corrispondenti con le stesse caratteristiche del mittente, il sistema propone uno dei corrispondenti che presentano le medesime caratteristiche (mail o mail e descrizione) del mittente interoperante. Se è attivo almeno uno dei due controlli precedentemente indicati, all'atto della protocollazione è disponibile per l'utente un avviso (Figura 17) in cui può selezionare uno dei corrispondenti presenti nell'elenco o crearne uno nuovo che, a seconda della natura del corrispondente, presenta unicamente lo stesso indirizzo mail o la stessa descrizione e lo stesso indirizzo mail del mittente

Quanto descritto è valido sia per corrispondenti interoperanti (Pubbliche Amministrazioni) che per corrispondenti non interoperanti dotati di PEC (privati cittadini, professionisti, imprese).

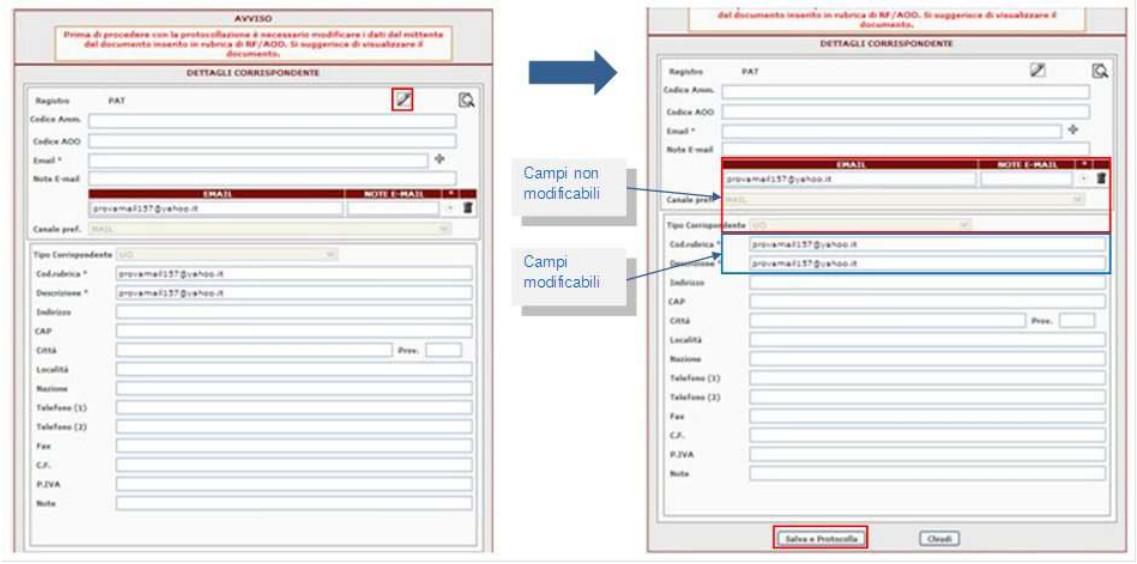


Figura 16 - Avviso che consente di modificare il codice e la descrizione del corrispondente

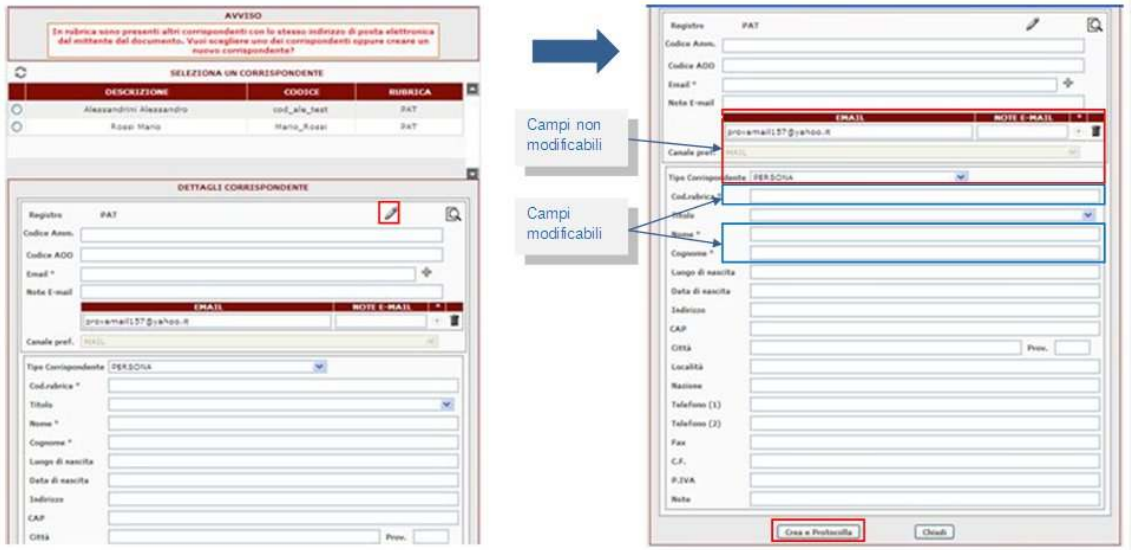


Figura 17 – Avviso contenente l'elenco dei corrispondenti con le medesime caratteristiche del mittente della mail

Il sistema è in grado di visualizzare le marche temporali (attached/detached) ricevute. I dettagli della marca saranno visibili nella maschera di associazione del timestamp. Nel caso di ricezione di marca detached, se fallisce l'associazione fra documento e marca temporale, quest'ultima viene acquisita come allegato utente (con estensione TSR). Se la marca è attached, l'immagine del documento sarà un file con estensione TSD, i dettagli della marca detached inclusa saranno comunque visibili nella maschera di visualizzazione dei timestamp.

2.5.2.4 Interoperabilità PI

Le trasmissioni con ragione caratterizzata da tale attributo sono previste nello scambio di documenti tra le diverse AOO di una stessa Amministrazione o tra Amministrazioni differenti che utilizzando il sistema VTDOCS, senza utilizzare la mail (si veda par. 2.7.2.3). A seconda che sia stata configurata la modalità manuale o automatica, nella lista delle cose da fare è presente:

- un documento predisposto alla protocollazione
- un documento protocollato.

La tramissione ricevuta presenta le seguenti caratteristiche:

- mittente trasmissione: utente creatore e ruolo creatore configurati sul Registro di AOO
- ragione di trasmissione: la ragione configurata con il tipo 'Interoperabilità PI'
- oggetto/mittente: oggetto del documento protocollato in partenza e spedito per interoperabilità semplificata/amministrazione che ha effettuato la spedizione.

Selezionando una trasmissione ricevuta per interoperabilità semplificata nella lista delle cose da fare e accedendo alla scheda documento, il sistema presenta il documento con i seguenti campi precompilati con i dati riportati dal mittente:

- oggetto: oggetto del documento protocollato in partenza dall'AOO mittente;
- mittente: mittente della spedizione (corrispondente della RC);
- protocollo mittente, in data, data di arrivo.

I ruoli opportunamente abilitati, visualizzeranno nel dettaglio della trasmissione il pulsante *Non di competenza dell'Amministrazione*. Cliccando sul pulsante sarà eliminato il documento e inviata una ricevuta di ritorno di eccezione al mittente con l'indicazione del destinatario e del motivo dell'eccezione, ovvero *Non di competenza dell'Amministrazione*.

A seguito della protocollazione del documento predisposto saranno presentati i pulsanti 'Visto' e 'Visto e ADL' nel dettaglio della trasmissione. Cliccando uno dei due pulsanti, la trasmissione di tipo uno scomparirà dalla lista delle cose da fare degli utenti inseriti nel fuolo abilitato alla ricezione dei documenti per interoperabilità semplificata.

Se previsto nella configurazione del Registro, i documenti potranno essere contrassegnati come privati prima di effettuare la registrazione di protocollo. Inoltre, nel caso di ricezione di un documento contrassegnato come privato dall'Amministrazione mittente, al momento della protocollazione, il sistema chiederà se far rimanere privato il documento ricevuto.
Tramite amministrazione è possibile abilitare specifici ruoli alla ricezione di documenti contrassegnati come privati dall'Amministrazione mittente.

Il sistema è in grado di visualizzare le marche temporali (attached/detached) ricevute. I dettagli della marca saranno visibili nella maschera di associazione del timestamp. Se la marca è attached, l'immagine del documento sarà un file con estensione TSD, i dettagli della marca detached inclusa saranno comunque visibili nella maschera di visualizzazione dei timestamp.

2.5.2.4.1 Centro Notifiche

Se il ruolo appartiene ad una AOO per cui è attivo il Centro notifiche e se l'utente è connesso con un ruolo opportunamente abilitato, nella homepage di VTDOCS viene visualizzata una barra orizzontale contenente tutte le notifiche non ancora visualizzate e in alto, nella barrà dei menù, una voce Notifiche (Figura 18) che consente di accedere all'archivio delle notifiche (Figura 20). Le notifiche di ricevute di mancata consegna e di eccezione saranno notificate soltanto all'utente che ha effettuato la spedizione.

Figura 18 – Centro Notifiche

Cliccando sull'icona RSS relativa ad una specifica ricevuta, viene aperta una finestra (Figura 19) che mostra i feed ancora non visti da un utente per un particolare canale.

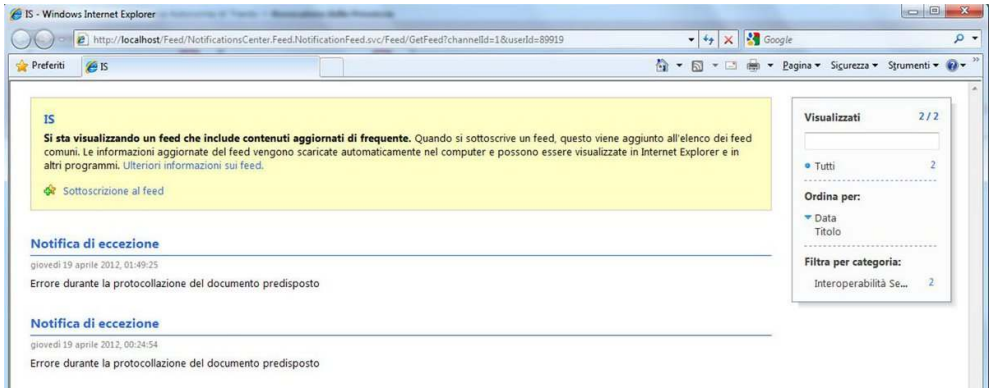


Figura 19 – Feed RSS

Tali feed potranno essere registrati in qualsiasi RSS Reader, come ad esempio quelli integrati in Internet Explorer o in Outlook o su apposite app installate su dispositivi mobili.

Selezionando la voce di menù Notifiche (Figura 18), l'utente accede ad una sezione (archivio notifiche) in cui è possibile effettuare una ricerca di tutte le notifiche ricevute (già visualizzate e non) mediante i seguenti filtri:

- numero di protocollo;
- data di ricezione della notifica;
- tipo evento: permette di selezionare i valori "qualsiasi", "mancata consegna" ed "eccezione".

Sia nel centro notifiche, sia nell'archivio notifiche, selezionando il numero di protocollo del documento, l'utente viene condotto al dettaglio del documento stesso.

Figura 20 – Archivio Notifiche

2.5.3 Evidenza della segnatura di repertorio nella Lista delle cose da fare

Se l'Amministrazione è abilitata alla gestione dei repertori e alla visualizzazione della segnatura di repertorio nella Lista delle cose da fare, l'utente che accede al sistema vedrà nella griglia delle trasmissioni ricevute due nuovi campi (Figura 21):

- **Tipologia**, in cui è mostrata la tipologia del documento/fascicolo nel caso di documenti/fascicoli tipizzati;
- **Repertorio**, in cui è visualizzata in rosso la segnatura di repertorio del documento trasmesso, sia che si tratti di un documento non protocollato, sia di un documento protocollato.

Se la registrazione di repertorio è stata annullata, nella Lista delle cose da fare la segnatura presenterà i caratteri barrati.

Figura 21 – *Visualizzazione Tipologia e Repertorio nella Lista delle cose da fare*

2.5.4 Smistamento

Lo smistamento è un'operazione che consente di far pervenire un documento all'Unità Organizzativa che lo deve trattare e permette di gestire in modo più efficiente l'elenco delle "cose da fare". L'obiettivo è quello di semplificare le operazioni di suddivisione dei documenti ricevuti, in modo da minimizzare le operazioni richieste all'utente. Lo smistamento dei documenti avviene "a cascata" seguendo la struttura gerarchica dell'organigramma dell'amministrazione.
La trasmissione del documento genera una e-mail agli utenti destinatari del documento, in base alla configurazione gestita dall'Amministratore del sistema con l'applicativo di amministrazione (l'Amministratore deve selezionare i ruoli di riferimento affinché siano visibili per lo smistamento).

Figura 22 - Tasto " Smista" nell'elenco "cose da fare"

Selezionando l'icona corrispondente alla funzione "Smista",si apre una nuova finestra che presenta la pagina dedicata alle operazioni di smistamento in cui sono proposte l'immagine e i dati caratteristici del primo documento presente nella lista delle *"Cose da fare"*. La pagina è suddivisa in due sezioni verticali: nella parte destra sono presenti i dati fondamentali, la lista dei ruoli, i relativi utenti della propria Unità Organizzativa e di quella immediatamente sottostante. Nella parte sinistra si

visualizza l'immagine del documento che si desidera smistare che è visibile solo se si seleziona la casella che si trova nel pannello di destra.
L'operazione termina solo quando l'utente ha preso visione di tutti i documenti presenti nell'elenco delle "cose da fare" o su esplicita richiesta da parte dell'utente di interrompere il processo di smistamento, che potrà essere ripreso in qualunque momento sempre a partire dall'elenco delle "cose da fare".
Terminata l'operazione di smistamento il sistema ripropone la Home page con l'elenco delle "cose da fare" aggiornato.
Un esempio dell'interfaccia dello smistamento è riportato nella figura seguente.

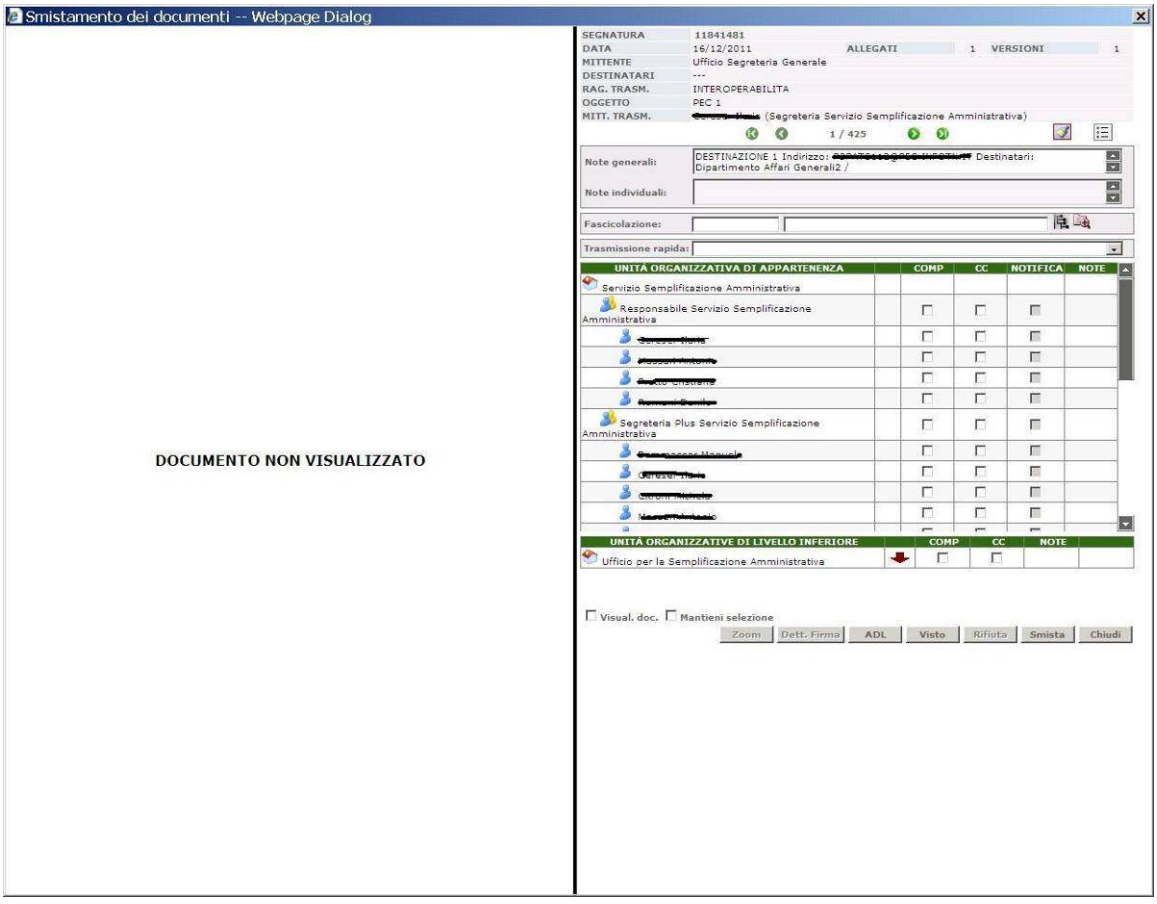


Figura 23 - Pagina per lo smistamento

In questa sezione si trovano tutte le informazioni relative al documento. Le frecce consentono di scorrere i documenti, con la correlata indicazione del numero rispetto a quello totale da smistare. L'immagine seguente propone un esempio.

Figura 24 - Dettaglio dati del documento

Se l'Amministrazione è abilitata alla gestione dei repertori e alla visualizzazione della segnatura di repertorio nella Lista delle cose da fare, sarà possibile visualizzare nell'interfaccia di smistamento due nuovi campi:

- **Tipologia**, in cui è mostrata la tipologia documento/fascicolo nel caso di documenti/fascicoli tipizzati;
- **Repertorio**, in cui è possibile visualizzare la segnatura di repertorio di tipologie documentali repertoriate.

L'immagine seguente propone un esempio.

Figura 25 - Nuovi campi Tipologia e Repertorio nell'interfaccia di smistamento

Nel campo "Note generali" è possibile inserire delle note che saranno allegate alla trasmissione durante la fase di smistamento.
Se il documento che si vuole smistare è stato trasmesso all'utente con l'aggiunta di note individuali, queste vengono visualizzate nella casella non editabile denominata "Note individuali".

La fascicolazione rapida può essere effettuata attraverso la semplice digitazione del codice del fascicolo o del sotto fascicolo (se conosciuto), oppure selezionando la figura che permette di scegliere (così come descritto dal paragrafo 2.8.1) il fascicolo/sotto fascicolo desiderato. Il documento di conseguenza verrà fascicolato contestualmente alla creazione del protocollo in

ingresso. E' possibile fascicolare i documenti, protocollati e non, in modalità "rapida" anche dopo la loro creazione.
Se accanto alla dicitura fascicolazione rapida vi è un asterisco, questa è obbligatoria.
La disponibilità di tale funzione è assegnata a ruolo dall'amministratore del sistema.

L'utente dovrà selezionare i destinatari ai quali smistare il documento corrente. Sarà possibile scegliere più di un destinatario, agendo sulla casella di riferimento.
Lo smistamento potrà avvenire "per competenza" o "per conoscenza". Si potrà smistare contemporaneamente a destinatari "per competenza" e destinatari "per conoscenza". Per poter trasmettere il documento è necessario che almeno un destinatario sia selezionato.
E' anche possibile navigare la struttura organizzativa, verso il basso o verso l'alto, attraverso le frecce associate accanto alle UO. La freccia orientata verso il basso serve per scendere di un livello e quindi, se selezionata, consente di visualizzare la UO inferiore; la freccia orientata verso l'alto serve per risalire di un livello e se selezionata, consente di visualizzare l'UO padre. Una volta scesi di livello, è possibile risalire fino alla propria UO. Dalla propria UO non è possibile risalire ad una UO sovra ordinata.

Dopo aver gestito il documento corrente (smistato, visto o inserito in Area di Lavoro), il sistema richiama il documento successivo. Se non è attiva l'opzione "Mantieni selezione" l'ambiente per la selezione dei destinatari si riposizionerà sull'UO di appartenenza dell'utente connesso (si ripristina quindi la situazione iniziale dello smistamento).

Figura 26 - UO, ruoli e utenti per lo smistamento

Dopo aver selezionato il destinatario della trasmissione, l'utente ha la possibilità di inserire dei dati aggiuntivi alla trasmissione (note individuali e data di scadenza) così come mostrato qui di seguito.

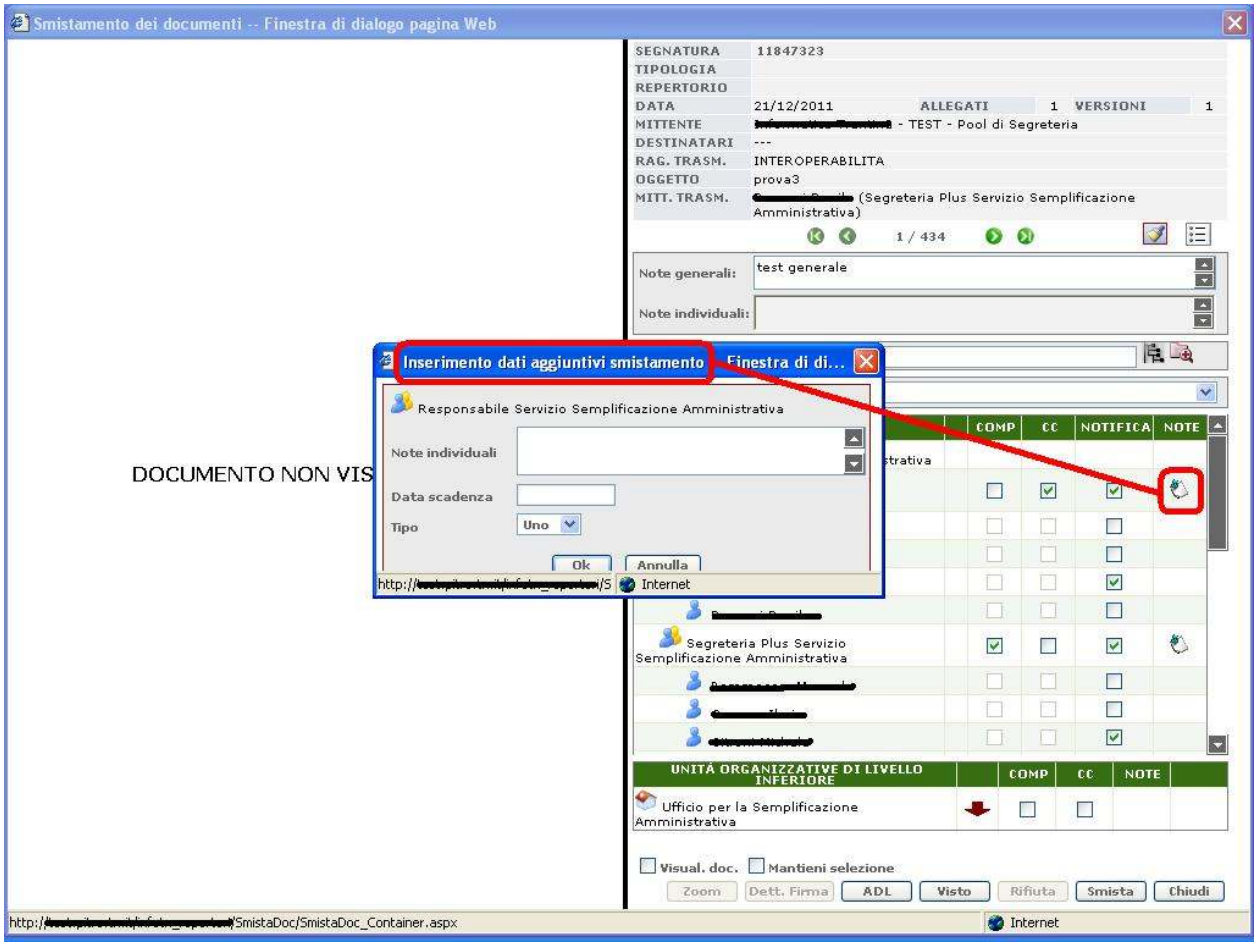


Figura 27 – Inserimento dati aggiuntivi alla trasmissione

Di seguito sono descritti brevemente il funzionamento delle caselle e dei pulsanti presenti nel panello dello smistamento:

- **Visualizza documento**: se selezionata, propone nel pannello di sinistra l'immagine e gli eventuali documenti elettronici associati, come mostrato Figura 28. La descrizione di tale funzionalità è riportata al paragrafo 2.14.2.1 ;

  Allo scopo di ottenere una miglior risoluzione dello schermo, è' possibile spostare (destra/sinistra) la linea di separazione dell'area dedicata alla visualizzazione dei documenti dall'area per eseguire lo smistamento, per meglio adattarsi alla situazione (risoluzione dello schermo, tipo di documento acquisito, ecc.)
  La visualizzazione delle informazioni si adatterà automaticamente alle dimensioni disponibili del'area.
  L'impostazione rimane per tutta la durata della sessione di smistamento.

- **Mantieni selezione**: se selezionata, rimane invariata la selezione dei destinatari anche per i successivi documenti;
- **Zoom**: amplia l'immagine a tutto schermo; il pulsante è attivo solo quando la casella "visualizza documento " è selezionata ed è presente un documento;
- **Dett. Firma**: mostra i dettagli della firma se il documento è firmato digitalmente;

- **Rifiuta**: rifiuta il documento con conseguente notifica automatica del rifiuto al mittente. Il pulsante è disattivato se la trasmissione non è di tipo workflow;
- **AdL**: inserisce il documento nell'Area di Lavoro. Da questo punto in poi il tasto non è più cliccabile e accanto al nome compaiono due asterischi.
- **Accetta**: imposta il documento come accettato, rimuovendolo dalla "lista delle cose da fare". Il tasto è visibile se la trasmissione è di tipo workflow;
- **Visto**: imposta il documento come visto, rimuovendolo dalla "lista delle cose da fare". Il tasto è visibile se la trasmissione non è di tipo workflow;
- **Smista**: trasmette il documento ai destinatari e lo elimina dalla lista delle cose da fare;
- **Chiudi**: chiude la pagina modale dello smistamento senza effettuare alcuna operazione

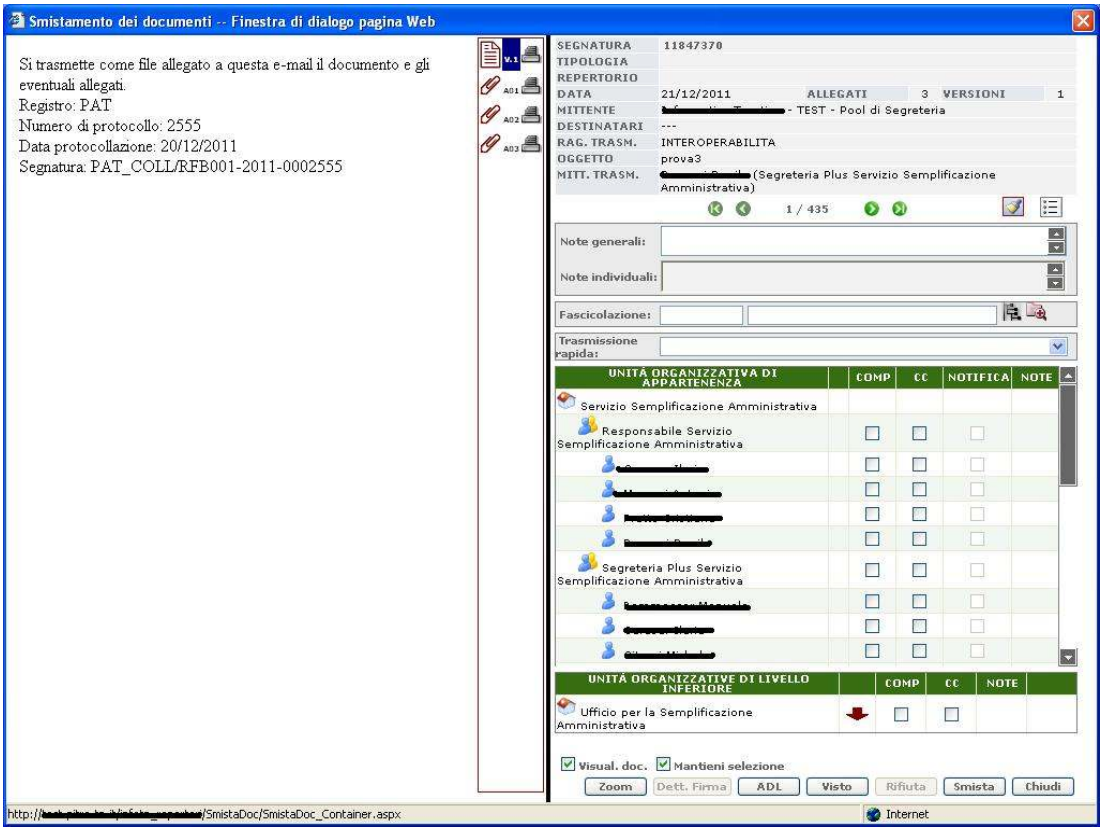


Figura 28 – Visualizzazione documenti e documenti elettronoci associati

Figura 29 - Pulsanti funzione

La gestione della notifica ad utente nello smistamento è stata resa simile a quella presente nella maschera utilizzata per la creazione manuale delle trasmissioni.
L'interfaccia utente per la selezione dei ruoli o degli utenti è stata modificata facendo ricorso ai *check box* (dei pulsanti a selezione che possono assumere due stati selezionato/non selezionato) ed è stata introdotta una nuova colonna di check box che permette, selezionato un ruolo, di attivare o meno la notifica a uno o più utenti del ruolo stesso.
Il sistema si preoccupa di mantenere la situazione delle selezioni sempre in uno stato coerente, in particolare:

- I check box COMP e CC sono mutualmente esclusivi rispetto allo stesso destinatario (non è possibile selezionare un ruolo contemporaneamente per competenza e per conoscenza);
- Il check box per la selezione/deselezione della notifica agli utenti del ruolo è attivo solo se il ruolo è selezionato.
- I check box per la selezione degli utenti di un ruolo sonno mutualmente esclusivi rispetto ai check box per la selezione del ruolo (non possono essere selezionati contemporaneamente un ruolo ed uno o più dei suoi utenti):

Lo smistamento alle UO gerarchicamente inferiori permette di navigare attraverso le UO e di scegliere i ruoli e/o gli utenti che vi appartengono.
In ogni caso ci sono tre possibilità di selezione

- L'utente può selezionare diversi utenti del ruolo senza aver selezionato l'opzione relativa al ruolo stesso. In tal caso è infatti possibile trasmettere a utenti diversi utilizzando ragioni di trasmissione differenti (conoscenza e competenza). L'effetto è quello di aver creato delle trasmissioni di tipo utente agli utenti selezionati.
- L'utente seleziona un ruolo. In questo caso vengono automaticamente selezionati tutti gli utenti appartenenti a tale ruolo. E' possibile poi de-selezionare gli utenti appartenti al ruolo a cui non si voglia effettuare la notifica. Non è possibile associare agli utenti la voce COMP o CC.

L'effetto sarà quello di aver creato una trasmissione al ruolo, dove tutti gli utenti avranno la visibilità del documento, poiché appartenenti al ruolo, ma naturalmente solo quelli selezionati riceveranno la notifica.

- L'utente seleziona una UO, in tal caso lo smistamento viene fatto al ruolo/ai ruoli di riferimento associato/i alla UO.

Se lo smistamento di un documento protocollato viene effettuato verso una UO i cui ruoli di riferimento operano su registri diversi da quello del documento da smistare, il sistema avvisa l'utente dell'impossibilità di effettuare tale operazione attraverso un messaggio a video.

Figura 30 - Messaggio di impossibilità smistamento

Nella pagina dello smistamento sono presenti alcune funzionalità che permettono di velocizzare l'operazione di smistamento:

- trasmissione rapida (utilizzando soltanto modelli di trasmissione fra i cui destinatari non compaiano ruoli inibiti alla ricezione di trasmissioni);
- fascicolazione rapida;
- consultazione elenco riassuntivo degli utenti selezionati per lo smistamento del documento.

In particolare l'ultima funzionalità consente di visualizzare l'elenco riassuntivo degli utenti/ruoli/UO selezionati per lo smistamento navigando le UO mediante la freccia ( )

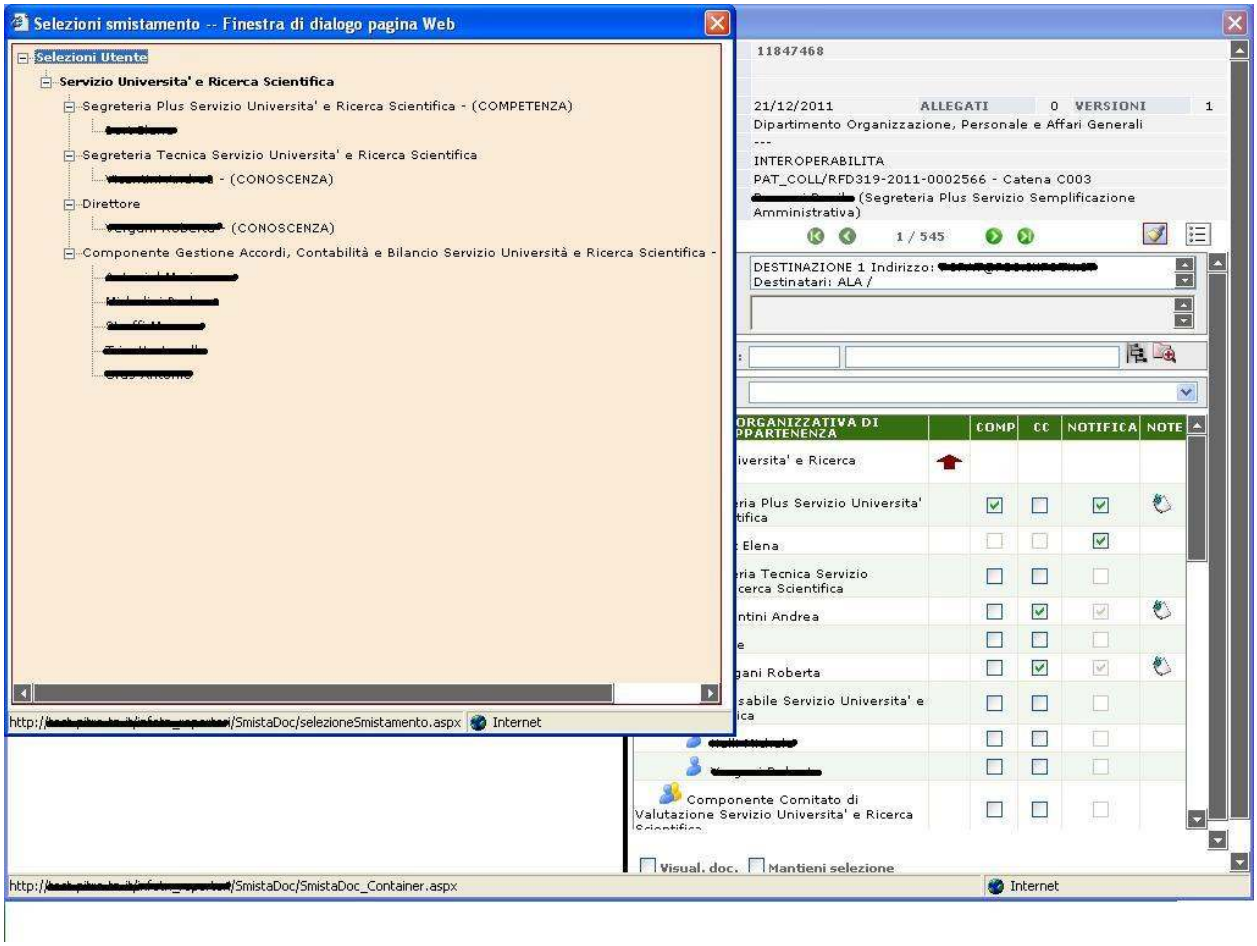


Figura 31 – Dettaglio selezioni

2.5.5 Rimuovi

Per i documenti ed i fascicoli si visualizza in alto a destra il termine “Rimuovi” associato all’icona . Tale funzione permette di poter eseguire la rimozione delle trasmissioni antecedenti una certa data. Prima di selezionare l’icona, l’utente deve pertanto:

- eventualmente modificare la data proposta automaticamente dal sistema;
- togliere o lasciare la selezione della casella che indica all’utente il mantenimento delle trasmissioni che richiedono accettazione.

A questo punto, dopo aver effettuato le dovute scelte, si seleziona l’icona “Rimuovi” e le trasmissioni precedenti alla data inserita vengono rimosse dalle “cose da fare”. Tale rimozione comporta solo l’eliminazione dall’elenco delle “cose da fare”; i documenti o i fascicoli sono sempre consultabili tramite funzionalità differenti.

Se si seleziona il pulsante “Annulla”, la condizione delle “cose da fare” resta immutata.

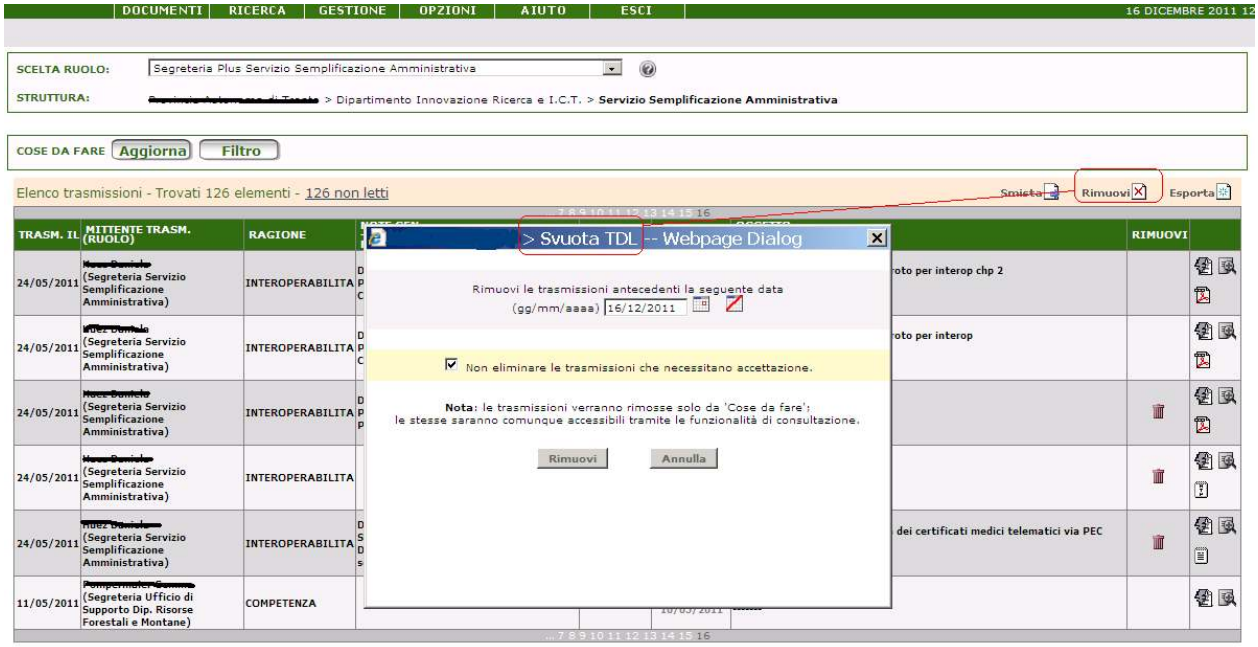


Figura 32 – Rimuovi

2.5.6 Esporta

Nella pagina di accesso è inoltre possibile esportare l'elenco delle trasmissioni documenti ricevute selezionando, in alto a destra, l'icona che attiva la funzione "Esporta". Tale funzione permette di poter eseguire l'esportazione dell'elenco nei seguenti formati:

1. Abobe Acrobat
2. Microsoft Excel
3. Open Office

Selezionando la suddetta icona viene visualizzata una finestra di dialogo (Figura 33 – Esporta) che consente di selezionare il formato desiderato di esportazione dei dati e di associare, non obbligatoriamente, un titolo o una descrizione al file che verrà generato. In particolare, per quanto riguarda il file Microsoft Excel, è possibile selezionare e quindi visualizzare solo i campi di interesse.

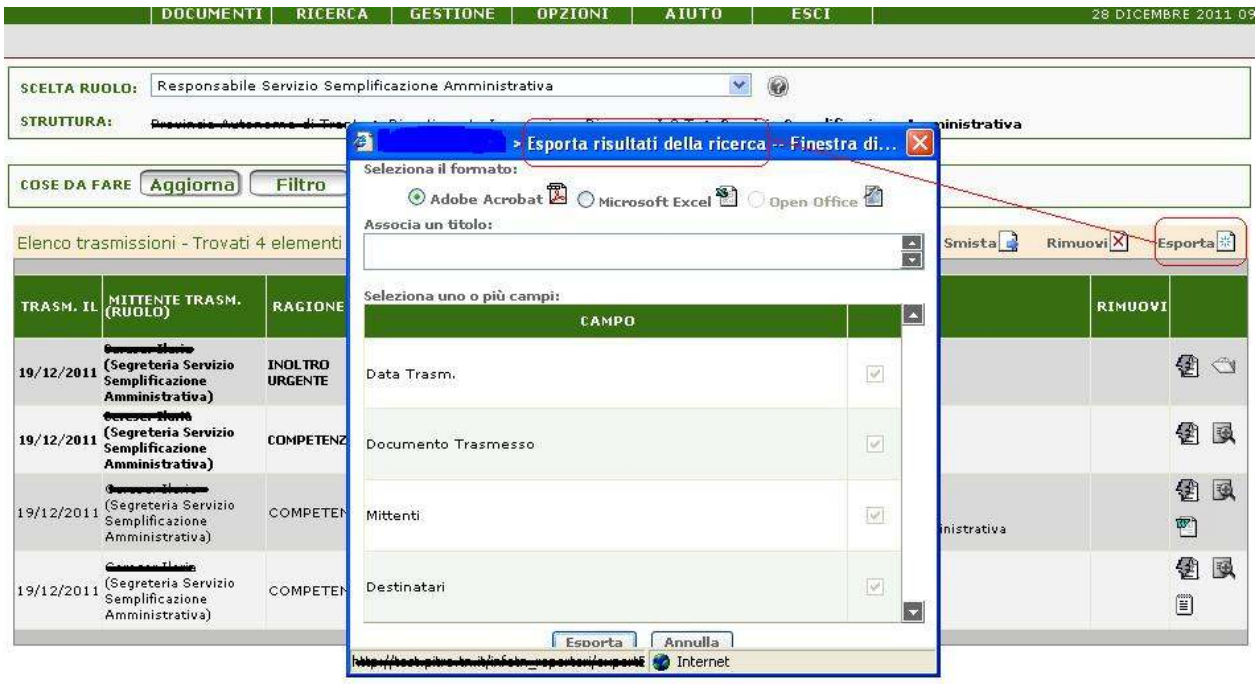


Figura 33 – Esporta

La procedura di generazione del file nel formato prescelto avviene tramite il pulsante “Esporta”.
La stampa riporta le seguenti informazioni:

- Data della trasmissione;
- Documento/fascicolo trasmesso: ID, protocollo, oggetto oggetto/descrizione;
- Mittente della trasmissione (Utente e Ruolo);
- Destinatari della trasmissione.

Dopo aver visualizzato l’elenco esportato tramite l’applicazione proprietaria, l’utente potrà stampare, modificare o salvare il file.
Questa funzionalità è presente, come vedremo in seguito, anche nella **ricerca documenti, ricerca fascicoli e ricerca trasmissione**, ed è sempre posizionata in alto rispetto alla griglia dei risultati.

Nel caso della ricerca documenti, si visualizza un elenco di documenti, dove l’esportazione dei dati riporta le seguenti informazioni:

- Registro;
- Protocollo;
- Data di protocollo;
- Tipologia di protocollo;
- Oggetto del documento;
- Mittenti o destinatari del documento;
- Codice del fascicolo che contiene il documento;
- Data dell’eventuale annullamento del protocollo.

Nella ricerca dei documenti, all'atto dell'esportazione in formato excel, se i documenti ricercati hanno una tipologia documento profilato, nell'elenco dei campi da esportare saranno selezionabili anche i campi profilati.

Nel caso della ricerca fascicoli si visualizza un elenco di fascicoli (es: Figura 204), dove l'esportazione dei dati riporta le seguenti informazioni:

- Registro;
- Tipo del fascicolo;
- Codice del fascicolo;
- Descrizione del fascicolo;
- Data di apertura;
- Data di chiusura;
- Collocazione fisica.

Nel caso della **ricerca trasmissioni**:

- se l'utente ha effettuato una ricerca delle trasmissioni di documenti (protocollati e/o non protocollati) l'esportazione dei dati delle trasmissioni riporterà le stesse informazioni inserite per gli elenchi documenti;
- se l'utente ha effettuato una ricerca delle trasmissioni di fascicoli i dati riportati nell'esportazione saranno uguali a quelli della ricerca fascicoli.

2.6 Tasto Back

L'utente nella navigazione di VTDOCS è accompagnato, escludendo la pagina iniziale, dalla presenza costante della funzione "Back" (in italiano "indietro"), associato all'icona  . Tale funzione mantiene la traccia delle pagine visitate e dà la possibilità di ripercorrere all'indietro il percorso effettuato fino a raggiungere la Home page.
Mantiene altresì in memoria i criteri di ricerca dei documenti/fascicoli/trasmissioni utilizzati per generare sia l'elenco sia l'elemento selezionato richiamando, se necessario, l'opportuna pagina della lista che lo contiene.

2.7 Documenti

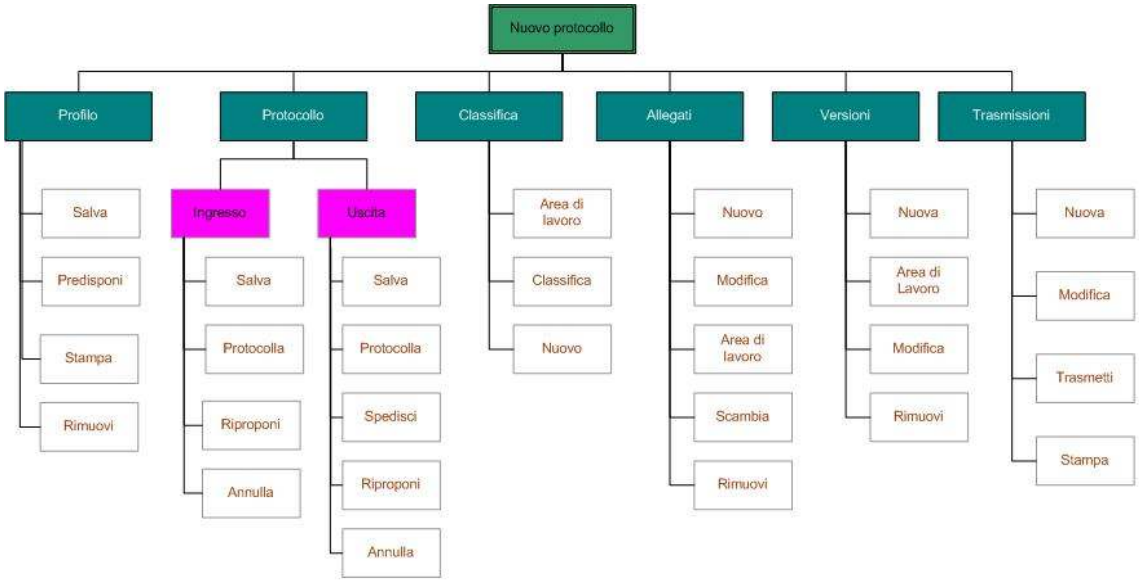


Figura 34 - Nuovo Protocollo: schema di navigazione

2.7.1 Protocollo in ingresso [1]

Per inserire un nuovo documento da protocollare in ingresso è necessario selezionare dal menù principale la voce “Documenti” e successivamente la voce “Nuovo protocollo”. Si visualizza la pagina del protocollo con l’opzione di selezione del protocollo posizionata in modo automatico su “INGRESSO”.
Il pannello riporta, in alto, la descrizione e lo stato del registro sul quale si sta operando. Il registro in cui inserire i documenti può essere selezionato dal menù a tendina impostato in automatico dal sistema.

[1] L’etichetta “ingresso” è configurabile mediante il tool di amministrazione. Alcune amministrazioni usano infatti la parola “Entrata”, altri “Arrivo”. Nelle figure del documento è pertanto possibile vedere nomi diversi.

Figura 35 - Protocollo in ingresso

Ogni utente ha a disposizione tutti i registri sui quali è abilitato a lavorare in relazione al ruolo che ricopre nell'amministrazione di appartenenza. Ogni stato del registro è rappresentato da un colore, ovvero:

- Rosso __ indica che il registro è chiuso;
- Verde __ indica che il registro è aperto;
- Giallo __ indica che la data di apertura del registro è precedente alla data odierna.

Nella parte sottostante a quella dei registri sono presenti le seguenti funzionalità elementari:

- Arrivo Partenza Interno: opzione grafica da selezionare per indicare se il protocollo che si sta creando è in ingresso, in uscita oppure interno. Nel caso del protocollo in ingresso basta lasciare selezionato il valore proposto in automatico dal sistema; il protocollo interno va utilizzato quando il documento protocollato è destinato a corrispondenti interni alla propria AOO;
- Privato: se selezionato indica che, nel protocollo che si sta creando, non viene ereditata la visibilità dai ruoli gerarchicamente superiori; quindi il protocollo con questa opzione risulta visibile soltanto agli utenti appartenenti allo stesso ruolo dell'utente che lo ha creato. All'atto della fascicolazione e/o della trasmissione si amplierà la visibilità del protocollo;
- :consente di inserire il documento nell'Area di lavoro (si veda il paragrafo 3.5);

- : consente di effettuare singole modifiche nel documento dopo la protocollazione;
- : consente di visualizzare le utenze (quindi ruoli/utenti) che hanno visibilità sul documento e come hanno acquisito tale visibilità. Per i ruoli abilitati dall'amministratore è possibile, tramite un apposito pulsante, all'interno della maschera di visibilità, rimuovere i diritti di un ruolo o di un utente. L'operazione può essere revocata. Non è possibile rimuovere i diritti di proprietà. Per ulteriori dettagli si veda il paragrafo 2.8.1.1;
- : icona consente di visualizzare tutte le operazioni che avvengono sul documento;
- : consente di visualizzare la storia del processo di conservazione a cui è stato sottoposto il documento;
- : consente di creare un documento predisposto alla protocollazione in uscita con lo stesso oggetto del documento protocollato in ingresso che si vuole inoltrare. Tale documento avrà tra gli allegati il documento protocollato (Figura 36), gli eventuali allegati del documento protocollato in ingresso più altri eventuali allegati del documento da protocollare in uscita che si vuole inoltrare ad un altro destinatario.
- : questa immagine viene visualizzata se il documento è arrivato per interoperabilità utilizzando un sistema di posta non certificata
- : questa immagine viene visualizzata se il documento è arrivato per interoperabilità utilizzando un sistema di posta certificata.
- : consente di consolidare un documento nella parte relativa a versioni ed allegati
- : consente di consolidare totalmente un documento, nella parte relativa a versioni ed allegati (se il documento non è stato consolidato parzialmente dalla funzione sopra descritta) e nei metadati. Per i dettagli si rimanda al paragrafo 2.7.1.6.

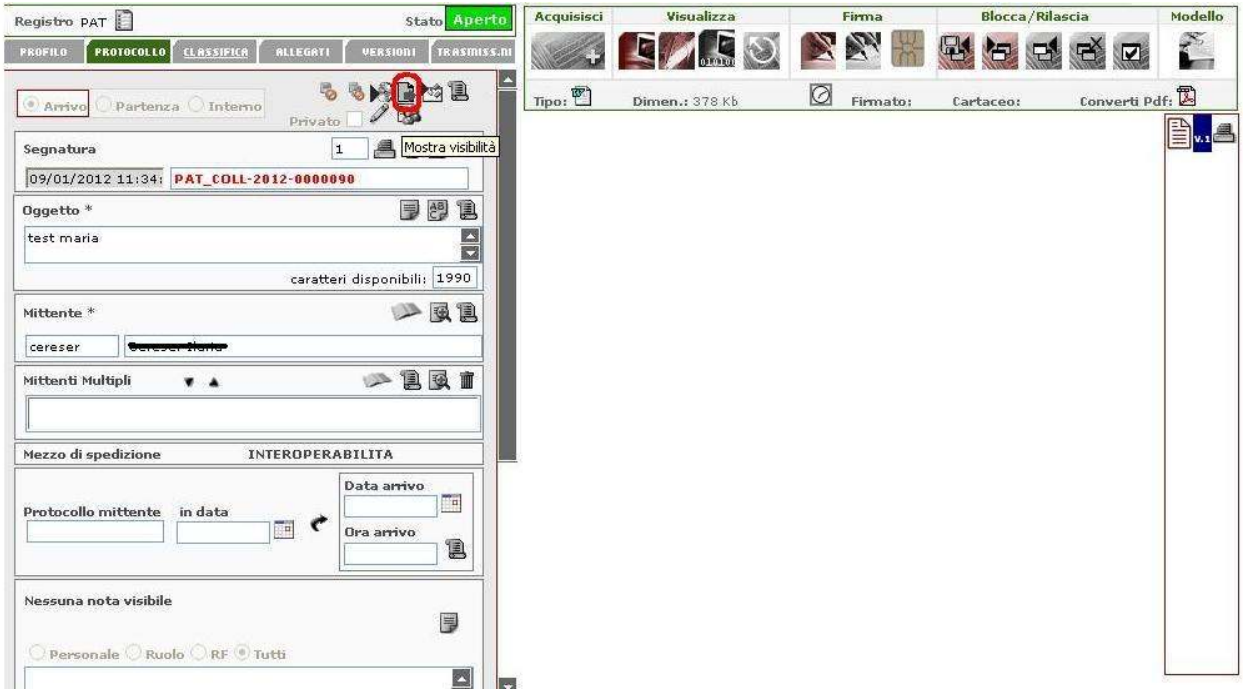


Figura 36 – Protocollo in ingresso da inoltrare ad un altro destinatario

Figura 37 – Documento ricevuto per interoperabilità

I dati relativi ad un documento da protocollare in ingresso sono i seguenti:

- **Segnatura:** la stringa di segnatura viene impostata automaticamente dal sistema in base a regole prefissate ed è costituita da diversi parametri configurabili mediante l'applicazione di amministrazione, come il numero di protocollo, data e anno di protocollazione (che coincide con la data di ultima apertura del registro), codice del registro, codice dell'amministrazione. L'ora della protocollazione è visualizzabile nella stringa di segnatura a video e stampabile in cartaceo sull'etichetta. A questo campo sono associate le seguenti icone:
  - : consente di stampare la segnatura tramite una stampante di etichette. Il sistema può essere configurato per consentire all'utente di impostare il numero di etichette da stampare in modo continuativo: in tal caso accanto all'icona della stampantina comparirà un campo per l'inserimento di tale numero (Figura 37). Il valore di default è 1. Se questa voce è attiva sull'etichetta viene riportato anche il progressivo dell'etichetta stampata.
  - : permette, dopo la protocollazione del documento, di stampare su un foglio A4 bianco, la segnatura del protocollo registrato secondo le coordinate impostate dall'utente oppure di stampare il timbro sempre su A4 bianco (così come mostrato nella Figura 38 - Stampa timbro in PDF su A4); è possibile definire un timbro di segnatura di protocollo in amministrazione e apporre lo stesso sui documenti tramite la funzionalità di visualizzazione timbro/etichetta su documenti in formato PDF. Il timbro può contenere le stesse informazioni della segnatura ed in più le indicazioni relative a classificazione e fascicolazione del documento.
  - : permette, dopo la protocollazione del documento, di stampare la ricevuta di protocollo in formato Word rispetto ad un modello rtf impostato dall'Amministratore di sistema per ogni registro. Se diversamente configurato, il sistema consente di stampare la ricevuta in

formato pdf. In tal caso il modello da impostare dal tool di amministrazione dovrà essere in formato pdf.

-  : permette di spedire la ricevuta di ritorno al mittente di un documento ricevuto per interoperabilità.

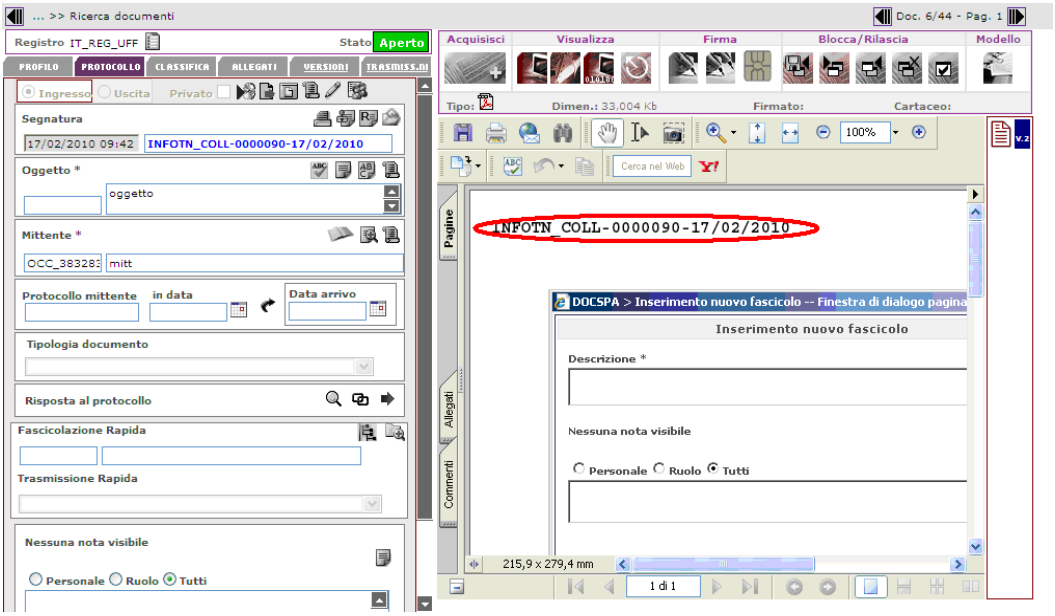
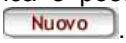


Figura 38 - Stampa timbro in PDF su A4

Quando il puntatore del mouse passa sul campo segnatura viene attivato lo zoom che consente di ingrandire le dimensioni del campo rendendolo più leggibile.

Figura 39 – Zoom del campo segnatura

- **Oggetto**: dato obbligatorio. Riporta una breve descrizione del contenuto del documento che si sta protocollando. il valore può essere digitato liberamente dall'utente, oppure , in caso di oggetti ricorrenti, può essere selezionato da una lista memorizzata denominata Oggettario, che è possibile raggiungere selezionando l'icona  . Un esempio è riportato Figura 53 (vedi Paragrafo 2.7.1.3.1). Se si inserisce una descrizione occasionale è possibile effettuare il controllo ortografico su quanto editato nel campo oggetto attraverso la selezione dell'icona  che apre la finestra di dialogo mostrata nella Figura 78. E' possibile valorizzare il campo oggetto anche attraverso la semplice digitazione del codice associato all'oggetto necessario collegato al Registro/RF di interesse. In tal caso, dopo aver digitato il codice oggetto, se si sposta il cursore in un altro campo del modulo, l'applicazione automaticamente valorizza il campo di testo, posto a fianco, mediante la descrizione associata al codice digitato, prelevandola dall'oggettario. Se l'oggetto interessato non è presente nell'oggettario, è possibile inserirlo selezionando un eventuale registro e digitando il codice (se necessario) ed il valore oggetto nel campo oggetto, e premendo sul pulsante  .
  Quando nel campo dell'oggetto viene digitato un testo molto lungo, per leggere interamente quanto in esso contenuto è possibile selezionare l'icona  . E' inoltre possibile visualizzare la storia delle modifiche ad esso apportate tramite l'icona  .
- **Mittente**: dato obbligatorio. Come per l'oggetto, anche il mittente può essere occasionale (in tal caso può essere inserito liberamente dall'utente valorizzando il campo descrizione mediante la tastiera) o abituale, selezionandolo dalla rubrica. Per l'inserimento da rubrica è necessario selezionare l'icona  associata al campo "mittente". Nella finestra di dialogo che si apre a seguito della selezione dell'icona sono presenti i campi per la ricerca, e quindi per la successiva valorizzazione del campo mittente, di utenti, ruoli o UO. Inoltre è possibile valorizzare il campo mittente anche attraverso la semplice digitazione del codice rubrica associato all'utente, al ruolo o all'UO di interesse. In tal caso, dopo aver digitato il codice rubrica, se si sposta il cursore in un altro campo qualsiasi del modulo, l'applicazione automaticamente valorizza il campo di testo, posto a fianco, con il nominativo o la descrizione associata al codice digitato, prelevandoli dalla rubrica. Se il mittente interessato non è presente in rubrica è possibile inserirlo accedendo al pannello riportato nella Figura 40 mediante l'icona  .
  Il campo mittente può essere configurato per consentire l'integrazione con la tecnologia Ajax per le ricerche in rubrica. In particolare, se attivata questa integrazione, viene visualizzato un campo in corrispondenza del campo mittente. Su tale campo è stata attivata la funzione di auto completamento di Ajax che fornisce dei suggerimenti sulle parole da inserire nel campo mittente sulla base delle prime lettere digitate.
  Il numero dei caratteri a partire dai quali visualizzare i suggerimenti è configurabile.
  I suggerimenti sono presi dalla rubrica (dalla descrizione dei corrispondenti) (Figura 40).

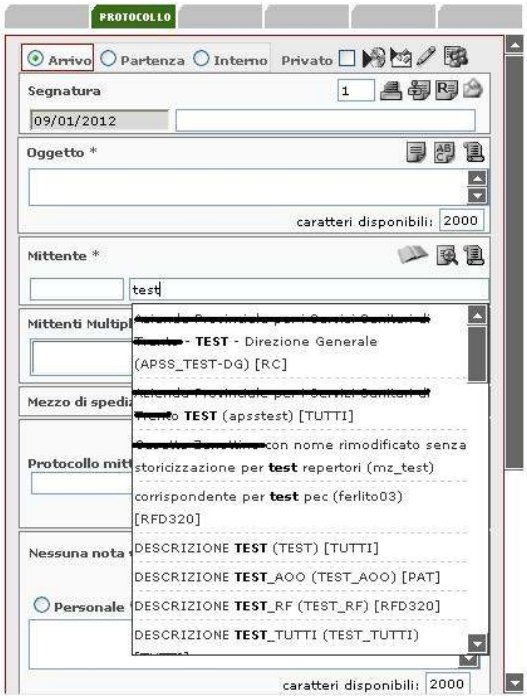


Figura 40 - Suggerimenti mittente Rubrica AJAX

- **Note**: campo di testo in cui è possibile inserire una o più note per ciascuna delle quali si può impostare una diversa visibilità scegliendo tra le alternative proposte (per dettagli maggiori sull'utilizzo della funzionalità si veda il paragrafo 2.8.1.2);
- **Tipologia documento**: in cui l'utente può scegliere una tipologia da indicare. Nel menu a tendina verranno mostrate solamente le tipologie in esercizio (non sospese). Una volta scelta la tipologia nella sezione destra della pagina, viene visualizzato il pannello con i campi della profilazione dinamica del documento (si veda l'esempio riportato in Figura 41). L'utente amministratore, in fase di costruzione della "tipologia documento" o successivamente, può associare ad un ruolo specifico la visualizzazione e l'utilizzo di una determinata tipologia, e in modo più specifico la visualizzazione anche di soli alcuni campi, per cui le informazioni relative alla tipologia documento sono visibili solo agli utenti abilitati. Se tra i dati della tipologia ci sono dei contatori con attivazione manuale, all'atto della creazione ci sarà una casella selezionabile denominata "Attiva" ed il contatore scatterà solo se l'utente selezionerà questa casella. Se alla tipologia scelta è associato un diagramma di stato, nella sezione "profilo" in automatico si visualizza anche il campo Stato che può essere valorizzato così come descritto nel paragrafo 2.8.1 alla voce "Stato" .

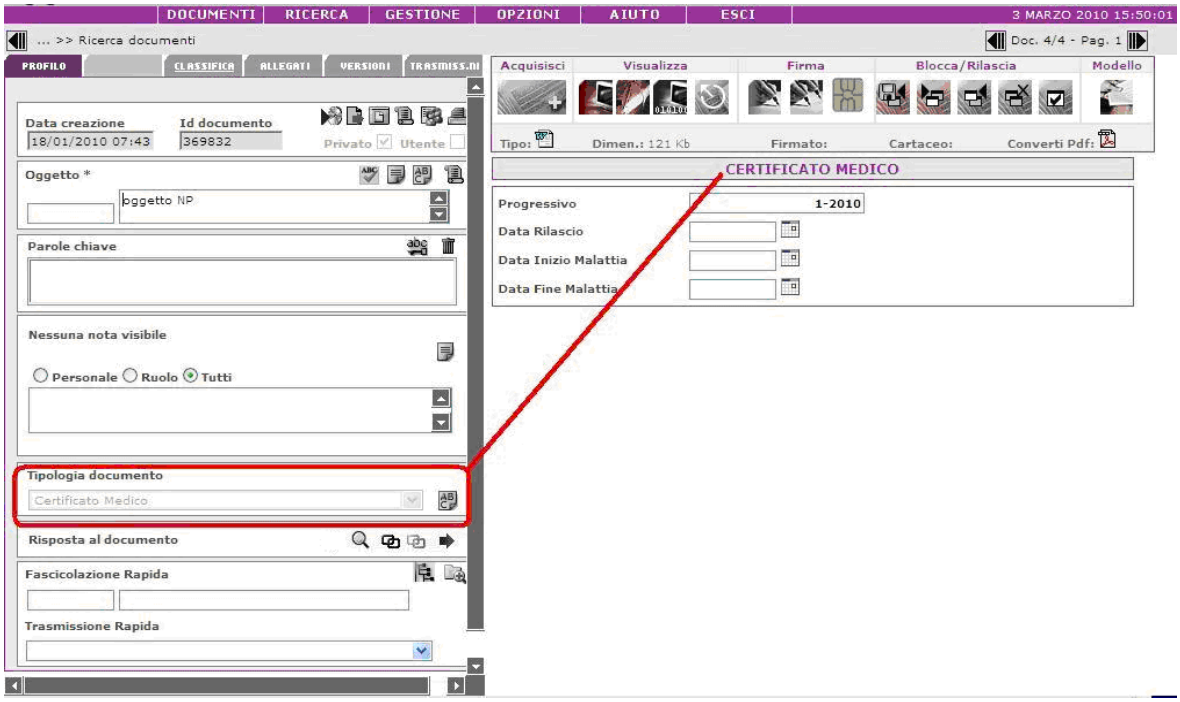


Figura 41 – Tipologia documento

In fase di definizione delle tipologie documentali, mediante il tool di amministrazione, è possibile definire dei "CAMPI COMUNI" che possono essere associati a più tipologie documentali.
All'utente che crea i documenti la presenza di questi campi è trasparente in quanto essi compariranno nel pannello con i campi di profilazione insieme agli altri campi associati al documento.
Nel paragrafo 2.7.1.1 vengono mostrate le tipologie di campo che possono essere associate ad una tipologia documentale.

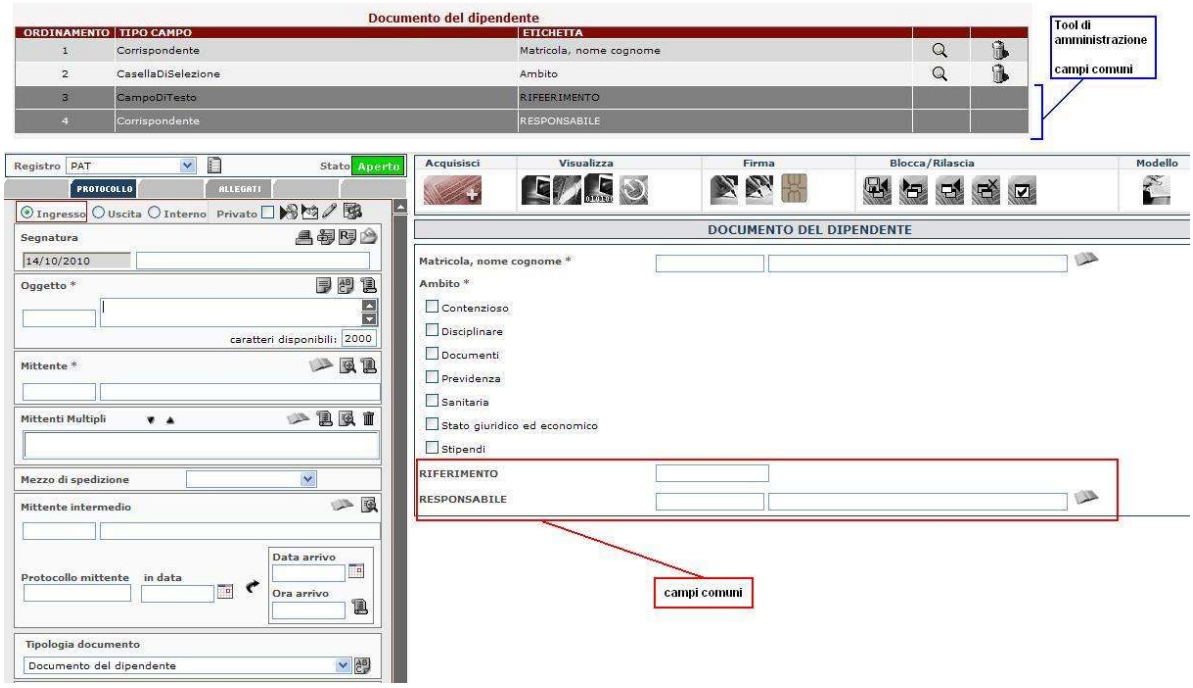


Figura 42 – Tipologia documento- campi comuni

Per le amministrazioni abilitate, è possibile tener traccia delle modifiche effettuate sui campi della tipologia documento (ad eccezione dei campi contatore, oggetti esterni e link). In tal caso, le modifiche apportate ai campi profilati, configurati e impostati con storicizzazione dei valori, sono tracciate dal sistema e sono visibili attraverso la selezione dell'icona (in alto a destra della sezione relativa ai campi profilati). In particolare il sistema registra le informazioni riguardanti la data della modifica, l'utente, il ruolo, il campo modificato, il valore contenuto nel campo prima della modifica (Figura 43). Verrà data evidenza anche della cancellazione/modifica di un corrispondente che compare in un campo di tipo corrispondente di una tipologia di documento.

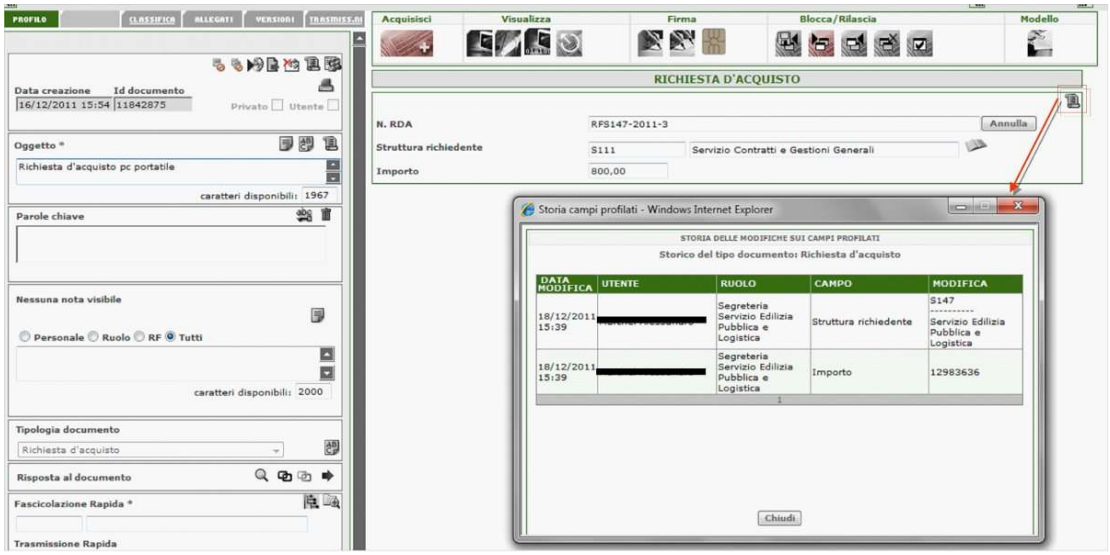


Figura 43 – Tipologia documento- storia delle modifiche dei campi profilati

- **Mittenti multipli**: dato non obbligatorio presente solo per le amministrazioni che ne hanno fatto richiesta. Rappresenta gli ulteriori mittenti di un documento. Nel caso in cui il mittente fosse costituito da un raggruppamento di persone, società, uffici, enti, etc, questo campo dà la possibilità di specificarne tutti i componenti. Anche i mittenti multipli possono essere occasionali (in tal caso può essere inserito liberamente dall'utente valorizzando il campo descrizione del campo mittente e poi spostato mediante la freccia) o abituale, selezionandolo dalla rubrica. Per la selezione da rubrica è necessario premere il pulsante associato al campo. Dalla rubrica sarà possibile utilizzare anche le liste di distribuzione: se si sceglie una lista dalla rubrica dei *mittenti* multipli, gli elementi della lista verranno riportati nel campo multi valore dei *mittenti multipli*. Con il pulsante sarà possibile eventualmente spostare uno dei mittenti nel campo *mittente* (principale). Per le funzionalità relative alla rubrica e al suo utilizzo, si rimanda al Paragrafo 4.5.
  In generale per spostare un nominativo dal campo "mittente" al campo "mittenti multipli" e viceversa selezionare il nominativo di interesse e successivamente l'icona freccia, (per spostarlo verso il basso) o (per spostarlo verso l'alto) a seconda di come si vogliono posizionare i mittenti nell'elenco. (Figura 44)
  La presenza di questo campo è configurabile. Se utilizzato, le ricerche di documenti fatte per mittente prenderanno in considerazione anche i mittenti multipli.
  I dati sui mittenti multipli vengono visualizzati in tutti i punti in cui viene riportato il mittente "principale" (ricerche documenti, lista delle cose da fare, elenco dei documenti presenti in un fascicolo, …).

Figura 44 - Mittenti multipli

- **Mezzo di spedizione**: è costituito da un menù a tendina che propone tutti i mezzi di spedizione creati ed abilitati nell'ambiente di amministrazione VTDOCS.
- **Protocollo mittente**, costituito da due campi: quello di sinistra è destinato a contenere la data di protocollo del mittente mentre quello di destra la stringa di segnatura del mittente. La data và inserita nel formato gg/mm/aaaa; è sufficiente scrivere il giorno, il mese (in formato numerico) e l'anno. I separatori "/" si posizionano in maniera automatica (ad esempio se la data del protocollo mittente è 3 aprile 2002 è sufficiente inserire 03042002 e si visualizza 03/04/2002). L'inserimento non è obbligatorio. A tale campo è associata l'icona "verifica del precedente", che controlla la presenza di documenti già presenti con lo stesso numero di protocollo mittente (insieme all'oggetto ed al mittente).
- **Data arrivo**: indica la data di arrivo effettivo del documento in formato gg/mm/aaaa, digitando semplicemente il giorno, il mese (in formato numerico) e l'anno, i separatori "/" si posizioneranno in maniera automatica. A tale campo è associata la funzionalità di modifica del dato selezionando l'icona che consente di modificare il valore inserito nel campo, salvando la variazione apportata.
- **Ora arrivo**: (presente solo per le amministrazioni che ne hanno fatto richiesta), indica l'ora di arrivo effettivo del documento in formato hh.mm.ss. Digitando semplicemente l'ora, i minuti e i secondi, i separatori "." si posizioneranno in maniera automatica. La visibilità di questo campo è configurabile. Inoltre se tale campo è presente, eventuali modifiche fatte su di esso e/o sulla data di arrivo verranno storicizzate (Figura 45).

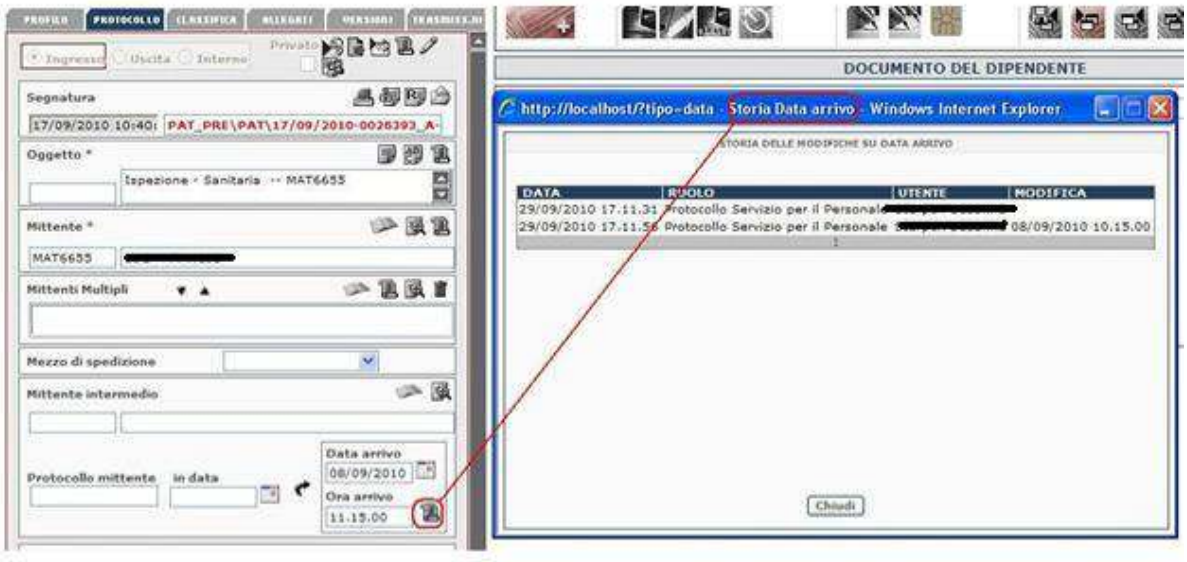


Figura 45 – Ora arrivo

- **Gestione risposta al protocollo**: Questa funzione consente di creare uno o più documenti protocollati o meno, in risposta ad un documento protocollato in ingresso, così come specificato in dettaglio nel paragrafo 2.7.1.5 e mostrato nella Figura 46

Figura 46 - Dettaglio Pulsanti Risposta ad un protocollo in ingresso

- **Fascicolazione rapida**: è possibile effettuare la fascicolazione rapida attraverso la semplice digitazione del codice del fascicolo o del sotto fascicolo (se conosciuto), oppure selezionando l'icona che permette di scegliere (così come descritto dal paragrafo 2.8.1.3) il fascicolo/sotto fascicolo desiderato. Il documento, contestualmente alla creazione del protocollo in ingresso, verrà anche direttamente classificato. È inoltre possibile fascicolare i documenti in modalità "rapida" anche dopo la creazione dei documenti protocollati e non. Se accanto alla dicitura fascicolazione rapida vi è un asterisco, questa è obbligatoria.
  E' anche possibile creare un fascicolo direttamente da questa sezione dove è presente (se la funzionalità è configurata per il ruolo) un ulteriore pulsante ( ) che consente di aprire la finestra per la creazione di un nuovo fascicolo. L'utente pertanto digita il codice del nodo di titolario nel campo presente nella sezione "fascicolazione rapida" ed il fascicolo verrà creato sotto questo nodo.

Figura 47 - Nuovo fascicolo

- **Trasmissione rapida:** è un menù a tendina che contiene una serie di modelli di trasmissione (vedi paragrafo 2.13.4). Selezionando un modello, al momento della protocollazione, il documento verrà anche trasmesso secondo le modalità previste dal modello selezionato. È inoltre possibile trasmettere i documenti in modalità "rapida" anche dopo la creazione dei documenti protocollati e non (tramite il tab 'Trasmissioni'). Se si utilizza un modello di trasmissione contenente una UO fra i destinatari, al momento della trasmissione viene fatto un controllo sull'esistenza dei ruoli di riferimento per la UO stessa. Se non ve ne sono, il sistema mostra un opportuno messaggio e la trasmissione alla specifica UO non viene effettuata.

I pulsanti presenti a fondo pagina permettono di svolgere le seguenti funzioni:

- **Salva:** consente di salvare le successive modifiche che si apportano ai campi contenuti nella sezione 'Protocollo' con opzione 'ingresso', per i quali è prevista la possibilità di modifica. Questo pulsante è abilitato solamente a seguito di protocollazione di un documento premendo sull'icona posta accanto alle opzioni "ingresso" – "uscita".
- **Protocolla**: permette di protocollare il documento ottenendo la stringa di segnatura,
- **Riproponi**: *consente agli utenti abilitati di richiedere la compilazione di una nuova videata di protocollazione che acquisisce in automatico i dati obbligatori dalla schermata di origine.* Cliccando su riproponi il sistema presenterà un messaggio di conferma che richiede se si desidera riproporre anche le immagini del documento principale (ultima versione) e degli allegati del documento originale.
- **Annulla:** ricopre una doppia funzionalità, Annulla documenti predisposti o Annulla documenti protocollati. L'utente può visualizzare lo stato di questo pulsante al passaggio del cursore su di esso.
  - In caso di **Documento predisposto alla protocollazione**, l'utilizzo del pulsante è consentito solo all'utente creatore della predisposizione, se da amministrazione gli sono stati associati i dovuti diritti funzionali.
  - In caso di **Documento Protocollato,** consente all'utente, avente il ruolo opportuno, di annullare la protocollazione effettuata inserendo obbligatoriamente le note d'annullamento.

Tranne il pulsante 'Protocolla', tutti gli altri pulsanti sono abilitatati soltanto dopo la creazione del documento.

Per il campo mittente, è inoltre possibile effettuare le seguenti operazioni tramite selezione della relativa icona:

- : consente di visualizzare i dettagli del nominativo del mittente;
- : consente di modificare il mittente. Viene memorizzata la storia delle modifiche;

-  : consente di visualizzare la storia delle modifiche apportate al corrispondente.

2.7.1.1 Tipologie di documenti

Le tipologie di documenti rappresentano un'estensione di dati con cui poter gestire informazioni più specifiche che caratterizzano sia i documenti protocollati sia quelli non protocollati (o profili). Di seguito è riportata la lista degli oggetti che si possono utilizzare per caratterizzare la tipologia di documenti (analogo discorso vale per le tipologie fascicolo a meno dei campi "Contatore con sottocontatore" e "Etichetta"):

Campo di testo	Per inserire testo libero.
Casella di selezione	Per inserie una serie di opzioni.
Selezione esclusiva	Per selezionare un'opzione particolare.
Menù a tendina	Per selezionare uno degli elementi presenti nella lista.
Campo data	Per aggiungere la data. Nel campo è presente un calendario che facilita l'individuazione della data. Se viene scelto un formato per l'ora accanto al campo data compaiono anche i campi relativi alle ore, ai minuti e ai secondi.
Corrispondente	Per inserire un corrispondente per la tipologia del documento che si sta creando. Nel campo è presente il pulsante che consente di aprire la rubrica e ricercare il corrispondente. E' comunque possibile l'inserimento da codice. Nel caso in cui la parte di codice inserito sia comune a più corrispondenti censiti in rubriche diverse, il sistema mostra l'elenco di tali corrispondenti, da cui l'utente potrà selezionare quello di interesse in base alla rubrica di appartenenza.
Contatore	Per inserire un numero incrementale allo scopo di identificare i documenti. Viene valorizzato in automatico dal sistema. Un contatore può essere normale o di repertorio (per maggiori dettagli si veda il paragrafo 2.9). Il contatore può essere azzerato all'inizio del nuovo anno, oppure su un intervallo temporale a cavallo di due anni consecutivi (contatore custom). In questo caso, se il contatore contiene l'indicazione dell'anno, verranno mostrati sia l'anno di attivazione del contatore che quello di azzeramento del contatore stesso (es.: RFD330-2013/2014-24).
Contatore con sottocontatore	Per inserire un identificativo di documenti costituito da una coppia di incrementi. Viene valorizzato in automatico dal sistema. (Non utilizzabile per i tipi fascicolo)
Link	Per inserire un link esterno al sistema oppure un link ad un documento o ad un fascicolo presenti nel sistema.
Oggetto esterno	Per utilizzare e registrare nel sistema informazioni prese da fonti di dati esterni
Etichetta	E' rappresentata da una label e da una riga sottostante la label e serve per separare ed organizzare meglio i campi. (Non utilizzabile per i tipi fascicolo)

Di seguito vengono descritte le tipologie di campo più complesse da trattare.

2.7.1.1.1 Link

Questo tipo di campo consente di creare dei collegamenti con altri oggetti del sistema VTDOCS oppure con oggetti esterni all'applicazione.

Figura 48 – Campo di tipo link

Se il link è di tipo "esterno" viene mostrato un campo descrizione ed un campo modificabile nel quale l'utente può inserire il riferimento all'oggetto da collegare, generalmente l'url di una pagina web.
Se il link è di tipo "interno" può essere ad un documento o ad un fascicolo presente nel sistema.
In entrambi i casi il sistema presenta un campo descrizione modificabile dall'utente e un campo in cui inserire il riferimento all'oggetto da collegare. Accanto a tale campo si trova il pulsante per consentire all'utente di ricercare l'oggetto da collegare. Cliccando su tale pulsante si apre una finestra che permette di effettuare una ricerca di documenti, oppure di fascicoli, a seconda del tipo di link configurato. L'icona consente di ripulire il campo.

2.7.1.1.2 Oggetto esterno

Questo tipo di campo si presenta con un codice ed una descrizione (nella Figura 49 sono *matricola* e *descrizione*) che devono essere riempiti mediante l'interrogazione di una base di dati esterna. L'accesso alla base di dati esterna per l'utente è trasparente.

Figura 49 – Campo di tipo Oggetto esterno

L'utente può fare una ricerca puntuale per codice oppure una ricerca per descrizione.
Nel primo caso inserisce un valore nel campo codice e poi clicca sulla freccia ▶.
Per effettuare una ricerca per descrizione o per una parte del codice si clicca sul pulsante presente accanto al campo descrizione che nella Figura 49 è rappresentato dall'icona W3C Si apre una finestra che consente di impostare i criteri di ricerca e avviare l'interrogazione mediante il tasto CERCA. I risultati vengono mostrati nel riquadro in basso della finestra consentendo all'utente di selezionare il valore di interesse. Premendo su Ok, il valore selezionato viene riportato nella maschera principale.

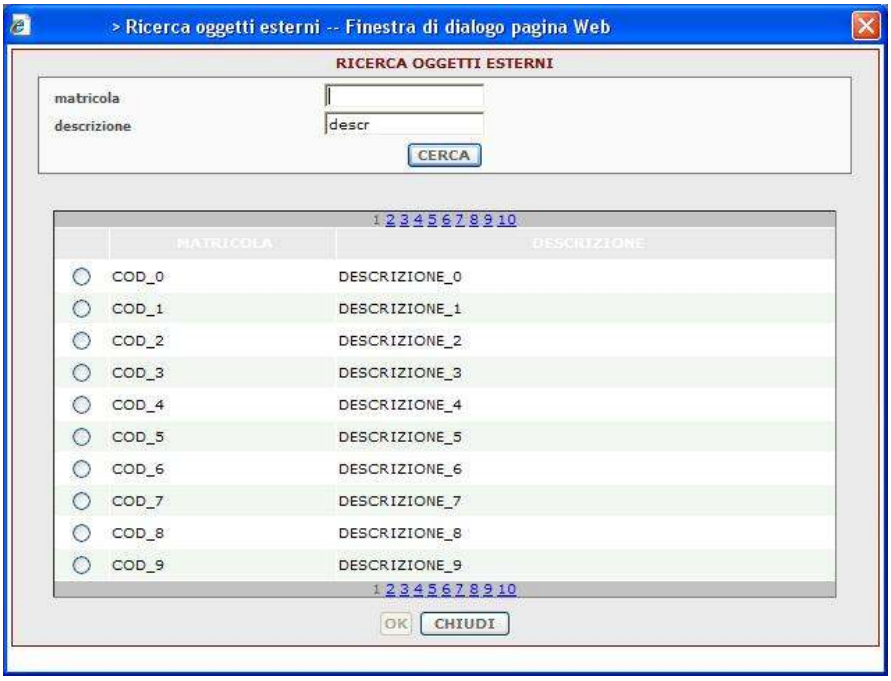


Figura 50 - Ricerca oggetto esterno

Se non si riesce ad accedere al servizio esterno il sistema rende i campi (codice e descrizione) modificabili dando all'utente la possibilità di inserire manualmente le informazioni. Un semaforo rosso mette in evidenza tale situazione. Il sistema inoltre tiene traccia dei dati che non sono stati inseriti da fonti esterne in modo tale che in un momento successivo gli utenti saranno in grado di riconoscerli ed eventualmente aggiornarli con le informazioni prese dalle fonti originali. I campi digitati manualmente sono riconoscibili perché a caratteri rossi fino a quando non saranno valorizzati successivamente con il dato esterno (*Figura 51*).
Accanto al campo descrizione dell'oggetto esterno è presente il pulsante (Figura 49) che consente di ripulire i campi impostati tramite selezione di uno dei valori presenti.

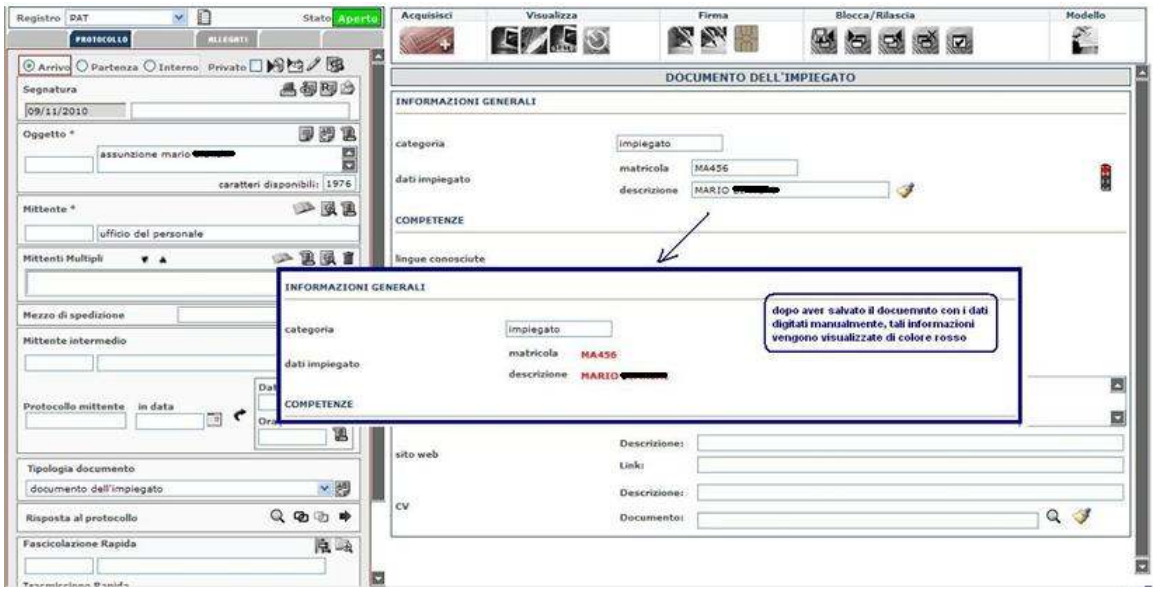


Figura 51 - Accesso alla base di dati esterna non disponibile. Campi editati dall'utente

2.7.1.2 **Acquisizione documento prima del salvataggio dei metadati**

E' possibile associare un file ad un documento e uno o più allegati prima di ogni altra operazione di inserimento e registrazione del documento stesso (solo se il sistema è stato configurato dall'amministratore per l'acquisizione del file prima della esecuzione della registrazione di protocollo o creazione di un documento non protocollato).

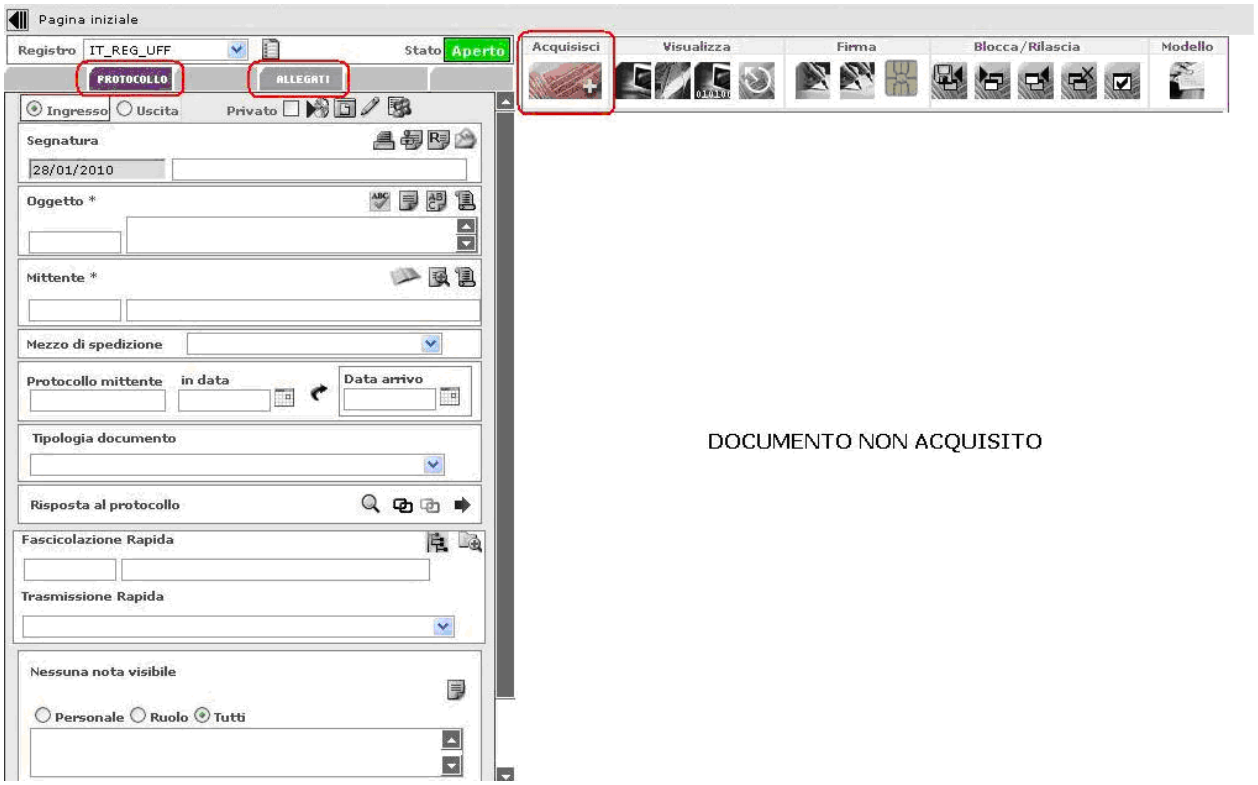


Figura 52 - Acquisizione del documento prima del salvataggio

2.7.1.3 Funzionalità di supporto alla protocollazione

2.7.1.3.1 Oggettario

L'oggettario si richiama attivando l'apposita icona posta vicino al campo oggetto presente sia nella sezione di protocollazione sia nella sezione di profilo di un documento non oggetto di protocollazione.

La selezione dell'icona comporta l'apertura di una nuova finestra di dialogo come mostrato nella figura che segue.

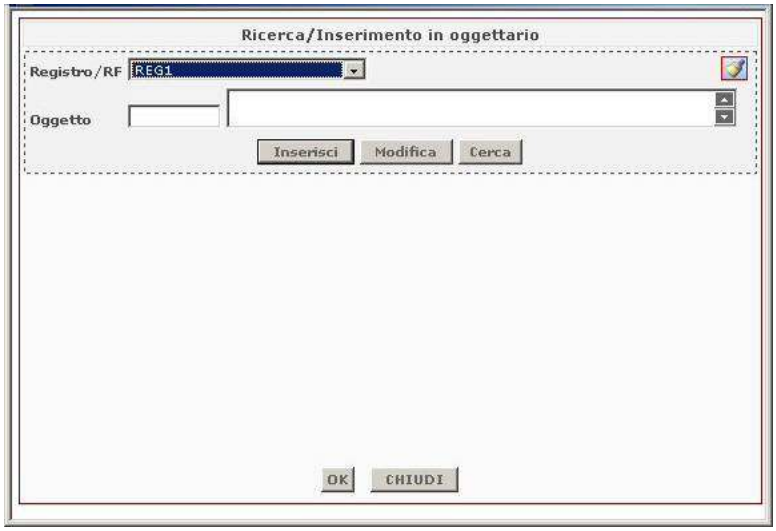


Figura 53 – Oggettario

Il pannello presente nella Figura 53 consente di:

- *cercare un oggetto tra quelli inseriti nella base dati*: La ricerca è effettuata attraverso tre differenti parametri: Registro/RF, Codice, Oggetto.
  - Registro/RF: è il registro/RF cui è visibile l'oggetto: il campo è selezionabile tramite un menù a tendina. I possibili valori sono "TUTTI", ossia l'insieme di tutti i registri dell'AOO, e i valori relativi ai registri cui l'utente può accedere in base alla configurazione del proprio ruolo;
  - Codice: campo in cui può essere inserito il codice esatto da ricercare;
  - Oggetto: campo in cui può essere inserita una parola (o parte di essa);

  Se si vuole pulire velocemente il campo dove è presente la descrizione dell'oggetto è possibile selezionare l'icona .

  Dopo aver popolato uno o entrambi i campi, selezionando il pulsante Cerca vengono mostrati tutti gli oggetti legati al registro selezionato, indicando per ciascuno il "Codice", la "Voce oggettario", il "Registro" a cui è associato e l'icona che permette di selezionare l'oggetto (come mostrato in Figura 54).

Figura 54 – Oggettario: cerca oggetto dalla sezione Profilo

- *inserire un nuovo oggetto nella base dati dell'oggettario*: l'inserimento è effettuato sempre attraverso i parametri: Registro, Codice, Oggetto. La funzionalità di inserimento è disponibile solo per i Ruoli in UO abilitati dall'Amministratore del sistema.
  Registro/RF: è il registro/RF cui è visibile l'oggetto: può essere selezionato tramite un menù a tendina. I possibili valori sono "TUTTI", ossia l'insieme di tutti i registri dell'AOO, e i valori relativi ai registri cui l'utente può accedere in base alla configurazione del proprio ruolo;
  Devono essere quindi valorizzati i campi:
  - codice: il codice da associare all'oggetto da inserire;
  - oggetto: il testo da inserire nel campo oggetto (dato obbligatorio); se si vuole pulire velocemente il campo dove è presente la descrizione dell'oggetto è possibile selezionare il pulsante ;

  Dopo aver selezionato Registri/RF e popolato adeguatamente gli altri due campi si seleziona il pulsante Inserisci; l'oggettario mostra la parte "Codice" che rappresenta il codice associato all'oggetto inserito, "Voce oggettario" che rappresenta il testo inserito, il "Registro/RF" a cui è stata associata la voce oggettario, e l'icona che permette di selezionare l'oggetto. Se l'oggetto è già presente nell'oggettario, compare una finestra di dialogo con dicitura: "Oggetto già presente".

Figura 55 – Inserisci oggetto in oggettario

- *selezionare ed inserire l'oggetto*: per inserire un testo nel campo Oggetto, dopo aver eseguito i passi descritti ai punti precedenti, si seleziona l'icona associata al testo a cui si è interessati e si preme il pulsante OK: il valore viene riportato nel campo del pannello da cui è stato richiamato l'oggettario.
- *modificare un elemento presente in oggettario*: la modifica di un elemento presente in oggettario, così come per l'inserimento, è disponibile solo ai Ruoli in UO abilitati dall'Amministratore del sistema. Per effettuare l'operazione su un elemento presente in oggettario , si seleziona l'oggetto da modificare, si apportano le modifiche e si preme il pulsante "modifica" per confermare l'operazione effettuata.
- *cancellare un elemento presente in oggettario*: la cancellazione di un elemento presente in oggettario è disponibile solo ai Ruoli in UO abilitati dall'Amministratore del sistema. Per l'eliminazione di un elemento selezionare l'icona cestino presente in corrispondenza dell'elemento che si vuole cancellare.

2.7.1.3.2 Rubrica per la selezione del mittente

Mediante l'icona , presente nella pagina di protocollo in ingresso, è possibile accedere alla Rubrica dei corrispondenti per la selezione del mittente.
Nel protocollo in ingresso, il mittente può essere occasionale, interno alla AOO su cui si sta protocollando, esterno ad essa o esterno all'Amministrazione.
Per i dettagli relativi alla rubrica, quali filtri di ricerca possibili, presentazione dei risultati e funzionalità ad essa collegate si rimanda al paragrafo 4.5.2.

2.7.1.4 Protocollazione in ingresso di una mail con i relativi allegati elettronici inoltrata da MS Outlook

Utilizzando la funzione di INOLTRA (FORWARD) presente sul client di posta è possibile inviare una mail ad una casella istituzionale per poi poterla protocollare in ingresso. L'utente, ricevuto il messaggio in una casella di posta adibita alla ricezione delle mail da protocollare, lo seleziona e poi lo inoltra alla casella istituzionale associata al registro di protocollo desiderato.

Attraverso l'operazione di consultazione della casella istituzionale prevista da VTDOCS, i messaggi di posta elettronica inoltrati alla casella stessa sono acquisiti e lavorati dal sistema. Ciascun messaggio viene inserito in VTDOCS come documento predisposto alla protocollazione con i seguenti dati impostati in modo automatico dal sistema:

Componente del messaggio di posta elettronica	Componente del documento in VTDOCS
From	**MITTENTE**
Subject	**OGGETTO**
Corpo (body)	**DOCUMENTO PRINCIPALE**
Attachment	**ALLEGATI**

Il documento è trasmesso a tutti i ruoli protocollisti configurati come destinatari dei protocolli ricevuti per interoperabilità. Inoltre, per permettere all'utente che ha inviato il messaggio originale alla casella istituzionale di acquisire la visibilità sul protocollo in ingresso creato, VTDOCS invia una trasmissione all'utente stesso, ricavando i dati dell'utente dall'indirizzo del mittente della mail (Tutti gli utenti censiti in VTDOCS devono avere indicato il relativo indirizzo di posta elettronica.).
L'utente deve avere configurato anche l'invio della mail associata alla trasmissione, così tramite una mail riceve la notifica dell'effettiva protocollazione del documento.

Il protocollo presenta nel campo mittente intermedio (campo opzionale) l'utente che ha effettuato l'INOLTRO.
Per poter utilizzare al meglio questa funzionalità è necessario impostare il client di posta elettronica, in modo che il messaggio mail originale sia inserito come allegato ogni qual volta lo si inoltra con un altro messaggio mail.

Questa impostazione è molto semplice, come mostrato nelle Figura 56, Figura 57:

- Selezionare dal menu Standard di Outlook la voce "Tools" (Impostazioni).
- Selezionare la voce "Options" (opzioni).
- Nella finestra successiva selezionare la voce "Email Options"(Opzioni Mail)
- Nella finestra successiva selezionare dal menu a tendina "when forwarding a message" (Quando Inoltro una mail), la voce "Attach original message" (inserisci messaggio originale come allegato).
- premere "OK".

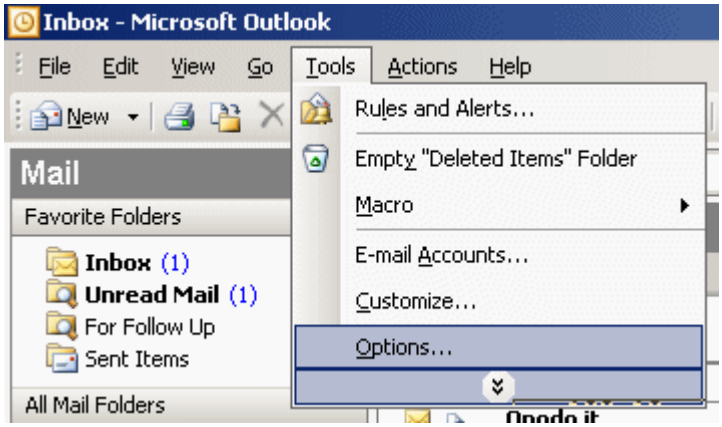


Figura 56 – Impostazioni MS Outlook

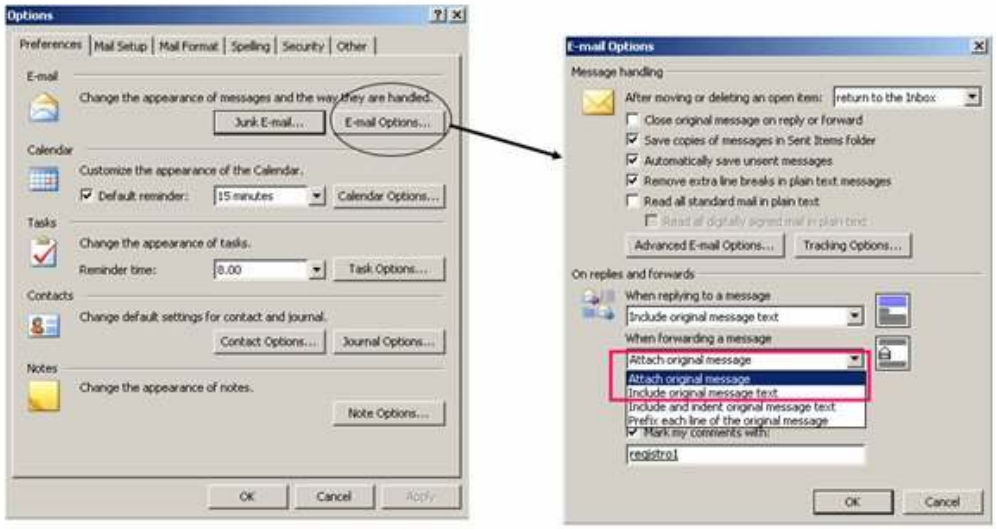


Figura 57 – Impostazioni Outlook

Se le impostazioni descritte hanno avuto successo, effettuando l'inoltro della mail il nuovo messaggio di posta elettronica si presenta come mostrato in Figura 58.

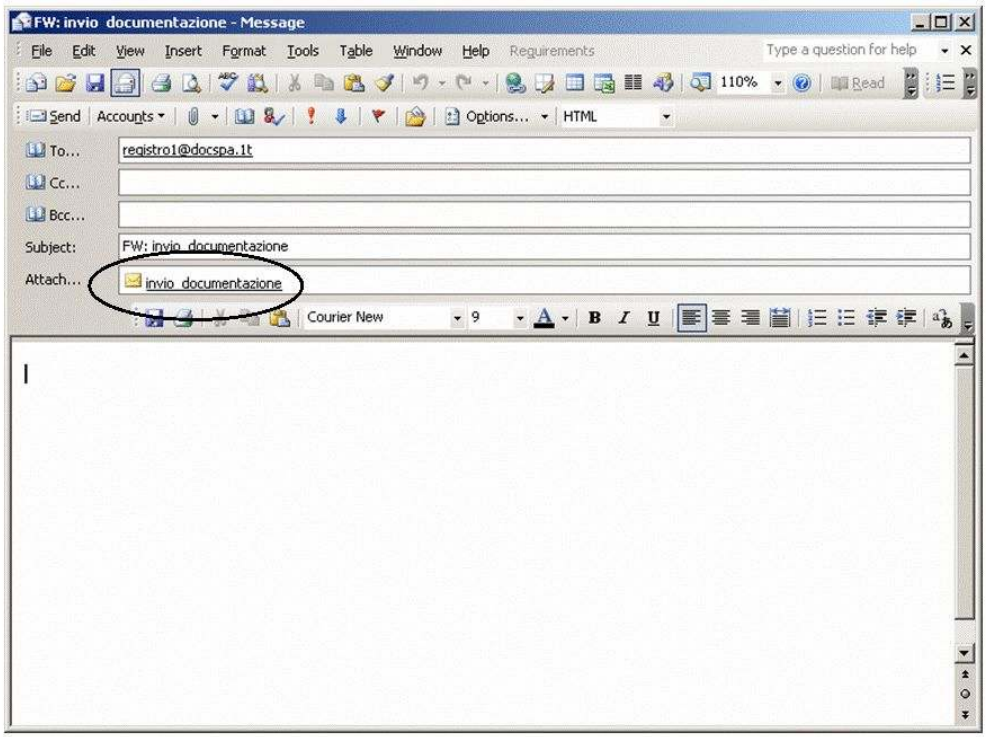


Figura 58 – Formato mail inoltrata in MS Outlook

Il protocollo così creato presenta come documento principale il testo della mail, mentre il documento principale inviato è registrato come uno degli allegati. Per risolvere questa inversione, è disponibile per l'utente una funzionalità che permette lo SCAMBIO di un allegato con il documento principale. Tale funzionalità è fruibile attraverso un tasto apposito della scheda Allegati. L'utente seleziona l'allegato che costituisce il documento principale e premendo il tasto SCAMBIA tale allegato viene scambiato con il documento principale.

2.7.1.5 Documenti di risposta

2.7.1.5.1 Creazione di un protocollo in risposta ad un documento protocollato in ingresso.

Questa funzione consente di creare una o più risposte ad un documento protocollato in ingresso. La funzionalità è accessibile a partire dalla scheda del documento protocollato in ingresso mediante l'icona presente nell'area "Risposta al protocollo" (Figura 59). Cliccando su tale pulsante viene predisposto un protocollo in uscita ma l'utente può modificare la tipologia del documento di risposta.
Pertanto la risposta ad un documento in ingresso potrà essere:

1. un *documento in uscita* o *predisposto in uscita* la cui scheda sarà automaticamente popolata nel modo seguente:
   - Il "*Destinatario*" coincide con il "*Mittente*" del protocollo in ingresso a cui si sta rispondendo
   - L'"*Oggetto*" coincide con l'"*Oggetto*" del protocollo in ingresso a cui si sta rispondendo.

2. un *documento in ingresso o predisposto in ingresso o un documento interno o predisposto interno* la cui scheda sarà automaticamente popolata nel modo seguente:
   - L'"*Oggetto*" coincide con l'"*Oggetto*" del protocollo in ingresso a cui si sta rispondendo.

Si noti che la possibilità di creare protocolli diversi da quello in uscita o predisposto in uscita è una funzionalità aggiuntiva configurabile e che il comportamento classico è quello di creare come risposte solo protocolli in uscita.

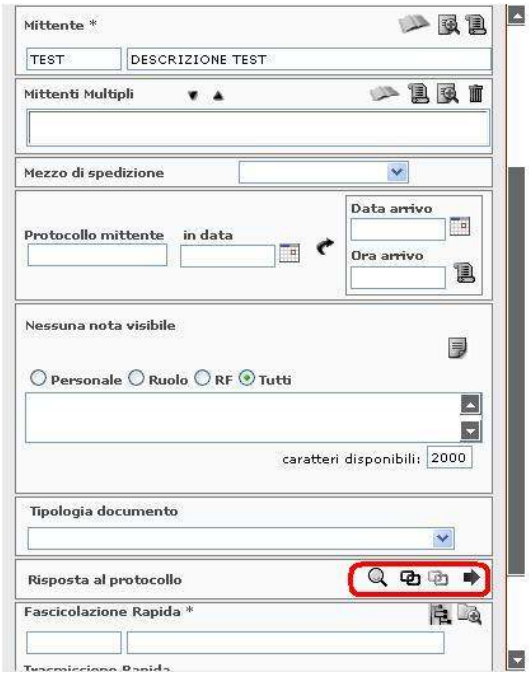


Figura 59- Risposta al protocollo in ingresso

2.7.1.5.2 Creazione di un documento non protocollato in risposta ad un documento protocollato in ingresso.

Questa funzione consente di creare una o più risposte ad un documento protocollato in ingresso. La funzionalità è accessibile a partire dalla scheda del documento protocollato in ingresso mediante l'icona presente nell'area "Risposta al protocollo" (Figura 59); cliccando su tale pulsante viene predisposta la scheda di profilo di un documento grigio popolata automaticamente nel seguente modo:

- L'"*Oggetto*" coincide con l'"*Oggetto*" del protocollo in ingresso a cui si sta rispondendo.

La possibilità di creare come risposte di un documento protocollato un documento grigio è una funzionalità aggiuntiva configurabile. Se non è attiva l'icona ad essa corrispondente non è attiva.

2.7.1.5.3 Documento protocollato in ingresso come risposta ad un documento (protocollato o non).

Questa funzionalità consente di creare un documento in arrivo come risposta di un documento già presente nel sistema (protocollato o no).

La funzionalità è accessibile, a partire dalla scheda del documento in arrivo in fase di protocollazione, mediante l'icona , presente nell'area "Risposta al protocollo" (Figura 59). Tale selezione consente l'apertura di una finestra di dialogo (Figura 60) per individuare, attraverso dei filtri di ricerca, il documento cui il documento in ingresso costituirà una risposta.

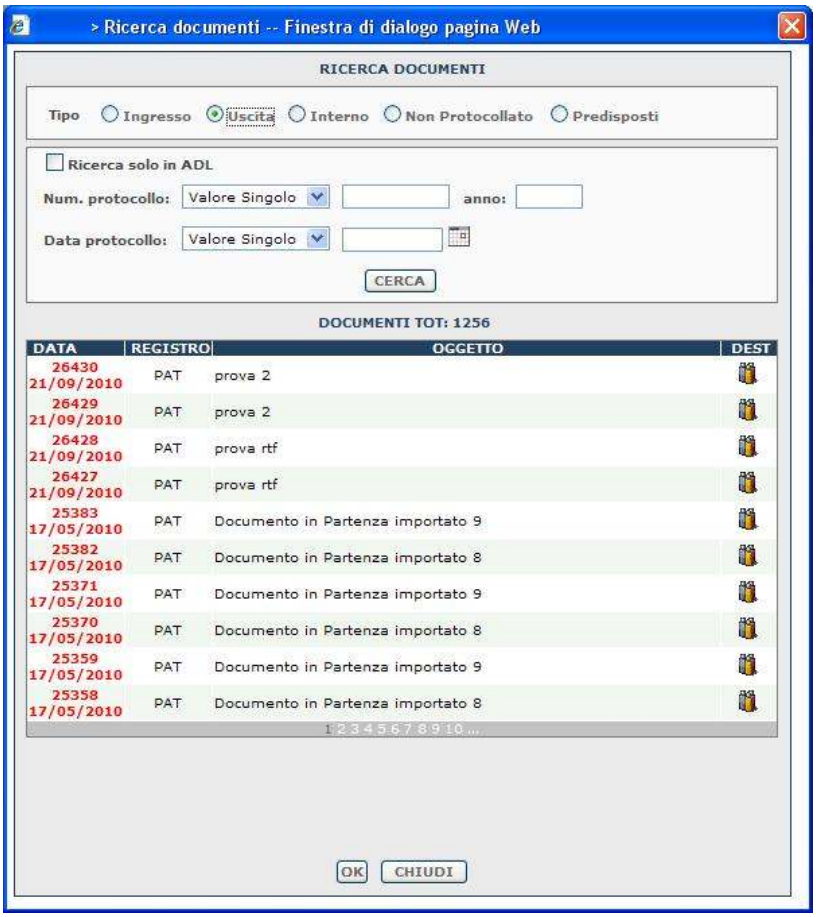


Figura 60 - Ricerca dei documenti cui rispondere

La finestra di dialogo presenta, nella parte superiore, dei filtri di ricerca (Figura 60):

- una casella di opzione "Ricerca solo ADL", che, se selezionata, disabilita tutti gli altri filtri di ricerca e consente di ricercare tutti i documenti contenuti nell'"Area di lavoro" (ADL) dell'utente;
- il tipo documento (protocollato in ingresso, in uscita, interno, non protocollato o predisposto) se si seleziona un documento protocollato appaiono i seguenti filtri:
  - numero di protocollo che, mediante scelta da menù a tendina, consente di inserire un "valore singolo" oppure un "intervallo" di valori relativi numero di protocollo del documento che si sta ricercando;
  - data protocollo che, mediante scelta da menù a tendina, consente di inserire un "valore singolo" oppure un "intervallo" di valori relativi alla data di creazione del documento in uscita che si sta ricercando.

  Se si seleziona un documento non protocollato appaiono i seguenti filtri:
  - id documento che, mediante scelta da menù a tendina, consente di inserire un "valore singolo" oppure un "intervallo" di valori relativi all'id del documento che si sta ricercando;

- data creazione che, mediante scelta da menù a tendina, consente di inserire un “valore singolo” oppure un “intervallo” di valori relativi alla data di creazione del documento che si sta ricercando.

La tipologia selezionata di default è “Uscita”.
La parte centrale mostra l’elenco dei documenti che soddisfano i criteri di ricerca.
Quando si individua il documento cui collegare il documento in arrivo, lo si seleziona e si conferma premendo il pulsante “OK”. A questo punto il sistema effettua dei controlli per verificare la congruenza dei dati tra i due documenti che si desidera collegare, in particolare, sul valore specificato nel campo oggetto e mittente.
L’utente prima di selezionare un documento può aver compilato, anche parzialmente, la scheda del protocollo in ingresso.
Se vengono trovati dei dati incongruenti, il sistema presenta una maschera di avviso nella quale vengono proposte tre strade alternative per il completamento dell’operazione (Figura 61):

- Continua e sovrascrivi i dati: consente di proseguire l’operazione utilizzando i valori del documento selezionato. Questa è l’opzione predefinita;
- Continua utilizzando i dati immessi: consente di proseguire il collegamento dei documenti con i dati immessi dall’utente nella scheda del protocollo in ingresso, nonostante siano diversi da quelli del documento a cui si sta rispondendo;
- Seleziona un altro documento: consente di chiudere la pagina di avviso e scegliere un altro protocollo in uscita a cui rispondere.

Figura 61 – Finestra di dialogo per avviso dati incongruenti per risposta ad un protocollo in uscita

Nel momento in cui si preme il pulsante OK, la scheda di protocollo in ingresso viene popolata in base all’opzione che è stata selezionata.
Inoltre, se è stato selezionato un documento in uscita che ha un solo destinatario esso diventerà il mittente del documento in ingresso. Se invece il protocollo in uscita ha più destinatari l’utente potrà scegliere quale utilizzare come mittente:

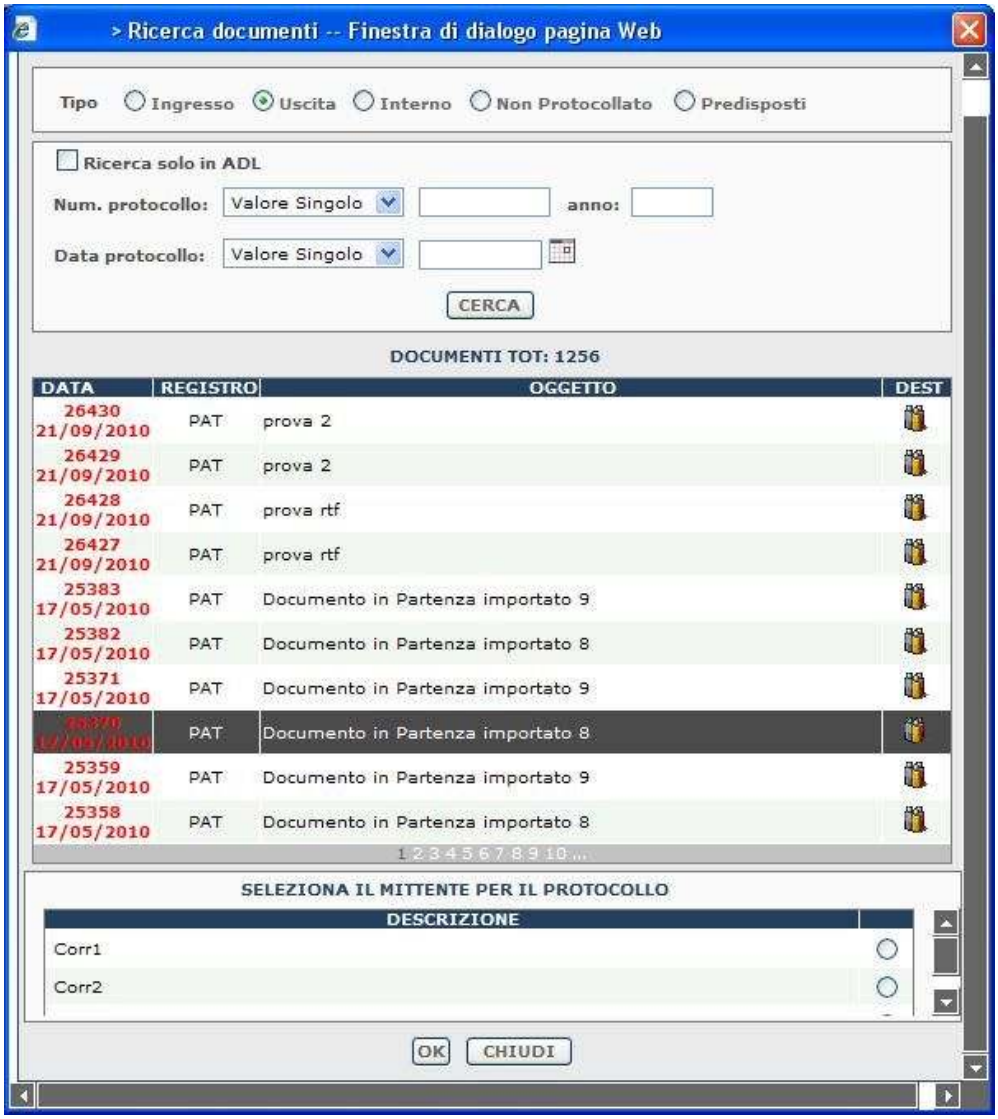


Figura 62 – Ricerca dei documenti in uscita cui rispondere

La parte inferiore della finestra di dialogo viene visualizzata selezionando l'icona relativa ad un documento presente nell'elenco dei risultati e mostra l'elenco dei destinatari indicati nel documento selezionato. L'utente dovrà indicare quale destinatario di quel documento si vuole sia il mittente del protocollo in ingresso che si sta registrando. Ciò deve essere fatto selezionando uno dei destinatari dall'elenco proposto e confermando con il pulsante "OK".

A questo punto selezionando il pulsante Protocolla, il documento viene protocollato e collegato al documento desiderato.

E' possibile collegare un documento in ingresso come riposta ad un altro documento in due momenti:

- In fase di creazione di un protocollo in ingresso, come già descritto;
- A partire da un protocollo in ingresso creato precedentemente.

Nel secondo caso, in cui l'utente desidera collegare un documento in ingresso già registrato precedentemente con un documento anch'esso già registrato, le operazioni da eseguire sono analoghe a quelle già descritte. Si cerca il documento in ingresso che si vuole collegare, se ne visualizzano i dettagli, e, sempre attraverso l'utilizzo dell'icona , si cerca il documento di cui il documento in ingresso in questione costituirà una risposta.
In questo caso, se nei due documenti i valori del campo oggetto e mittente/destinatario (nel caso di scelta di un documento protocollato) non coincidono, stante il fatto che non è possibile modificare una registrazione di protocollo l'utente avrà due opzioni: continuare comunque l'operazione, lasciando inalterate le registrazioni di entrambi i documenti, oppure selezionare un altro documento in archivio (Figura 63).

Figura 63 – Finestra di dialogo per avviso dati incongruenti per risposta ad un protocollo in entrata

Una volta confermata la selezione di un documento:

- Viene popolato il campo "Risposta al protocollo" del documento in ingresso con la segnatura o l'id documento dell'uscita protocollo o del documento protocollato a cui si sta rispondendo;
- Viene abilitato il pulsante Salva.

Confermata l'operazione di collegamento con il pulsante "Salva" verrà effettuato il collegamento tra i documenti in questione.
Un protocollo in ingresso può costituire una risposta per un solo documento quindi la funzione "Cerca documenti in uscita" sarà disattivata se il documento in ingresso è già collegato ad un documento.

C'è da mettere bene in evidenza che il procedimento illustrato è relativo al caso più generico di documenti di risposta di qualsiasi tipo. Nella modalità classica la ricerca dei documenti a cui rispondere sarà limitata ai soli documenti in uscita.
Subito dopo la protocollazione o in qualunque momento successivo è possibile visualizzare il dettaglio del protocollo a cui si è risposto mediante l'uso dell'icona .
Un protocollo in ingresso può essere la risposta di un solo documento ma può avere più risposte.

Dalla scheda di un documento protocollato in ingresso è possibile visualizzare la lista dei relativi documenti in risposta mediante l'uso dell'icona . Si apre una pagina che mostra tutti i documenti che rispondono a quel particolare protocollo in ingresso (Figura 64).

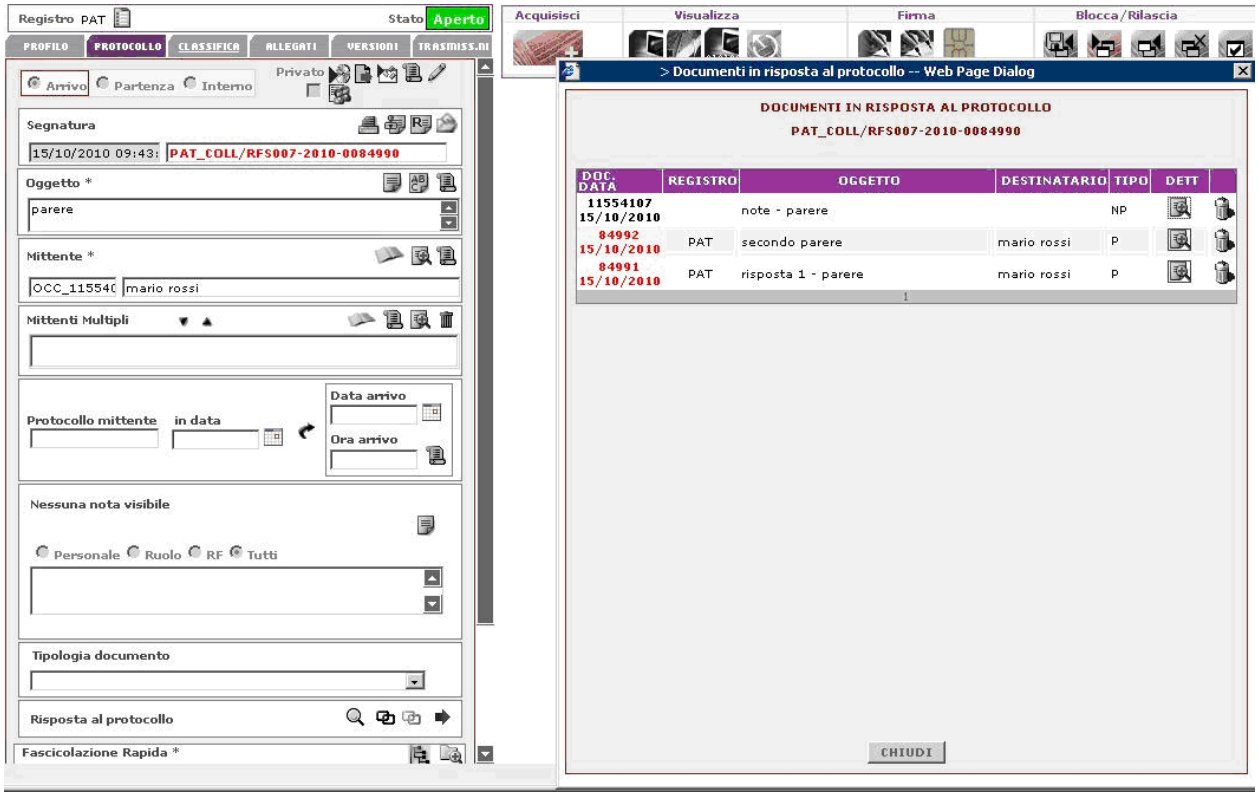


Figura 64 – Documenti di risposta di un protocollo in ingresso

L'icona consente di visualizzare la scheda del protocollo di risposta corrispondente, da dove sarà possibile ritornare alla scheda del documento in uscita dal quale si è partiti.
L'icona consente di eliminare quella particolare risposta dalla lista delle risposte del protocollo in uscita in questione.

2.7.1.6 Consolidamento di un documento

Su un documento (protocollato o non) è possibile applicare una funzione di "consolidamento", a due stadi, irreversibile. Il primo stadio è detto "Consolidamento documento", il secondo "Consolidamento metadati" Se tale funzione viene applicata:

Stadio 1 (Consolidamento Documenti):
Non sarà possibile:

- Aggiungere / Eliminare versioni
- Aggiungere / Eliminare allegati della tipologia "Inseriti dall'utente" o modificare versioni di allegati
- Firmare
- Predisporre alla protocollazione

Stadio 2 (Consolidamento Metadati)
Non sarà possibile

- Modificare l'oggetto
- Modificare mittente(i) / destinatario(i)
- Modificare la data arrivo
- Modificare l'ora arrivo
- Annullare la registrazione di protocollo

Continuerà ad essere possibile:

- Inserire / modificare note (personale, ruolo, RF, tutti)
- Inserire / modificare i dati del profilo dinamico
- Inserire parole chiave
- Apporre il time stamp
- Classificare e De-classificare / Fascicolare e De-fascicolare
- Trasmettere il documento
- Associare gli allegati automatici relativi alle ricevute PEC

Una scritta presente nelle pagine di dettaglio del documento metterà in evidenza che il documento è nello stato:

- Consolidato contenuto
- Consolidati contenuto e metadati

Questa azione può essere eseguita dalla pagina di profilo e di protocollo di un documento dove sono presenti due nuovi pulsanti. Sarà inoltre possibile consolidare più documenti come azione massiva presente nella pagina di ricerca dei documenti. Per i dettagli si rimanda al paragrafo 3.1.1.1

Il consolidamento dei documenti è una funzionalità attivabile tramite chiave di configurazione e può essere eseguito solo dai ruoli abilitati a tali azioni.

2.7.2 Protocollo in Uscita[2]

Per creare un nuovo protocollo in uscita è necessario selezionare dal menù principale la voce "Documenti" e successivamente la voce "Nuovo protocollo".

Il pannello, riportato in Figura 65, (come per il protocollo in ingresso), mostra in alto la descrizione e lo stato del registro sul quale si sta operando. Il registro in cui inserire i documenti può essere selezionato dal menù a tendina impostato in modo automatico dal sistema, collocato sotto la descrizione del ruolo a cui l'utente appartiene. Ogni utente ha a disposizione tutti i registri sui quali è abilitato a lavorare in relazione al ruolo che ricopre nell'amministrazione di appartenenza. Ogni stato del registro è rappresentato da un colore, ovvero:

- Rosso __ indica che il registro è chiuso;
- Verde __ indica che il registro è aperto;
- Giallo __ indica che la data di apertura del registro è precedente alla data odierna.

[2] L'etichetta "uscita" è configurabile mediante il tool di amministrazione. Alcune amministrazioni usano infatti la parola "Partenza". Nelle figure del documento è pertanto possibile vedere nomi diversi.

Nella parte sottostante a quella dei registri, si devono selezionare:

- 

: pulsante di selezione per indicare se il protocollo che si sta creando è in ingresso, in uscita o è interno. Per effettuare la protocollazione in uscita si deve selezionare l'opzione "Uscita".;
- 

: selezione "Privato"; se valorizzato, indica che il protocollo che si sta creando non eredita la visibilità dai ruoli gerarchicamente superiori; quindi il protocollo con questa opzione risulta visibile soltanto agli utenti appartenenti allo stesso ruolo dell'utente che lo ha creato. All'atto della fascicolazione e/o della trasmissione si amplia la visibilità del protocollo;
-  : consente di inserire il documento nell'Area di lavoro (si veda il paragrafo 3.5.1);
-  : consente di effettuare singole modifiche nel documento dopo la protocollazione;
-  : consente di visualizzare le utenze (quindi ruoli/utenti) che hanno visibilità sul documento e come hanno acquisito tale visibilità. Per i ruoli abilitati dall'amministratore è possibile, tramite un apposito pulsante all'interno della maschera di visibilità, rimuovere i diritti di un ruolo o di un utente. L'operazione può essere revocata. Non è possibile rimuovere i diritti di proprietà. Per ulteriori dettagli si veda il paragrafo 2.8.1.1;
-  : consente di visualizzare tutte le operazioni che avvengono sul documento;
-  : consente di visualizzare la storia del processo di conservazione a cui è stato sottoposto il documento.
-  : consente di visualizzare, se presenti, le notifiche relative alla spedizione del documento dai destinatari della spedizione.
-  : consente di consolidare un documento nella parte relativa a versioni ed allegati
-  : consente di consolidare totalmente un documento, nella parte relativa a versioni ed allegati (se il documento non è stato consolidato parzialmente dalla funzione sopra descritta) e nei metadati. Per i dettagli si rimanda al paragrafo 2.7.1.6.

I dati relativi ad un documento da protocollare in uscita sono i seguenti:

- **Segnatura:** la stringa di segnatura viene impostata automaticamente dal sistema in base a regole prefissate ed è costituita da diversi parametri configurabili mediante l'applicazione di amministrazione, come il numero di protocollo, data e anno di protocollazione (che coincide con la data di ultima apertura del registro), codice del registro, codice dell'amministrazione. A questo campo sono associate le seguenti icone:
  -  : consente di stampare la segnatura tramite una stampante di etichette;
  -  : permette, dopo la protocollazione del documento, di stampare su un foglio A4 bianco la segnatura del protocollo effettuato, secondo le coordinate impostate dall'utente oppure di stampare il timbro sempre su A4 bianco (così come mostrato nella Figura 38);
  -  : permette, dopo la protocollazione del documento, di stampare la ricevuta di protocollo in formato Word rispetto ad un modello pre-impostato dall'Amministratore di sistema per ogni registro. Se diversamente configurato, il sistema consente di stampare la ricevuta in formato pdf. In tal caso il modello da impostare dal tool di amministrazione dovrà essere in formato pdf.
  -  : permette di spedire la ricevuta di ritorno al mittente di un documento trasmesso per interoperabilità.

  Quando il puntatore del mouse passa sul campo segnatura viene attivato lo zoom che consente di ingrandire le dimensioni del campo rendendolo più leggibile.

- **Oggetto**: dato obbligatorio. Rappresenta una breve descrizione del documento che si sta protocollando. Può essere una descrizione occasionale, quindi scritta liberamente dall'utente,

oppure un valore selezionato da una lista memorizzata, che è possibile raggiungere selezionando l'icona . Se si inserisce una descrizione occasionale è possibile effettuare il controllo ortografico su quanto editato nel campo oggetto attraverso la selezione del pulsante , che apre la finestra di dialogo mostrata nella Figura 78. Inoltre è possibile valorizzare il campo oggetto anche attraverso la digitazione del codice associato all'oggetto necessario collegato al Registro/RF di interesse. In tal caso, dopo aver digitato il codice oggetto, se si sposta il cursore in un altro campo qualsiasi del modulo, l'applicazione automaticamente valorizza il campo di testo, posto a fianco, con la descrizione associata al codice digitato, prelevandoli dall'oggettario. Se l'oggetto che si vuole inserire non è presente nell'oggettario, è possibile inserirlo accedendo alla maschera dell'oggettario premendo l'icona , digitando codice e descrizione nel campo oggetto e premendo il pulsante Inserisci. Quando nel campo oggetto viene digitato un testo molto lungo, per leggere interamente quanto in esso contenuto, basta selezionare l'icona . E' inoltre possibile visualizzare la storia delle modifiche ad esso apportate tramite l'icona .

- **Destinatario**: dato obbligatorio. Come per l'oggetto, anche il destinatario può essere occasionale (in tal caso può essere inserito liberamente dall'utente valorizzando il campo descrizione mediante la tastiera) o abituale, selezionandolo dalla rubrica. Per la selezione da rubrica è necessario premere il pulsante associato al campo "Destinatario". Nel caso del protocollo in uscita, i destinatari possono essere occasionali, interni alla AOO su cui si sta protocollando, esterni ad essa o esterni all'Amministrazione. Per le funzionalità relative alla rubrica e al suo utilizzo, si rimanda al Paragrafo 4.5. Inoltre è possibile valorizzare il campo destinatario anche attraverso la semplice digitazione del codice rubrica associato al corrispondente di interesse. In tal caso, dopo aver digitato il codice rubrica, se si sposta il cursore in un altro campo qualsiasi del modulo, l'applicativo automaticamente valorizza il campo di testo, posto a fianco, con il nominativo o la descrizione associata al codice digitato, prelevandoli dalla rubrica. Se il destinatario interessato è presente in rubrica è possibile inserirlo nella lista dei destinatari mediante l'icona . Se invece è assente, viene mostrato all'utente un avviso di errore del tipo "Codice rubrica non esistente".
  Il campo destinatario può consentire (per le amministrazioni che ne hanno fatto richiesta) l'integrazione con la tecnologia ajax per le ricerche in rubrica. In particolare, se attivata questa integrazione, viene visualizzato un campo in corrispondenza del campo destinatario. Su tale campo è stata attivata la funzione di auto completamento di Ajax che fornisce dei suggerimenti sulle parole da inserire nel campo destinatario sulla base delle prime lettere digitate.
  Il numero dei caratteri a partire dai quali visualizzare i suggerimenti è configurabile; i dati sono prelevati direttamente dalla rubrica (descrizione dei corrispondenti).
  Per spostare un nominativo dal campo "destinatario" al campo "destinatario cc" e viceversa selezionare il nominativo di interesse e successivamente l'icona freccia, (per spostarlo verso il basso) o (per spostarlo verso l'alto) a seconda di come si vogliono posizionare i destinatari nell'elenco.
  Il destinatario può essere presentato all'utente con le seguenti informazioni:
  - esito di eventuali precedenti spedizioni per interoperabilità (in una visualizzazione del documento successiva alla creazione/protocollazione):
    - simbolo (*) per indicare l'eventuale protocollazione in ingresso da parte del destinatario interoperante;
    - simbolo (*)(A): per documenti già inviati, protocollati in ingresso dal destinatario e successivamente annullati;

- simbolo (!): per indicare un destinatario non raggiunto dalla spedizione effettuata.

- (CANALE PREFERENZIALE) per indicare quale canale interoperante (MAIL, INTEROPERABILITÀ, INTEROPERABILITÀ PI) è stato associato al corrispondente in anagrafica;
- descrizione del corrispondente.

È possibile associare per ogni destinatario la tipologia di spedizione del documento attraverso l'icona  , scegliendo il mezzo di spedizione tra i predefiniti dall'ambiente di amministrazione. Tale scelta, a prescindere dal canale preferenziale associato al corrispondente, determina la modalità di spedizione del documento per ciascun destinatario.

L'elenco dei mezzi di spedizione effettivamente disponibili per l'utente è condizionato dalla valorizzazione di alcuni campi nei dettagli del corrispondente. In particolare, se il corrispondente presenta un indirizzo mail, nella finestra per la selezione del mezzo di spedizione è presente anche il valore MAIL. Se il corrispondente è stato registrato con indirizzo mail, codice AMM e codice AOO, nella finestra per la selezione del mezzo di spedizione è presente anche il valore INTEROPERABILITA'.

- **Mittente**: dato non obbligatorio. Nel protocollo in uscita il mittente può essere valorizzato solamente con i corrispondenti (UO, ruoli, persone) interni alla AOO su cui si sta protocollando il documento.

  Il campo mittente può consentire (per le amministrazioni che ne hanno fatto richiesta) l'integrazione con la tecnologia Ajax per le ricerche in rubrica. In particolare, se attivata questa integrazione, viene visualizzato un campo in corrispondenza del campo mittente. Su tale campo è stata attivata la funzione di auto completamento di Ajax che fornisce dei suggerimenti sulle parole da inserire nel campo mittente sulla base delle prime lettere digitate.

  Il numero dei caratteri a partire dai quali visualizzare i suggerimenti è configurabile.

  I suggerimenti sono presi dalla rubrica (dalla descrizione dei corrispondenti).
- **Documento in evidenza**: indica che il documento ha un certo rilievo. Può essere successivamente utilizzato come criterio di ricerca nella ricerca completa (vedi paragrafo 3.1.2.3.)
- **Tipologia documento**: in cui l'utente può scegliere una tipologia da indicare. Nel menu a tendina verranno mostrate solamente le tipologie in esercizio (non sospese). Una volta scelta la tipologia nella sezione destra della pagina, il sistema visualizza il pannello con i campi della profilazione dinamica del documento. L'utente amministratore, in fase di costruzione della "tipologia documento" o successivamente, può associare ad un ruolo specifico la visualizzazione e l'utilizzo di una determinata tipologia, per cui le informazioni relative alla tipologia documento sono visibili solo agli utenti abilitati. L'utente inserisce i dati in base alle impostazioni predefinite dall'utente. Tra i dati della tipologia se ci sono dei contatori con attivazione manuale all'atto della creazione ci sarà una casella selezionabile denominata "Attiva" ed il contatore scatterà solo quando l'utente seleziona questa casella. Se alla tipologia scelta è associato un diagramma di stato, nella sezione "profilo" in automatico si visualizza il campo Stato e si popola così come descritto nel paragrafo 2.8.1 al capoverso "Stato" .

  In fase di definizione delle tipologie documentali, mediante il tool di amministrazione, è possibile definire dei "CAMPI COMUNI" che possono essere associati a più tipologie documentali. Per i dettagli su questa funzionalità si rimanda al manuale di amministrazione.

All'utente che crea i documenti la presenza di questi campi è trasparente in quanto essi compariranno nel pannello con i campi di profilazione insieme agli altri campi associati al documento.

Per le amministrazioni abilitate, è possibile tener traccia delle modifiche effettuate sui campi della tipologia fascicolo (ad eccezione dei campi contatore, oggetti esterni e link). In tal caso, le modifiche apportate ai campi profilati, configurati e impostati con storicizzazione dei valori, sono tracciate dal sistema e sono visibili attraverso la selezione dell'icona (in alto a destra della sezione relativa ai campi profilati). In particolare il sistema registra le informazioni riguardanti la data della modifica, l'utente, il ruolo, il campo modificato, il valore contenuto nel campo prima della modifica (Figura 43).

- **Note**: campo di testo in cui è possibile inserire una o più note per ciascuna delle quali si può impostare una diversa visibilità scegliendo tra le alternative proposte (per dettagli maggiori sull'utilizzo della funzionalità si veda il paragrafo 2.8.1.2);
- **Risposta al protocollo**: consente di creare una o più risposte ad un protocollo in uscita;
- **Fascicolazione rapida:** è possibile effettuare la fascicolazione rapida attraverso la semplice digitazione del codice del fascicolo o del sotto fascicolo (se conosciuto), oppure selezionando la figura che permette di scegliere (così come descritto dal paragrafo 2.8.1.3) il fascicolo/sotto fascicolo desiderato. Il documento, contestualmente alla creazione del protocollo in uscita, verrà anche direttamente classificato. È inoltre possibile fascicolare i documenti protocollati e non in modalità rapida, anche dopo la loro creazione. Se accanto alla dicitura fascicolazione rapida vi è un asterisco, questa è obbligatoria.

  C'è anche la possibilità di creare un fascicolo direttamente da questa sezione dove è presente (se attivata la funzionalità) un ulteriore pulsante ( ) che consente di aprire la finestra per la creazione di un nuovo fascicolo. L'utente pertanto digita il codice del nodo di titolario nel campo presente nella sezione "fascicolazione rapida" ed il fascicolo verrà creato sotto questo nodo (Figura 47).
- **Trasmissione rapida**: è un menù a tendina che contiene una serie di modelli di trasmissione (vedi paragrafo 2.13.4). Selezionando un modello al momento della protocollazione, il documento verrà anche trasmesso secondo le modalità previste dal modello selezionato. È inoltre possibile trasmettere i documenti in modalità "rapida" anche dopo la creazione dei documenti protocollati e non (tramite il tab 'Trasmissioni'). Se si utilizza un modello di trasmissione contenente una UO fra i destinatari, al momento della trasmissione viene fatto un controllo sull'esistenza dei ruoli di riferimento per la UO stessa. Se non ve ne sono, il sistema mostra un opportuno messaggio e la trasmissione alla specifica UO non viene effettuata.

Per i campi relativi ai destinatari del documento protocollato sono presenti le icone:

- Dettaglio**:** consente di visualizzare il dettaglio del destinatario selezionato;
- Cancella**:** consente di eliminare il destinatario selezionato dalla lista dei destinatari o destinatari cc;
- Stampa**:** consente di stampare le buste dei destinatari.
- Storia: visualizza le modifiche apportate sul destinatario selezionato
- Spedizione: visualizza il tipo di spedizione associata al destinatario (fax, a mano, per email,…)
- Visualizzazione: quando nel campo destinatario o destinatario CC vengono inseriti molti nominativi, per leggere interamente quanto contenuto nel campo, si clicca su questo pulsante

-  Notifiche: consente di visualizzare, se presenti, le notifiche della spedizione del documento relative al destinatario selezionato. Se è presente almeno una notifica accanto al nome del destinatario compare un asterisco.

I pulsanti presenti in fondo alla pagina permettono di svolgere le funzioni illustrate qui di seguito:

- **Salva**: consente di salvare le successive modifiche che si apportano ai campi contenuti nella sezione 'Protocollo' con opzione 'Uscita', per i quali è prevista la possibilità di modifica. Questa funzione è abilitata solamente a seguito di protocollazione di un documento premendo sull'icona posta accanto alle opzioni "Ingresso" – "Uscita";
- **Protocolla:** permette di protocollare il documento ed eventualmente classificarlo e/o trasmetterlo se vengono opportunamente riempiti i campi di fascicolazione e trasmissione rapida illustrati precedentemente. Al momento della protocollazione viene inoltre effettuata una trasmissione ai destinatari e destinatari per conoscenza del protocollo con la ragione di trasmissione specificata mediante l'applicativo di amministrazione del sistema;
- **Spedisci:** consente di spedire un documento protocollato in uscita ad un'altra AOO interoperante o a un corrispondente interoperante (tramite PEC);
- **Riproponi:** permette all'utente avente il ruolo opportuno di riproporre la schermata della protocollazione con i dati del protocollo realizzato in precedenza;
- **Annulla:** ricopre una doppia funzionalità, Annulla documenti predisposti o Annulla documenti protocollati. L'utente può visualizzare lo stato di questo pulsante al passaggio del cursore su di esso. In caso di **Documento predisposto alla protocollazione**, l'utilizzo del pulsante è consentito solo all'utente creatore della predisposizione e se da amministrazione gli sono stati associati i dovuti diritti funzionali. Per i ruoli abilitati a tale funzionalità è inoltre possibile annullare la predisposizione del documento alla protocollazione.
  In caso di **Documento Protocollato**, il sistema consente all'utente, avente il ruolo opportuno, di annullare la protocollazione effettuata inserendo obbligatoriamente le note d'annullamento.

Tranne i pulsanti 'Protocolla' e 'Salva', tutti gli altri pulsanti sono abilitatati soltanto dopo la creazione del documento.

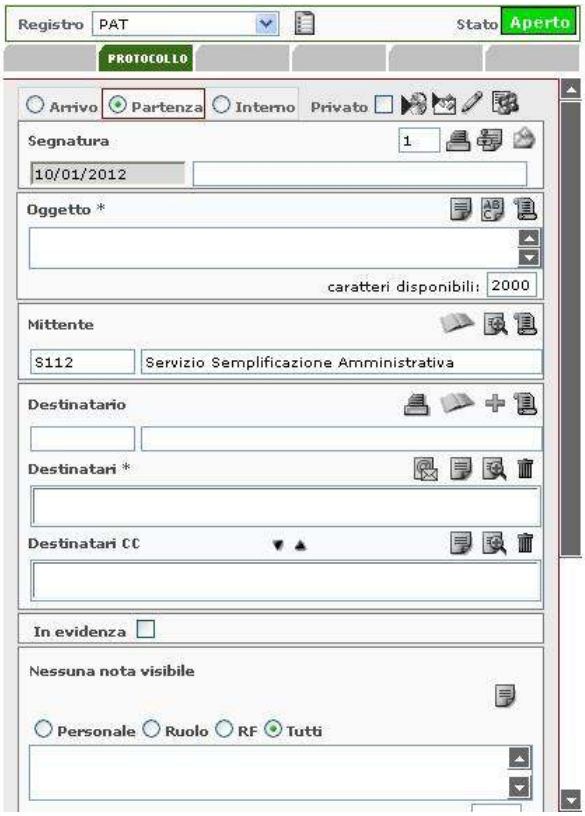


Figura 65 - Protocollo in uscita (prima parte)

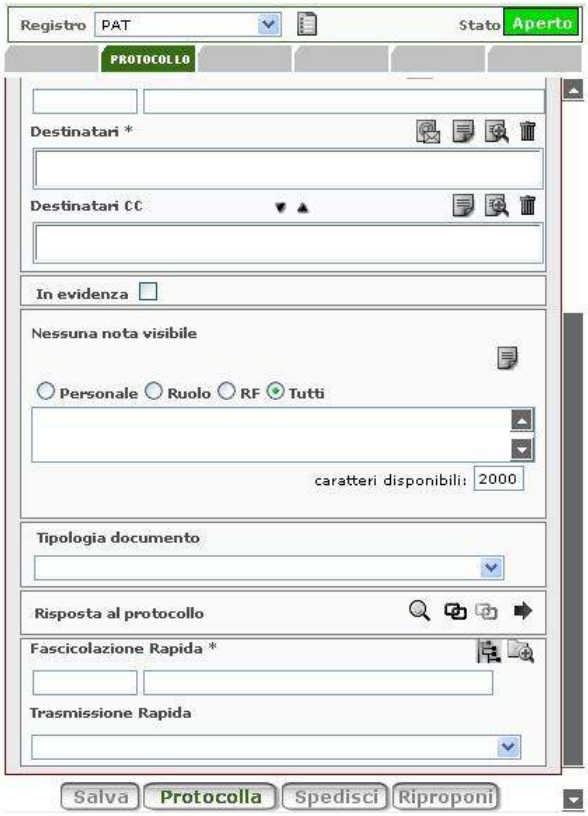


Figura 66 - Protocollo in uscita (seconda parte)

2.7.2.1 Documenti di risposta

2.7.2.1.1 Creazione di un protocollo in risposta ad un documento protocollato in uscita.

Questa funzione consente di creare una o più risposte ad un documento protocollato in uscita. La funzionalità è accessibile a partire dalla scheda del documento protocollato in uscita mediante l'icona presente nell'area "Risposta al protocollo" (Figura 59); cliccando su tale pulsante viene predisposto un protocollo in ingresso. L'utente può modificare autonomamente la tipologia del documento di risposta.

La risposta ad un documento in uscita potrà pertanto essere:

1. un *documento in ingresso* o *predisposto in ingresso* la cui scheda sarà automaticamente popolata nel modo seguente:
   - Il "*Mittente*" coincide con il "*Destinatario*" del protocollo in uscita a cui si sta rispondendo (se ci sono più destinatari all'utente viene data la possibilità di sceglierne uno)
   - L'"*Oggetto*" coincide con l'"*Oggetto*" del protocollo in uscita a cui si sta rispondendo.

2. un documento in uscita o predisposto in uscita o un documento interno o predisposto interno la cui scheda sarà automaticamente popolata nel modo seguente:
   - L'"*Oggetto*" coincide con l'"*Oggetto*" del protocollo in uscita a cui si sta rispondendo.

Si noti che la possibilità di creare protocolli diversi da quello in ingresso o predisposto in ingresso è una funzionalità aggiuntiva configurabile e che il comportamento classico è quello di creare come risposte solo protocolli in ingresso.

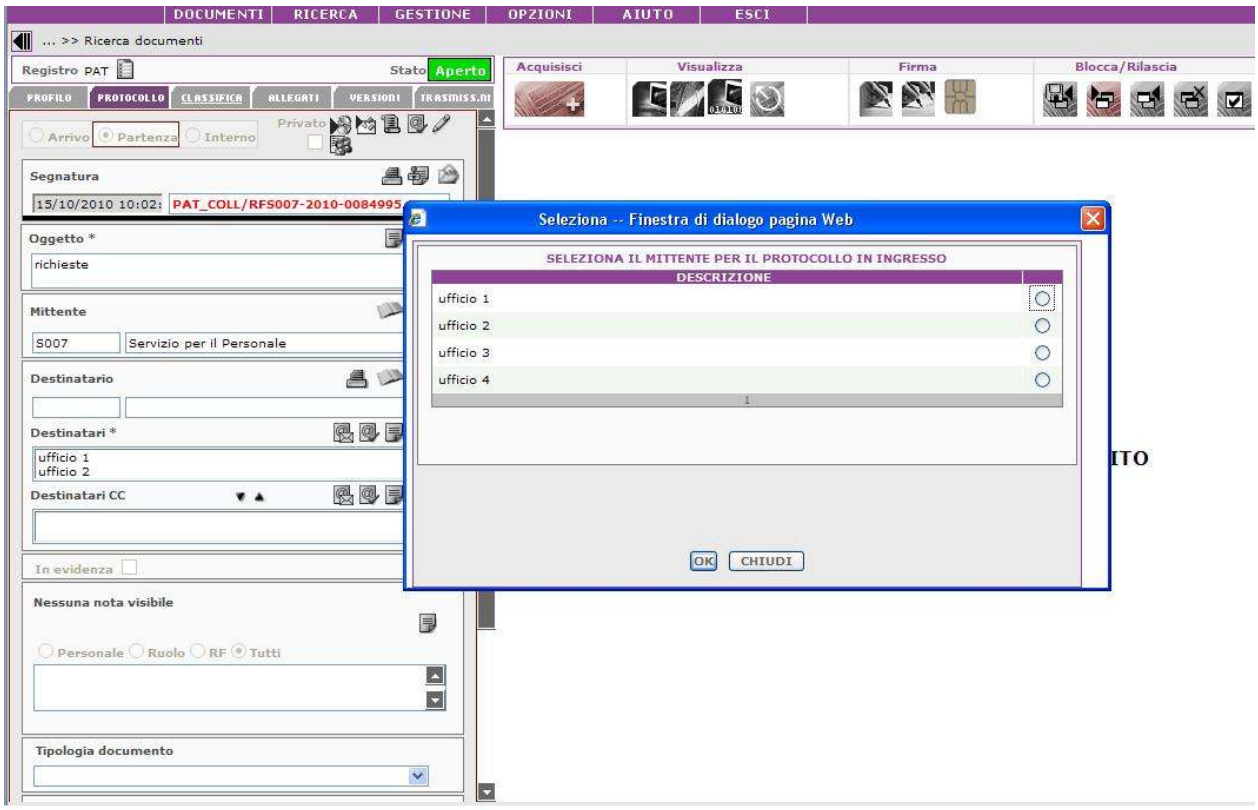


Figura 67- Risposta al protocollo in uscita

2.7.2.1.2 Creazione di un documento non protocollato in risposta ad un documento protocollato in uscita.

Questa funzione consente di creare una o più risposte ad un documento protocollato in uscita. La funzionalità è accessibile a partire dalla scheda del documento protocollato in uscita mediante l'icona presente nell'area "Risposta al protocollo"; cliccando su tale pulsante viene predisposta la scheda di profilo di un documento grigio popolata automaticamente nel seguente modo:

- L'"*Oggetto*" coincide con l'"*Oggetto*" del protocollo in uscita a cui si sta rispondendo.

La possibilità di creare come risposta di un documento protocollato un documento grigio costituisce una funzionalità aggiuntiva configurabile. Non è disponibile se non risulta attiva l'icona ad essa corrispondente.

2.7.2.1.3 Documento protocollato in uscita come risposta ad un documento (protocollato o non).

Questa funzionalità consente di creare un documento in uscita come risposta di un documento già presente nel sistema (protocollato o no).

La funzionalità è accessibile, a partire dalla scheda del documento in uscita in fase di protocollazione, mediante l'icona , presente nell'area "Risposta al protocollo" (Figura 59); tale selezione consente l'apertura di una finestra di dialogo (Figura 60) per individuare, attraverso dei filtri di ricerca, il documento cui il documento in uscita costituirà una risposta. Per default la tipologia selezionata è "ingresso". In questo caso:

- Il "*Destinatario*" coincide con il "*Mittente*" del protocollo in ingresso a cui si sta rispondendo
- L'"*Oggetto"* coincide con l'"*Oggetto*" del protocollo in uscita a cui si sta rispondendo.

"*Destinatario*" e "*Oggetto*" sono modificabili prima della conferma della registrazione.

Per le altre tipologie di documento quello che viene ereditato è solo il valore dell'"Oggetto".
Se si compilano i campi del protocollo prima di scegliere il documento a cui rispondere vengono effettuati dei controlli di coerenza sui valori dei campi oggetto e mittente/destinatario (se si seleziona la tipologia "ingresso").

La modalità di funzionamento è analoga a quella relativa ai protocolli in ingresso e dettagliata nel paragrafo 2.7.1.5.3.

Una volta confermata la selezione di un documento:

- Viene popolato il campo "Risposta al protocollo" del documento in uscita con la segnatura o l'id documento del protocollo o del documento non protocollato a cui si sta rispondendo;
- Viene abilitato il pulsante Protocolla o Salva a seconda di quando viene creata la catena documentale (in fase di creazione del documento in uscita o successivamente)

Confermata l'operazione di collegamento verrà effettuato il collegamento tra i documenti in questione.
Un protocollo in uscita può costituire una risposta per un solo documento quindi la funzione "Cerca documenti" sarà disattivata se il documento in uscita è già collegato ad un documento.

Subito dopo la protocollazione o in qualunque momento successivo è possibile visualizzare il dettaglio del protocollo a cui si è risposto mediante l'uso dell'icona .
Un protocollo in uscita può essere la risposta di un solo documento ma può avere più risposte.
Dalla scheda di un documento protocollato in uscita è possibile visualizzare la lista dei relativi documenti in risposta mediante l'uso dell'icona . Si apre una pagina che mostra tutti i documenti che rispondono a quel particolare protocollo in uscita, in modo analogo a quanto spiegato per i protocolli in ingresso (2.7.1.5.3). .

2.7.2.2 Spedizione di un documento in interoperabilità

Dopo aver protocollato un documento in uscita, inserendo o meno un'immagine (si veda il paragrafo 2.14.1) e/o eventuali allegati (si veda il paragrafo 2.11), è possibile spedirlo ad un'altra AOO della stessa Amministrazione o di un'Amministrazione differente o a qualsiasi altro corrispondente esterno presente in rubrica con una casella di posta elettronica certificata.
Con la selezione del pulsante **Spedisci** il sistema spedisce il documento al destinatario indicato.

Se è stata attivata l'opportuna funzionalità, l'ultima nota visibile a tutti viene inclusa nella segnatura xml. Se anche chi riceve per interoperabilità ha la medesima funzione abilitata, tale nota viene riportata nel documento ricevuto.
Al momento della spedizione il sistema propone all'utente di spedire con il tipo di ricevuta di avvenuta consegna predefinita, impostata per il registro/RF selezionato tramite interfaccia di amministrazione. L'utente può impostare manualmente (si veda Figura 68) un tipo di ricevuta diversa da quella predefinita, a scelta fra (per le definizioni riferirsi al § 1.3 - Definizioni e abbreviazioni):

- completa
- breve
- sintetica.

Figura 68- Selezione tipo ricevuta PEC

Nella spedizione sia il mittente che il destinatario possono avere una o più (se l'amministrazione è stata opportunamente configurata) caselle di posta elettronica associate. Occorre, tramite opportuni menu a tendina, selezionare la casella da cui il mittente intende spedire e quella a cui vuole spedire (agevolata dalle note di utilizzo). Le caselle principali, se presenti, sono contraddistinte da un asterisco.

Figura 69 – Spedizione con mittenti e destinatari multicasella

Il pulsante **Spedisci** viene rinominato **Rispedisci** se sono state effettuate le operazioni automatiche di trasmissione e spedizione, indicando così che il documento è già stato trasmesso e/o spedito. L'esecuzione del comando rispedisci apre una finestra che elenca, raggruppandoli per tipologia, i destinatari esterni interoperanti, i destinatari esterni per conoscenza interoperanti e i destinatari interni a cui è stato trasmesso il documento automaticamente. L'elenco riporterà per ogni elemento il nome del destinatario, la data e l'ora della trasmissione/spedizione e una casella di selezione. Nel caso di primo utilizzo della funzione Spedisci, tutti i destinatari saranno selezionati per default ma sarà possibile eseguire la trasmissione/spedizione solo verso alcuni di essi lasciando selezionati solo

quelli di interesse. Sarà anche possibile rimediare ad eventuali errori di protocollazione in cui non sono stati specificati i destinatari: l'utente autorizzato a modificare la registrazione di protocollo potrà inserire i destinatari mancanti e ri-eseguire la spedizione selezionando solo questi ultimi. Nel caso di destinatari interoperanti, sarà inoltre possibile rispedire il documento a quei destinatari che per problemi sul sistema di posta elettronica non hanno ricevuto il documento spedito in sede di registrazione protocollo.
Nel caso di rispedizione di un documento a cui sono associati allegati relativi alle ricevute PEC, il sistema spedisce il documento principale e gli allegati inseriti dagli utenti; pertanto non vengono recapitate le ricevute PEC relative alle precedenti spedizioni.
In fase di spedizione viene mantentuo il nome originario del file sia per l'immagine del documento che per quella degli eventuali allegati. Tale informazione viene quindi inviata al destinatario della spedizione.

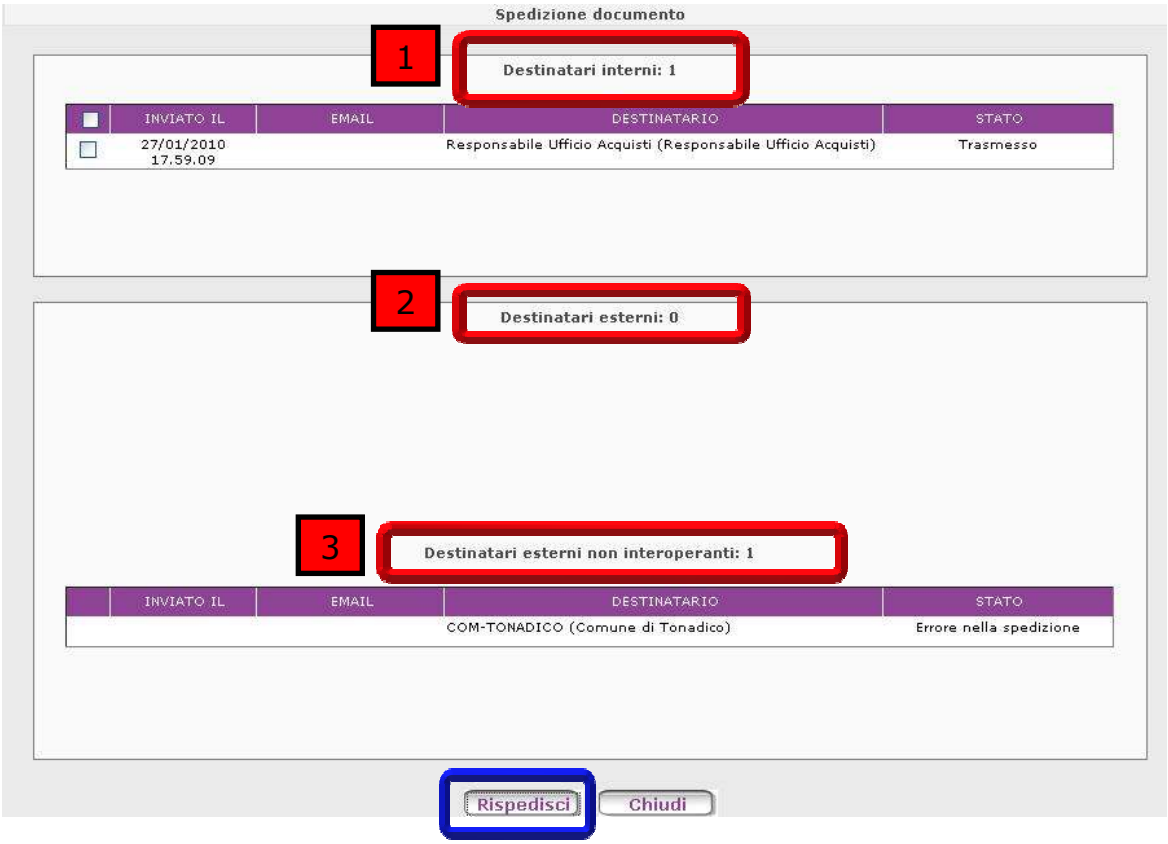


Figura 70 – Dettaglio spedizione documento

Il pulsante sarà rinominato "Rispedisci" ad indicare che il documento è stato già trasmesso e/o spedito.
Al momento della spedizione, se fra i destinatari interni è presente una UO, viene fatto un controllo sull'esistenza dei ruoli di riferimento per la UO stessa. Se non ve ne sono, il sistema mostra un opportuno messaggio e la trasmissione alla specifica UO non viene effettuata.

Il sistema spedisce anche l'eventuale marca temporale (attached/detached) associata al documento.

2.7.2.2.1 Ricevute di spedizione

Il mittente che ha spedito il documento in interoperabilità attraverso il sistema di protocollo informatico, per accertarsi dell'avvenuta protocollazione del documento, deve effettuare il controllo della casella istituzionale (vedi paragrafo 4.1). Il passaggio successivo è la ricerca del documento inviato e la visualizzazione delle notifiche del documento che si ottiene selezionando l'icona posta accanto ai campi destinatari/destinatari cc all'interno del tab protocollo..

Nella finestra delle notifiche di spedizione l'utente ha la possibilità di applicare dei filtri relativi all'indirizzo mail del destinatario (intero o parte di esso) ed al tipo di ricevuta.

Per ciascuna ricevuta relativa al documento vengono riportati i seguenti dati:

- ***Tipo di ricevuta:*** dove viene indicato il tipo di notifica (per le definizioni riferirsi al paragrafo 1.3 - Definizioni e abbreviazioni) [13]:
  - Ricevuta di accettazione
  - Ricevuta di avvenuta consegna
  - Avviso di mancata accettazione
  - Avviso di mancata consegna
  - Annullamento protocollazione
  - Conferma di ricezione
  - Eccezione
  - Con errori

- ***Destinatario:*** il mittente della notifica (generalmente il destinatario della spedizione del documento, o nel caso di notifiche PEC, il server di posta certificata mittente o destinatario);

- ***Dettaglio:*** riporta il dettaglio della specifica notifica. Nel caso di ricevute relative a spedizioni PEC, il dettaglio non è altro che il contenuto del file eml che costituisce la ricevuta stessa.

Tramite il pulsante , inoltre, l'utente ha la possibilità di esportare l'elenco delle ricevute di spedizione in formato Excel.

Tramite la casella di selezione 'Seleziona/deseleziona tutti' è possibile selezionare o deselezionare tutti i tipi di ricevuta indicati.

Il filtro 'Mail destinatario' consente, nel caso l'amministrazione sia abilitata alla gestione multicasella, di visualizzare le ricevute collegate ad uno o più indirizzi associati al corrispondente (Figura 71).

Se la spedizione è avvenuta per interoperabilità semplificata (si veda par. 2.7.2.3) verrà mostrato anche il codice del corrispondente selezionato (Figura 72).

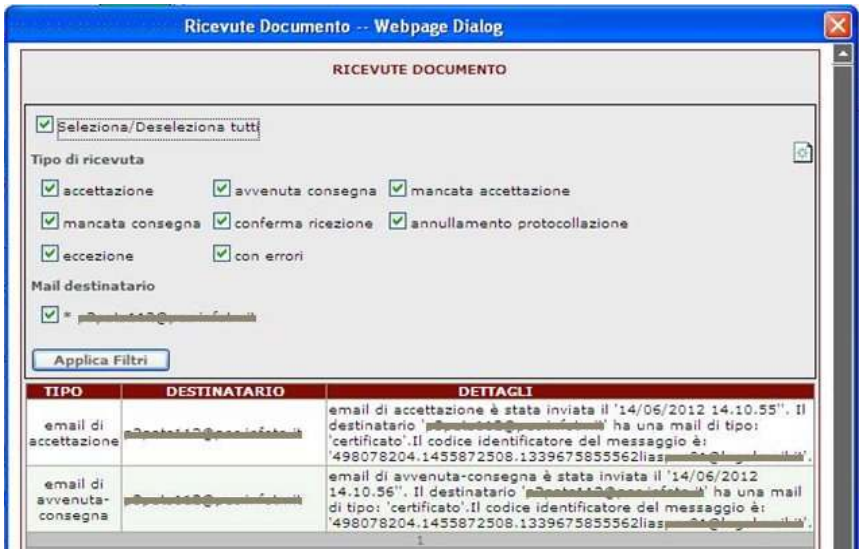


Figura 71 – Ricevute di spedizione

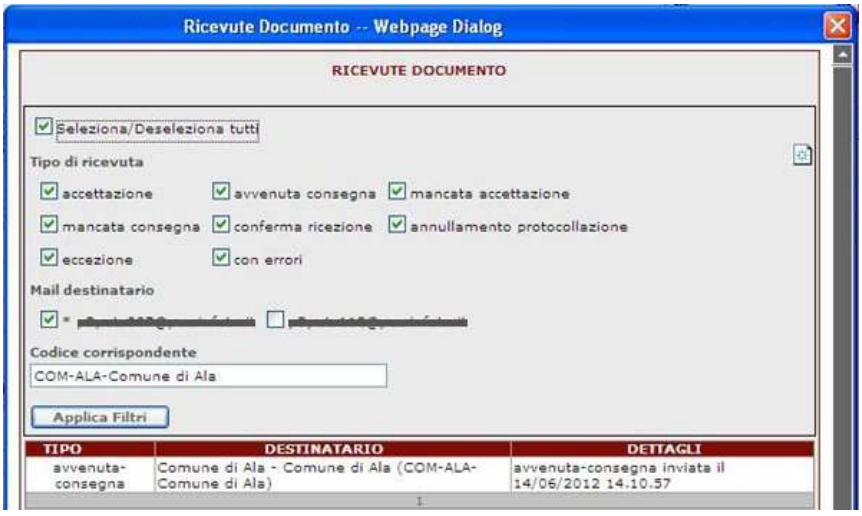


Figura 72 – Ricevute di spedizione (interoperabilità semplificata)

2.7.2.3 Spedizione di un documento mediante interoperabilità semplificata

Se l'amministrazione è stata opportunamente configurata, oltre all'interoperabilità tramite mail (vedere par. 2.7.2.2 e 2.7.2.2.1), è possibile interoperare con altre Amministrazioni che utilizzino il protocollo informatico VTDOCS, tramite l'Interoperabilità Protocollo Informatico VTDOCS (Interoperabilità PI VTDOCS). Le modalità con cui si interopera senza mail sono sostanzialmente analoghe a quelle per l'interoperabilità via mail.

In fase di creazione del protocollo in uscita, occorre utilizzare come mezzo di spedizione “Interoperabilità PI”. Al momento della spedizione, nella maschera di dettaglio della spedizione, viene mostrata una nuova sezione (Figura 73) ‘Destinatari interoperanti PI’, analoga alla sezione relativa ai destinatari interoperanti PEC. Il campo email, in corrispondenza della spedizione ad un destinatario interoperante PI, sarà vuoto.
In fase di spedizione viene mantentuo il nome originario del file sia per l’immagine del documento che per quella degli eventuali allegati. Tale informazione viene quindi inviata al destinatario della spedizione.

Figura 73 – Spedizione interoperabilità semplificata

La gestione delle ricevute di interoperabilità semplificata è analoga a quella delle ricevute generate per l’interoperabilità PEC, eccezion fatta per:

- ricevute di avvenuta/mancata accettazione da parte del provider mittente che non hanno un corrispondente per l’interoperabilità semplificata
- ricevute di mancata consegna e di ritorno di eccezione che verranno visualizzate tramite il centro notifiche (si veda par. 2.5.2.4.1).

Il sistema spedisce anche l’eventuale marca temporale (attached/detached) associata al documento.

2.7.3 Protocollo interno

Il protocollo interno è un’ulteriore categoria di documenti protocollati che vengono scambiati all’interno della stessa AOO. Non tutte le amministrazioni fanno uso dei protocolli interni potendo utilizzare a tale scopo i documenti grigi. Pertanto la voce ‘interno’ e le relative funzionalità sono soggette a configurazione.
La creazione di un documento interno è simile a quella dei documenti in uscita. Le caratteristiche principali che li distinguono dai protocolli in uscita sono:

- anche il mittente è un dato obbligatorio
- mittente e destinatari sono interni all’organigramma (cioè appartengono alla stessa AOO dell’utente/ruolo che sta effettuando la protocollazione)
- I protocolli interni sono indicati con la lettera **I**.
- le ricerche possono essere filtrate per protocolli interni
- è possibile configurare il sistema in modo tale che quando si effettua la protocollazione vengono automaticamente inviate le trasmissioni ai destinatari interni indicati (trasmissione automatica). Se invece è configurata la modalità “manuale” sarà possibile effettuare le trasmissioni cliccando sul

tasto “Trasmetti”, che analogamente allo “Spedisci” dei protocolli in uscita, permette di scegliere i destinatari e di effettuare le trasmissioni o ritrasmissioni del documento.

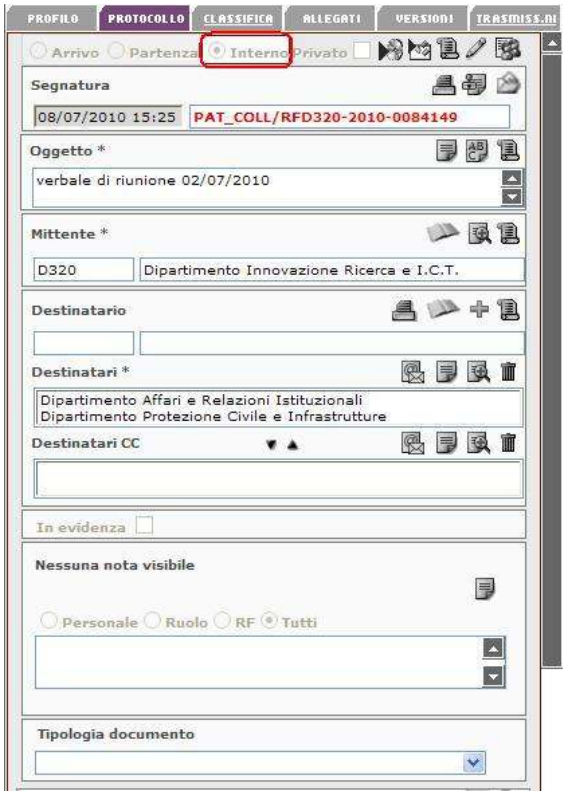


Figura 74 – Protocollo interno

Figura 75 – Ricerca protocollo interno

Le gestione dei documenti di risposta è analoga a quella dei protocolli in ingresso e in uscita. Il comportamento standard è quello di collegare tra loro documenti interni.
Per i dettagli si vedano i paragrafi 2.7.1.5 e 2.7.2.1.

2.8 Nuovo documento

La prima voce della barra di menù, presente nella testata di tutti i pannelli, consente di creare un nuovo documento, che sarà possibile protocollare subito o in un secondo momento. Nel corrente paragrafo viene fornita una descrizione della funzione Nuovo Documento (Profilo).

Figura 76 – Nuovo Documento: schema di navigazione

2.8.1 Profilo

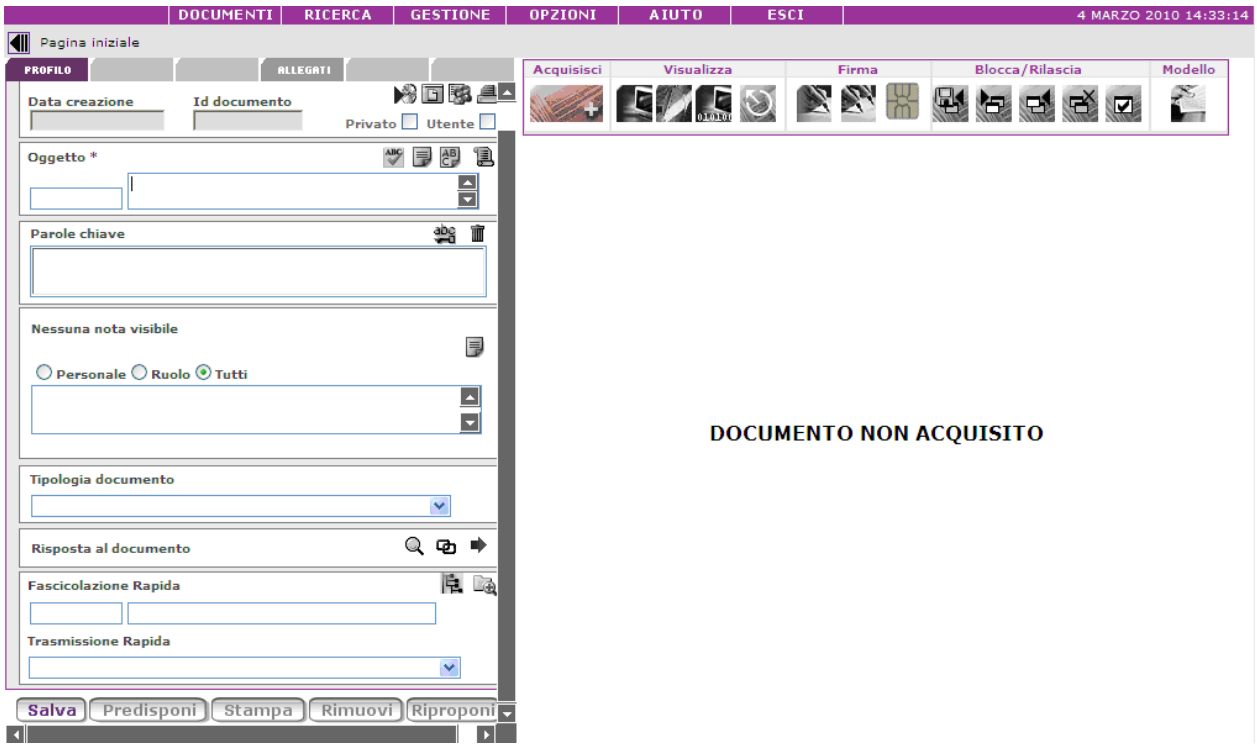


Figura 77 – Nuovo documento

Consente l'inserimento di un documento senza richiederne contestualmente la protocollazione.
La protocollazione può essere richiesta in un momento successivo selezionando il pulsante "Predisponi" posizionato in fondo alla pagina.
Nella parte alta del profilo del documento (Figura 77) vi sono una serie di icone utilizzabili dopo la creazione del documento:

- : consente di inserire il documento nell'Area di lavoro;
- : visualizza gli utenti ed i ruoli che hanno visibilità sul documento e con quale diritto di visibilità è stato acquisito (PROPRIETARIO/ACQUISITO/TRASMISSIONE). Tale funzionalità è descritta in maniera dettagliata nel paragrafo 2.8.1.1;
- : stampa etichetta dell'identificativo del documento non protocollato;
- : consente di visualizzare la storia del processo di conservazione a cui è stato sottoposto il documento;
- : partendo da un documento non protocollato questo pulsante consente di creare un documento predisposto alla protocollazione in uscita con lo stesso oggetto del documento non protocollato. Il nuovo documento predisposto avrà tra gli allegati il documento principale, gli eventuali allegati del documento, più altri eventuali allegati del documento da protocollare in uscita che si vuole inoltrare ad un altro destinatario. Gli allegati al documento predisposto alla protocollazione sono costituiti dalla copia dell'ultima versione del documento che si inoltra e delle ultime versioni dei relativi allegati;
- : una volta creato il documento consente di visualizzare tutte le operazioni che avvengono sul documento, come creazione documento, inserimento allegato, trasmissione etc. ; specificando "Data", "Operatore", "Azione" .
- : consente di consolidare un documento nella parte relativa a versioni ed allegati
- : consente di consolidare totalmente un documento, nella parte relativa a versioni ed allegati (se il documento non è stato consolidato parzialmente dalla funzione descritta al punto precedente) e nei metadati. Per i dettagli si rimanda al paragrafo 2.7.1.6.

I dati caratteristici di un documento non protocollato sono i seguenti:

- **Data creazione**: impostata dall'applicativo con la data del sistema e l'ora;
- **Id. Documento**: identificativo univoco associato ad ogni documento in modo automatico dal sistema;
- **Privato**: se selezionato indica che, per il documento che si sta inserendo, non viene ereditata la visibilità dai ruoli gerarchicamente superiori; quindi il documento con questa opzione risulterà visibile soltanto agli utenti appartenenti allo stesso ruolo associato all'utente che invia il documento;
- **Utente** (solo per i ruoli abilitati): se selezionato indica che, per il documento che si sta inserendo, non viene ereditata la visibilità dai ruoli gerarchicamente superiori e dal ruolo di appartenenza; quindi il documento con questa opzione risulterà visibile soltanto all'utente creatore;
- **Oggetto**: dato obbligatorio. Rappresenta una breve descrizione del documento che si sta inserendo. Può essere una descrizione occasionale, quindi digitato liberamente dall'utente, oppure selezionato da una lista memorizzata, che è possibile raggiungere selezionando l'icona (vedi Paragrafo 2.7.1.3.1). Se si inserisce una descrizione occasionale è possibile effettuare il controllo ortografico su quanto editato nel campo oggetto attraverso la selezione dell'icona che apre la finestra di dialogo mostrata nella Figura 78. Inoltre è possibile valorizzare il campo oggetto anche attraverso la digitazione del codice associato all'oggetto necessario collegato al Registro/RF di interesse. In tal caso, dopo aver digitato il codice rubrica, se si sposta il cursore in un altro campo qualsiasi del modulo, l'applicazione automaticamente valorizza il campo di testo, posto a fianco,

mediante la descrizione associata al codice digitato, prelevandoli dall'oggettario. Se l'oggetto interessato non è presente nell'oggettario è possibile inserirlo, selezionando un eventuale registro e digitando il codice (se necessario) ed il valore oggetto nel campo oggetto, e premendo sul pulsante Inserisci. Quando nel campo oggetto viene digitato un testo molto lungo, per leggere interamente quanto in esso contenuto basta selezionare l'icona . Una volta creato il documento è possibile modificare l'oggetto digitando direttamente la variazione nel campo preposto o reinserendolo da oggettario, visualizzando la storia delle modifiche ad esso apportate mediante l'icona .

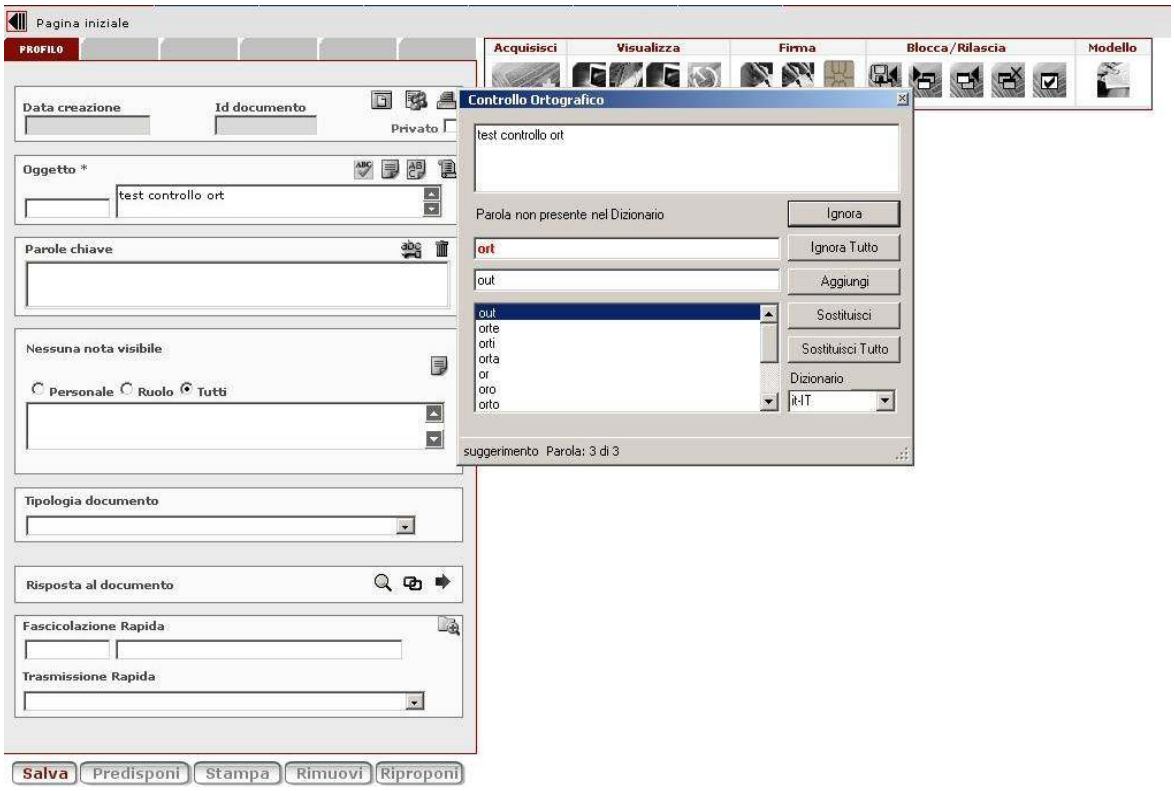


Figura 78 – Controllo ortografico

- **Parole chiave**: elenco delle parole che possono essere considerate chiave di ricerca per il documento. Queste consentono, una volta effettuato l'inserimento, di ricercare il documento all'interno del sistema in maniera più rapida. Selezionando l'icona viene presentata una finestra di dialogo (Figura 79) con l'elenco di tutte le parole chiave già inserite nel sistema, dalla quale è possibile selezionare quelle di interesse.

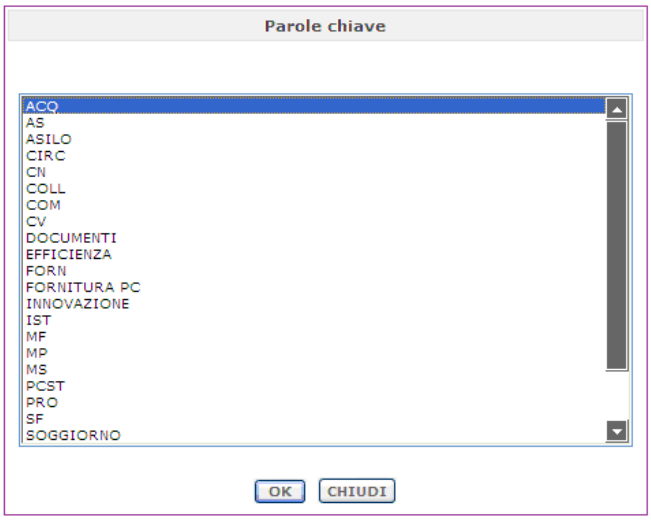


Figura 79 – Selezione parola chiave

Se la voce da inserire è già presente nell'elenco proposto occorre selezionarla e premere il pulsante OK posto in basso a sinistra della schermata. Se la voce da inserire non è ancora presente, un utente con i permessi opportuni può inserire nuove parole chiave. Selezionando l'icona viene presentata la finestra di dialogo mostrata in Figura 80 nella quale, dopo aver digitato la parola da inserire, premendo il bottone "Inserisci", quest'ultima viene memorizzata all'interno del sistema.

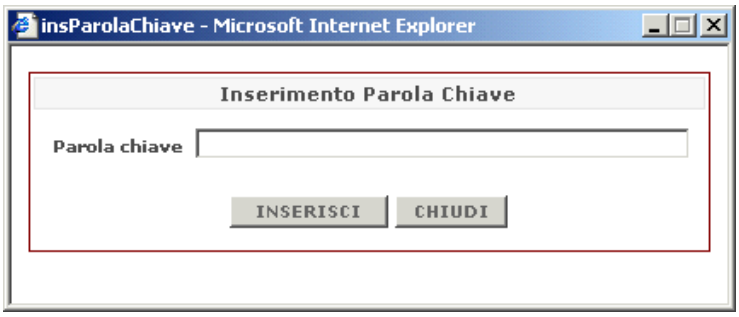


Figura 80 – Inserimento parola chiave

- **Note**: campo di testo in cui è possibile inserire una o più note per ciascuna delle quali si può impostare una diversa visibilità scegliendo tra le alternative proposte (per dettagli maggiori sull'utilizzo della funzionalità si veda il paragrafo 2.8.1.2);
- **Tipologia documento**: in cui l'utente può scegliere una tipologia da indicare. Nel menu a tendina verranno mostrate solamente le tipologie in esercizio (non sospese). Una volta scelta la tipologia nella sezione destra della pagina il sistema visualizza il pannello con i campi della profilazione dinamica del documento. L'utente amministratore, in fase di costruzione della "tipologia documento" o successivamente, può associare ad un ruolo specifico la visualizzazione e l'utilizzo di una determinata tipologia, per cui le informazioni relative alla tipologia documento sono visibili solo agli utenti abilitati. L'utente inserisce i dati in base alle impostazioni predefinite dall'utente amministratore e con il tasto "Salva" conferma gli inserimenti effettuati. Se la tipologia prescelta

prevede dei campi di tipo “contatore” con attivazione manuale, quando si crea il documento sarà disponibile un pulsante “Attiva” che consente di far partire il contatore nell’istante desiderato.

- **Risposta al documento** (vedi paragrafo 2.8.1.4): nella pagina del profilo del documento; è possibile:
  - associare il documento che si sta creando a documenti (protocollati e non protocollati) già precedentemente salvati (documento in risposta) mediante l’icona;
  - creare un documento in risposta a partire da un documento non protocollato, mediante l’icona , attiva solo per documenti già salvati;
  - creare un protocollo in risposta a partire da un documento non protocollato, mediante l’icona , attiva solo per documenti già salvati;

  La possibilità di creare collegamenti anche con i documenti protocollati è una funzionalità aggiuntiva configurabile. La modalità classica è quella di collegare tra loro solo documenti non protocollati. In tal caso l’icona non è attiva.
- **Stato**: nella pagina del profilo del documento, dopo aver selezionato la tipologia documentale se a questa è stato associato un “diagramma di stato”, immediatamente sotto il menù a tendina compare:
  - un ulteriore menù a tendina relativo allo stato del documento. E’ presente soltanto il valore che, per lo specifico “diagramma di stato”, è stato definito come “stato iniziale”.;
  - una data di scadenza per i documenti di un certo tipo cui è associato un diagramma di stato (se preventivamente impostata dall’utente amministratore). La scadenza di un documento viene definita in numero di giorni entro cui il documento deve raggiungere uno stato finale. Il sistema invia delle trasmissioni a tutti i destinatari del documento quando si avvicina la data di scadenza o quando la data di scadenza è trascorsa senza che il documento abbia raggiunto uno stato finale.

  Ad ogni successivo accesso al documento, nel menu a tendina “Stato”, se l’utente ne ha visibilità, sarà possibile selezionare lo stato successivo a quello corrente. Nel caso in cui lo stato corrente sia uno stato di sistema, lo stato successivo non è disponibile e verrà raggiunto al verificarsi di un determinato evento relativo al documento.
- **Fascicolazione rapida**: E’ possibile effettuare la fascicolazione rapida attraverso la digitazione del codice del fascicolo o del sotto fascicolo (se conosciuto), oppure selezionando l’icona che permette di scegliere (così come descritto dal paragrafo 2.8.1.3) il fascicolo/sotto fascicolo desiderato. Il documento, contestualmente alla creazione del documento grigio, verrà anche direttamente classificato. Se accanto alla dicitura fascicolazione rapida vi è un asterisco, questa è obbligatoria. Tale campo è mostrato solamente al momento della creazione del documento.

  E’ anche possibile creare un fascicolo direttamente da questa sezione dove è presente (se attivata la funzionalità) un ulteriore pulsante ( ) che consente di aprire la finestra per la creazione di un nuovo fascicolo. L’utente pertanto digita il codice del nodo di titolario nel campo presente nella sezione “fascicolazione rapida” ed il fascicolo verrà creato sotto questo nodo.
- **Trasmissione rapida**: è un menù a tendina che contiene una serie di modelli di trasmissione (vedi paragrafo 2.13.4). Selezionando un modello al momento della creazione del documento grigio, il documento verrà anche trasmesso secondo le modalità previste dal modello selezionato (vedi paragrafo 2.13.4). Se si utilizza un modello di trasmissione contenente una UO fra i destinatari, al momento della trasmissione viene fatto un controllo sull’esistenza dei ruoli di riferimento per la UO stessa. Se non ve ne sono, il sistema mostra un opportuno messaggio e la trasmissione alla specifica UO non viene effettuata.

Dopo aver effettuato il salvataggio, è possibile associare un file che rappresenta l’immagine del documento. Non si può modificare la tipologia del documento una volta che sia stata selezionata la prima

volta. E' invece possibile cambiarne lo stato: nel menù a tendina il sistema mostra il valore dello stato corrente e, di seguito, il possibile valore definito come stato successivo per lo stato corrente. Ogni modifica effettuata nel campo "stato" viene tracciata nel sistema ed è visualizzabile in qualsiasi momento. In particolare viene memorizzato l'autore della modifica (utente e ruolo), la data ed il valore dello stato precedente alla modifica stessa.
Al momento della creazione di un documento, il sistema mostra un menù a tendina (campo stato) contenente il valore "Inserito nel sistema". Dopo aver effettuato il salvataggio, la tipologia documentale non è modificabile. Il sistema mostra l'indicazione del valore corrente del campo "stato" e, di seguito, un menù a tendina contenente tutti gli altri possibili per lo stato successivo (nella Figura 81 "In Lavorazione"). Dopo aver modificato il campo stato ed effettuato il salvataggio, il sistema mostra il valore corrente del campo stato e, nel menù a tendina sottostante, tutti gli altri possibili per lo stato successivo. Discorso analogo vale per gli stati successivi fino al raggiungimento di uno degli stati finali possibili: quando il documento è pervenuto in uno di questi stati, non sarà più possibile effettuare alcuna modifica sul documento stesso. E' possibile effettuare le sole operazioni di classificazione/fascicolazione e trasmissione in sola lettura. Il sistema chiede sempre conferma all'utente prima di passare ad uno stato "finale".
E' possibile visualizzare in qualsiasi momento la storia delle modifiche apportate al campo stato attraverso la selezione dell'icona .

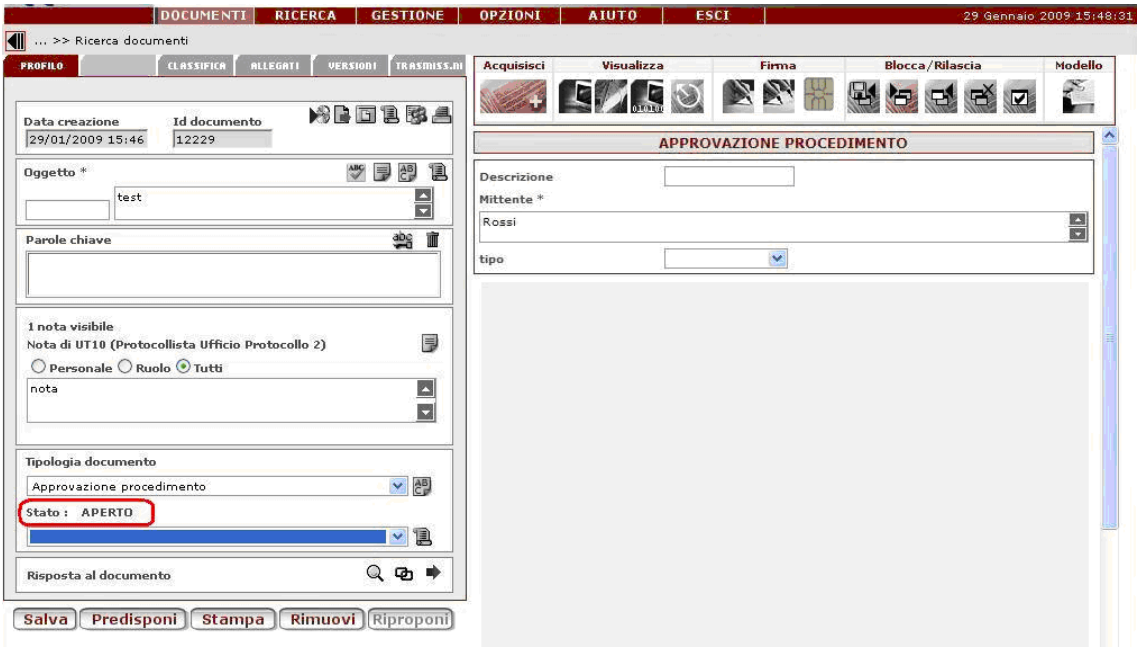


Figura 81 – Stato del documento associato al tipo approvazione procedimento

I pulsanti presenti a fondo pagina permettono di svolgere le funzioni illustrate qui di seguito:

- **Salva**: consente di creare un documento non protocollato e di salvare le successive, eventuali, modifiche apportate alle informazioni visualizzate nella sezione 'Profilo';
- **Predisponi**: permette di visualizzare la schermata di inserimento dei dati di protocollazione nel caso si voglia protocollare il documento creato come non protocollato;
- **Stampa**: permette di stampare la scheda con i dati presenti nel profilo del documento;
- **Rimuovi**: consente di rimuovere i documenti non protocollati e/o predisposti, anche quelli già trasmessi ad altro utente.

La funzione è' consentita solo al proprietario del documento e se il documento in questione non contiene una tipologia documento con un contatore repertoriato. La rimozione può essere effettuata o attraverso l'apposito pulsante rimuovi presente sul foglio del documento o direttamente dalla lista delle cose da fare. I documenti rimossi sono in realtà inseriti all'interno di una apposita area denominata "cestino". Analogamente al cestino del sistema operativo, è possibile revocare la rimozione definitiva e quindi la cancellazione fisica dei metadati dal data-base e dei file eventualmente associati. L'accesso all'area cestino è possibile dal menù gestione solo ai ruoli autorizzati. Inoltre, tramite un apposito comando di configurazione, è possibile abilitare la cancellazione dei documenti trasmessi e non di proprietà dell'utente che effettua la cancellazione.

- **Riproponi**: permette all'utente di riproporre la schermata del documento con i dati Oggetto, la Parola Chiave, la Fascicolazione e la Tipologia Documento se presenti. Il sistema non riproporrà il documento principale e gli allegati ad esso associati. Selezionano il pulsante **riproponi**, il sistema presenterà un messaggio di conferma che richiede se si desidera riproporre anche le immagini del documento principale (limitatamente all'ultima versione) e degli allegati del documento originale.

Esiste un solo caso in cui la rimozione è consentita ad utenti non proprietari:

- gli utenti devono appartenere a ruoli configurati per ricevere i documenti prelevati dalla casella di posta istituzionale e predisposti alla protocollazione;
- i documenti sono quelli predisposti alla protocollazione ricevuti attraverso il sistema di interoperabilità, e quindi ricevuti con ragione di trasmissione di tipo "interoperabilità".

Per la rimozione di un documento non protocollato o predisposto, il sistema prevede due scenari distinti:

- le utenze sono autorizzate: il sistema richiede la conferma della cancellazione rispondendo "OK" ad un opportuno messaggio; in tale ambiente è possibile inserire un commento, non obbligatorio, per motivare la cancellazione; se il documento viene rimosso questo viene inserito nell'area "Documenti in cestino" (vedi paragrafo 4.10);
- le utenze non sono autorizzate: il sistema visualizza un messaggio che indica la mancanza dei diritti necessari per rimuovere il documento.

Tranne il pulsante 'Salva', tutti gli altri vengono abilitatati soltanto dopo la creazione del documento e se l'utente ha le relative autorizzazioni.

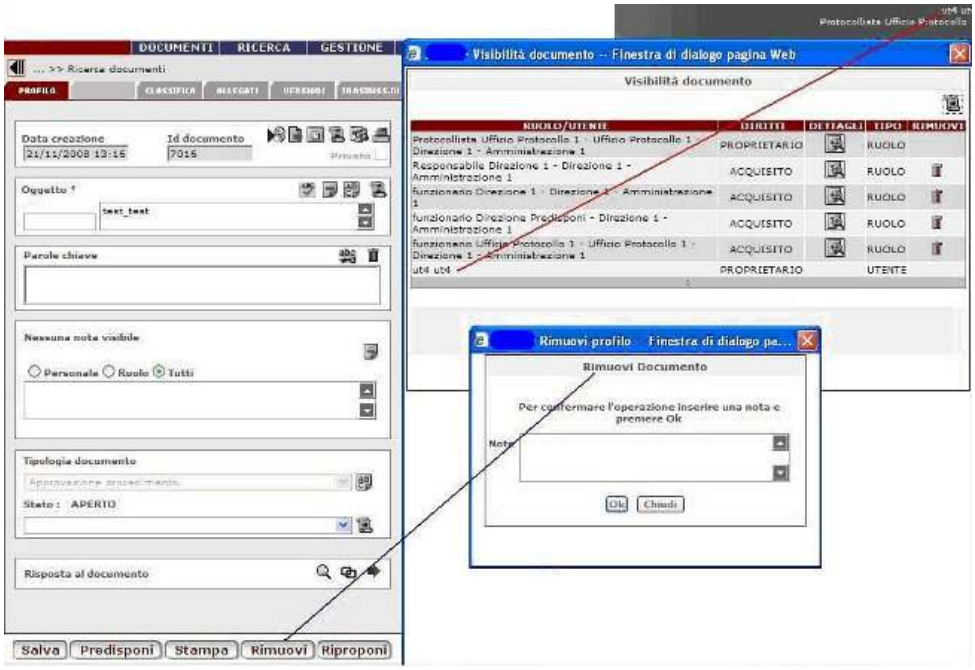


Figura 82 – Sezione profilo: rimozione documento non protocollato per il proprietario

2.8.1.1 Visibilità

Selezionando l'icona , si visualizza la finestra di dialogo che mostra gli utenti ed i ruoli che hanno visibilità sul Documento/Fascicolo , così come mostrato nella Figura 83.

La finestra di dialogo mostra una lista di Ruoli/Utenti e per ciascuno riporta le seguenti informazioni:

- : consente di selezionare il ruolo/utente corrente. Non è possibile selezionare il ruolo/utente proprietario
- **Ruolo/Utente**: indica i ruoli e le utenze che hanno visibilità sul documento/fascicolo. Accanto ai ruoli che hanno subito modifiche, viene visualizzata un'icona che consente di visualizzare la storia delle modifiche di tale ruolo (Figura 84):
  Le informazioni riportate sono:
  - azione: C (Creazione), M (Modifica), S (Storicizzazione)
  - data azione
  - dettaglio ruolo: descrizione, descrizione UO, descrizione tipo ruolo.

  La storia delle modifiche al ruolo è esportabile, tramite il pulsante 'Esporta', in formato PDF, Excel, Calc.
- **Diritti**: indica con che tipo di diritto il ruolo o l'utente ha acquisito la visibilità ;
- **Dettagli**: ad ogni ruolo è associata l'icona che permette la visualizzazione, nella parte bassa della finestra, degli utenti presenti nel ruolo;
- **Tipo**: Utente/Ruolo;
- **Dta fine**: indica la data di cessazione dell'utente/ruolo;
- **Rimuovi**: tale funzione è visibile solo se l'Amministratore VTDOCS ha abilitato il ruolo all'utilizzo della funzionalità. Laddove sia presente l'icona è possibile pertanto cancellare la visibilità del ruolo/utente associato. Selezionando l'icona in fondo alla finestra di dialogo compare un campo

editabile in cui si può inserire la motivazione della rimozione, come è visibile in Figura 85; selezionando il pulsante “OK” la rimozione è effettiva, con “Annulla” non accade nulla.

- **Note acquisizione**: viene riportata in caso di acquisizione del diritto per particolari motivi (es.: copia di visibilità fra ruoli);
- **Data diritto/revoca**: è la data in cui il diritto è stato acquisito o revocato rispettivamente.

Per chiudere la finestra di dialogo della Visibilità selezionare il pulsante Chiudi.

In cima alla lista sono riportati i pulsanti che consentono di rimuovere/ripristinare in modo massivo i diritti di sivilibiltà:

- : permette di rimuovere la visibilità ai ruoli/utenti selezionati
- : permette di ripristinare la visibilità ai ruoli/utenti selezionati
- Seleziona/Deseleziona: consente di selezionare/deselezionare tutti gli utenti/ruoli presenti nella lista

Una volta avviata l’operazione ‘massiva’ un opportuno messaggio mostra i ruoli/utenti su cui si va ad agire o su cui non si può agire e ne indica il motivo.

Se è attivato il tracciamento delle operazioni di rimozione della visibilità (tramite amministrazione), ogni modifica apportata al documento/fascicolo viene tracciata dal sistema ed è visibile attraverso la selezione dell’icona , che visualizza le informazioni riguardanti l’utente, il ruolo, la data, il Cod. Operazione, la Descrizione.

La Figura 86 figura mostra invece la storia della visibilità del documento evidenziando la perdita di visibilità sul documento ottenuta per precedente delega temporanea.

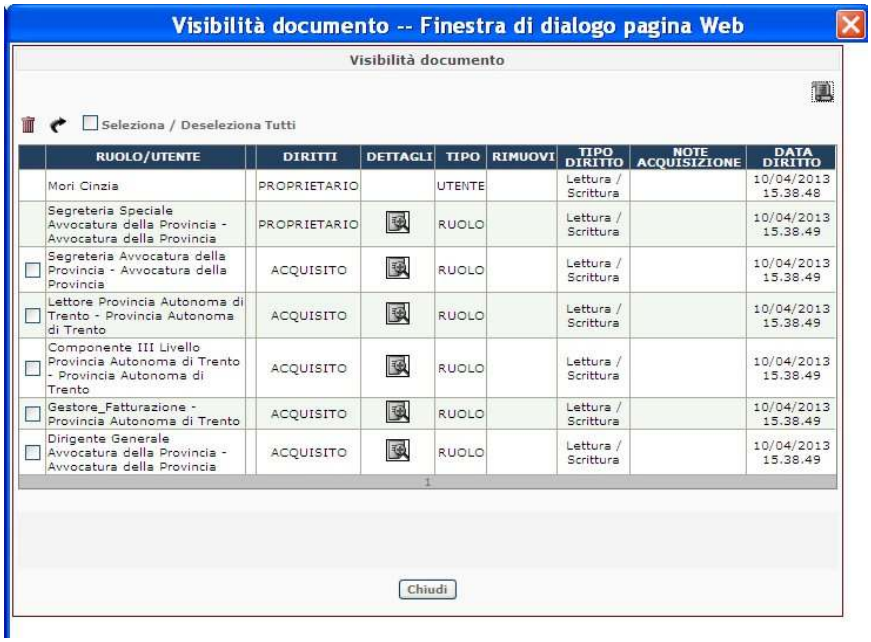


Figura 83 – Dettaglio visibilità

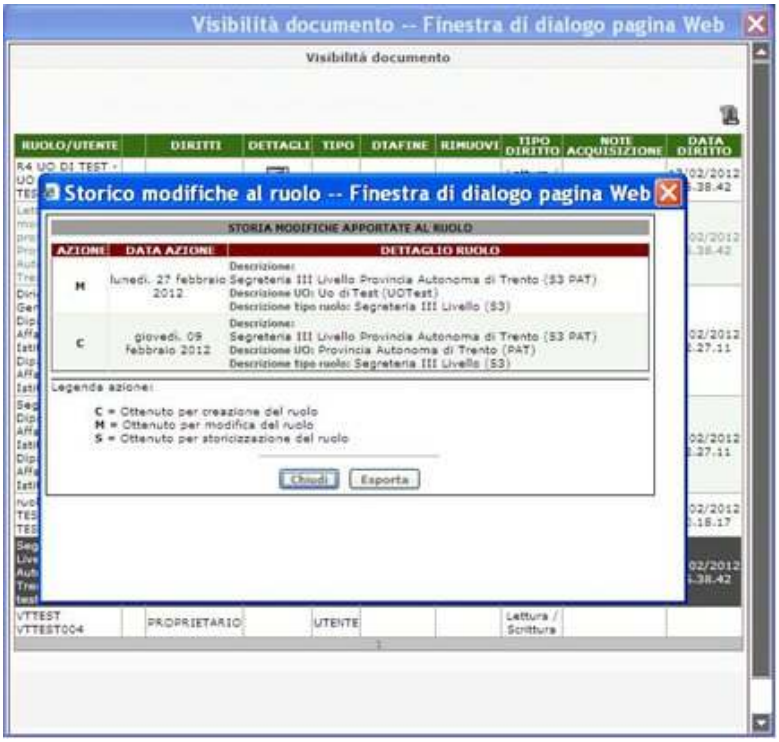


Figura 84 – Dettaglio visibilità: storia delle modifiche al ruolo

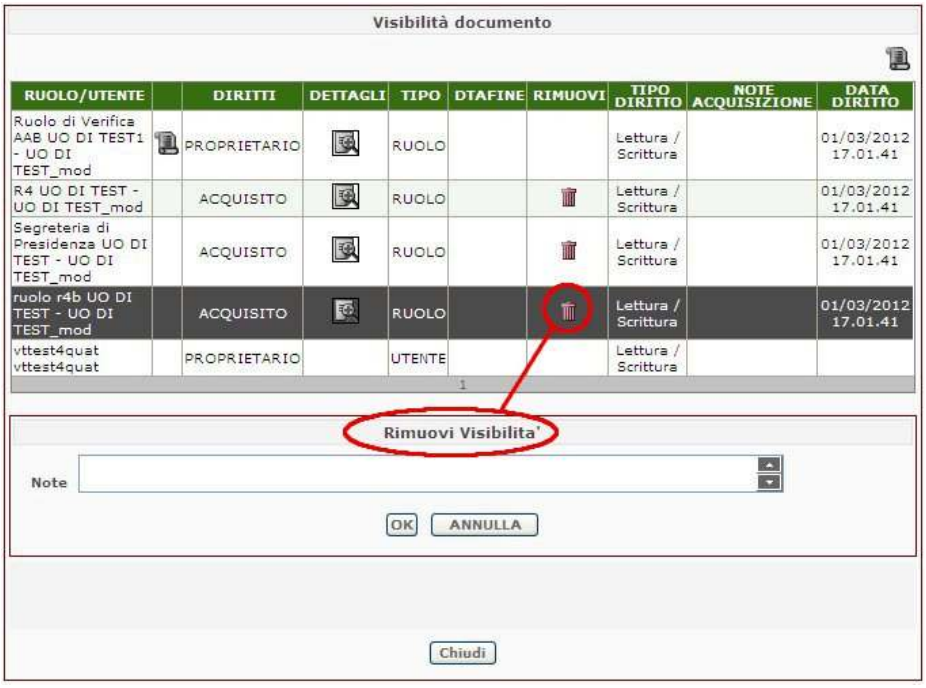


Figura 85 – Dettaglio visibilità: rimozione visibilità

Figura 86 – Dettaglio visibilità: storia revoche

2.8.1.2 Nota

E' possibile associare più di una nota al documento/fascicolo; per ciascuna può essere impostata una tra le seguenti tipologie di visibilità:

- **Tutti:** è visibile a tutti gli utenti che hanno la visibilità sul documento /fascicolo;
- **Ruolo**: è visibile solamente agli utenti del ruolo dell'utente creatore della nota;
- **Personale:** è visibile solamente all'utente che l'ha creata.
- **RF (se gli RF sono configurati nel sistema):** è visibile ai soli ruoli appartenenti all'RF

Figura 87 – Nota

Nella creazione del documento e del fascicolo per inserire la nota è necessario selezionare una delle tipologie riportate ed inserire la nota nel campo visualizzato nella Figura 87.
Se si sceglie la tipologia "RF" vi è anche la possibilità di selezionare le note da un elenco pre-configurato.
In tal caso infatti, compare un campo di testo mediante il quale ricercare le note disponibili da un elenco precedentemente alimentato come illustrato nel paragrafo 4.13.
La ricerca avviene nel modo di seguito descritto.
Digitando nel campo di testo alcuni caratteri della nota desiderata, il sistema effettua la ricerca presentando i risultati da un menù a tendina che comparirà direttamente dal campo di testo. Questa ricerca verrà effettuata in modalità "Contiene" (like %<testo>%). La selezione di una frase dal menu a tendina provocherà l'inserimento di una nuova nota.

Figura 88 – Scelta nota dall'elenco

In ognuno dei precedenti casi, modifiche e cancellazioni di note sono consentite solamente all'utente creatore.

La creazione e la modifica della nota del documento e del fascicolo può essere effettuata selezionando l'icona , che consente di visualizzare il numero di note inserite nel documento/fascicolo e riporta il dettaglio:

- **Note**: in cui è presente il testo;
- **Utente**: indica l'utente ed il ruolo con cui ha creato la nota;
- **Data**: il giorno in cui è stata inserita;
- **Visibilità**: (della nota) indica se la nota è visibile solo all'utente creatore, al ruolo, all'RF o a tutti quelli che hanno visibilità sul documento/fascicolo;
- : se si seleziona l'icona si cancella la nota a cui è associata. La rimozione è consentita solo all'utente creatore della nota.
- **Seleziona**: permette di selezionare la nota.

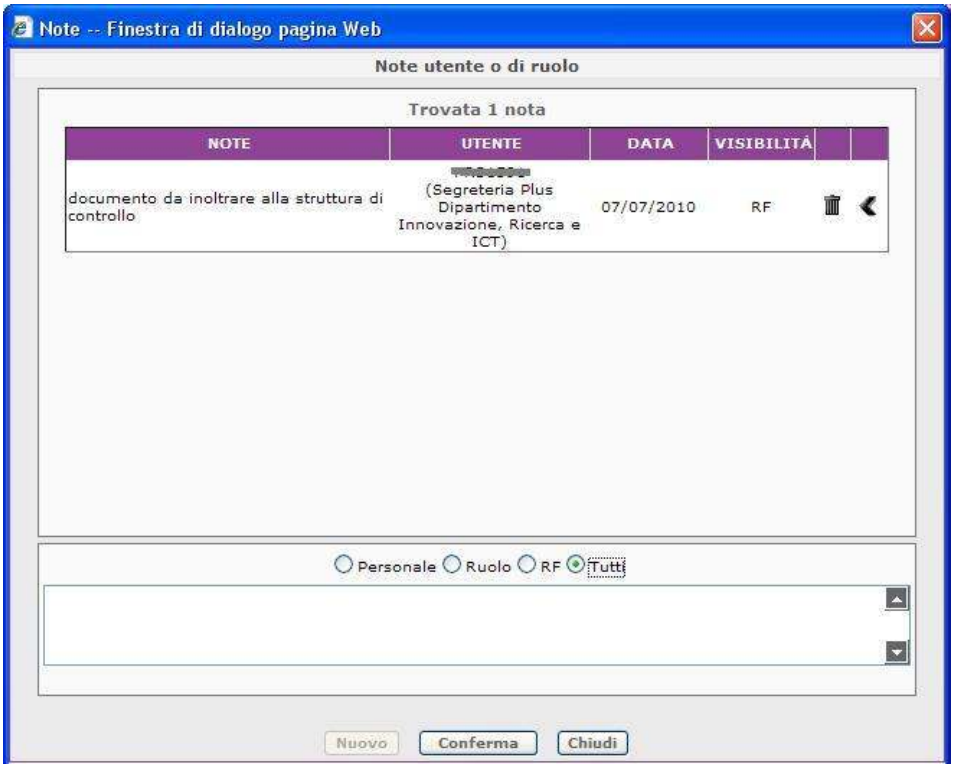


Figura 89 – Dettaglio nota

Nella parte bassa della pagina è presente la selezione del tipo visibilità sulla nota, il campo per digitare il testo ed infine i pulsanti Nuovo, Conferma, Chiudi.

Per modificare la nota visualizzata, si inserisce la modifica nel campo testo e se necessario si cambia la tipologia della visibilità e si seleziona il pulsante Conferma.
Per inserire una nuova nota si seleziona il pulsante Nuovo, si sceglie la tipologia di visibilità che si vuole dare alla nota, si inserisce il testo e si seleziona il pulsante Conferma.
Se si vuole uscire dal dettaglio selezionare il pulsante Chiudi.

2.8.1.2.1 Nota presente su un documento/fascicolo in sola lettura

Quando un documento/fascicolo è in sola lettura, selezionando l'icona della matita è possibile modificare la nota solo per le 2 seguenti tipologie di visibilità:

- **Ruolo**: è visibile solamente agli utenti del ruolo dell'utente creatore della nota;
- **Personale:** è visibile solamente all'utente che l'ha creata.

In ognuno dei precedenti casi, modifiche e cancellazioni di note sono consentite solamente all'utente creatore.

Figura 90 – Nota in sola lettura

2.8.1.3 Fascicolazione rapida – ricerca fascicoli e sottofascicoli

Attraverso la selezione dell'icona presente vicino al campo Fascicolazione rapida, si apre una finestra di dialogo per la ricerca dei fascicoli/sotto fascicoli, in cui è possibile impostare una serie di filtri ed effettuare la ricerca. Questi sono:

- **Titolario**: permette di selezionare il Titolario di interesse, che può essere:
  - *"titolario attivo":* su tale titolario l'utente può effettuare ogni tipo di operazione (creazione/fascicolazione/apertura del fascicolo/chiusura del fascicolo);
  - *"titolario in vigore dal gg/mm/aaaa al gg/mm/aaaa" :* su cui l'utente non può creare nuovi fascicoli; ma può solamente effettuare la fascicolazione/classificazione fino alla chiusura dei fascicoli;
- **Registro**: per i protocolli mostra, in modalità non selezionabile, il registro a cui è associato il protocollo e a cui devono essere legati i fascicoli / sotto fascicoli che si possono selezionare. Per i documenti grigi, se il ruolo che sta utilizzando l'applicativo VTDOCS può lavorare su più di un registro, mostra un menù a tendina da cui l'utente può selezionare il registro;
- **Aperto il**: permette di specificare la data di apertura del fascicolo. E' possibile effettuare la selezione da un menù a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di apertura fascicolo. La data può essere inserita attraverso la selezione da calendario o semplicemente editandola;
- **Creato il**: permette di specificare la data di creazione del fascicolo. E' possibile effettuare la selezione da un menù a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di creazione fascicolo. La data può essere inserita attraverso la selezione da calendario o semplicemente editandola;
- **Numero**: è il numero progressivo del fascicolo che si vuole cercare;
- **Anno**: consente di indicare l'anno di creazione del fascicolo;
- **Tipo**: permette di effettuare ricerche per fascicoli procedimentali o generali. Se si seleziona l'opzione 'Generali' vengono disabilitati i filtri "Stato", "Numero", "Anno";
- **Descrizione**: consente di effettuare ricerche in base a parole presenti nella descrizione del fascicolo;
- **Note**: permette di effettuare le ricerche in base alle parole contenute nelle note del fascicolo;
- **Collocazione fisica**: permette di specificare l'esatta collocazione del fascicolo (selezionabile attraverso la rubrica o mediante digitazione del codice nel primo dei due campi);

- **Data collocazione**: permette di specificare la data di collocazione fisica del fascicolo. E' possibile effettuare la selezione da un menù a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di collocazione. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Sottofascicoli**: in tale campo se si edita la descrizione del sottofascicolo la ricerca restituisce i fascicoli che contengono un sottofascicolo, a qualunque livello, la cui descrizione contiene il testo specificato;

Dopo aver ottenuto la lista dei fascicoli è possibile, premendo l'icona  , aprire un'ulteriore finestra di dialogo che mostra l'albero dei sottofascicoli. Da quest'ultima, come per la ricerca dei nodi di titolario, è possibile ricercare un sottofascicolo attraverso il contenuto del campo "descrizione".
La selezione del sottofascicolo e la conferma mediante il pulsante OK chiude entrambe le finestre.
Nel caso della fascicolazione rapida il sistema popola i campi "codifica" e "descrizione" che nel caso del sottofascicolo sono strutturate come segue:

Codice: <codice fascicolo>//<sottofascicolo>
Descrizione: <Descrizione fascicolo>//<sottofascicolo>

Quindi, nell'esempio mostrato nella Figura 91 il risultato è:

Codice = 4-2008-2.2.2//Aumenti/PM
Descrizione = Remunerazione//Aumenti/PM

Nel caso del dettaglio fascicolo si posiziona automaticamente sul sottofascicolo visualizzandone il contenuto.

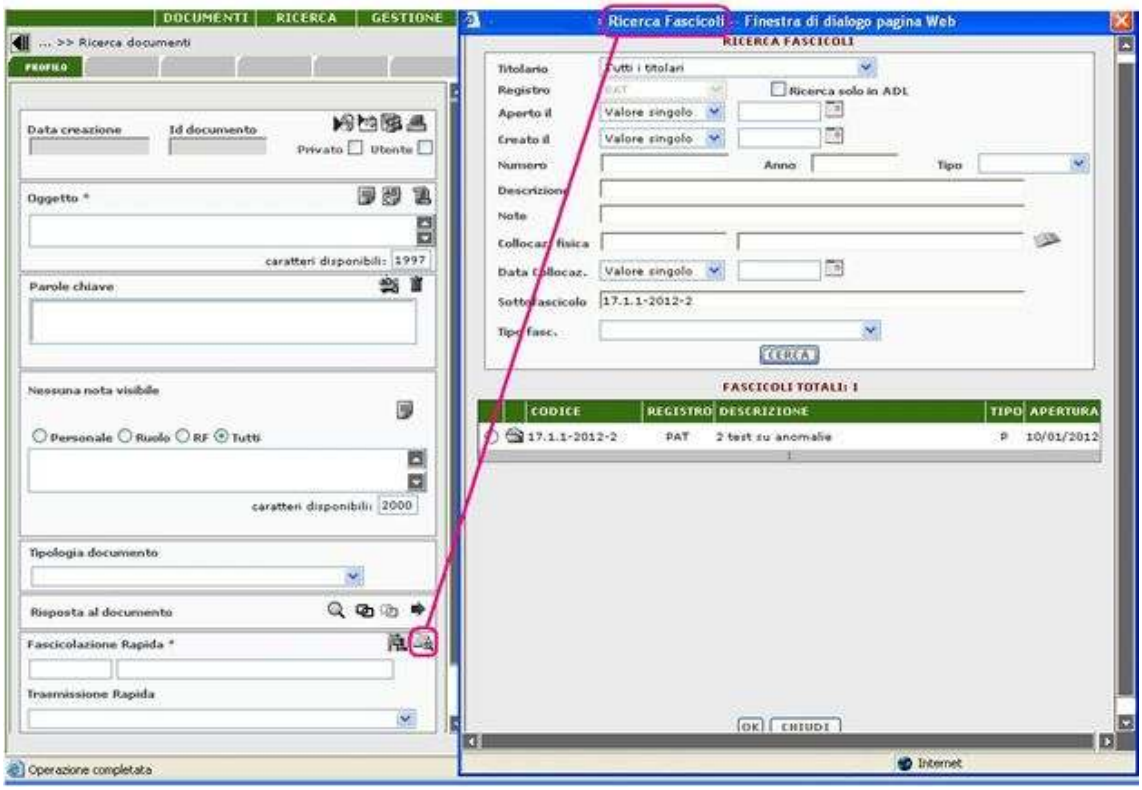


Figura 91 – Ricerca fascicoli/sotto fascicoli per fascicolazione rapida: prima parte

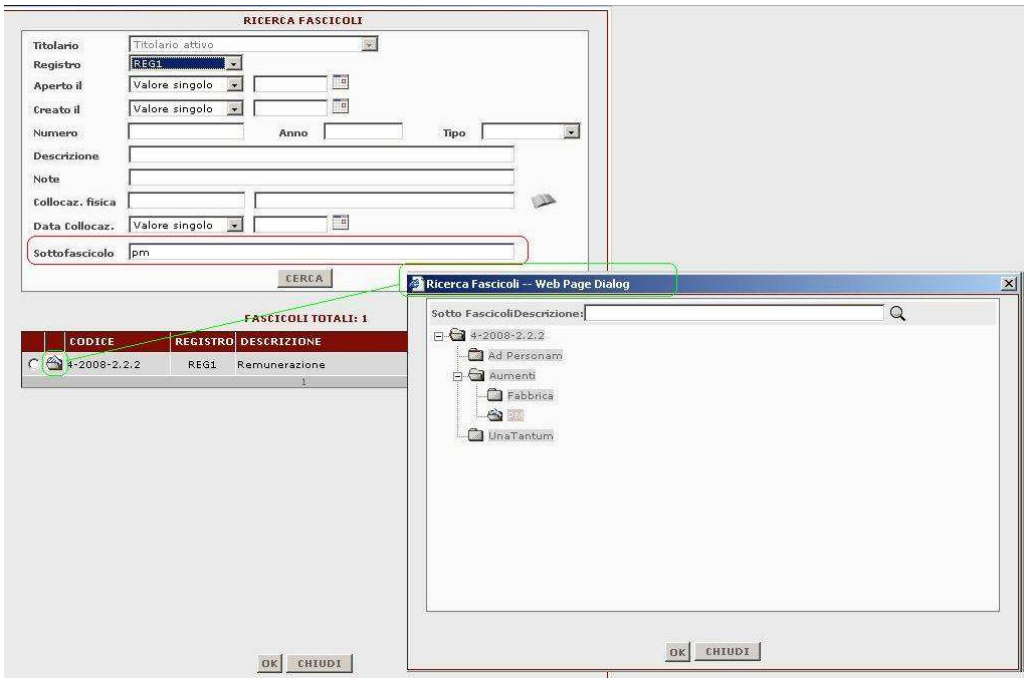


Figura 92 – Ricerca fascicoli/sotto fascicoli per fascicolazione rapida: seconda parte

2.8.1.4 Risposta al documento

2.8.1.4.1 Documento in risposta ad un documento (protocollato o non)

Tale funzionalità consente di associare il documento che si sta creando a documenti non protocollati e, se attivata la funzionalità generalizzata, anche a documenti protocollati.
La funzionalità è accessibile, a partire dalla scheda di creazione di un documento, mediante l'icona , presente nell'area "Risposta al documento", che apre una finestra di dialogo che consente di individuare, attraverso dei filtri di ricerca, il documento cui si vuole rispondere.
La modalità di funzionamento è analoga a quella utilizzata nelle risposte dei documenti protocollati (2.7.1.5.3).

Dopo aver inserito i dati relativi al documento da ricercare, selezionando il pulsante "Cerca", il sistema restituirà nella parte centrale l'elenco dei documenti che soddisfano i criteri di ricerca.

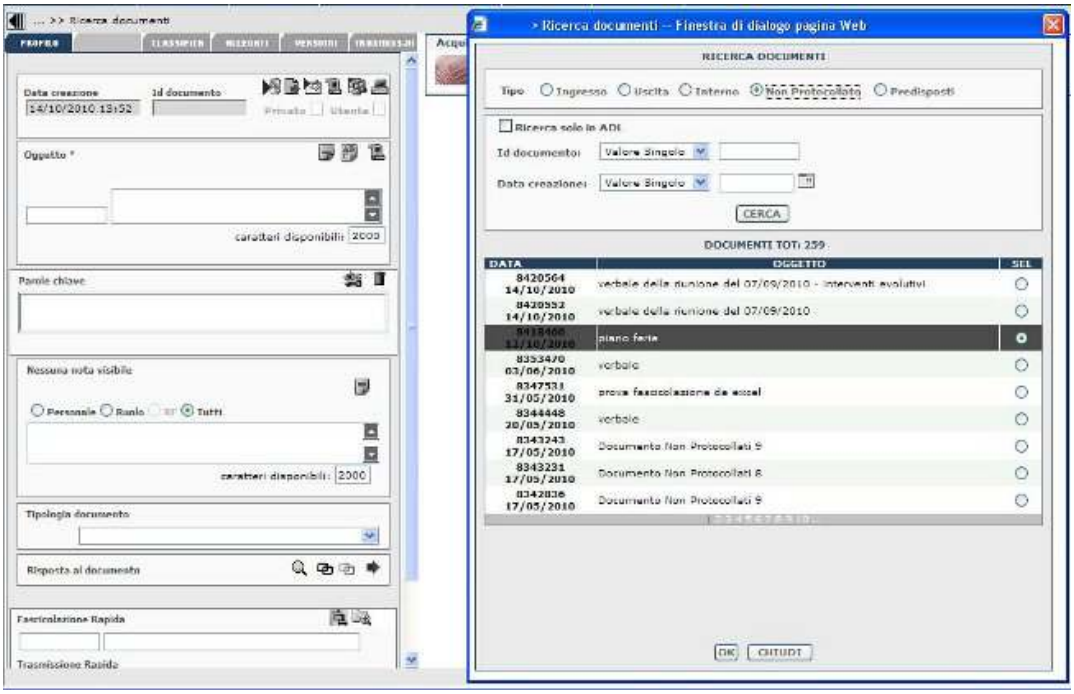


Figura 93- Ricerca dei documenti cui rispondere

Quando si individua il documento cui rispondere, lo si seleziona e si conferma con il pulsante "OK".
A questo punto il sistema effettua dei controlli per verificare la congruenza dei dati tra i due documenti che si desidera collegare. In particolare, si verifica la congruenza del valore specificato per il campo oggetto.
L'utente prima di selezionare un documento può aver compilato, anche parzialmente, la scheda del documento grigio in creazione. Se vengono trovati dei dati incongruenti, si avvisa l'utente aprendo una opportuna finestra di dialogo (Figura 94) nella quale sono presentate diverse possibilità per proseguire l'operazione:

- Continua e sovrascrivi i dati: consente di proseguire l'operazione utilizzando i valori del protocollo in uscita selezionato. Questa è l'opzione predefinita;

- Continua utilizzando i dati immessi: consente di proseguire il collegamento dei documenti con i dati immessi dall'utente nella scheda del protocollo in ingresso, nonostante siano diversi da quelli del protocollo a cui si sta rispondendo;
- Seleziona un altro documento: consente di chiudere la pagina di avviso e scegliere un altro protocollo in uscita a cui rispondere.

Figura 94 – Finestra di dialogo per avviso dati incongruenti per risposta ad un documento

Nel momento in cui si seleziona il pulsante OK, la scheda del documento in risposta viene popolata di conseguenza, secondo l'opzione che è stata selezionata. Inoltre viene popolato il campo "Risposta al documento" con il codice identificativo del documento (se è stato selezionato un documento grigio) o con la segnatura di protocollo se è stato selezionato un documento protocollato. Viene abilitato il pulsante Salva per poter confermare gli inserimenti effettuati.

E' inoltre possibile creare, a partire da un documento non protocollato già inserito nel sistema, un documento in risposta, selezionando l'icona presente nell'area "Risposta al documento", attiva solo per documenti già salvati.
Selezionando l'icona si apre la scheda relativa al nuovo documento grigio (in fase di creazione), in risposta al documento da cui si è partiti, dove è abilitato il pulsante Salva e dove sono stati automaticamente compilati i seguenti campi:

- Risposta al documento: tale campo viene popolato con l'id del documento grigio cui il documento in esame costituisce risposta;
- Oggetto: tale campo viene popolato con l'oggetto relativo al documento cui si sta rispondendo.

Una volta confermata l'operazione di collegamento con il pulsante "Salva" verrà effettuato il collegamento tra i documenti in questione.

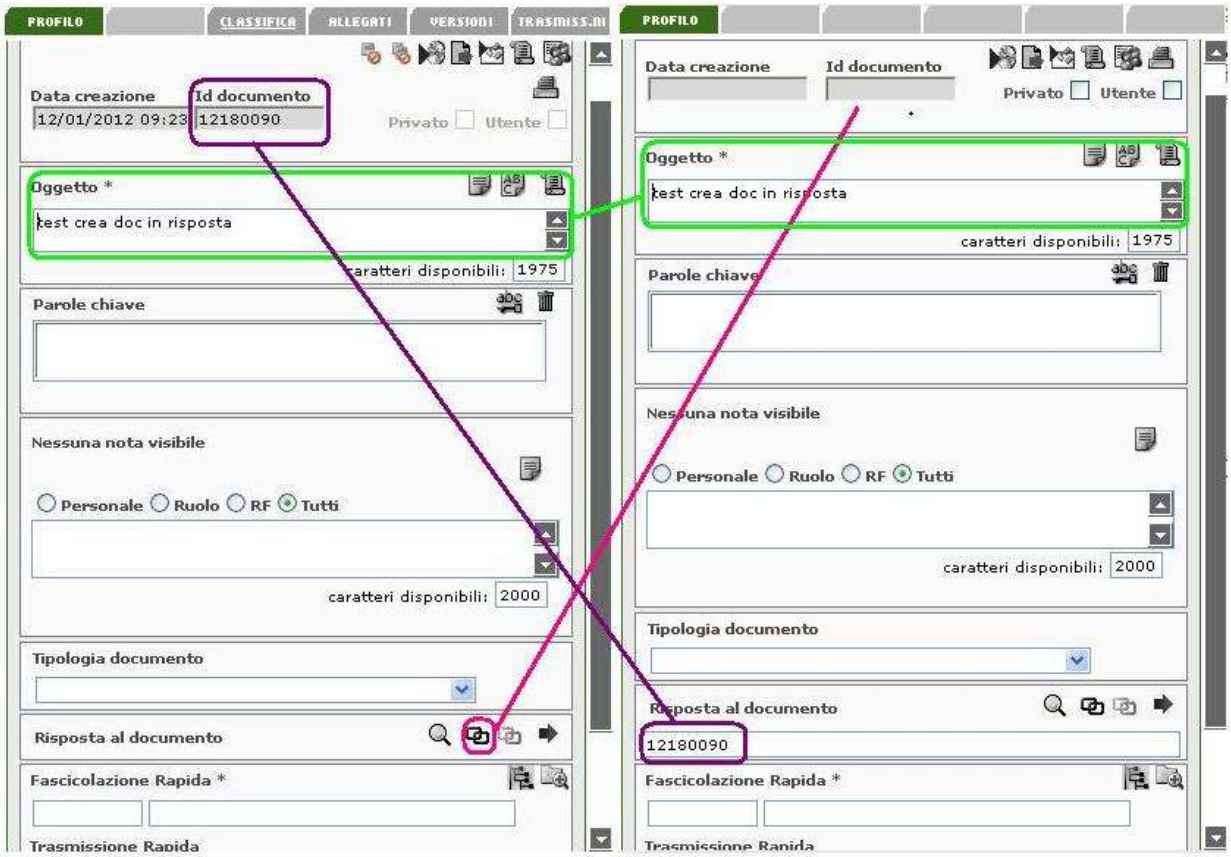


Figura 95 - Creazione documento in risposta: funzionalità relativa al "crea documento in risposta"

E' anche possibile creare un protocollo come risposta ad un documento grigio selezionando l'icona . In questo caso si apre la scheda di un nuovo documento in ingresso (in fase di creazione) dove sono stati compilati automaticamente i seguenti campi:

- Risposta al documento: tale campo viene popolato con l'id del documento grigio cui il documento in esame costituisce risposta;
- Oggetto: tale campo viene popolato con l'oggetto relativo al documento cui si sta rispondendo.

L'utente può selezionare anche una tipologia diversa da quella "ingresso", compilare i campi relativi ed effettuare la protocollazione.

In qualunque momento successivo è possibile visualizzare il dettaglio del documento a cui si è risposto mediante l'uso dell'icona .
Dalla scheda di un documento è possibile visualizzare direttamente mediante l'uso dell'icona la scheda del documento in risposta (se esiste un unico documento in risposta), oppure la lista dei documenti in risposta (se esistono più documenti in risposta). In quest'ultimo caso si apre una pagina che mostra tutti documenti che rispondono a quel particolare documento come è visibile in Figura 96

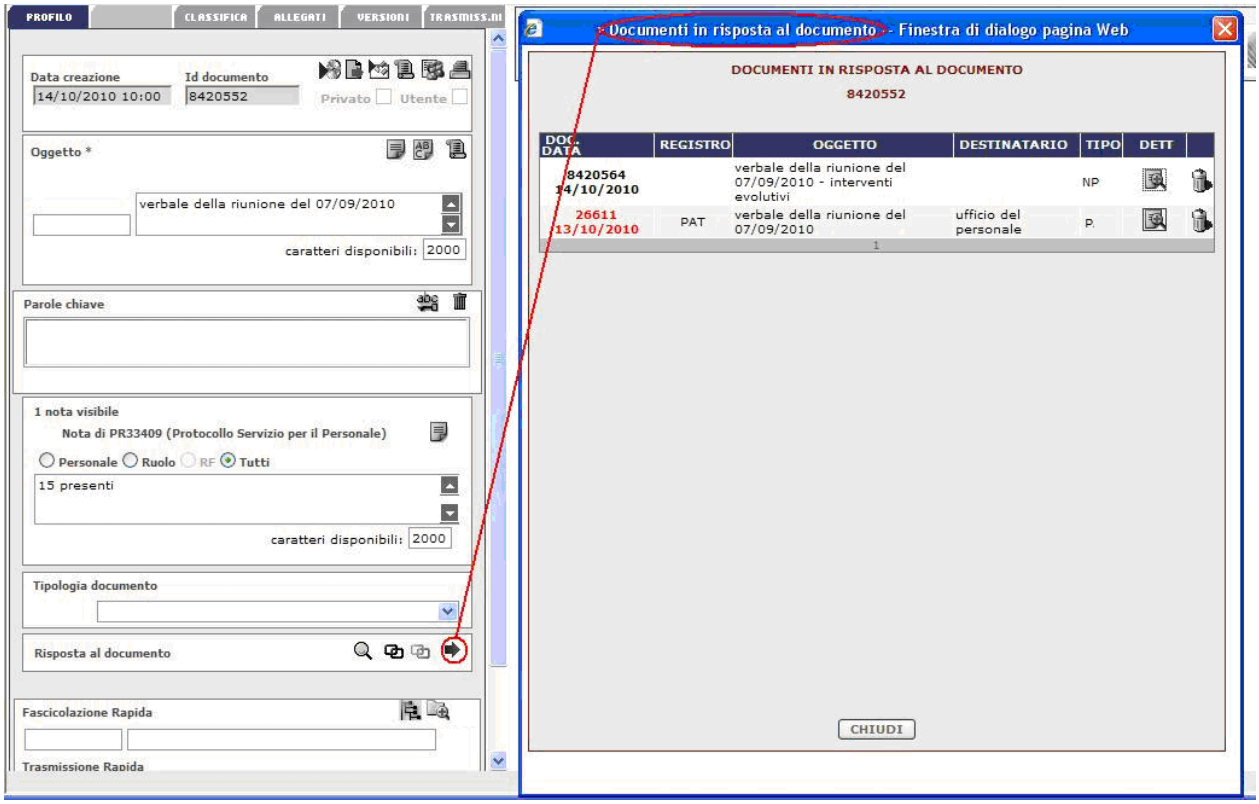


Figura 96 – Elenco documenti in risposta

Si noti che la possibilità di creare documenti diversi da quello grigio è una funzionalità aggiuntiva configurabile e che il comportamento classico è quello di creare come risposte solo documenti grigi.

2.9 Documento repertoriato

Se l'Amministrazione è abilitata alla gestione dei Repertori, è possibile definire un contatore di repertorio. Tale contatore può riferirsi:

- alla tipologia
- ad un RF
- ad una AOO

Tutti i documenti di una tipologia repertoriata (ossia in cui è definito un contatore di repertorio) vengono associati al registro di repertorio corrispondente.
Per tale registro esistono funzionalità di apertura, chiusura e stampa analoghe a quelle previste per il registro di protocollo (vedere par. 3.1.2.6, 4.2).

In analogia a quanto definito per i documenti protocollati, dalla pagina di dettaglio dei campi profilati (Figura 97), tramite il pulsante 'Annulla' in corrispondenza della segnatura di repertorio, è possibile annullare il documento repertoriato. L'annullamento deve essere motivato con una nota (Figura 98). Una volta confermato l'annullamento, la segnatura di repertorio sarà visibile evidenziata in rosso con i caratteri barrati. Accanto alla segnatura è possibile visualizzare la data di annullamento. La nota di annullamento sarà visibile nello storico dei campi profilati (Figura 98).

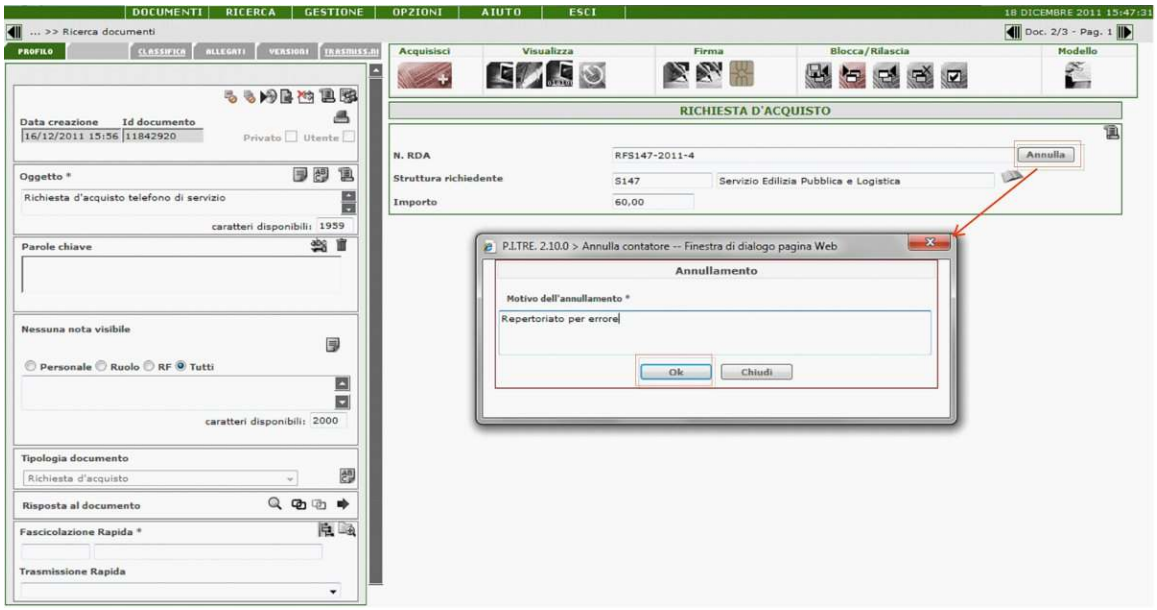


Figura 97 – Annullamento di un documento repertoriato

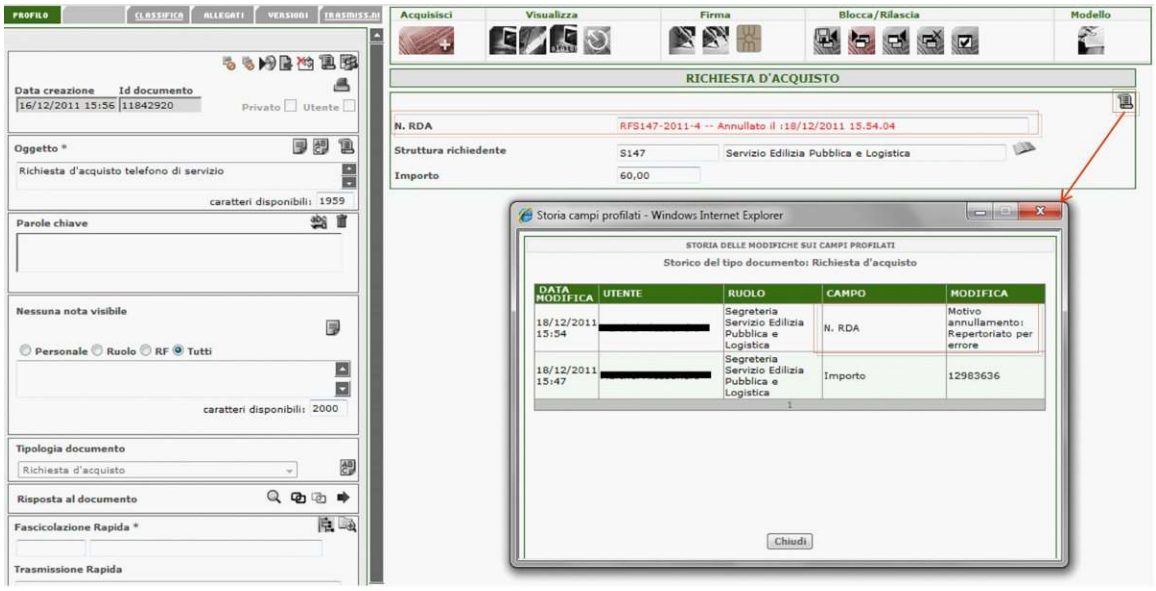


Figura 98 – Visualizzazione di un documento repertoriato annullato

2.10 Classifica

I documenti possono essere organizzati logicamente in fascicoli virtuali. Ogni documento può appartenere ad uno o più fascicoli; tale appartenenza si realizza mediante semplice associazione fra il documento e i fascicoli, il che permette di evitare la moltiplicazione dei documenti all'atto dell'inserimento nei fascicoli. Il

pannello riportato in Figura 99 consente all'utente di inserire un documento protocollato all'interno di un fascicolo già esistente, popolando in modo opportuno i campi "Cod. Classifica" (in tal caso il documento verrà inserito nel fascicolo generale associato al nodo di titolario indicato) e/o "Cod. Fascicolo".

E' possibile popolare tali campi secondo tre differenti modalità:

- impostando la casella di selezione accanto alla voce "codice" ed editando direttamente un codice di titolario;
- impostando la casella di selezione accanto alla voce "livello" e scegliendo i valori dei 6 livelli di catalogazione con l'ausilio di menù pre-impostati presenti nella pagina;
- accedendo al titolario di classificazione tramite la selezione dell'icona . Viene in questo modo visualizzato un pannello con la struttura del titolario dal quale è possibile selezionare il livello da riportare nel pannello di classificazione. Il titolario viene visualizzato a partire dal livello digitato dall'utente nel campo 'Cod.Classifica' o per intero qualora l'utente non abbia specificato alcun codice prima di selezionare l'icona.

Dopo aver impostato i valori per tutti i campi è possibile:

- inserire il documento all'interno di un fascicolo generale selezionando il pulsante Classifica;
- inserire il documento nell'area di lavoro premendo il pulsante ADL;
- creare un nuovo fascicolo tramite il pulsante Nuovo (abilitato soltanto dopo che è stato selezionato un codice classifica esistente). Dopo aver selezionato il pulsante, si visualizza il pannello mostrato nella Figura 101.

L'utente deve inserire obbligatoriamente una **descrizione** che identifica il fascicolo che si sta creando.
In base alle esigenze ed alle proprietà a cui è soggetto il fascicolo che si sta creando, si possono:

- inserire eventuali note annesse al fascicolo in questione, così come descritto nel paragrafo 2.8.1.2;
- selezionare il campo "Privato" se il fascicolo deve avere una visibilità limita, quindi visibile solo all'utente e al ruolo creatore. La visibilità del fascicolo può essere modificata solamente attraverso la trasmissione con un messaggio che indica che: "Si sta trasmettendo un fascicolo marcato come privato. Procedere comunque?" Selezionando "OK" si modifica la visibilità del fascicolo, con l'opzione "annulla" non viene effettuata alcuna operazione;
- selezionare il campo "Cartaceo" se esiste o si andrà a creare un fascicolo cartaceo con le stesse caratteristiche di quello virtuale;
- modificare il campo "Collocazione fisica", popolato in automatico dal sistema;
- modificare il campo "data collocazione" del fascicolo, popolato in automatico dal sistema;
- se esistono delle tipologie fascicolo, selezionare un valore dal menù a tendina "Tipologia Fascicolo". Nel menu a tendina verranno mostrate solamente le tipologie in esercizio (non sospese). Dopo aver selezionato la tipologia di interesse, si visualizzano le informazioni che sono state inserite dall'utente amministratore in fase di configurazione della tipologia. Nel caso in cui, al nodo selezionato, sia stata associata una tipologia di fascicolo bloccata, si visualizza il pannello di creazione del fascicolo con un'unica tipologia associata e non modificabile. Per questa tipologia è possibile popolare solo i campi associati con le informazioni adeguate.
  Per i dettagli sui campi da utilizzare nelle tipologie si rimanda al paragrafo 2.7.1.1 dove sono descritti i campi dei tipi documento e che possono essere utilizzati anche per i tipi fascicolo, con l'eccezione di "*contatore con sottocontator"e* ed "*etichetta".*

In fase di definizione delle tipologie di fascicoli, mediante lo strumento di amministrazione, è possibile definire dei "CAMPI COMUNI" che possono essere associati a più tipologie di fascicoli.

All'utente che crea i fascicoli la presenza di questi campi non sarà evidente, in quanto essi compariranno nel pannello con i campi di profilazione insieme agli altri campi associati al fascicolo senza particolari formattazioni che ne specifichino la particolare natura.

Dopo aver inserito i dati necessari per la creazione del fascicolo procedimentale, si seleziona il pulsante Inserisci .
A questo punto è possibile classificare il documento sulla voce di classificazione selezionata e inserirlo nel fascicolo procedimentale appena creato, selezionando il pulsante "Classifica".

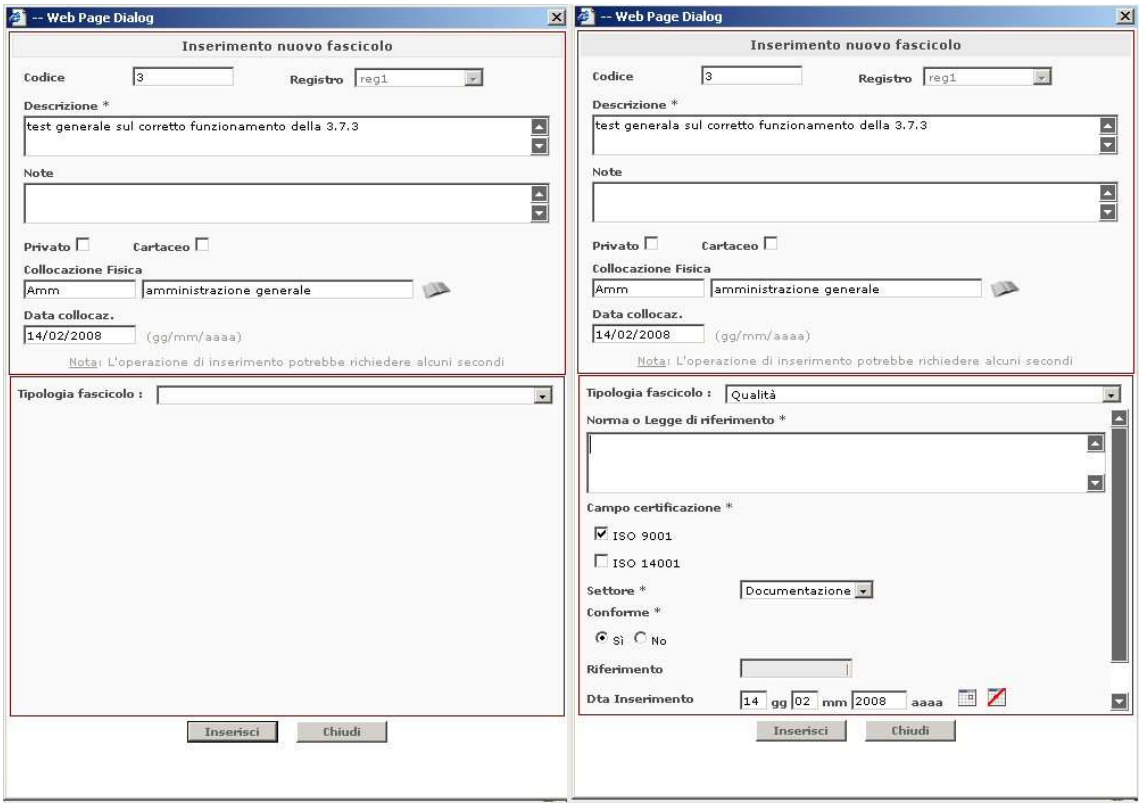


Figura 99 – Creazione fascicolo procedimentale (senza selezione tipologia fascicolo e con selezione tipologia fascicolo)

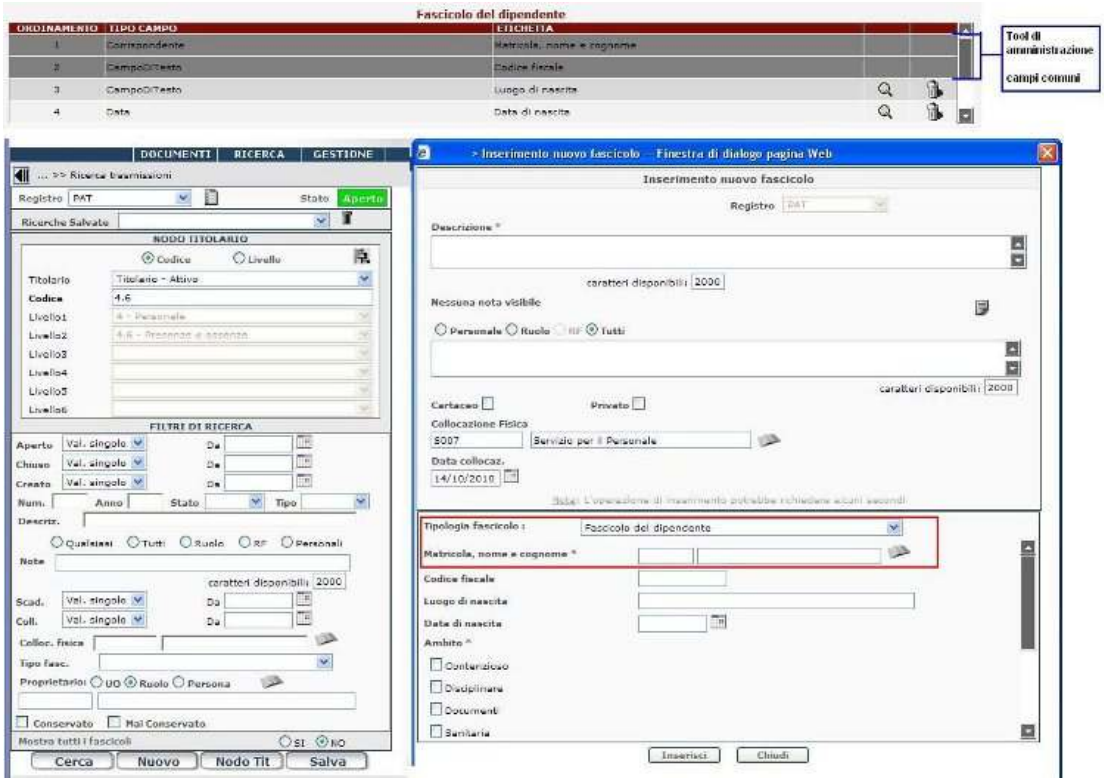


Figura 100 – Fascicolo procedimentale- tipologia fascicolo con campi comuni

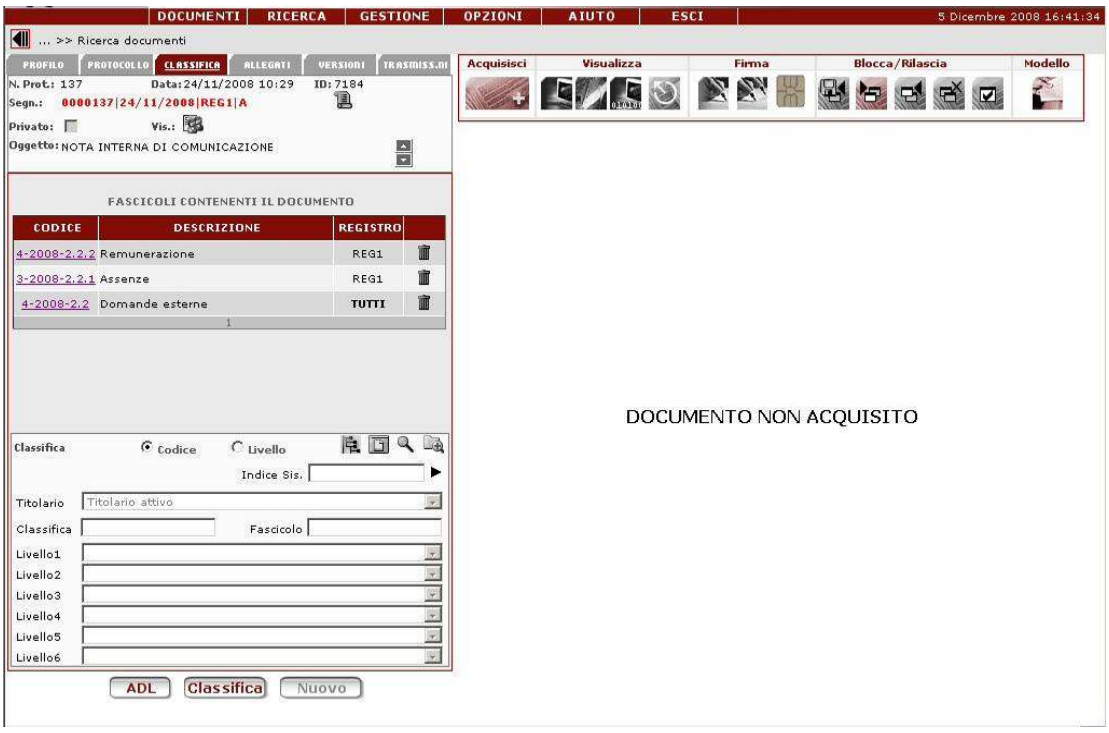


Figura 101 - Classificazione di un documento

VTDOCS permette di attivare un nuovo titolario storicizzando quello in uso (operazione che si effettua tramite l'applicazione di amministrazione). Il titolario corrente viene indicato come *"titolario attivo"*. I titolari cessati sono indicati come *"titolario in vigore dal gg/mm/aaaa al gg/mm/aaaa"*, dove le due date sono rispettivamente la data di attivazione e la data di cessazione del titolario.

Come prima operazione l'utente deve selezionare il Titolario di interesse, che può essere:

- *"titolario attivo":* su tale titolario l'utente può effettuare ogni tipo di operazione (creazione/fascicolazione/apertura del fascicolo/chiusura del fascicolo);
- *"titolario in vigore dal gg/mm/aaaa al gg/mm/aaaa" :* su cui l'utente non può creare nuovi fascicoli; può solamente effettuare la fascicolazione/classificazione fino alla chiusura dei fascicoli.

Se non ci sono titolari storicizzati la voce che appare è "titolario attivo" altrimenti all'apertura della pagina compare la scritta "Tutti i titolari".
Il sistema in realtà può essere configurato affinché la scelta di default sia "titolario attivo" che è quello sul qualche presumibilmente si classificano/fascicolano più di frequente i documenti.

Dopo aver verificato ed eventualmente selezionato il titolario di interesse, bisogna valorizzare il campo 'Classifica' utilizzando le icone , e descritte di seguito oppure inserire nel campo "Indice sis." la voce di indice sistematico cui il documento che si sta classificando fa riferimento. In questo caso il sistema restituisce la valorizzazione del campo "Classifica" e dei rispettivi livelli sulla base dell'associazione "voce di indice sistematico > nodo di titolario". Dall'interfaccia utente è possibile importare/esportare da uno specifico file excel le voci dell'indice sistematico per i ruoli preposti a tale funzionalità.

L'icona permette di visualizzare nella parte destra del pannello tutti i fascicoli generali/procedimentali presenti nell'Area di Lavoro fascicoli dell'utente, così come mostrato nella Figura 102.
Nella lista dei fascicoli procedimentali e/o generali a ciascun fascicolo è associata una casella selezionabile, che per default risulta non selezionata. L'utente può utilizzarla per selezionare singolarmente i fascicoli di interesse. Se l'utente ha necessità di classificare il documento in tutti i fascicoli presenti nell'area di lavoro, per velocizzare l'operazione, potrà selezionare la casella "Seleziona/deseleziona Tutti" e selezionare l'icona .
Da questa sezione è possibile anche cancellare i fascicoli presenti in area di lavoro; basterà cliccare sulle caselle dei fascicoli che non interessano e attivare l'icona .

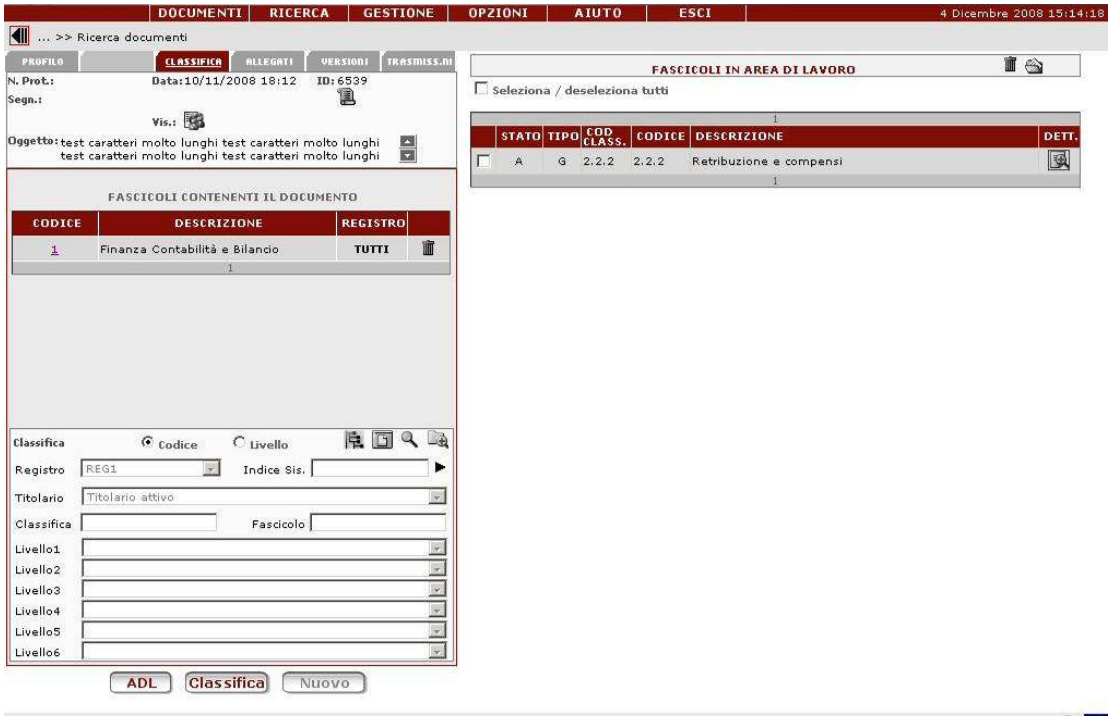


Figura 102 - Multiclassificazione di un documento

Le icone e servono entrambe per effettuare ricerche su fascicoli.
Agendo sull'icona ed il codice del fascicolo di interesse, si effettua la ricerca di tutti i fascicoli procedimentali e generali, collegati a quel nodo di titolario.
Selezionando l'icona si visualizza un pannello, mostrato nella Figura 103, che permette di impostare un filtro di ricerca così come descritto nel paragrafo 2.8.1.3 avendo cura preventivamente di selezionare il titolario su cui si vuole effettuare la ricerca. I dettagli relativi ai campi presenti in tale pannello sono stati illustrati nel paragrafo 3.2.

In questo pannello inoltre sono presenti ulteriori campi per filtrare i risultati della ricerca con i fascicoli descritti in un foglio Excel e con un'ulteriore indicazione disponibile da una lista a tendina che specifica quale attributo è elencato nel foglio excel selezionato. Valori possibili sono:

- Numero di fascicolo;
- Data di apertura;
- Descrizione;
- Codice di classifica;
- Tipologia:
    - Lista delle tipologie di fascicolo
    - Lista attributi della tipologia.

Nel caso di selezione di *Tipologia*, un ulteriore menu a tendina riporterà le tipologie di fascicoli visibili e quindi un'ulteriore combo box riporterà gli attributi per la tipologia selezionata.
Una volta eseguita la normale ricerca dei fascicoli, questa verrà ulteriormente filtrata in modo che tutti i fascicoli trovati siano solo quelli che soddisfano anche la condizione *"Valore dell'attributo selezionato è contenuto nell'elenco indicato dal foglio excel specificato*".

Es.
Un foglio Excel, denominato “Matricole.xls” contenuto nella directory “C:\dipendenti” contiene un elenco di matricole relativi ai dipendenti.
La ricerca verrà filtrata con
Filtra risultati con = C:\DIPENDENTI\MATRICOLE.XLS
Attributo fascicolo = Tipologia
Tipologia = Fascicolo Personale
Attributo tipologia = Matricola

A seguito dell’utilizzo delle icone sopra descritte, è possibile visualizzare nella parte destra del pannello, l’elenco dei fascicoli procedimentali e/o generali richiesti con la classifica indicata. Selezionando, attraverso l’icona , uno dei fascicoli mostrati nella parte destra del pannello viene restituito nella parte bassa un pannello che mostra tutti i dettagli legati al fascicolo. I dati inseriti nella tipologia fascicolo sono visualizzabili attraverso la selezione dell’icona (un esempio è riportato nella Figura 104).

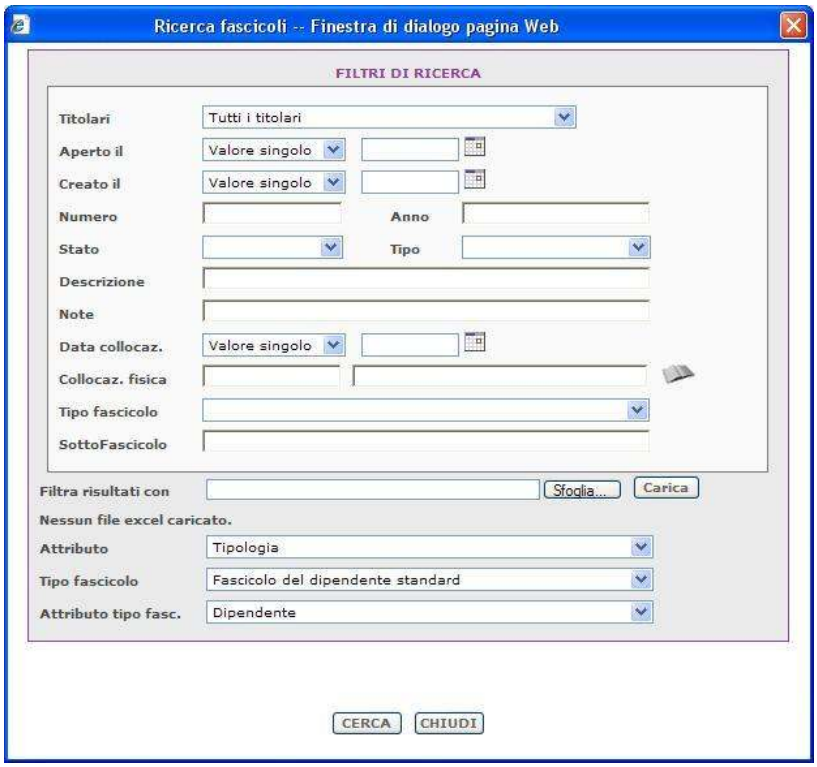


Figura 103 – Finestra di dialogo di ricerca

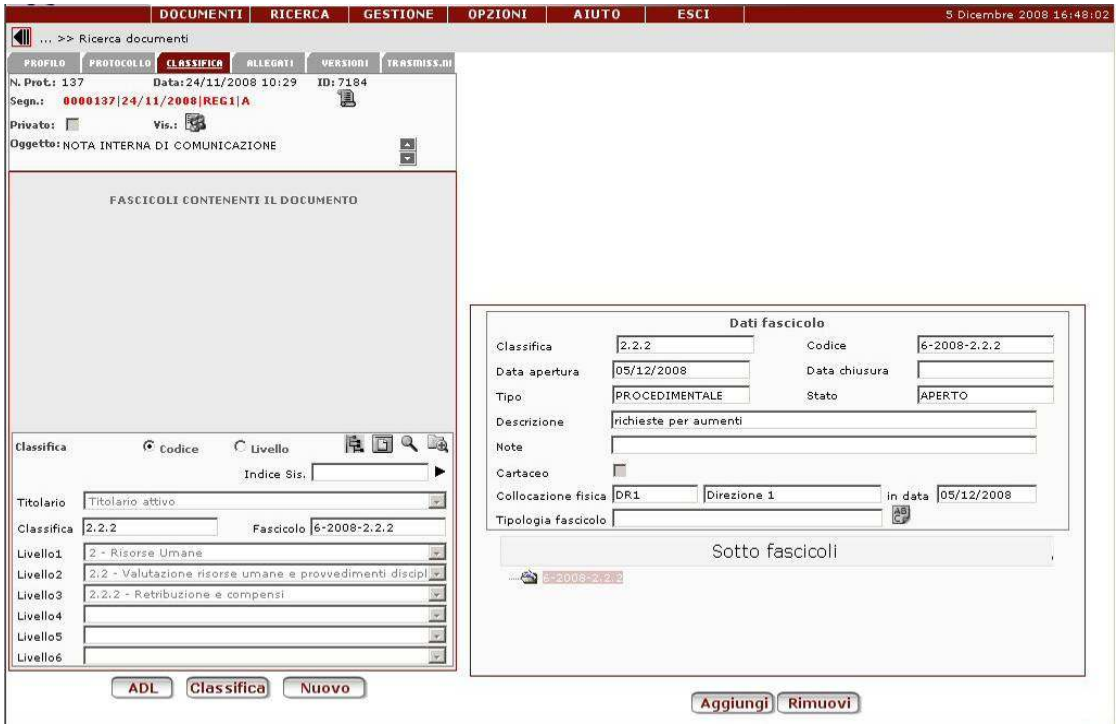


Figura 104 – Dettaglio di un fascicolo procedimentale

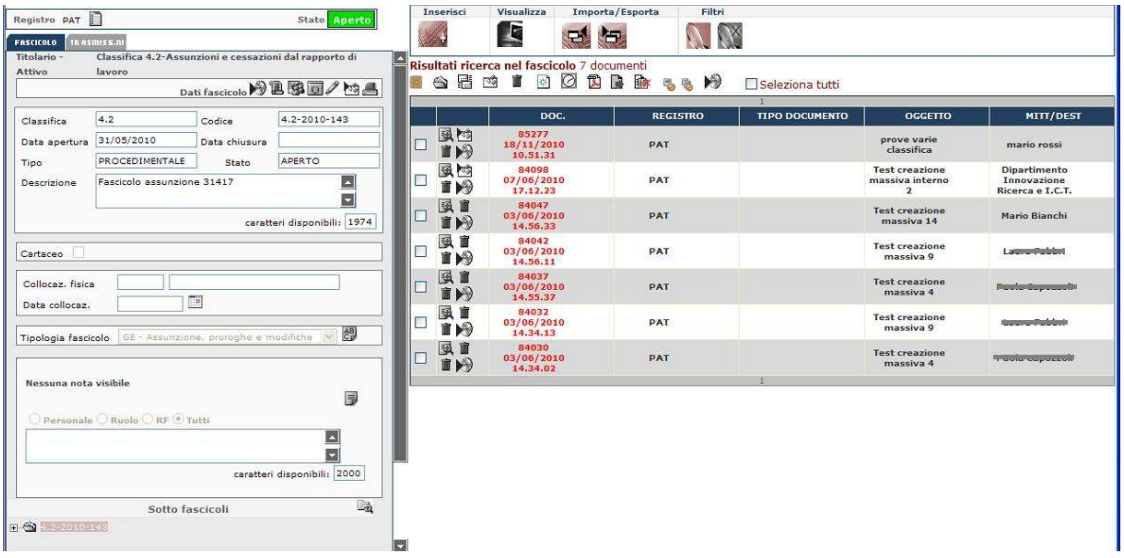


Figura 105 – Profilo di un fascicolo procedimentale

Nella sezione nominata “Fascicoli contenenti il documento” (Figura 104) è mostrato l’elenco dei fascicoli /sottofascicoli in cui è presente il documento e dei quali l’utente che sta visualizzando la pagina ha visibilità.

E' disponibile una funzionalità "avanzata" che consente di visualizzare tutte le classificazioni di un documento. In particolare, in caso di mancanza di diritti di visibilità il codice del fascicolo non apparirà come un LINK ma come testo semplice. Inoltre in tale eventualità NON verrà mostrata la descrizione del fascicolo, ma al suo posto verrà presentata la scritta "*descrizione non visualizzabile*".
La visualizzazione degli elementi nella scheda classifica sarà tale da mettere in prima posizione i fascicoli di cui l'utente ha la visibilità allo scopo di evidenziarli rispetto agli altri.
Un'ulteriore funzionalità attivabile o meno consente di individuare la fascicolazione primaria di un documento. Se questa funzionalità è attiva, nella sezione contenente l'elenco dei fascicoli che contengono il documento, sarà visualizzata in una colonna apposita, l'informazione sulla fascicolazione primaria. L'utente abilitato potrà modificare tale informazione. Per default è primaria la classificazione corrispondente al primo fascicolo/nodo di titolario in cui è stato fascicolato/classificato il documento. Se tale informazione è presente essa verrà riportata anche nella pagina del protocollo nella sezione della fascicolazione rapida.

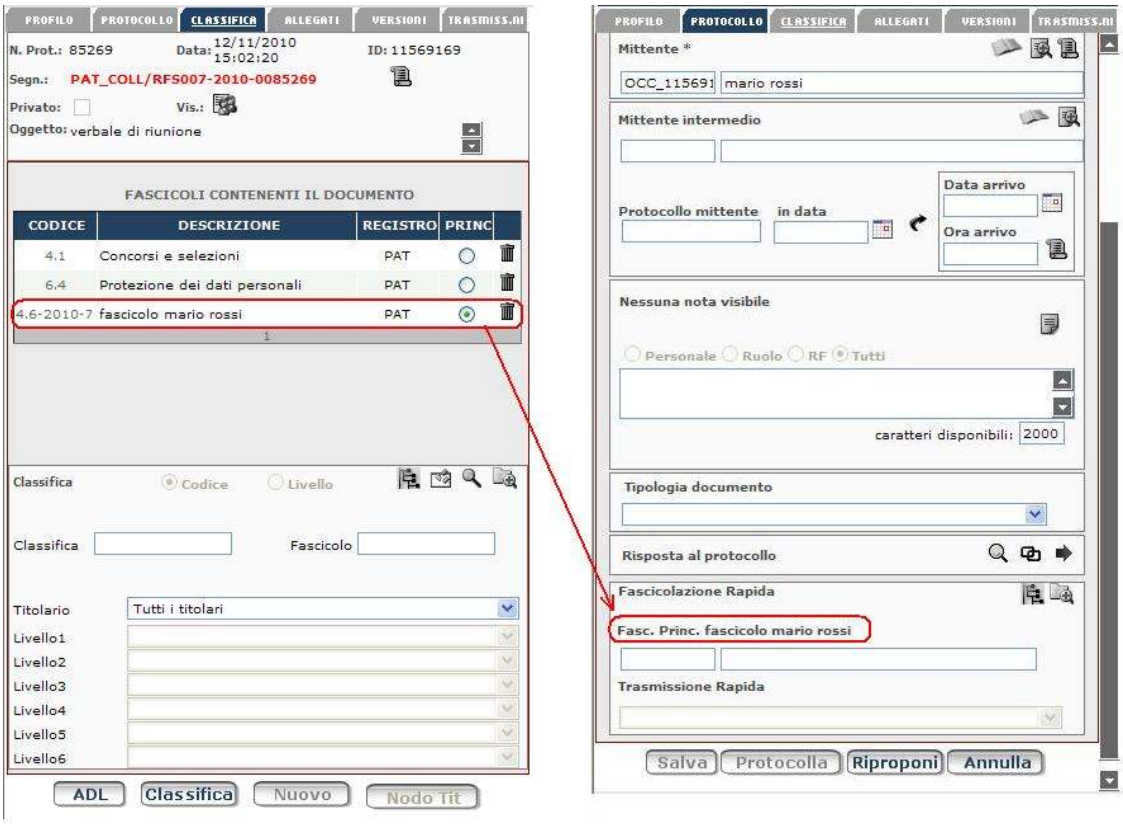


Figura 106 – Fascicolazione primaria

2.11 Allegati

Il pannello proposto in Figura 107 consente di gestire l'associazione tra allegati e documento principale. Si presenta con la dicitura "**ALLEGATI NON TROVATI**".
Il pannello proposto in Figura 107 consente di gestire le diverse tipologie di allegati disponibili per l'utente.
Il sistema in automatico mostra gli Allegati inseriti dall'utente. Mediante opportuni filtri è possibile anche:

- tutti gli allegati del documento (opzione "*Tutti*")

- gli allegati relativi alle ricevute PEC (avvenuta/mancata accettazione, avvenuta/mancata consegna, con errori) (opzione "*PEC*")
- gli allegati relativi alle ricevute PI VTDOCS, se l'amministrazione è abilitata all'utilizzo dell'interoperabilità semplificata (opzione "PI VTDOCS")
- gli allegati generati da sistemi esterni, se l'amministrazione è stata opportunamente abilitata (opzione "*Sist. esterni*").

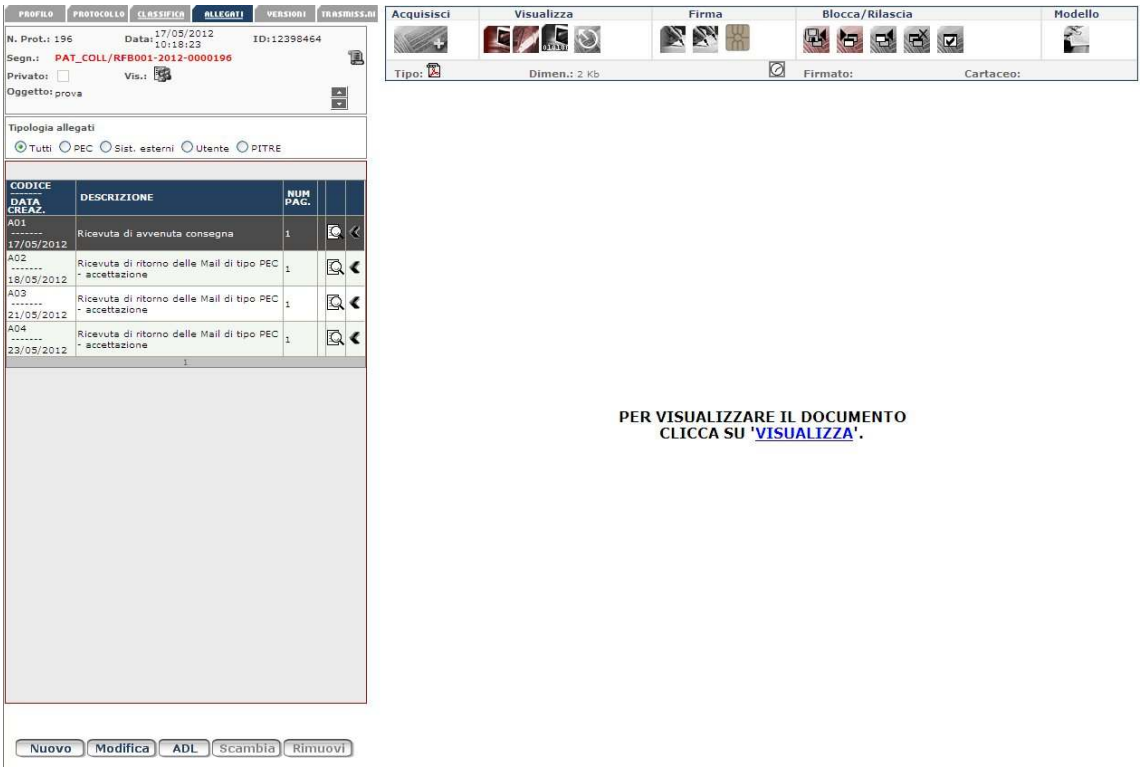


Figura 107 - Sezione allegati

Nel caso di documento ricevuto tramite interoperabilità, fra gli allegati utente sarà compreso anche il file segnatura.xml (Figura 108). La visualizzazione di tale file sarà possibile direttamente dal browser o tramite un visualizzatore dedicato al formato XML (pulsante "Apri versione stampabile") installato precedentemente sulla postazione dell'utente.

Figura 108 - Sezione allegati – Segnatura.xml

Selezionando il pulsante **Nuovo** viene proposto il pannello riportato in Figura 109 nel quale l'utente può inserire sia la descrizione del nuovo allegato, sia il numero di pagine che lo compongono.

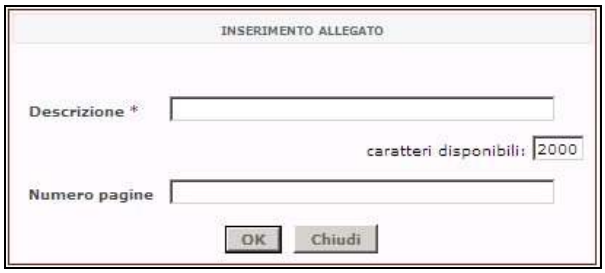


Figura 109 - Inserimento di un nuovo allegato

L'elenco degli allegati già creati riporta le seguenti informazioni (Figura 107):

- **Codice** : rappresenta il codice che viene associato automaticamente da VTDOCS all'allegato;
- **Descrizione**: è un dato obbligatorio che prevede l'inserimento di una breve descrizione al documento che si sta allegando;
- **N.ro pagine**: dato non obbligatorio che prevede la possibilità di indicare il numero di pagine del documento che si sta allegando;
- oppure : visualizza il dettaglio dell'allegato per il quale ancora non è ancora stata acquisita l'immagine del documento; visualizza il dettaglio dell'allegato con immagine del documento ;

- : attraverso la selezione di questa icona è possibile acquisire l'immagine dell'allegato con le modalità descritte per l'acquisizione dell'immagine di un documento (si rimanda a quanto dettagliato nel paragrafo 2.14.1)

Dopo la creazione, l'allegato compare nella lista degli allegati ed è possibile visualizzarne il dettaglio (Profilo e Versioni) selezionando l'icona (o); si rimanda per la descrizione delle funzionalità presenti nella scheda di dettaglio dell'allegato ai paragrafi 2.11.1e 2.11.2.

Tramite l'utilizzo dei seguenti pulsanti, posti a fondo pagina, sono attivabili ulteriori operazioni sugli allegati:

- **Modifica:** dopo aver selezionato un allegato permette di modificare i campi relativi (solo per documenti grigi);
- **ADL:** permette di inserire il documento nell'area di lavoro;
- **Scambia:** sostituisce il contenuto dell'allegato con il contenuto del documento principale (solo per documenti non protocollati). Viene generalmente utilizzato per i documenti inviati senza segnatura xml alla casella istituzionale;
- **Rimuovi:** permette di eliminare un allegato del documento (solo per documenti non protocollati).

La visibilità degli allegati è identica a quella del documento principale. È possibile creare delle versioni degli allegati; non è possibile fascicolari o trasmetterli separandoli dal documento principale.

2.11.1 Profilo del documento allegato

La gestione del Profilo di un documento allegato è analoga a quella del documento principale. Infatti la scheda di profilo con i dettagli del documento si presenta con gli stessi campi e le stesse funzionalità del documento principale.
L'utente ha la possibilità di distinguere gli Allegati inseriti dall'utente da quelli relativi alle ricevute PEC, grazie alla presenza dei seguenti simboli:

- indica un allegato inserito dall'utente;
- indica un allegato relativo ad una ricevuta PEC;
- indica un allegato relativo ad una ricevuta PI VTDOCS.

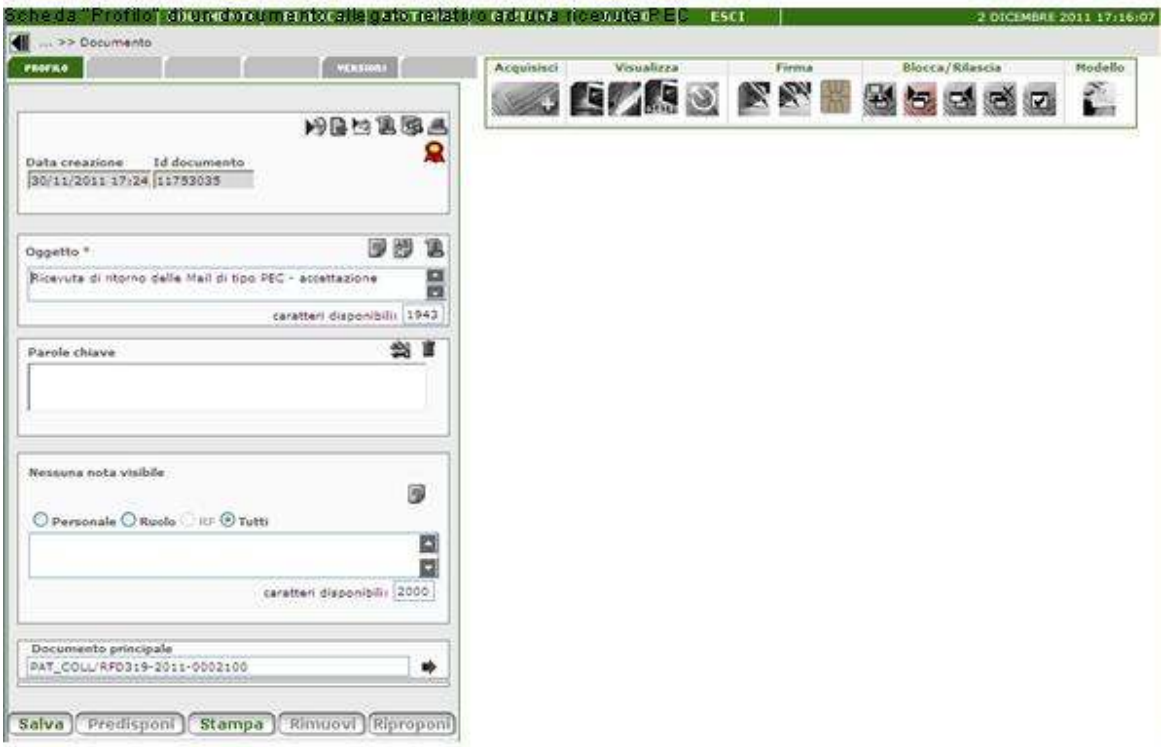


Figura 110 - Scheda "Profilo" di un documento allegato relativo ad una ricevuta PEC

Figura 111 - Scheda "Profilo" di un documento allegato inserito dall'utente

E' quindi possibile profilarli con le informazioni basilari del documento:

- Identificativo del documento;
- Data creazione;
- Oggetto;
- Parole chiave;
- Note.

Sul dettaglio di un allegato è altresì presente il campo "Documento principale", che riporta:

- la segnatura se il documento principale è protocollato;
- l'identificativo del documento se questo è un documento non protocollato.

Accanto a tale campo è presente l'icona  che, se selezionata, permette di visualizzare il dettaglio del documento principale.
L'etichetta "Oggetto" viene sostituita per gli allegati con l'etichetta "Descrizione" e coincide con l'attuale descrizione dell'allegato.

A differenza dei documenti principali, sui documenti allegati non è possibile:

- effettuare trasmissioni;
- classificare/fascicolare;
- inserire in Area di Lavoro;
- utilizzare le tipologia documento;
- stampare l'etichetta;
- crearlo come "privato" o "utente".

Queste ultime azioni/informazioni sono legate al documento principale e quindi non direttamente gestibili dall'allegato.
Si ribadisce che l'allegato non ha visibilità propria, ma è soggetto alla medesima visibilità del documento principale a cui è stato associato e da cui non può essere scisso.
Il dettaglio di un allegato ha i pannelli "CLASSIFICA", "ALLEGATI" e "TRASMISSIONI" disabilitati, mentre è attivo il pannello "VERSIONI".

2.11.1.1 Acquisizione del file del documento allegato

La funzione "Acquisisci", presente nel blocco funzioni dedicato al file del documento, consente di acquisire l'immagine del file da scanner, se cartaceo, oppure in formato elettronico. E' inoltre possibile selezionare la conversione del documento in formato pdf. In quest'ultimo caso il sistema provvederà a creare due versioni del documento, una relativa al documento nel formato originale e l'altra al documento in formato pdf. La conversione viene realizzata tramite l'utilizzo del server Adobe LC. La modalità di conversione è asincrona. Il sistema notifica nella lista delle cose da fare l'avvenuta conversione del PDF. Questa funzionalità è attivabile tramite un apposito parametro di configurazione.

Se è stato acquisito un documento, la parola Visualizza all'interno del messaggio "Per visualizzare il documento clicca su visualizza", è stata trasformata in un link (collegamento). Trascinando con il mouse questa voce in una mail o su un documento, l'indirizzo del link viene riportato su di essi per consentire l'accesso al documento dall'esterno.

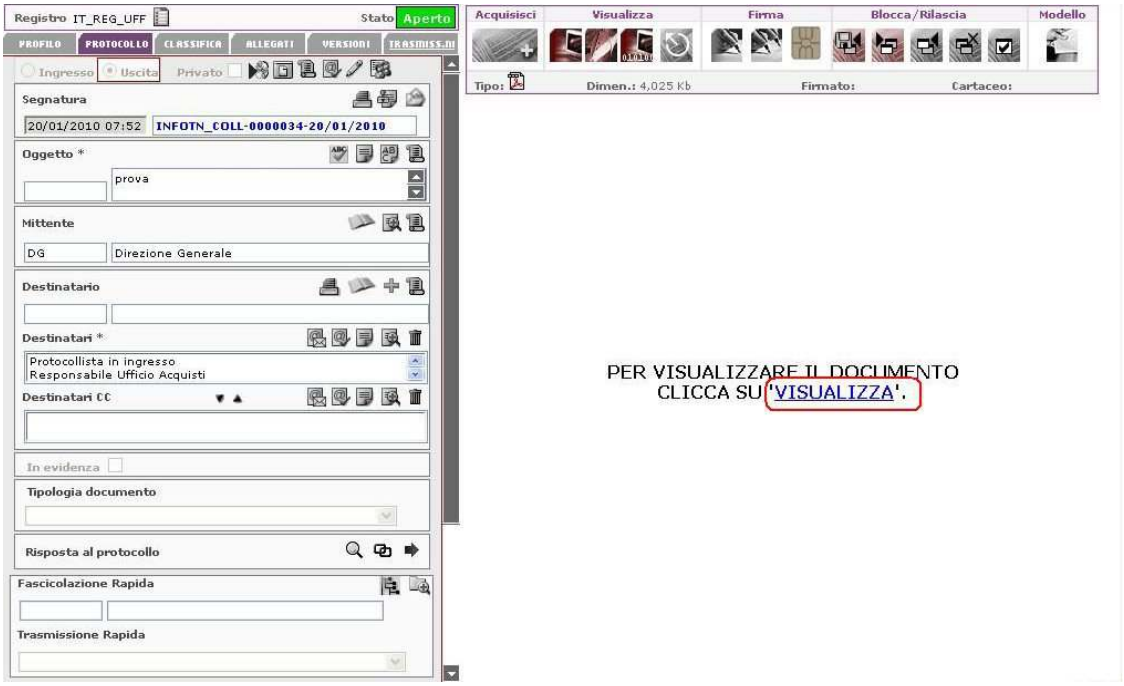


Figura 112 - Visualizza documento da collegamento

2.11.2Versioni del documento allegato

Il sistema consente la gestione delle versioni degli allegati accedendo alla scheda di dettaglio dell'allegato e attivando la scheda "Versioni" (Figura 113). In tal modo sono disponibili le funzioni "Blocca", "Rilascia", "Rilascia senza salvare" (oltre alle funzioni applicabili ad un qualunque documento: "Acquisisci", "Visualizza", "Esporta", "Firma", "Modello").
Nella scheda "Allegati" del documento principale viene visualizzata esclusivamente l'ultima versione del documento allegato; per l'accesso alle versioni precedenti è necessario andare nella scheda di dettaglio dell'allegato alla sezione "Versioni".

Figura 113 - Scheda "Versioni" di un documento allegato

2.11.3 Ricerca dei documenti allegati

E' possibile ricercare gli allegati attraverso l'ambiente "RICERCA/Documenti" mediante l'opzione "All.". Alla selezione di tale voce vengono visualizzati altri tre filtri, con le seguenti etichette:

- "Tutti" , consente di cercare qualsiasi tipologia di allegato;
- "PEC", cerca esclusivamente allegati PEC;
- "Utente", cerca esclusivamente allegati inseriti dall'utente;
- "PI", cerca esclusivamente allegati realtivi a spedizioni tramite interoperabilità semplificata.

E' possibile ricercare contemporaneamente documenti protocollati, non protocollati,predisposti o allegati.

Gli allegati non possono essere ricercati attraverso:

- la tipologia di documento;
- la data di scadenza;
- il codice del fascicolo;
- la mancanza di assegnatario;
- la mancanza di fascicolazione.

2.12 Versioni

Selezionando la sezione Versioni viene visualizzato il pannello riportato in Figura 114 dal quale è possibile gestire le versioni di un documento.

La prima versione di un nuovo documento viene automaticamente generata contestualmente alla creazione del documento stesso, di cui riporterà la data di creazione. Per creare ulteriori versioni, è disponibile nel pannello il pulsante **"Nuova"** premendo il quale appare un pannello (Figura 115) in cui l'utente può inserire delle note relative alla nuova versione del documento.

Figura 114 - Versioni di un documento

Figura 115 - Nuova versione di un documento

L'elenco delle versioni già create riporta le seguenti informazioni:

- **Vers.**: rappresenta il numero della versione;

- **Note**: se eventualmente inserite;
- **Data**: è la data di creazione della versione;

Selezionando una versione (icona) è possibile poi eseguire alcune operazioni tramite i seguenti pulsanti:

- **ADL** permette di inserire il documento nell'area di lavoro;
- **Modifica** consente di modificare i dati di una versione (solo per documenti non protocollati);
- **Rimuovi** consente di cancellare una versione (solo per documenti non protocollati).

2.13 Trasmissioni

Il sistema di protocollo informatico VTDOCS consente l'invio di documenti interni non protocollati ("Documenti" → "Nuovo Documento" → sezione "Trasmissioni"), di protocolli ("Documenti" → "Nuovo Protocollo" → sezione "Trasmissioni") e di fascicoli (vedi paragrafo 3.2.1) ad utenti, ruoli ed UO all'interno dell'AOO dell'Amministrazione. La trasmissione non comporta l'invio fisico del documento, se non di una o più notifiche, ma l'estensione di diritti di visibilità sul documento stesso.
Il pannello che gestisce la trasmissione del documento presenta nella parte in alto a sinistra i dati del documento (evidenziato nell'immagine sottostante da un ellisse di colore rosso). Nella parte inferiore, l'utente può scegliere se visualizzare trasmissioni effettuate su quel documento o quelle ricevute da un altro utente selezionando "effettuate" o "ricevute" (evidenziato nell'immagine sottostante da un ellisse di colore celeste). In basso è riportato l'elenco delle trasmissioni effettuate/ricevute in base all'opzione selezionata. Selezionando l'icona "dettaglio" viene proposto nella sezione di destra il dettaglio della trasmissione selezionata dalla lista. Se il documento/fascicolo non è mai stato trasmesso nel pannello è presente il messaggio "Trasmissioni non trovate". Il campo "trasmissioni rapide" (cerchiato da un ellisse di colore verde nell'immagine sottostante) riguarda le trasmissioni con i modelli di trasmissione (descritte al paragrafo 2.13.4).

A fondo pagina (come evidenziato da un ellisse di colore nero nell'immagine sottostante) sono presenti i pulsanti:

- **Nuova** per inserire una nuova trasmissione;
- **Modifica** per modificare i dati di trasmissioni precedentemente salvate;
- **Trasmetti** per effettuare una delle trasmissioni precedentemente salvate.
- **Stampa** per l'apertura di un report in formato PDF che mostra l'elenco delle trasmissioni relative al documento in questione.

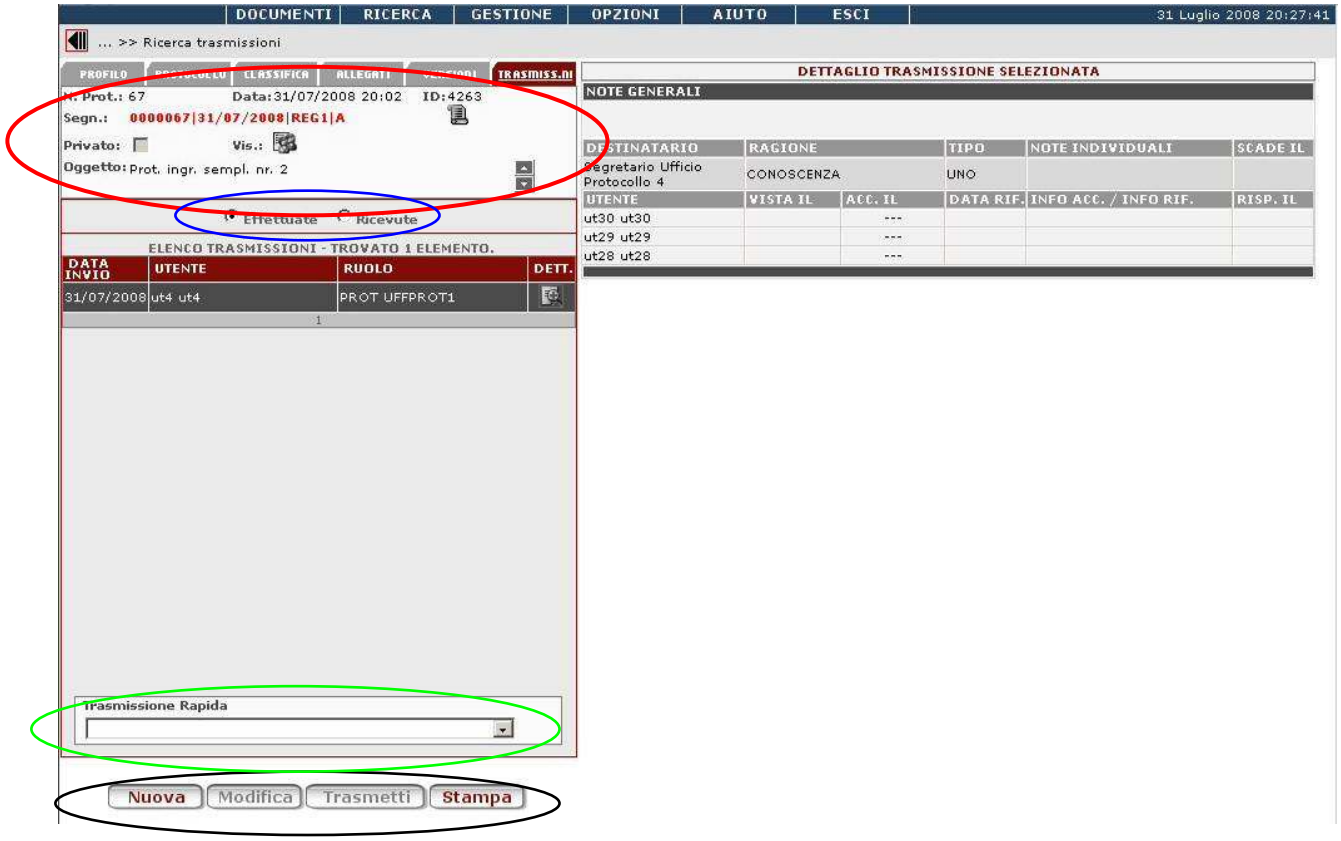


Figura 116 - Trasmissione di un documento

2.13.1 Nuova trasmissione di un documento

Per creare una nuova trasmissione relativa ad un documento è necessario selezionare il pulsante Nuova all'interno della scheda "trasmissioni". In questo modo si visualizza un nuovo pannello (Figura 117), all'interno del quale si impostano gli estremi della trasmissione stessa relativamente a ragioni di trasmissione e destinatari, ovvero le persone, i ruoli, le UO o i Raggruppamenti funzionali di ruoli in UO (RF) a cui si vuol trasmettere il documento.

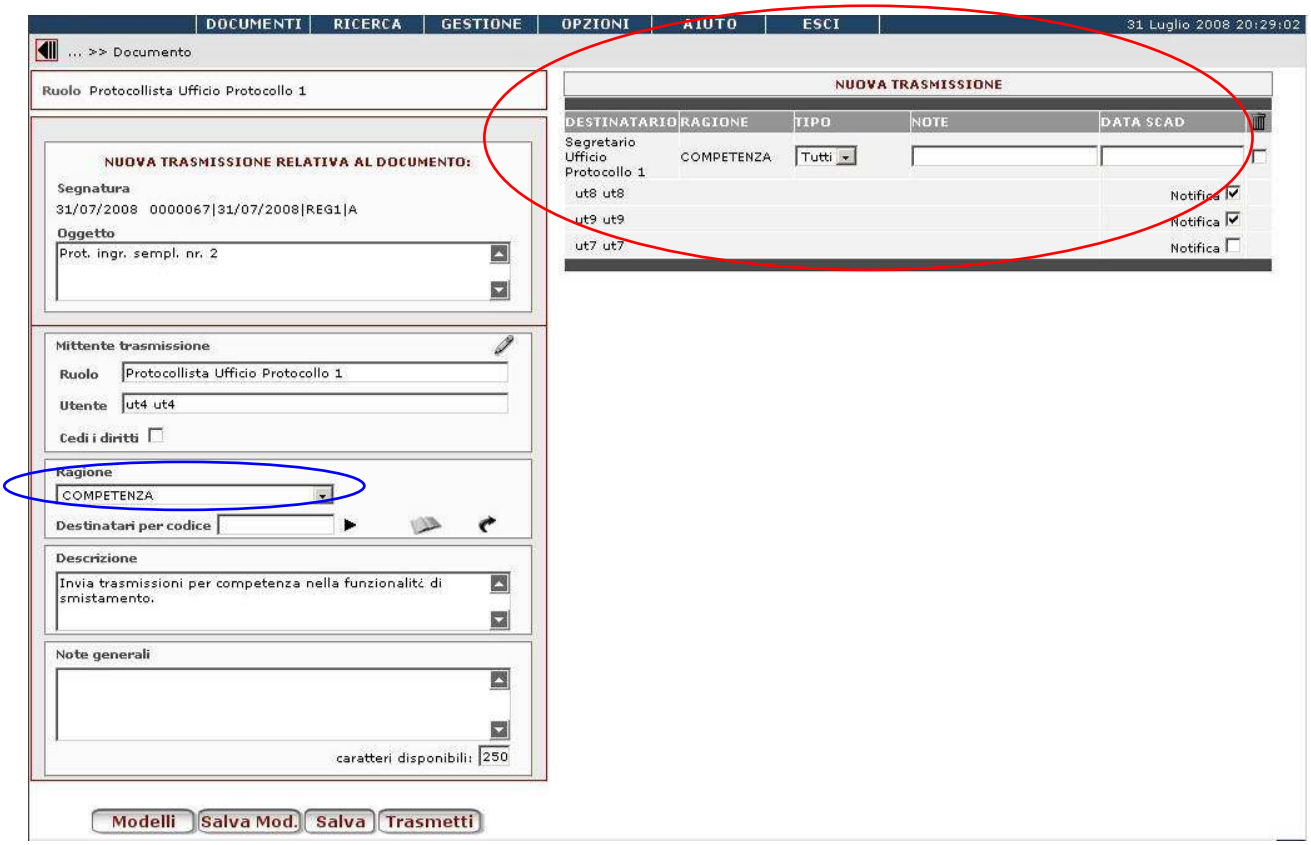


Figura 117 - Creazione di una nuova trasmissione

Le informazioni che il pannello presenta sono:

- i dati relativi al documento che si trasmette;
- il collegamento al profilo del documento;
- il mittente della trasmissione: indica il ruolo ed il nominativo del mittente della trasmissione. Il sistema propone in automatico il ruolo ed il nominativo dell'utente che sta utilizzando il sistema. Selezionando l'icona  è possibile visualizzare il pannello mostrato nella Figura 118 dal quale è possibile selezionare sia un nominativo diverso con lo stesso ruolo, sia un ruolo diverso all'interno della stessa Unità Organizzativa;

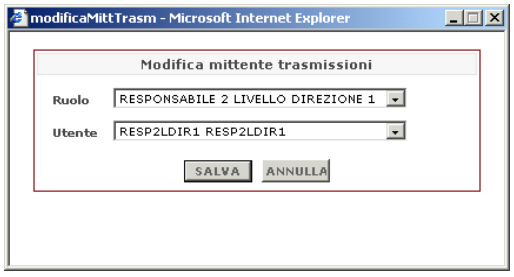


Figura 118 - Modifica mittente di una trasmissione

- la possibilità di cedere i diritti di visibilità sul Documento/fascicolo che si vuole trasmettere, selezionando la casella accanto a “cedi diritti” (tale funzionalità è profilabile in Amministrazione del sistema e quindi disponibile solo agli utenti abilitati dall’Amministratore del sistema stesso). Se un ruolo effettua una trasmissione in modalità cessione si possono verificare i seguenti casi:
  - Nel caso il ruolo cedente abbia sul documento/fascicolo diritti LETTURA o LETTURA SCRITTURA questi sono eliminati dalla Access Control List (Lista dei soggetti aventi diritti di visibilità sul documento/Fascicolo) e trasferiti al destinatario o ai destinatari. Nel caso in cui i destinatari abbiano diritti maggiori di quelli del cedente, allora verranno mantenuti i diritti originari (maggiori). Al termine della trasmissione l’utente collegato viene riportato alla *home page*. Nel caso in cui, all’atto della trasmissione, altri utenti con lo stesso ruolo siano collegati, la trasmissione con cessione viene inibita e contestualmente il sistema propone un messaggio di avviso all’utente.
  - Nel caso in cui il cedente abbia diritti di PROPRIETA’ il destinatario della trasmissione può essere costituito esclusivamente da un singolo ruolo in UO (sono inibite trasmissioni ad-personam e trasmissioni con multipli destinatari) ed è obbligatorio specificare un solo utente nel ruolo destinatario della **notifica trasmissione**: il ruolo in UO destinatario e l’utente nel ruolo che riceve la notifica è il nuovo proprietario del documento.

  E’ possibile, configurando opportunamente le ragioni di trasmissione, effettuare delle particolari trasmissioni con cessione dei diritti parziale. Più in dettaglio, è possibile utilizzare delle ragioni di trasmissioni che consentano la cessione dei diritti in lettura e scrittura con il mantenimento dei diritti in lettura o scrittura sull’oggetto trasmesso, da parte di chi cede i diritti.
- Ragione di trasmissione: indica il motivo per cui un documento viene trasmesso e viene selezionata da un elenco di ragioni presenti nel sistema. Nella Figura 119 è proposto un esempio (evidenziato da un ellisse di colore rosso).

  Nel caso in cui si volesse trasmettere un documento PRIVATO, è stato inserito un controllo per evitare che vengano erroneamente trasmessi documenti “privati” utilizzando ragioni di trasmissione che invece prevedono l’estensione della visibilità verso i ruoli gerarchicamente superiori. L’utente riceve un messaggio con il quale viene chiesto se desideri sbloccare la trasmissione per via gerarchica oppure vuole proseguire nell’operazione.

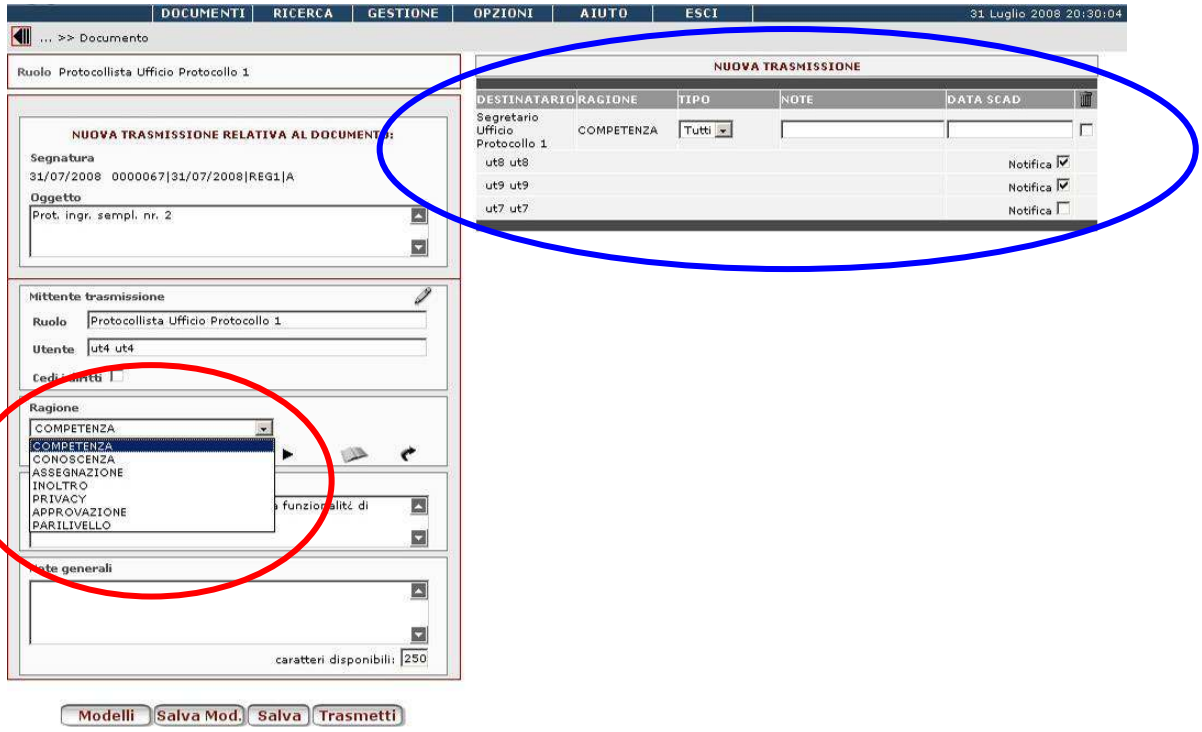


Figura 119 - Ragioni di trasmissione

Le ragioni di trasmissione sono impostate dall'Amministratore del sistema e sono suddivise secondo due modalità distinte nel flusso dei documenti:

- *Con Workflow*: prevede che il destinatario accetti/rifiuti in modo obbligatorio la trasmissione, indicandone la motivazione. Se il sistema è stato opportunamente configurato dall'amministratore, per documenti trasmessi con ragione di tipo workflow, l'ereditarietà della visibilità sul documento stesso si attiva dal momento in cui il destinatario accetta la trasmissione stessa.
  L'accettazione/rifiuto è gestita dal destinatario anche nella lista delle "Cose da fare", presente nella pagina iniziale. Successivamente, queste informazioni sono visibili nel pannello di destra "Dettaglio trasmissione selezionata" così come mostrato nella Figura 120 (evidenziata da un ellisse di colore rosso). Il dettaglio indica una serie di informazioni, riportate qui di seguito, in base al lavoro svolto sul documento dal destinatario:
  - la data in cui è stato visto il documento;
  - la data di accettazione/rifiuto;
  - la nota indicata dal destinatario riferita all'accettazione o al rifiuto ;
  - la data di risposta.
- *Senza Workflow*: non prevede nessuna forma di accettazione o rifiuto da parte del destinatario ai fini della fruizione del documento.

Le trasmissioni sono impostate dall'Amministratore del sistema. Quando l'utente utilizza una trasmissione con *diritti di sola lettura* (ad esempio Visione), il documento inviato con tale ragione, non è modificabile dal destinatario, nel senso che non possono essere variati i dati del protocollo, nè inseriti allegati e/o versioni, impostati dal mittente. Tale documento può essere solo visionato ed eventualmente trasmesso dal destinatario con la stessa ragione con cui è stato ricevuto.

Vi sono poi altre ragioni di trasmissione non selezionabili dall'utente, che il sistema genera in automatico in corrispondenza di operazioni ben specifiche. Queste sono:

- Interoperabilità: questa ragione è prevista solo nello scambio di documenti tra AOO di una stessa Amministrazione (aventi registri differenti) o tra Amministrazioni differenti.
- Rifiuto: questa ragione comparirà nella lista delle "Cose da fare" dell'utente che ha effettuato una trasmissione con workflow, a cui è ritornata la risposta da parte della persona/ruolo/amministrazione che non ha preso in carico il documento o il fascicolo .

- Destinatari della Trasmissione: in questa sezione è possibile selezionare utenti/ruoli/UO/RF a cui effettuare la trasmissione del documento/fascicolo. Tale selezione può avvenire con due differenti modalità, attraverso:
  - l'inserimento del codice utente/ruolo/UO/RF nel campo "Destinatari per codice" e pulsante selezione dell'icona (come mostrato dalla Figura 117 cerchiato di blu);
  - la selezione dell'icona "rubrica" dove si effettua la ricerca ed il relativo inserimento. L'utilizzo della rubrica viene illustrato con maggiore dettaglio nel paragrafo 4.5.

  In entrambi i casi i destinatari di una trasmissione sono esclusivamente i corrispondenti interni dell'Amministrazione di appartenenza, che sono opportunamente filtrati in base alla ragione di trasmissione selezionata e quella del ruolo ricoperto dall'utente all'interno dell'amministrazione. Il sistema propone cioè i destinatari (Utenti, Ruoli, UO, RF) in base alla ragione prescelta (con o senza Workflow) e il tipo ruolo dell'utente all'interno dell'amministrazione.

  Se fra i destinatari della trasmissione è presente una UO, il sistema effettua delle verifiche sull'esistenza di ruoli di riferimento sulla UO stessa. Nel caso tali ruoli non esistano il sistema avvisa l'utente tramite opportuno messaggio e non effettua la trasmissione alla UO in questione.
  In particolare, i controlli vengono effettuati:
    - quando si indica come destinatario il codice di una UO o di una lista contenente una UO
    - se si seleziona una UO (o una lista contenente una UO) tramite rubrica

- Descrizione: indica la ragione con cui è stata effettuata la trasmissione. Il campo viene popolato in automatico dall'applicativo quando viene selezionata una ragione di trasmissione.
- Note generali: campo a disposizione per annotazioni di carattere generale relative alla trasmissione che diviene dato obbligatorio nel caso in cui si sta creando un nuovo modello di trasmissione (vedi paragrafo 2.13.4).

Nel pannello di destra è presente il dettaglio dei destinatari (vedi Figura 119 evidenziato da un ellisse di colore blu), in cui sono presenti:

- L'indicazione del **destinatario**: utente, ruolo, UO, RF
- **Ragione**: la ragione con cui si vuole effettuare la trasmissione
- **Tipo**: si visualizza solo, quando la trasmissione è effettuata a ruolo, sia che la ragione selezionata sia di tipo "con workflow" sia che sia di tipo "senza workflow". E' possibile impostare 2 differenti parametri :
  - Uno: se basta la risposta/visione di un unico utente appartenente al ruolo;
  - Tutti: se ci si attende la risposta/visione di tutti. L'opzione è impostata automaticamente dal sistema con il valore "UNO" .
- **Note**: sono note individuali verso il singolo destinatario;
- **Data scadenza**: solo per le trasmissioni con ragione di tipo workflow (che richiedano cioè una risposta da parte del destinatario);
- **Elimina**: si seleziona il campo contrassegnato con il cestino per eliminare destinatari inseriti in maniera non corretta;

- **Notifica**: permette di selezionare gli utenti del ruolo che riceveranno la notifica della trasmissione. All'atto della selezione si visualizza la configurazione effettuata dall'amministratore che può fare in modo che la trasmissione al ruolo:
  - selezioni in automatico le notifiche per tutti gli utenti appartenenti al ruolo.
    oppure:
  - non selezioni nessuno degli utenti.

La trasmissione alla persona presenta le seguenti caratteristiche:
- la visibilità è estesa al solo utente destinatario;
- la notifica nella lista delle cose da fare sarà presente per il solo utente destinatario;
- è indipendente dai ruoli del destinatario.

La trasmissione al ruolo presenta invece le seguenti caratteristiche:
- la visibilità viene estesa a tutti i componenti del ruolo;
- la visibilità viene estesa ai superiori gerarchici del ruolo (dopo l'accettazione per trasmissioni con ragione di tipo workflow, se opportunamente configurata dal'amministratore di sistema).

Il comportamento della trasmissione al ruolo viene modificato solamente nella gestione delle notifiche nella lista delle cose da fare che verranno inoltrate non a tutti gli utenti del ruolo, ma solamente a quelli selezionati, come mostrato Figura 119.
Se il ruolo destinatario ha associato un solo utente, questo si presenta automaticamente già selezionato e non modificabile.
Per la trasmissione dei fascicoli valgono analoghe considerazioni.

Dopo aver inserito tutti i dati è possibile salvarli senza effettuare contestualmente la trasmissione selezionando il pulsante **Salva** per poi trasmetterli in seguito, oppure è possibile salvare i dati ed effettuare contestualmente la trasmissione premendo il tasto **Salva e Trasmetti**.
Tramite i pulsanti riportati in fondo alla pagina è inoltre possibile:
- Salvare i dati relativi alla trasmissione in un nuovo modello **Salva Mod**, da utilizzare per trasmissioni successive (vedi paragrafo 2.13.4);
- Effettuare una trasmissione (**Modello**) prelevando i dati di una trasmissione precedentemente memorizzata come modello (vedere paragrafo 2.13.4). E' possibile modificare i dati riproposti per la trasmissione oppure utilizzarli direttamente per la nuova trasmissione.

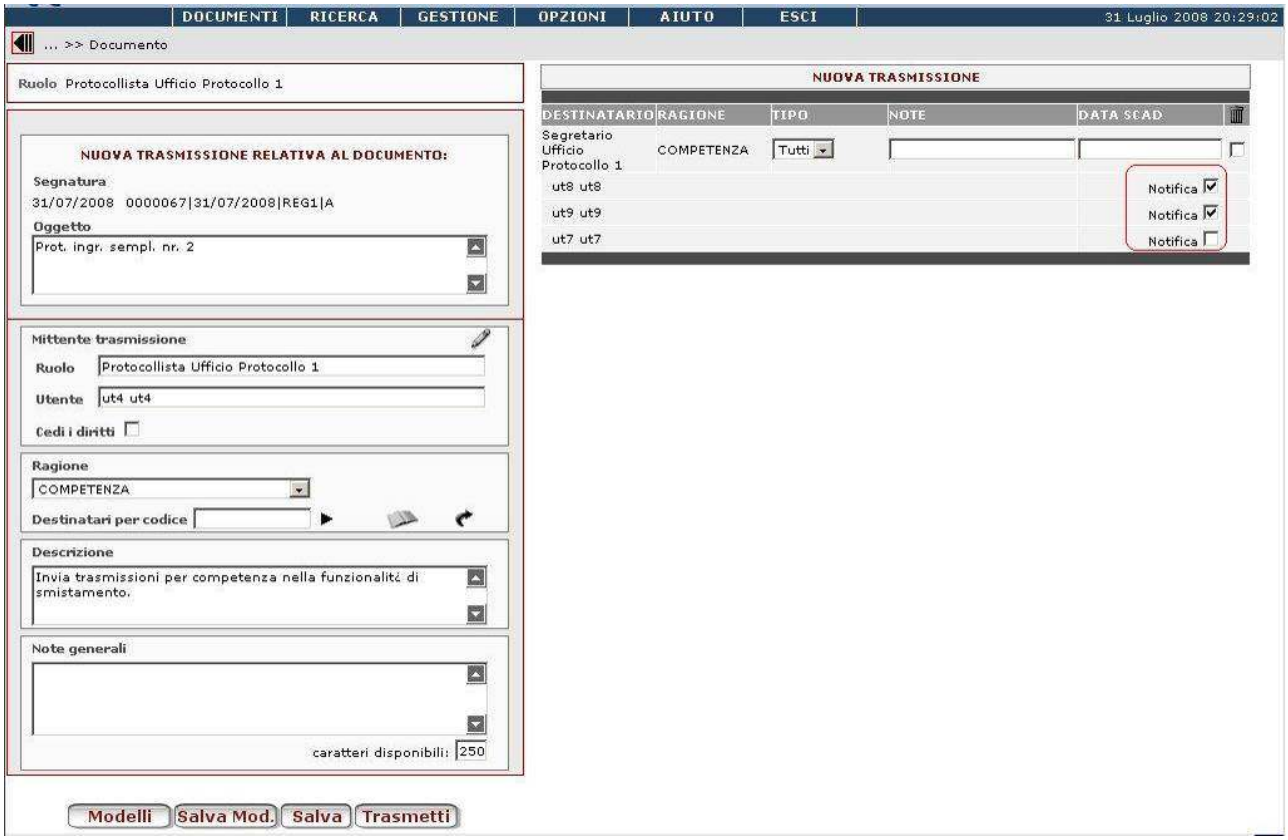


Figura 120 - Notifica di una trasmissione a ruolo nel caso di una trasmissione di un documento

Figura 121 - Trasmissione effettuata

2.13.1.1 Cedi diritti

Se si possiede il diritto di “sola lettura” o “lettura e scrittura”, la trasmissione dell’oggetto comporta la perdita del diritto da parte del mittente sia come utente che come ruolo. La perdita del diritto si estende di conseguenza a tutti i componenti del ruolo mittente.
Se si possiede il diritto “proprietario”, la trasmissione dell’oggetto richiede quale, tra i ruoli destinatari, deve acquisire la proprietà ed all’interno del ruolo selezionato quale utente. La richiesta è effettuata attraverso un’opportuna finestra di dialogo che elenca i ruoli destinatari e, per ogni ruolo, gli utenti componenti. La selezione avviene in modo esclusivo solo sugli utenti individuando contestualmente il ruolo di appartenenza. L’utente viene avvisato attraverso un opportuno messaggio .
Nel caso in cui la trasmissione prevede solo un ruolo destinatario e sia attiva la notifica della trasmissione solo ad un componente del ruolo, il sistema attribuisce a quest’ ultimo la proprietà del documento senza necessità di ulteriori interazioni.
La trasmissione con cessione dei diritti non elimina l’informazione concernente il diritto ceduto sulla finestra di visualizzazione dei diritti (ACL) relativamente all’oggetto trasmesso ma lo marca come revocato (analogamente a quanto avviene per la rimozione visibilità dei documenti/fascicoli), eccezion fatta per la cessione dei diritti di proprietà: in tal caso i diritti dell’utente vengono eliminati, rimangono invece, come revocati, quelli del ruolo.
E’ possibile, configurando opportunamente le ragioni di trasmissione, effettuare delle particolari trasmissioni con cessione dei diritti parziale. Più in dettaglio è possibile utilizzare delle ragioni di trasmissioni che consentano la cessione dei diritti in lettura e scrittura con il mantenimento dei diritti in lettura o scrittura sull’oggetto trasmesso, da parte di chi cede i diritti.

2.13.2Trasmissioni con l'opzione nascondi versioni

Questo tipo di trasmissione può essere effettuata solo se è attiva la funzione "Consolidamento" e solo su documenti consolidati relativamente alle versioni o ai metadati.
In tal caso infatti l'utente che effettua la trasmissione e che ha visibilità sul documento e su tutte le sue versioni ha la possibilità di trasmettere il documento mostrandone solo l'ultima versione.
In fase di creazione di una trasmissione, per ogni destinatario (ruolo o utente), è possibile specificare se nascondere le vecchie versioni selezionando la casella "NASCONDI VERSIONI PRECEDENTI".
In questo modo il destinatario della trasmissione avrà visione solo dell'ultima versione del documento e dei suoi allegati, se presenti.

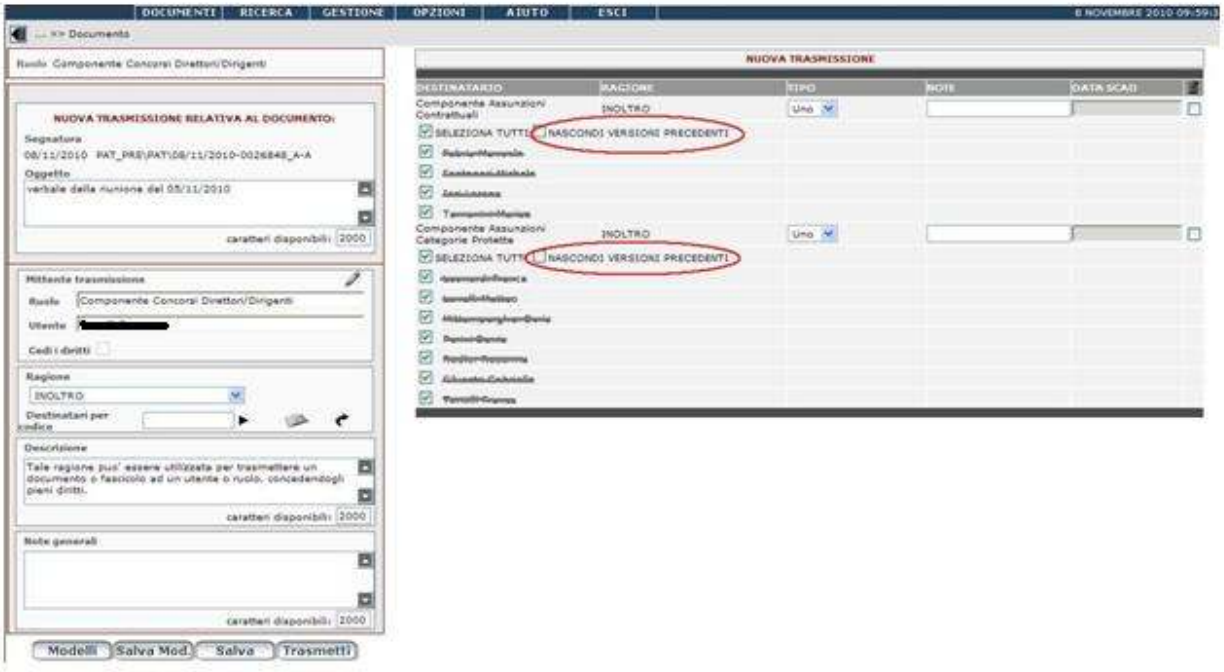


Figura 122 – Trasmissione con l'opzione 'nascondi versioni'

Se un utente al quale viene trasmesso un documento nella modalità 'nascondi versioni precedenti', riceve un'altra trasmissione dello stesso senza tale opzione, esso acquisirà sul documento la visione complessiva e quindi potrà vederne tutte le versioni.
Un utente che già vedeva un documento nella modalità completa se riceve una trasmissione dello stesso nella modalità 'nascondi versioni precedenti', continuerà a vedere il documento nella sua globalità.

La modalità 'nascondi versioni precedenti' può essere utilizzata anche con i modelli di trasmissione.
E' infatti possibile creare dei modelli di trasmissioni nei quali è selezionata l'opzione 'nascondi versioni precedenti'. Tali modelli non verranno mostrati e quindi non saranno utilizzabili per i documenti non consolidati.

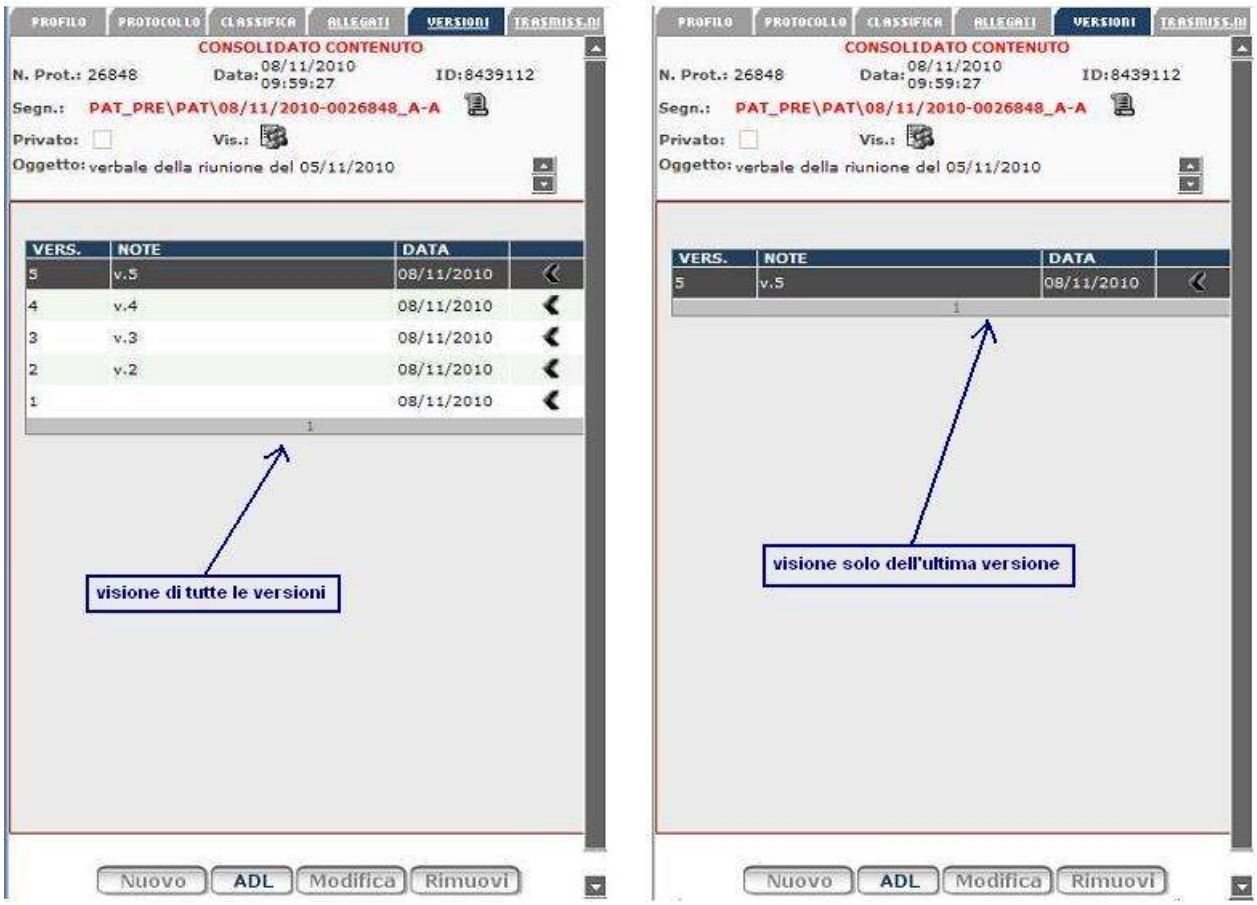


Figura 123 – Visibilità solo dell'ultima versione del documento

Un utente che ha una visione parziale del documento (solo dell'ultima versione) potrà trasmettere il documento nella sola modalità 'nascondi versioni'. In questo caso infatti il sistema renderà l'opzione 'NASCONDI VERSIONI PRECEDENTI' selezionata e l'utente non potrà modificarla poiché il campo verrà reso in sola lettura.

Figura 124 – Trasmissione con l'opzione 'nascondi versioni precedenti' obbligatoria

2.13.3 Trasmissioni in risposta

Alcune trasmissioni prevedono una risposta da parte del destinatario. In tal caso, nel momento in cui si effettua una trasmissione di risposta, tramite l'icona , è possibile indicare la trasmissione ricevuta a cui si vuole rispondere. In questo caso il destinatario di questa nuova trasmissione è automaticamente individuato con il mittente della trasmissione cui si sta rispondendo e la ragione di trasmissione sarà 'RISPOSTA'.

2.13.4 Modelli e trasmissioni rapide

Per agevolare l'esecuzione di trasmissioni aventi le stesse caratteristiche (destinatari e/o ragione), il sistema di protocollo informatico VTDOCS mette a disposizione i modelli di trasmissione. Come visto nel paragrafo 2.13, una volta impostati ragione e destinatari di trasmissione è possibile salvare il modello mediante il pulsante Salva Mod.
Prima del salvataggio è necessario inserire il nome del modello e decidere se renderlo disponibile solo a se stessi o a tutto il ruolo di appartenenza (Figura 125).

Figura 125 - Modello di trasmissione

Nel momento in cui si vuole effettuare una nuova trasmissione utilizzando il modello esistente è possibile:

- selezionare il modello nel menù a tendina delle trasmissioni rapide (vedi Figura 121). Non saranno visibili i modelli di trasmissione che contengono come destinatari ruoli inibiti (tramite il tool di amministrazione) alla ricezione delle trasmissioni;
- creare una nuova trasmissione utilizzando un modello già esistente ed apportando, dove necessario, delle modifiche prima di effettuare la trasmissione vera e propria. La scelta di un modello di trasmissione in questo caso avviene mediante il pulsante Modelli che mostra una finestra di dialogo contenente i modelli a disposizione dell'utente Figura 126.

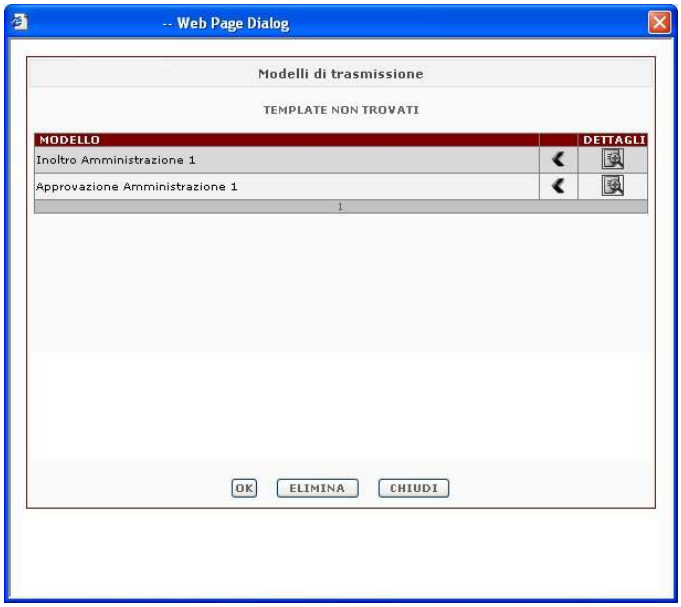


Figura 126 - Elenco Modelli di trasmissione

Al momento dell'utilizzo dei modelli di trasmissione (relativi a documenti o a fascicoli), nel menu a tendina delle trasmissioni rapide:

- saranno opportunamente evidenziati con un colore diverso i modelli contenenti fra i destinatari ruoli inibiti alla ricezione di trasmissioni . Tali modelli non saranno selezionabili
- non compariranno[3] i modelli di trasmissione fra i cui destinatari compare almeno un ruolo storicizzato a fronte di spostamento/modifica (nel caso in cui l'amministratore abbia deciso di non aggiornare i modelli stessi).

Inoltre, al momento della trasmissione di un documento/fascicolo privato tramite utilizzo di un modello di trasmissione già esistente, il sistema chiede se bloccare o meno l'estensione gerarchica della visibilità che normalmente (se il documento/fascicolo non fosse privato) avverrebbe a seguito della trasmissione stessa.

2.13.5 Notifica via mail

Nel caso in cui l'utente decida di ricevere una notifica via mail (sulla casella di posta personale) delle trasmissioni ricevute in VTDOCS, tale mail contiene sia il link alla scheda del documento che quello che conduce direttamente al visualizzatore esterno (se al documento è associata un'immagine).

[3] Se è stata abilitata la gestione avanzata dei ruoli tramite interfaccia di amministrazione

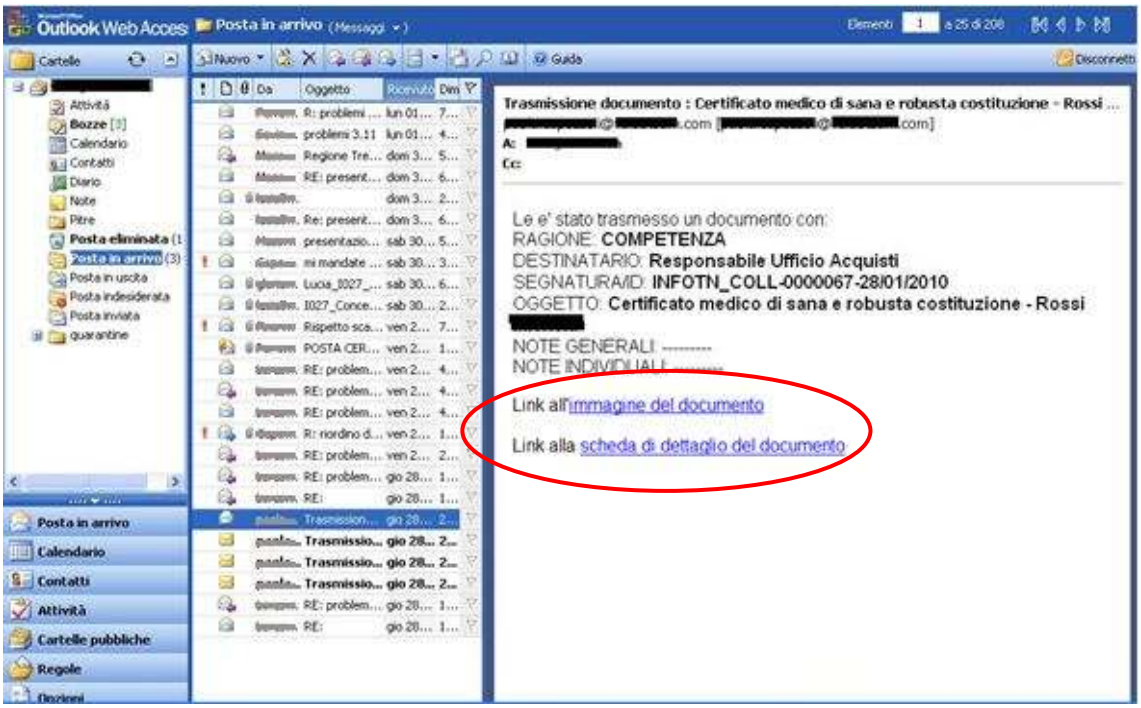


Figura 127 - Link a trasmissione

2.14 Gestione del documento elettronico

La parte destra del pannello visualizza una serie di immagini, ciascuna delle quali ha una funzione specifica. Tali immagini sono suddivise in 5 blocchi, in base al tipo di operazione da effettuare.

2.14.1 Blocco "ACQUISISCI"

Acquisisci: è possibile scegliere la tipologia di acquisizione da scanner o da file system. In presenza di un documento in formato solo cartaceo consente di acquisire l'immagine del documento da scanner o se è disponibile il documento in formato elettronico l'acquisizione è possibile da file system.
Dopo aver selezionato il tipo di acquisizione (da scanner o da file system) ed eventualmente ulteriori opzioni (es. conversione in PDF) si clicca sul pulsante **INVIA.** Nel caso dell'utilizzo dello scanner viene aperta una finestra di dialogo per effettuare le operazioni tipiche di questo tipo di acquisizione (avviare lo scanner, visualizzare le pagine che man mano vengono scansionate, ruotarle, eliminare quelle acquisite male, dare conferma dell'operazione ad acquisizione completa di tutti i fogli). Il sistema può essere configurato affinché dopo aver cliccato sul pulsante INVIA, lo scanner si avvia automaticamente evitando all'utente un click in più.
Il sistema memorizza il nome dell'immagine acquisita. Dopo l'acquisizione tale nome diviene immodificabile e viene mostrato in visualizzazione (vedere par. 2.14.1, 2.14.2.1). In particolare:

- acquisizione da scanner: a seconda del tipo di documento (protocollato, non protocollato, allegato) il nome del file ha il seguente formato: Documento_Principale_<segnatura>, Documento_Principale_<id documento>, <Descrizione allegato>_<id allegato> (es.:Documento_Principale_PAT_2013-0000013.pdf, Documento_Principale_12465248.pdf, Tabella_partecipanti concorso_12465756.xls)
- acquisizione da file system: viene memorizzato il nome del file acquisito.

Per entrambe le tipologie di acquisizione è possibile richiedere al sistema di convertire il documento in formato PDF, *lato server* o *client*, a seconda di come è stato configurato il sistema.
Conversione in PDF lato server (Figura 128):

Figura 128 - Acquisisci file

Questo tipo di conversione si ottiene se è impostata l'opzione *Centrale.* In questo caso è anche possibile scegliere se la conversione può avvenire contestualmente all'acquisizione (*sincrona*) oppure in modo differito (*asincrona*).
A conversione avvenuta, il sistema effettua una trasmissione con ragione "notifica" o all'utente che ha richiesto la conversione o a tutti gli utenti appartenenti al ruolo con cui è stato acquisito e convertito il documento (a seconda di come l'amministratore ha gestito e configurato la notifica di tale evento). Nell'elenco delle trasmissioni ricevute sarà pertanto presente una notifica del documento convertito come è mostrato in Figura 129.

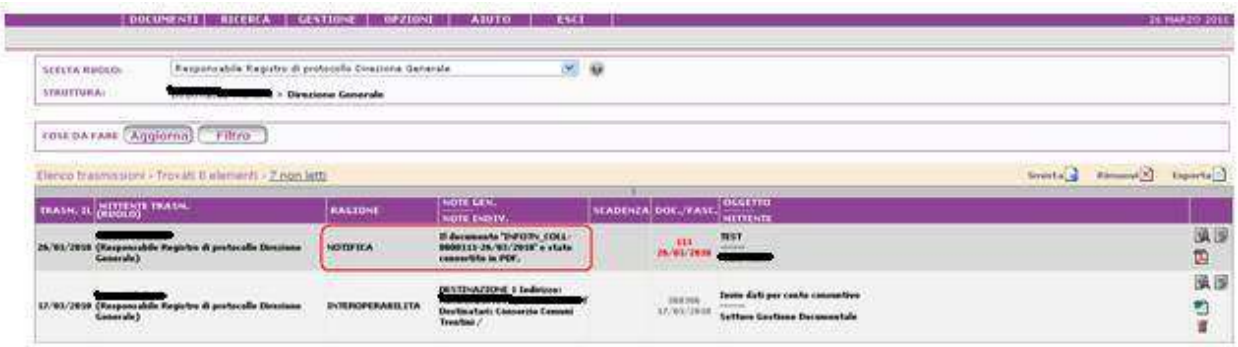


Figura 129 - Notifica in elenco trasmissioni ricevute della conversione del documento

Conversione in PDF lato client: se il sistema è configurato in modo da consentire acquisizioni lato client, la voce *Centrale* è disabilitata ed è invece attiva la voce *Locale*.

Per entrambe le tipologie di conversione in PDF verranno create due versioni, la prima relativa al documento con la sua estensione originale, la seconda relativa al documento in formato PDF (si veda la Figura 130); In automatico viene mostrata l'ultima versione creata (PDF).

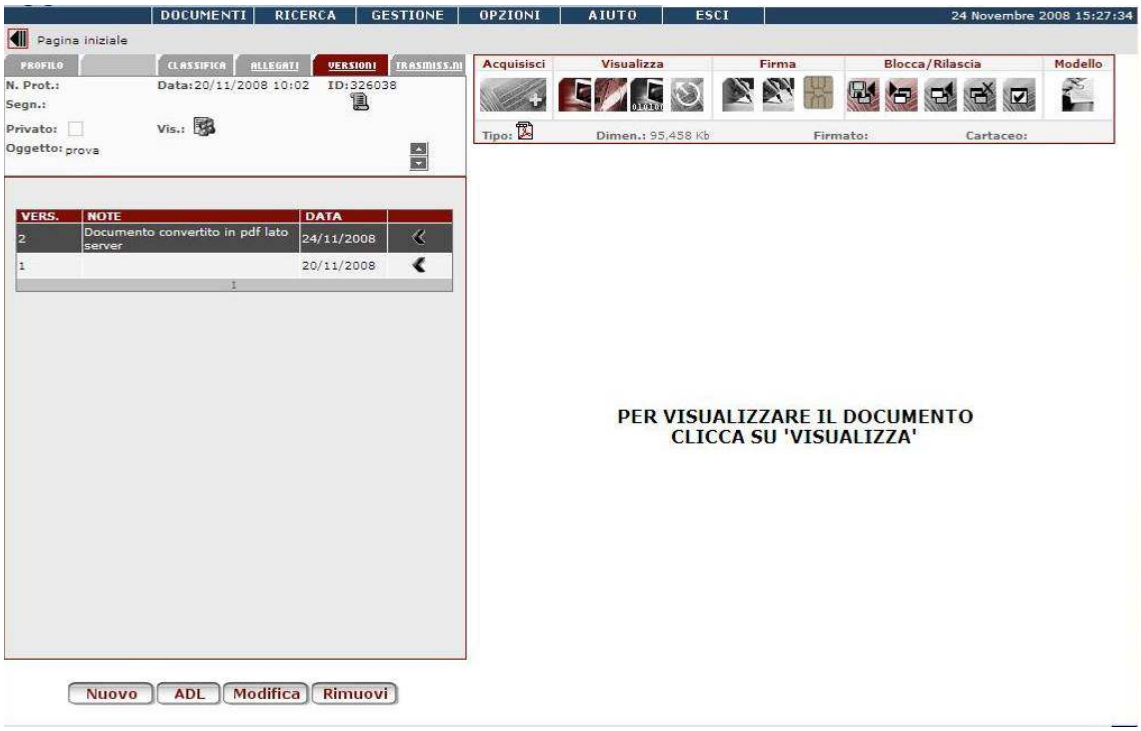


Figura 130 - Versioni del documento

Una volta effettuata l'acquisizione, il sistema presenta le informazioni relative al documento acquisito come mostrato anche in Figura 134 in alto a destra:

- tipo: indica il tipo di file, l'estensione. Se si posizione il mouse su questa icona viene mostrato il nome originario del file acquisito
- dimensione: indica la dimensione del file acquisito;
- firmato: indica se è stata apposta la firma digitale;
- cartaceo: se esiste la versione cartacea del documento (si specifica all'atto dell'acquisizione).

All'atto dell'acquisizione del file, il sistema automaticamente chiama il servizio esterno di verifica[4] del formato il quale accerta che il formato del file sia conforme alla sua estensione e ai formati ammessi per la gestione documentale dell'ente. In caso di esito positivo il file viene correttamente inserito nel sistema, in caso contrario, il sistema restituisce all'utente un avviso (Figura 131) e il file non viene acquisito.

[4] Tale verifica fa parte delle funzionalità relative alla conservazione dei documenti e deve essere opportunamente abilitate tramite intrefaccia di amministrazione

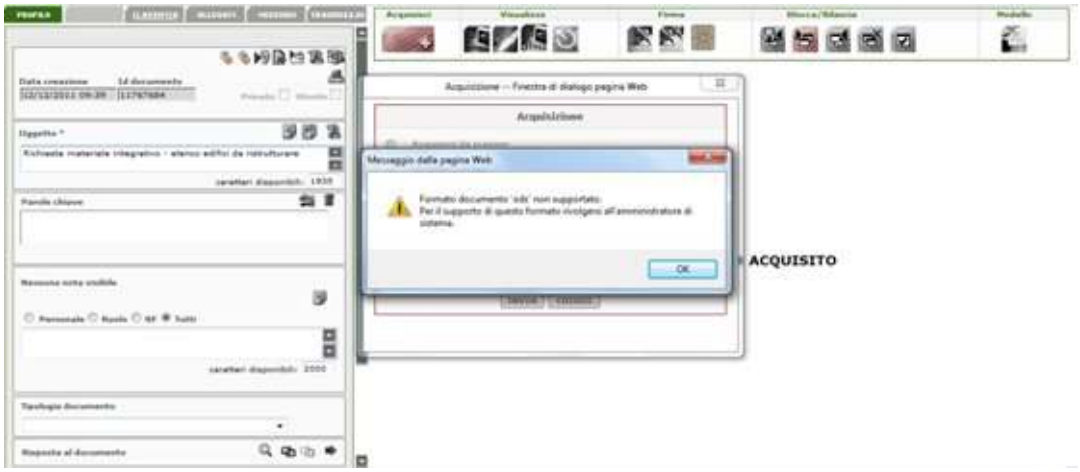


Figura 131 – *Esito della verifica di conformità del formato del file*

2.14.2 Blocco "VISUALIZZA"

Visualizza documento: mostra l'immagine del documento acquisito o del documento elettronico associato. La visualizzazione dell'immagine del documento non è proposta automaticamente, ma soltanto su richiesta dell'utente. In presenza di un documento molto grande infatti, tale operazione richiederebbe l'impiego di molte risorse, e quindi potrebbe richiedere molto tempo. A tal proposito è stato scelto di non gravare il sistema di un'operazione così onerosa, perché non richiesta per lo svolgimento delle altre operazioni. L'icona è selezionabile solo quando è stata già acquisita l'immagine del documento o è associato un documento elettronico, così come descritto nel Paragrafo 2.14.2.1.
Le ricevute di ritorno della Posta Elettronica Certificata (PEC), presentano un formato nativo .eml, ma la visualizzazione di tali documenti avviene nel browser Internet Explorer in formato HTML, al fine di agevolare la consultazione da parte dell'utente.

Zoom: permette di ingrandire a video l'immagine del documento acquisito. L'icona è selezionabile soltanto quando è stata già acquisita l'immagine del documento.

Visualizza documento con segnatura: visualizza il documento protocollato con impressa la segnatura relativa o il timbro (Figura 132). In caso di documento non protocollato repertoriato, verrà visualizzata la segnatura di repertorio e la tipologia di documento. Se si accede a questa visualizzazione dalla scheda di dettaglio di un allegato, verrà visualizzata oltre ai dati identificativi del documento anche la tipologia di allegato ed il numero allegato.

Figura 132 – *Visualizzazione documento con segnatura*

Posizionamento della segnatura: permette di impostare la visualizzazione della segnatura o del timbro, del documento protocollato in base alle coordinate inserite dall'utente.
La maschera si divide in tre sezioni:

- *Posizione delle informazioni*: consente di visualizzare la segnatura e/o la firma ad uno dei quattro angoli della pagina, selezionando il rettangolo corrispondente alla posizione prescelta
- *Posizione personalizzata*: indicando direttamente le coordinate ("X" ed "Y") è possibile invece collocare segnatura e/o firma in una posizione a scelta dell'utente
- *Caratteristiche Timbro/Segnatura:* è possibile scegliere carattere e colore di segnatura e/o firma e scegliere se si vuole visualizzare:
    - timbro (orizzontale o verticale)
    - segnatura
    - nessuna delle informazioni precedenti.

  Qualsiasi delle opzioni venga scelta è possibile mostrare, per documenti firmati, i dati di firma (in prima o ultima pagina). Se l'amministrazione è stata opportunamente configurata, è inoltre possibile scegliere se visualizzare i dati di firma completi (dati standard, ente certificatore, didascalia di firma configurata in amministrazione) o in forma sintetica (solo firmatari).
  Segnatura/timbro/firma verranno mostrati in base alle opzioni scelte nelle sezioni "Posizione delle informazioni" e "Posizione personalizzata".

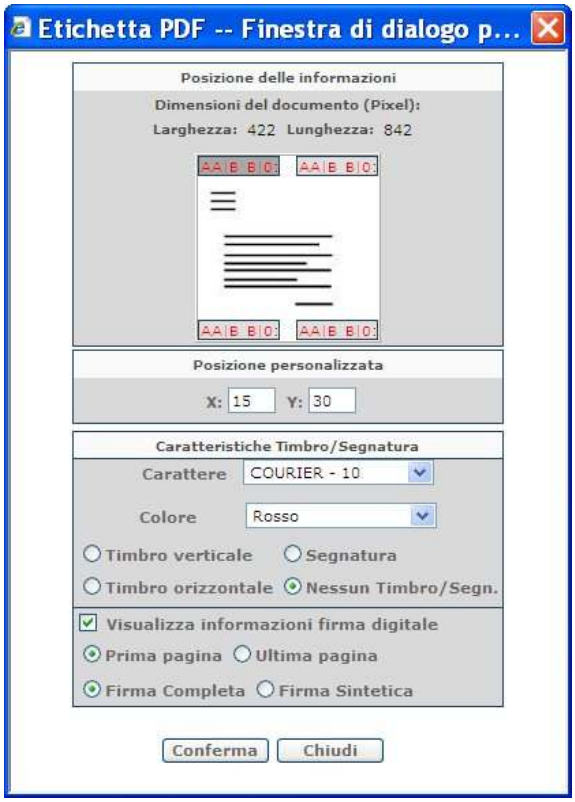


Figura 133 – Posizionamento segnatura

2.14.2.1 Visualizzatore documento principale e dei relativi allegati

Il visualizzatore permette di avere una visione complessiva del documento su cui si sta operando, andando a mostrare, il documento principale e i suoi allegati come un unico oggetto facendo in modo che, sia il contenuto dei documenti sia dei relativi allegati, siano raggiungibili con una semplice selezione.
A destra dell'immagine visualizzata si hanno tante graffette quanti sono gli allegati più l'icona relativa al documento principale.
Nel caso di documenti con allegati la visualizzazione del documento mostra inizialmente il documento principale, a cui è associata l'icona indicante la versione ed il relativo numero di versione (V1 indica che è la prima versione del documento, V2 = seconda versione del documento , V3.= terza versione del documento, e così via...), se sono presenti anche degli allegati questi saranno referenziati attraverso il loro codice (così come indicato nel pannello dedicato agli allegati : A01, A02, A03,...) ; nel caso di un numero elevato di allegati, non visibili in un'unica pagina, è possibile scorrere la lista degli allegati.

Posizionando il mouse sull'icona corrispondente al documento principale viene mostrata la didascalia riportante l'oggetto del documento. Analogamente, posizionando il mouse sulla graffetta relativa ad un allegato saranno visualizzati i primi 128 caratteri della descrizione dell'allegato. Posizionando invece il mouse sul numero di versione viene visualizzato il nome del file.

Il visualizzatore è raggiungibile tramite:

- la selezione dell'icona presente nella pagine delle:
  - "Cose da Fare";
  - "Ricerca Documenti";

- “Documenti contenuti in un fascicolo”;
- “Documenti presenti in ADL”;

- la selezione del campo accanto alla dicitura Visual. Doc. nella pagina dello smistamento (Visual. doc.);
- la selezione dell’immagine dalla scheda di dettaglio del documento nella sezione di gestione del documento elettronico, blocco visualizza..

E’ possibile stampare il documento principale o i suoi allegati dalla sezione del visualizzatore unificato. Il pulsante per la stampa appare a destra di ogni pulsante di visualizzazione. Il pulsante stampa scarica il documento in locale ed apre il documento con l’applicazione nativa. In questo modo sono disponibili tutte le funzioni di stampa native senza limitazioni presenti nella visualizzazione tramite browser.

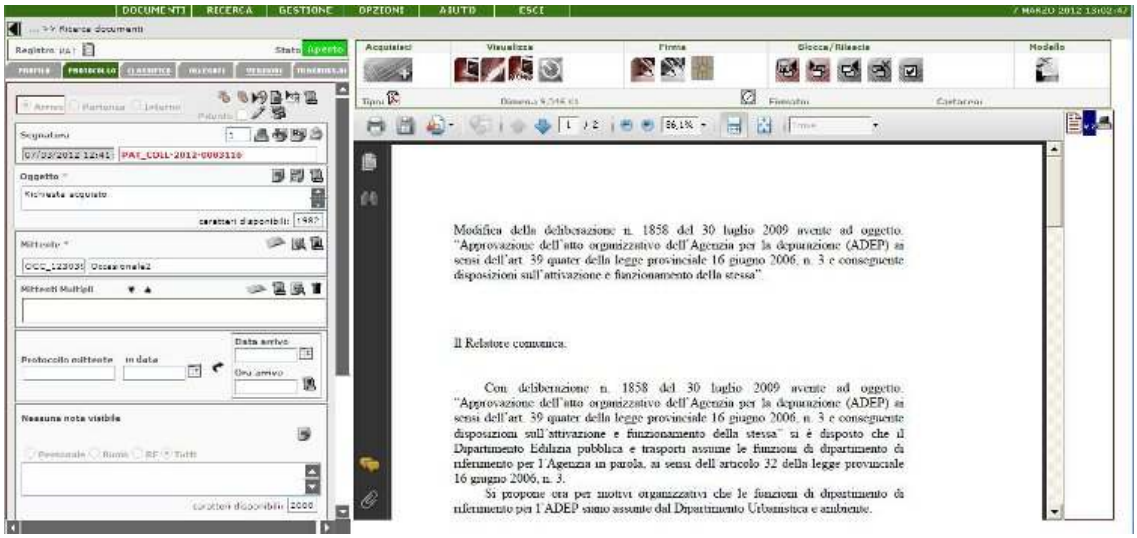


Figura 134 - Consultazione del documento principale e degli allegati con il visualizzatore

2.14.3 Blocco FIRMA

Firma: consente di firmare digitalmente il documento acquisito. E’ possibile apporre una firma digitale singola o multipla (ad esempio nel caso di firme per l’approvazione di un documento a vari livelli: 1° firma del Funzionario, 2° firma del Dirigente, 3° firma del Direttore). L’icona è selezionabile solo quando è già stata acquisita l’immagine del documento**.**

Co-Firma: consente di firmare digitalmente il documento acquisito. Selezionando tale immagine è possibile apporre una firma digitale multipla di pari livello (come una firma congiunta). L’icona è selezionabile solo quando è stata già acquisita l’immagine del documento**.**

Alla pressione del pulsante **Firma** o del pulsante **Co-Firma** viene mostrata una finestra per la scelta del certificato da utilizzare. Vengono visualizzati solo i certificati con estensione KeyUsage “nonRepudiation”, come previsto dalla normativa. L’utente sceglie il certificato e mediante l’utilizzo dell’apposita smart card effettua la firma sul documento.

Le due icone **Firma e Co-firma** non sono attivate se il file da firmare ha un formato non ammesso per la firma. La scelta dei formati validi viene fatta mediante lo strumento di Amministrazione.

Dettaglio Firma: consente di visualizzare il dettaglio della firma in una finestra esterna all'applicativo (**Errore. L'origine riferimento non è stata trovata.**). Tale dettaglio essenzialmente è costituito da due parti:

- Il dettaglio di una o più firme del documento acquisito, composto da quattro sezioni:
  - Risultato di verifica rispetto allo stato della firma, allo stato del certificato e verifica del Codice Riservato al Notaio (CRN);
  - Certificato di cui si controllano il numero di serie, valido dal, valido sino al, soggetto;
  - Soggetto di cui si indicano nome, cognome, codice fiscale, data di nascita, organizzazione, ruolo, paese, ID titolare;
  - Firma documento che indica l'algoritmo di firma e la firma digitale.
- i dati generali del documento originale quali :
  - Stato del documento ;
  - Tipo del documento ;
  - Nome file originale ;
  - Dimensioni ;
  - Nome file P7M che è il formato della firma originale.

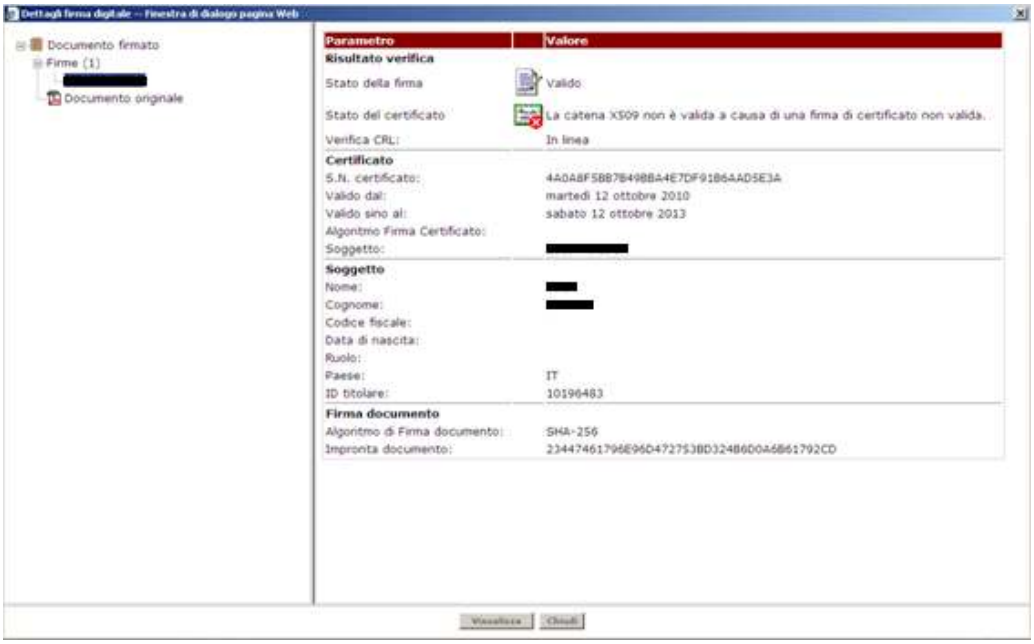


Figura 135 – Dettaglio Firma

Una volta apposta la firma sul documento all'interno del sistema, al lato della denominazione "firmato" compare il flag ✔ (Figura 136). Questo, se cliccato, permette di effettuare delle verifiche di validità della firma interrogando le CRL – *Certificate Revocation List* .
L'utente avrà evidenza dell'esito della verifica effettuata che sarà segnalato da un'apposita icona; in caso di validità di firma verrà mostrato una spunta di colore verde: Firmato: ✔, mentre in caso di non validità la spunta sarà di colore rosso: Firmato: ✔.

In generale la denominazione “firmato” viene visualizzata per qualsiasi documento/allegato che risulti essere stato firmato internamente o esternamente al sistema.

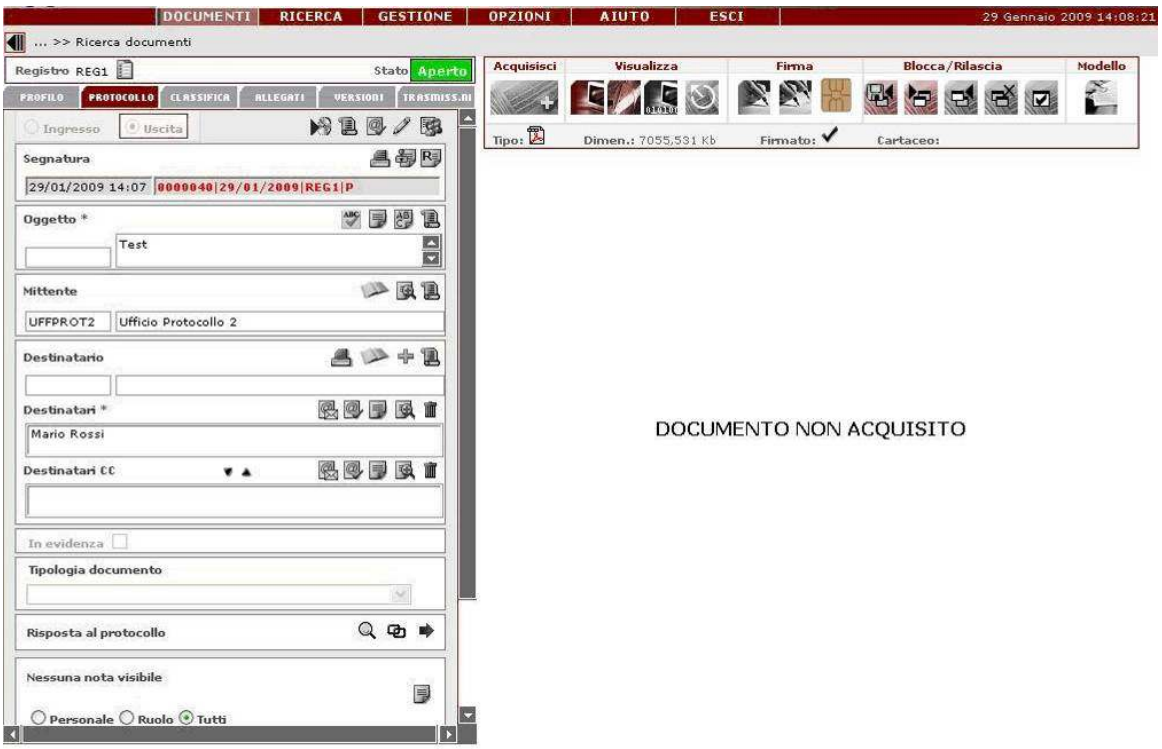


Figura 136 – Protocollo in uscita firmato

Il sistema, al momento dell’acquisizione di file PDF (acquisizione manuale, automatica, import), è in grado di riconoscere anche firme PAdES. Se il documento risulta essere firmato, il sistema verifica l’eventuale marcatura temporale per consentirne la visualizzazione (Figura 137).

Figura 137 – Dettagli marca temporale

2.14.4 Blocco BLOCCA/RILASCIA

Questo blocco si suddivide in 6 differenti sezioni, di cui 5 sempre visibili ed una visibile solo se vi è un documento in stato di blocco e/o lavorazione. Queste sezioni sono:

- Copia documento in locale;

- Blocca;
- Rilascia;
- Rilascia Senza Salvare ;
- Apri;
- Informazioni di stato sul blocco.

2.14.4.1 Copia Documento in Locale

E' possibile salvare sulla propria postazione di lavoro i file associati ai documenti, agli allegati e alle versioni. Di default, per il salvataggio, viene proposto il nome originario del file.
Tale funzione è accessibile, nella parte destra del pannello di un documento, nella sezione: "Blocca/Rilascia" con l'icona , attiva solo se il documento ha associato un documento elettronico (file).
Una volta selezionata l'icona "Copia locale" , se:

- il file ha un'estensione diversa da p7m, quindi non firmato, si visualizza una finestra di dialogo (vedi Figura 138) attraverso la quale si specifica la cartella di destinazione e il nome che si vuole dare alla copia locale del documento e si conferma l'operazione con il pulsante "OK"; VTDOCS provvede alla copia del documento ed al termine visualizza il messaggio: "Copia Terminata";
- il file ha un'estensione p7m, quindi firmato, si visualizza una finestra di dialogo in cui oltre alla cartella di destinazione ed al nome del file è necessario selezionare dal menù a tendina riportato, il formato con cui si intende copiare il file: p7m o il formato originario del documento firmato. Nel caso si selezioni il formato originale per la copia, il sistema provvede alla verifica della firma:
  - Se è valida: salva la copia ed al termine si visualizza il messaggio: "Copia Terminata";
  - Se non è valida: segnala all'utente, attraverso un messaggio, che è impossibile salvare il file.

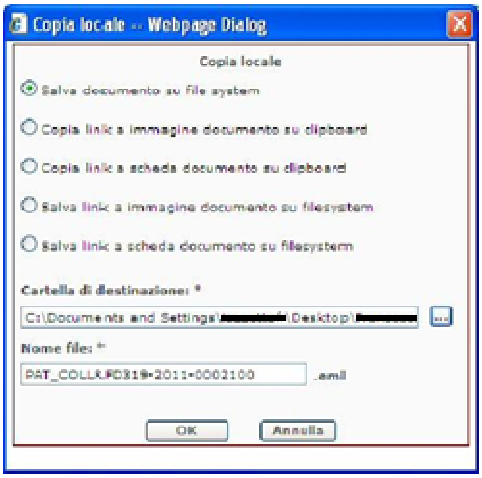


Figura 138 - Salva documento in locale, documento non firmato

2.14.4.2 Blocca

La funzione è attiva solamente se l'utente è abilitato all'inserimento di una nuova versione e se il documento non risulta bloccato da un altro utente.
La selezione del pulsante provoca l'impossibilità da parte di altri utenti a creare nuove versioni, e la copia sulla postazione di lavoro del file associato al documento stesso in un percorso scelto dall'utente. Il sistema propone come nome file il nome del file originale (quello che aveva al momento della prima

acquisizione). Eventuali modifiche del nome proposto avranno effetto sul nome del file originario della successiva versione del documento (vreata con il rilascio del documento stesso).

Dopo la selezione del percorso, il sistema effettua le seguenti operazioni:

- effettua l'operazione di blocco della versione corrente da parte dell'utente;
- copia il file associato al documento nel percorso specificato;
- esegue l'applicazione associata al formato del file (es. Word, Excel, ….);

L'operazione di "blocco" del file è tracciata nel sistema. In particolare, sono registrate le seguenti informazioni:

- l'autore del blocco (utente e ruolo);
- la data e ora del blocco;
- il nome di rete della postazione di lavoro da cui è avvenuto il blocco;
- il percorso in cui è stato estratto il file.

Il blocco può essere effettuato anche su un documento per cui la versione corrente non ha alcun file acquisito. L'utente, come nel caso precedente, deve selezionare il percorso locale in cui copiare il file. Il sistema restituisce, in maniera automatica, un modello di file vuoto corrispondente alla tipologia di file richiesto (i modelli di documenti supportati sono: .txt, .doc, .ppt, .xls, .ppt, .rtf).
Nel caso in cui è richiesto un tipo di file non presente tra i modelli predefiniti, il blocco sul documento viene annullato e viene mostrato un messaggio di errore;

2.14.4.3 Rilascia

Tale pulsante è attivo solo dopo aver bloccato il file e solo per l'utente che ha effettuato il blocco. Anche per l'utilizzo di questo pulsante è necessario che l'utente sia in possesso dell'abilitazione alla funzione relativa alla creazione di una nuova versione.

La selezione del pulsante provoca:

- La richiesta da parte del sistema della descrizione della nuova versione del documento che si sta creando;
- la creazione della nuova versione del documento cui sarà automaticamente associato il file il cui percorso è stato definito in fase di blocco;
- l'eliminazione del blocco.

Di fatto la funzione corrisponde alla sequenza delle operazioni "nuova versione" e "acquisisci file".
La generazione della nuova versione non è effettuata se, per qualsiasi motivo, il file salvato nella postazione di lavoro non è accessibile (tipicamente per operazioni accidentali di cancellazione o rinomina del file) nel percorso scelto in fase di blocco. In questo caso sarà visualizzato un messaggio in cui si può sbloccare o meno il documento e ricorda all'utente il percorso originario del file.

2.14.4.4 Rilascia senza salvare

Tale pulsante è attivo solamente se il file è stato bloccato e solo per l'utente che ha effettuato tale blocco.
La selezione del pulsante provoca:

- La cancellazione del file locale;
- Lo sblocco del documento.

A questo punto, il documento si visualizza così come era in origine (cioè prima del blocco).

2.14.4.5 Apri

Tale pulsante è attivo solamente se il file è stato bloccato e solo per l'utente che ha effettuato il blocco. La selezione del pulsante provoca l'apertura del file (fuori da VTDOCS) con l'applicazione associata al formato del file (es. Word, Excel, ….).
Nel caso il file non fosse accessibile, si visualizza un opportuno messaggio di errore.

2.14.4.6 Informazioni di stato sul blocco

Per gli utenti diversi da colui che ha bloccato il documento, sono disattivate tutte le funzioni di nuova versione, rimuovi versione e firma (quindi, in generale,sono disattivate tutte le funzioni che richiedono la creazione di nuova versione), cancellazione documento.
Per chi ha bloccato il documento, la funzione di "nuova versione" è disabilitata e sostituita da quella di "Rilascia".
Non è possibile Predisporre il documento alla protocollazione.
I dati generali del documento stesso sono comunque modificabili e seguono le regole usuali di VTDOCS.
Il tradizionale pulsante di visualizzazione del documento rimane invariato e visualizza sempre in sola lettura la versione del file richiesta.
Se il file è bloccato, il sistema visualizza nella testata del documento un'icona (un lucchetto) che indica che il file non è modificabile da altri utenti.
Un file bloccato, è tale anche per lo stesso utente che ha effettuato il blocco, se l'utente è connesso con un ruolo diverso.

2.14.5 Blocco MODELLI

I modelli, se configurati e associati alla tipologia di documenti profilati, sono visibili nell'applicativo in tutte le parti riguardanti documenti protocollati e non e sono utilizzabili dalla pagina "profilo", "protocollo", o "versioni". Il sistema effettua dei controlli per rendere disponibile la gestione dei modelli ed il loro corretto funzionamento. Se vi è un modello associato alla tipologia di documento che si sta lavorando, selezionando l'icona  , si apre una finestra di dialogo che è indicata come "Blocca documenti" (come mostrato nella Figura 139). Tale finestra di dialogo è costituita da due differenti campi che obbligatoriamente devono essere riempiti:

- *Cartella di destinazione:* indica dove fisicamente il sistema va a depositare il file che si sta bloccando. E' possibile digitare manualmente o selezionare tramite l'icona  il percorso di destinazione del file;
- *Nome file:* mostra un campo in cui digitare il nome che si vuole assegnare al file che si sta bloccando. E' disponibile un menù a tendina che mostra le due differenti estensioni disponibili per il modello (doc, rtf).

Mediante il pulsante  , è possibile bloccare il documento, oppure premendo  .non si dà luogo all'operazione.
Se si blocca il documento, si visualizza il modello che è possibile completare e/o modificare, a seconda di come è stato impostato nell'applicazione di amministrazione di VTDOCS, ed in alto a destra compare l'icona  ; il documento resta bloccato fino a quando non si "Rilascia" o si "Rilascia senza salvare".

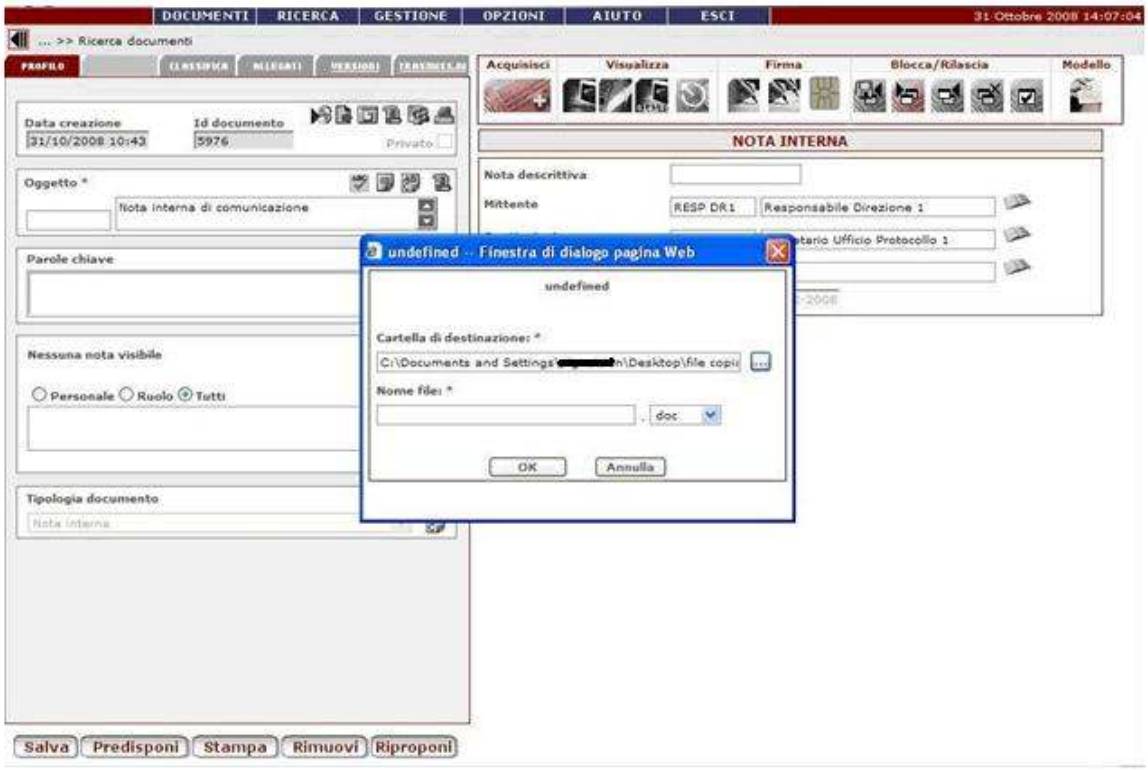


Figura 139 – Selezione Modello

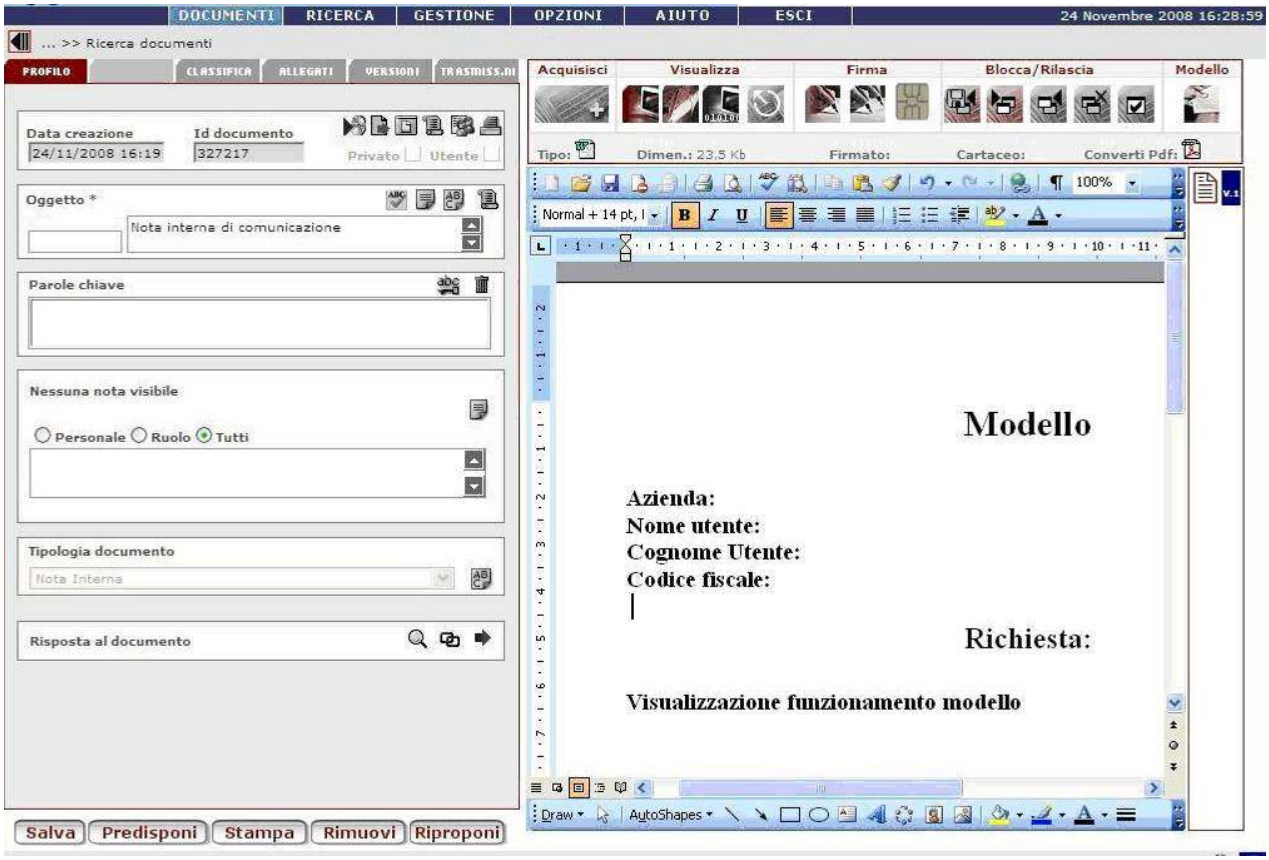


Figura 140 – Visualizzazione dei modelli

2.14.6Converti documenti già acquisiti in formato PDF

Nella sezione relativa al blocco Acquisisci, è stato mostrato come all'atto dell'acquisizione di un documento è possibile effettuare contestualmente la conversione dello stesso mediante la selezione di "converti in PDF lato server".

Allo stesso modo è possibile convertire in un secondo momento il documento acquisito: si seleziona il documento, protocollato o meno, di interesse nella sezione evidenziata in rosso in Figura 141. Agendo sull'icona "converti PDF" (evidenziata in blu) si effettua la conversione.

Analogamente a quanto accade nel caso di conversione contestuale all'acquisizione del documento, saranno presenti due versioni del documento. Sarà altresì possibile inviare una notifica dell'avvenuta conversione all'utente che l'ha richiesta oppure a tutti gli utenti appartenenti al suo ruolo. Il sistema può essere eventualmente configurato in modo da non inviare notifiche.

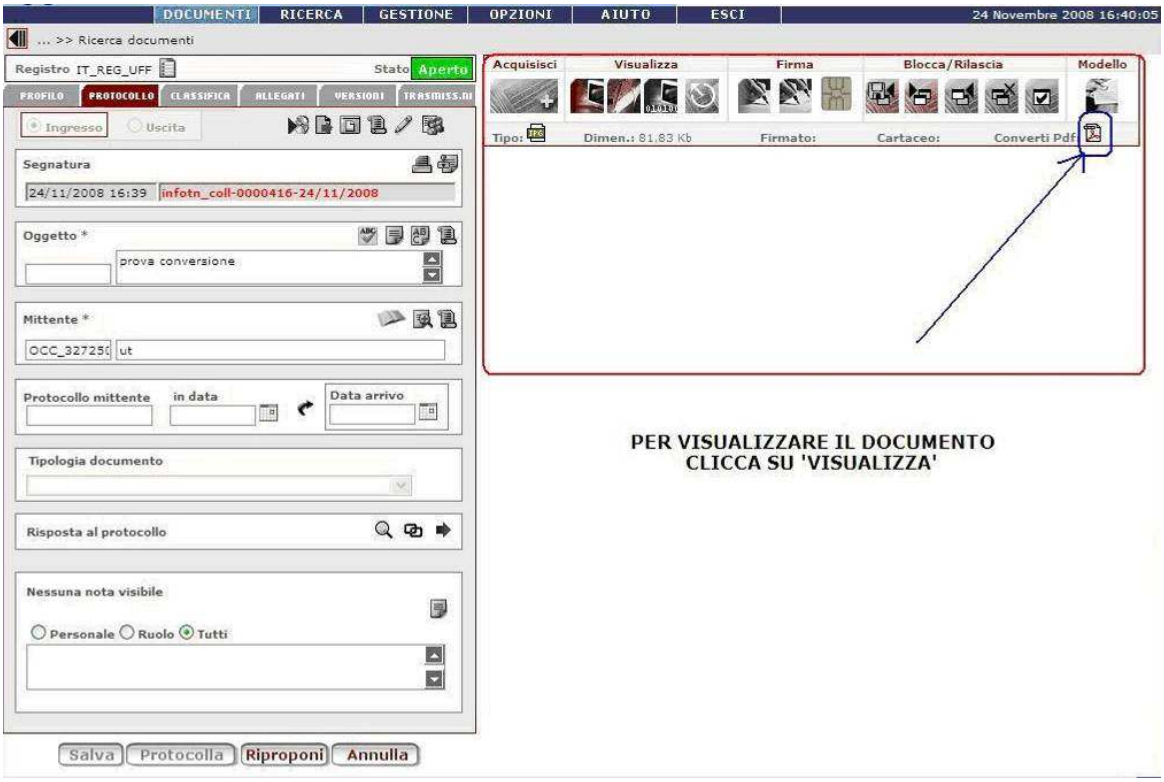


Figura 141 - Conversione PDF lato server dei documenti già acquisiti

2.14.7 Timestamping dei documenti

Questa funzionalità è presente solo se l'amministrazione ne ha fatto richiesta.
Nella maschera di dettaglio di un documento, nella sezione evidenziata in rosso nella Figura 143, è presente un pulsante che consente di visualizzare e/o apporre il timestamp ad un documento.
In particolare il colore dell'icona associata al pulsante indica se:

- il documento non ha timestamping (grigio)
- il documento ha un timestamping valido (verde)
- il documento ha un timestamping scaduto (rosso)

Figura 142 – Icone del timestamping

Cliccando sul pulsante si apre una pagina in cui sono mostrati i timestamp presenti ed è possibile aggiungerne altri.
Nella stessa pagina è possibile salvare un timestamp in locale come file in formato TSR.

Il timestamp può essere aggiunto su tutte le versioni e gli allegati del documento, solamente dai ruoli abilitati alla funzione di timestamping.

Una volta associata una marca temporale, è possibile creare, tramite il pulsante “Crea TSD” (Figura 143), una nuova versione del documento (nota di versione: “Versione creata per conversione in TSD” (Figura 144)) avente per immagine un file TSD contenente la marca temporale ed il file originario.

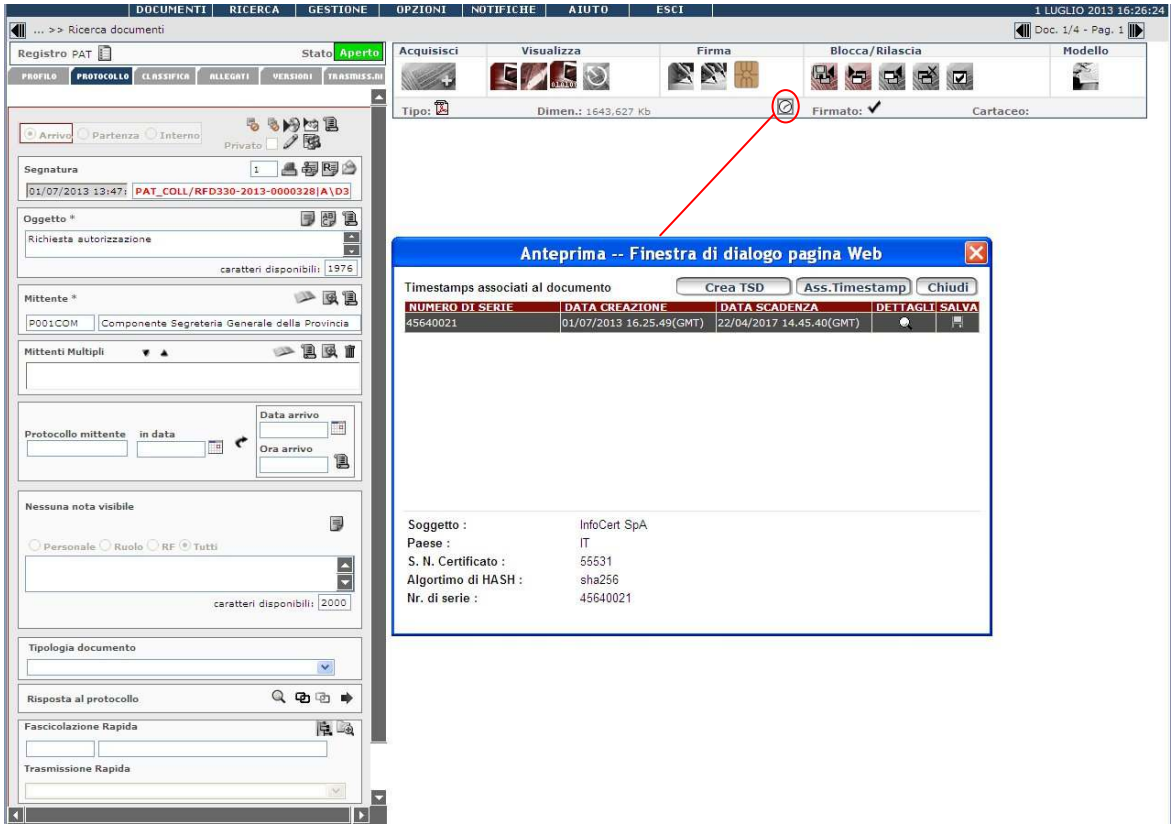


Figura 143 – Timestamping documento

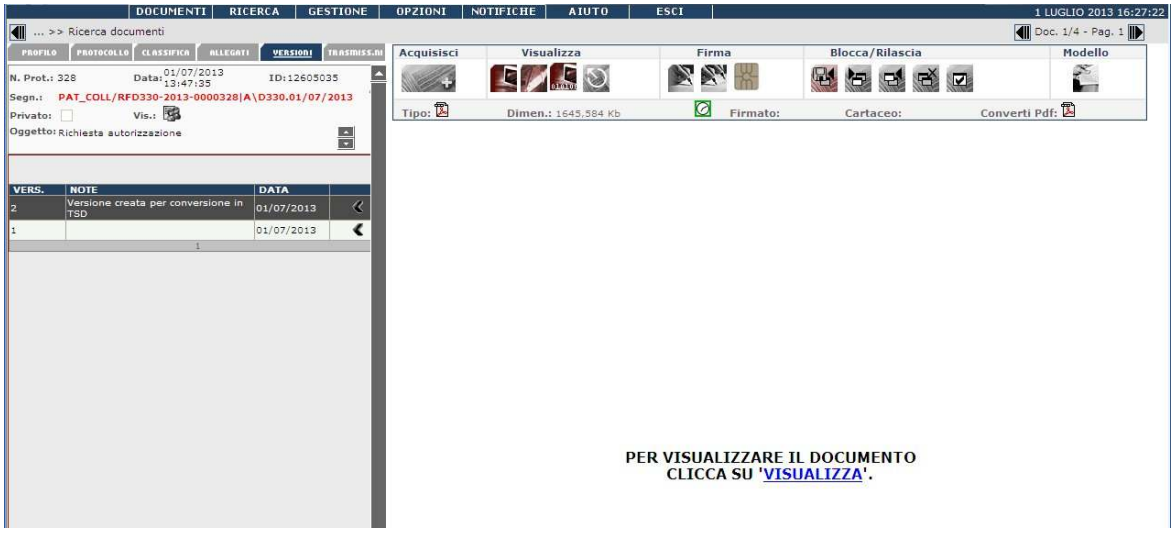


Figura 144 – Creazione file TSD

2.15 Protocollazione in ingresso semplificata

La funzionalità di protocollo in ingresso semplificata presenta le seguenti funzioni:

- Protocollazione in ingresso;
- Smistamento dei documenti ad una lista definita di UO destinatarie (attraverso il ruolo di riferimento);
- Acquisizione e visualizzazione di documenti da scanner e anche da file system per le amministrazione che ne abbiano fatto richiesta;
- Gestione allegati;
- Stampa dell'etichetta di segnatura.

2.15.1 Protocollazione in ingresso

La pagina di protocollazione in ingresso semplificata si apre selezionando dal menù principale del prodotto VTDOCS "Documenti" – "Prot. ingresso".

Figura 145 – Menù "Documenti" – "Prot. Ingresso"

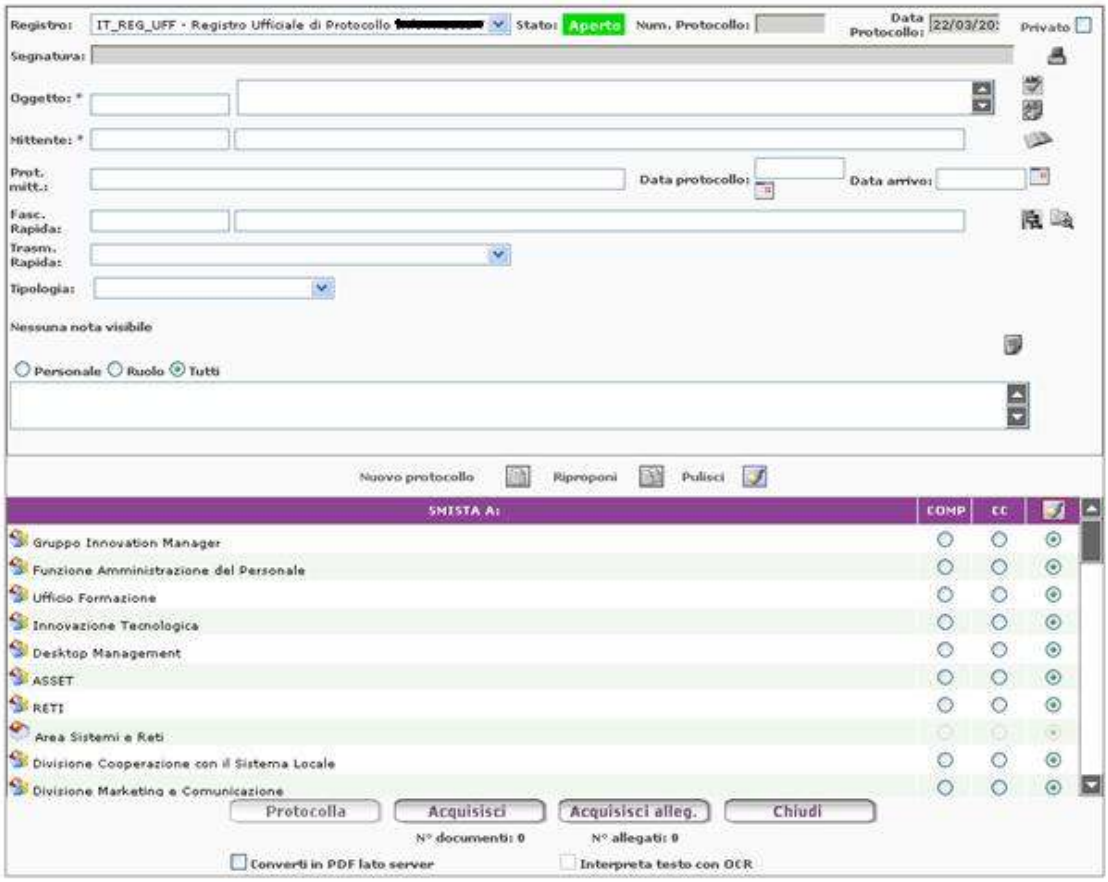


Figura 146 - Protocollazione in ingresso semplificata

L'inserimento dei dati del documento da protocollare si effettua popolando i campi presenti nella figura sottostante:

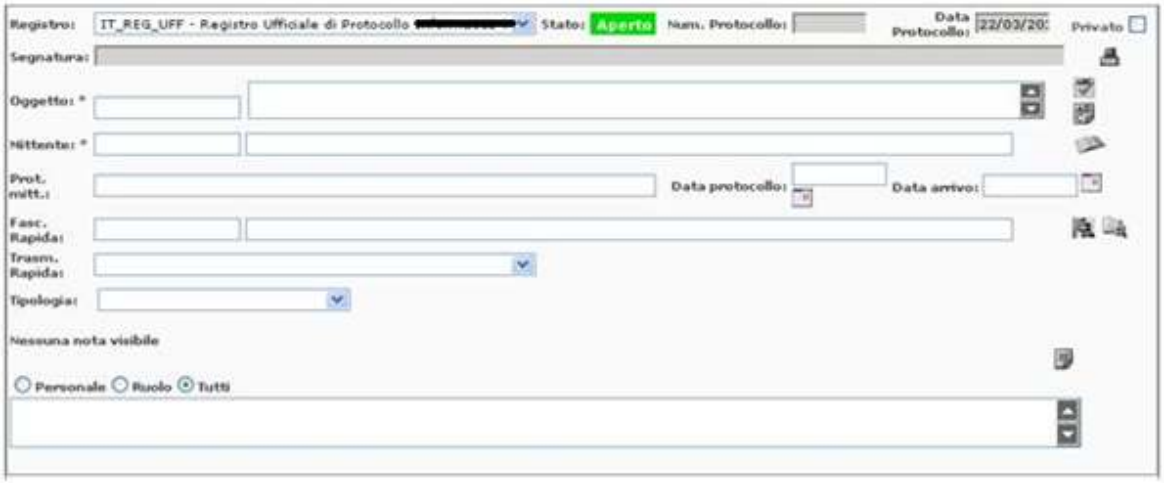


Figura 147 – Campi di registrazione dei dati del documento

Il registro di protocollo è lo stesso di quello presente in VTDOCS di cui segue la numerazione e lo stato; il numero e la data del protocollo vengono impostati in automatico dal sistema. I campi presenti per la registrazione dei dati del documento sono:

- **Oggetto**: inserito manualmente dall'utente o selezionato dall'oggettario (così come descritto nel paragrafo 2.7.1.3.1);
- **Mittente**, con una rubrica per la selezione del mittente che propone solo l'anagrafica esterna (come descritte per l'inserimento del corrispondente descritto al paragrafo 2.7.1.3.2);
- **Protocollo mittente**;
- **Data protocollo mittente** e **Data arrivo** (con un calendario per facilitarne l'inserimento);
- **Fascicolazione rapida**: è possibile effettuare la fascicolazione rapida attraverso la digitazione del codice del fascicolo o del sottofascicolo (se conosciuto), oppure selezionando l'icona che permette di scegliere (così come descritto dal paragrafo 2.8.1.3) il fascicolo/sotto fascicolo desiderato. Il documento, contestualmente alla creazione del protocollo in ingresso, verrà anche direttamente classificato. Se accanto alla dicitura fascicolazione rapida vi è un asterisco, questa è obbligatoria.
  C'è anche la possibilità di creare un fascicolo direttamente da questa sezione dove è presente (se attivata la funzionalità) un ulteriore pulsante ( ) che consente di aprire la finestra per la creazione di un nuovo fascicolo. L'utente pertanto digita il codice del nodo di titolario nel campo presente nella sezione "fascicolazione rapida" ed il fascicolo viene creato sotto questo nodo.
- **Trasmissione rapida**: è possibile effettuare la trasmissione del documento per il quale si sta eseguendo la registrazione di protocollo nel caso in cui siano stati definiti dei modelli di trasmissione rapida.
- **Tipologia documento**: in cui l'utente può scegliere una tipologia da indicare. Una volta scelta la tipologia, nella sezione destra della pagina si visualizza il pannello con i campi della profilazione dinamica del documento. L'utente amministratore in fase di costruzione della "tipologia documento" può associare ad un ruolo specifico la visualizzazione e l'utilizzo di una determinata tipologia, per cui le informazioni relative alla tipologia documento sono visibili solo agli utenti abilitati. L'utente inserisce i dati in base alle impostazioni predefinite dall'amministratore. Tra i dati della tipologia se ci sono dei contatori con attivazione manuale all'atto della creazione ci sarà una casella selezionabile denominata "Attiva" ed il contatore scatterà solo quando l'utente seleziona questa casella. Per i dettagli sui campi delle tipologie documento si rimanda al paragrafo 2.7.1.1. Se alla tipologia selezionata è associato un diagramma di stato, viene automaticamente visualizzato il campo "Stato" che può essere popolato così come descritto nel paragrafo 2.8.1 al capoverso "Stato".
- **Note**: campo di testo in cui è possibile inserire una o più note per ciascuna delle quali si può impostare una diversa visibilità scegliendo tra le alternative proposte (per dettagli maggiori sull'utilizzo della funzionalità si veda il paragrafo 2.8.1.2);
- **Mittenti multipli**: dato non obbligatorio presente solo per le amministrazioni che ne hanno fatto richiesta. Rappresenta gli ulteriori mittenti di un documento: nel caso in cui il mittente fosse costituito da un raggruppamento di persone, società, uffici, enti, etc, questo campo dà la possibilità di specificarne tutti i componenti. Anche i mittenti multipli possono essere occasionali (in tal caso può essere inserito liberamente dall'utente valorizzando il campo descrizione della stringa mittente e poi spostato mediante la freccia) o abituale, selezionandolo dalla rubrica. Per la selezione da rubrica è necessario premere il pulsante associato al campo. Dalla rubrica sarà possibile utilizzare anche le liste di distribuzione. Se si sceglie una lista dalla rubrica dei *mittenti* multipli, gli elementi della lista verranno riportati nel campo multi valore dei *mittenti multipli*. Con il pulsante

sarà possibile eventualmente spostare uno dei mittenti nel campo *mittente* (principale). Per le funzionalità relative alla rubrica ed al suo utilizzo, si rimanda al Paragrafo 4.5.
In generale per spostare un nominativo dal campo "mittente" al campo "mittenti multipli" e viceversa, selezionare il nominativo di interesse e successivamente l'icona freccia, (per spostarlo verso il basso) o (per spostarlo verso l'alto) a seconda di come si vogliono posizionare i mittenti nell'elenco. (Figura 148)
La presenza di questo campo è configurabile. Se utilizzato, le ricerche fatte per mittente prenderanno in considerazione non solo il mittente (principale) ma anche i mittenti multipli.
I dati sui mittenti multipli vengono visualizzati in tutti i punti in cui viene riportato il mittente "principale" (ricerche documenti, lista delle cose da fare, elenco dei documenti presenti in un fascicolo, …).

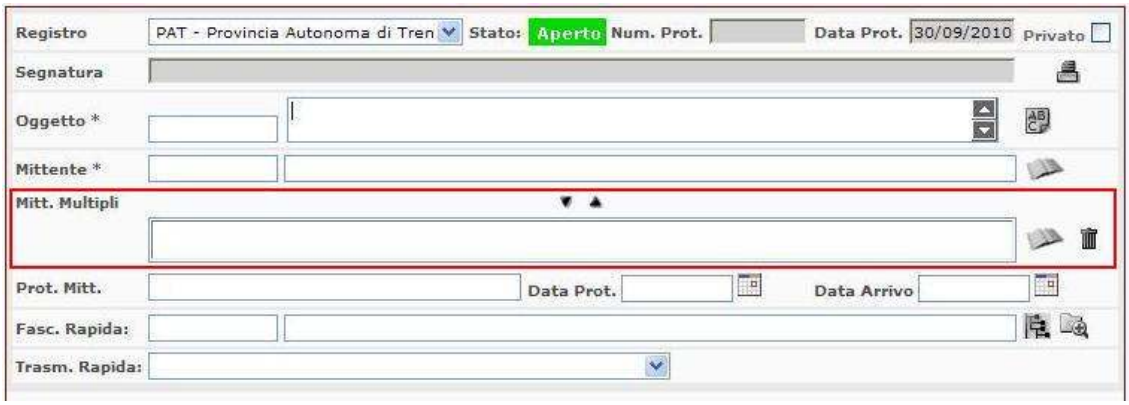


Figura 148 – Mittenti multipli

L'oggetto ed il mittente come sempre sono campi obbligatori.

2.15.2Smistamento

Dopo aver popolato i campi obbligatori per la registrazione del documento, la segnatura si ottiene indicando a quale UO sia indirizzato il documento (per competenza o per conoscenza). Si possono selezionare una o più UO a cui smistare il documento che, dopo la protocollazione, verrà trasmesso al ruolo di riferimento (in precedenza impostato dall'amministratore di sistema) delle UO prescelte. Si propone di seguito l'immagine del pannello che riguarda lo smistamento.

Figura 149 – Smistamento

Dopo aver inserito i dati di registrazione e selezionata l'UO a cui smistare il documento, è possibile procedere alla protocollazione selezionando il pulsante "Protocolla" posto in basso al pannello.
Per le amministrazioni che ne abbiano fatto richiesta, lo smistamento non è obbligatorio, pertanto sarà possibile protocollare un documento anche senza aver selezionato una UO a cui smistarlo.

Figura 150 – Dettaglio pulsanti

Dalla figura precedente si evidenziano due tasti che propongono altre funzionalità:

- **Acquisisci** e **Acquisisci alleg.** (vedi paragrafo 2.15.3.2).
- **Chiudi**: consente di chiudere il pannello di protocollazione in ingresso semplificata, visualizzando la pagina iniziale del sistema VTDOCS.

2.15.3 Ulteriori funzionalità

Dopo aver protocollato il documento il sistema propone in automatico, se opportunamente impostato, le seguenti operazioni:

- Stampa dell'etichetta;
- Acquisizione del documento principale;
- Acquisizione degli allegati (a seconda che sia stato acquisito il documento principale).

2.15.3.1 Stampa etichetta

Al termine dell'operazione di protocollazione viene stampata in automatico l'etichetta (se impostato dall'amministratore di sistema) su cui è impressa la segnatura del documento. Inoltre, è possibile stampare altre etichette selezionando l'icona posta a fianco al campo "Segnatura".

2.15.3.2 Acquisizione del documento principale e gestione allegati

Dopo aver prodotto la stampa dell'etichetta, se predefinito, si apre in automatico la pagina che gestisce l'acquisizione di un documento da scanner (le caratteristiche dell'acquisizione del documento sono riportate nel paragrafo 2.14.1). La fase di acquisizione può essere effettuata anche successivamente, operando dal sistema VTDOCS (paragrafo 2.14.1).
Dopo aver acquisito il documento principale, si attiva il pulsante "Acquisisci allegato", che consente di gestire gli eventuali allegati. Anche in questo caso l'operazione di acquisizione può essere effettuata in una seconda fase.
Sia per i documenti principali che per gli allegati è indicato il numero di documenti che sono stati acquisiti.

Per le amministrazioni che ne abbiano fatto richiesta, l'acquisizione potrà essere effettuata anche da file system. In questo caso, cliccando sul pulsante "Acquisisci" o "Acquisisci allegati", non apparirà il pannello per l'acquisizione da scanner, ma quello classico per la scelta del tipo di acquisizione come mostrato nella figura successiva:

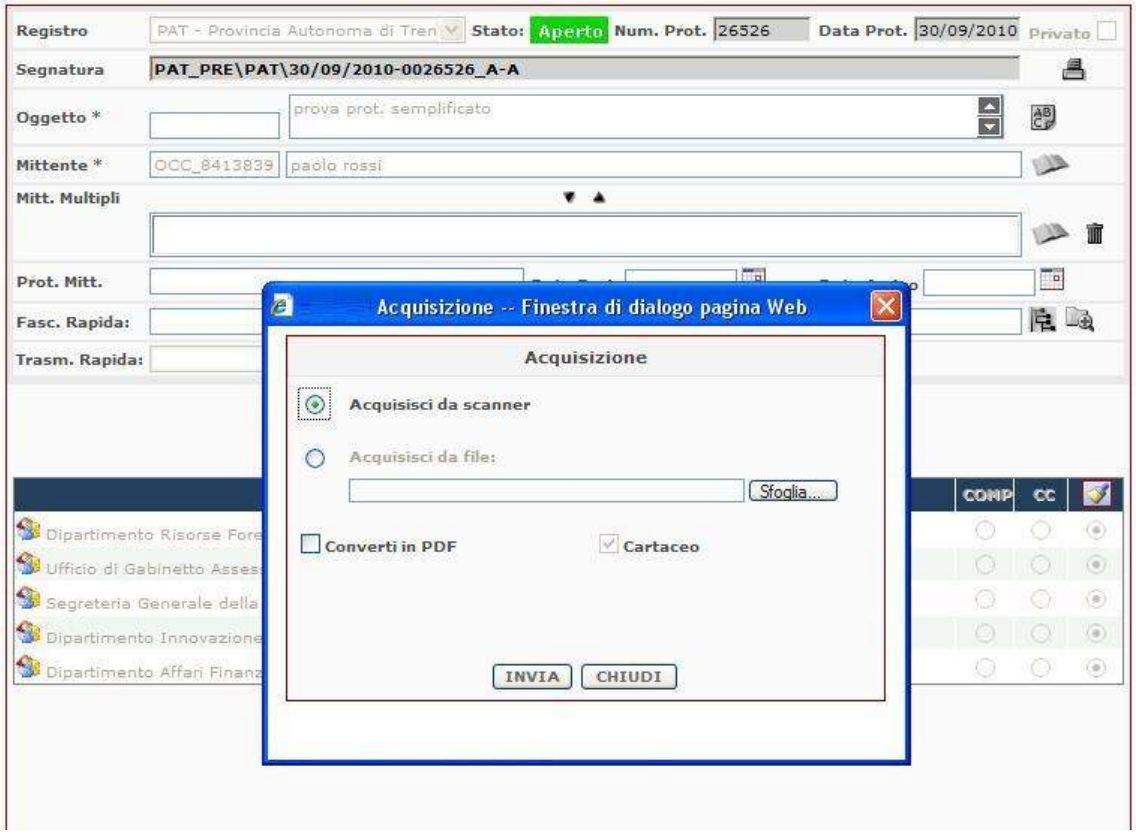


Figura 151 – Acquisizione da scanner o da file system

2.15.3.3 Pulsanti di funzione

Le icone riportate nella figura successiva consentono di effettuare le seguenti attività:

- Nuovo Protocollo: permette di creare un nuovo protocollo;
- Riproponi: predispone la sezione di protocollo con i dati obbligatori (oggetto e mittente) del protocollo precedente;
- Pulisci: elimina tutti i dati inseriti nella sezione prima che sia avvenuta la protocollazione.

Figura 152 – Pulsanti di funzione

2.16 Protocollazione in uscita semplificata

La funzionalità di protocollo in uscita semplificata presenta le seguenti funzioni:

- Protocollazione in uscita;
- Fascicolazione;

- Smistamento dei documenti ad una lista definita di UO destinatarie (attraverso il ruolo di riferimento);
- Acquisizione e visualizzazione di documenti solo da scanner;
- Gestione allegati;
- Stampa dell'etichetta di segnatura.

2.16.1 Protocollazione in uscita

La pagina di protocollazione in uscita semplificata si apre selezionando dal menù principale "Documenti" – "Prot. Uscita".

Figura 153 – Menù "Documenti" – "Prot. Uscita"

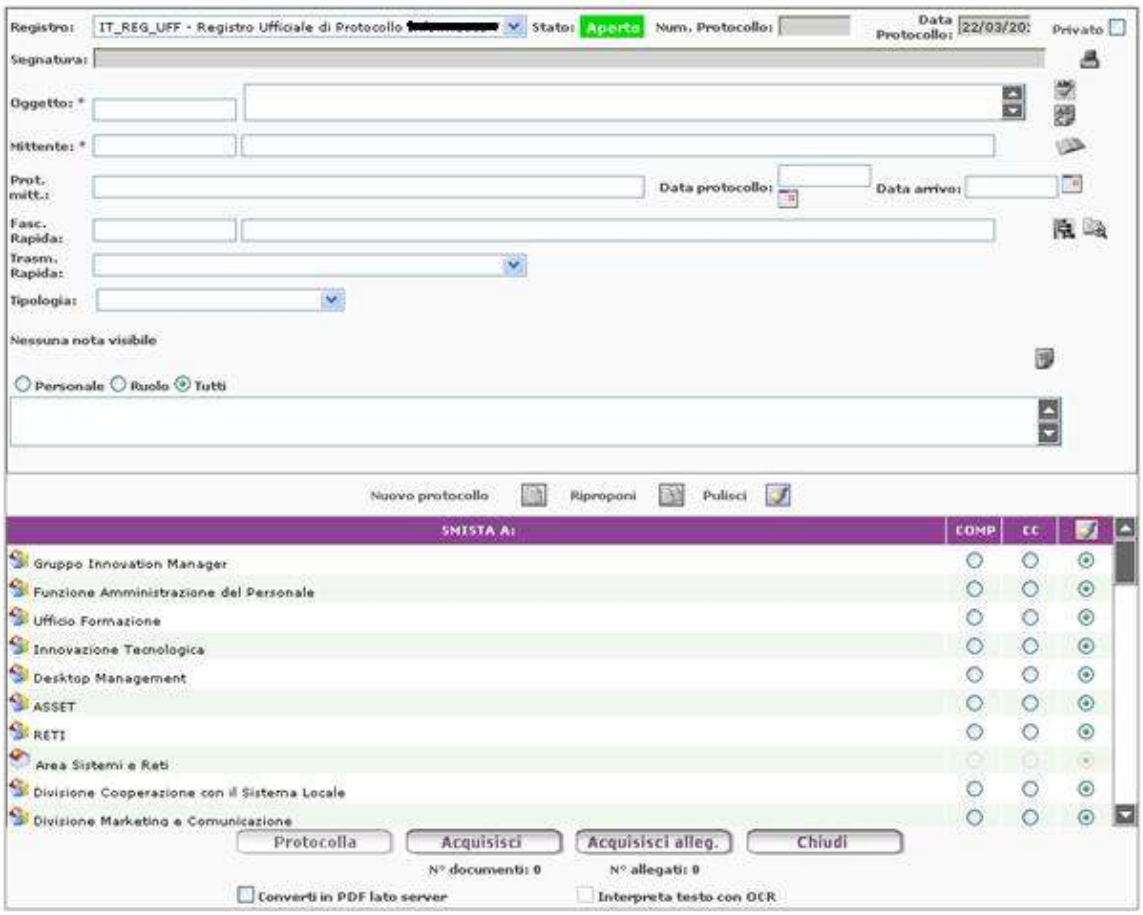


Figura 154 – Protocollazione in uscita semplificata

L'inserimento dei dati del documento da protocollare si effettua popolando i campi presenti nella figura sottostante:

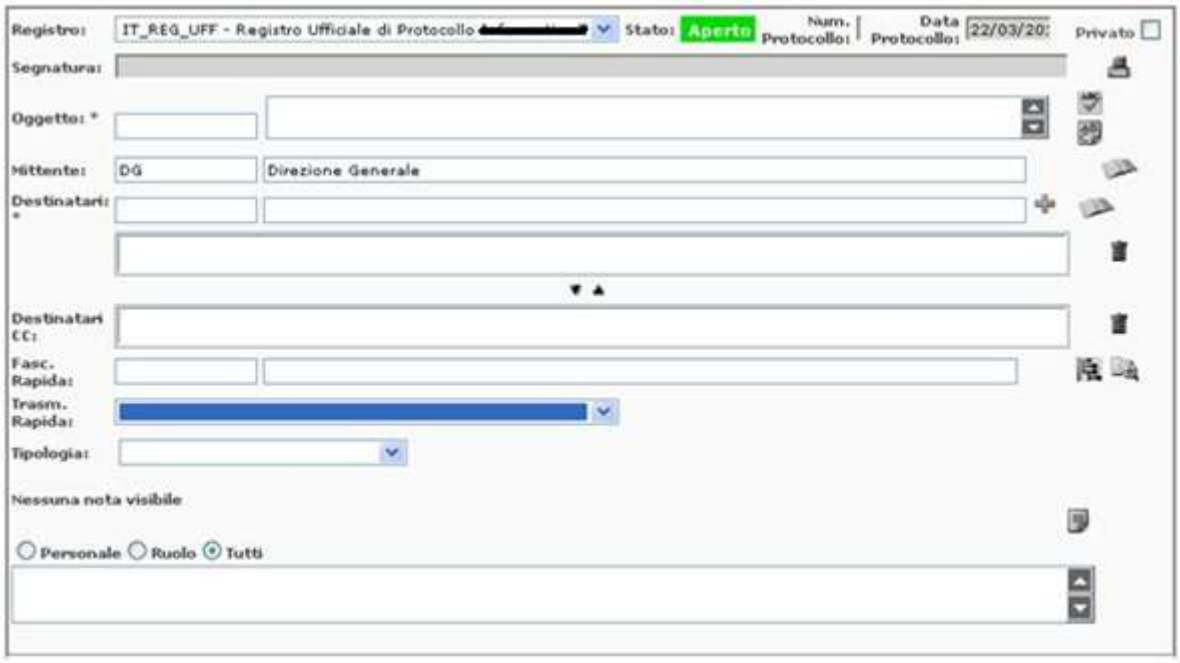


Figura 155 – Campi di registrazione dei dati del documento

Il registro di protocollo è lo stesso di quello presente in VTDOCS, di cui segue la numerazione e lo stato; il numero e la data del protocollo vengono impostati in automatico dal sistema. I campi presenti per la registrazione dei dati del documento sono:

- **Oggetto** inserito dall'utente o selezionato dall'oggettario (così come descritto al paragrafo 2.7.1.3.1);
- **Mittente**, con una rubrica per la selezione del mittente che propone solo l'anagrafica interna (come descritto per l'inserimento del corrispondente al paragrafo 2.7.1.3.2);
- **Destinatari**, con una Rubrica, richiamata tramite l'icona , per la selezione del destinatario che propone l'anagrafica Tutti (le modalità d'inserimento del corrispondente sono descritte nel paragrafo 2.7.2), l'icona per inserire codici inseriti manualmente dall'utente, e l'icona per eliminare le utenze non necessarie (dopo averle selezionate);
- **Destinatari CC**, con una rubrica, richiamata tramite l'icona , per la selezione del destinatario che propone l'anagrafica Tutti (le modalità d'inserimento del corrispondente sono descritte nel paragrafo 2.7.2), l'icona per inserire codici inseriti manualmente dall'utente, e l'icona per eliminare le utenze non necessarie (dopo averle selezionate);
- **Fascicolazione rapida:** è possibile effettuare la fascicolazione rapida attraverso la digitazione del codice del fascicolo o del sottofascicolo (se conosciuto), oppure selezionando l'icona che permette di scegliere (così come descritto dal paragrafo 2.8.1.3) il fascicolo/sotto fascicolo desiderato. Il documento, contestualmente alla creazione del protocollo in uscita, verrà anche direttamente classificato. Se accanto alla dicitura fascicolazione rapida vi è un asterisco, questa è obbligatoria.

- **Trasmissione rapida**: è possibile effettuare la trasmissione del documento per il quale si sta eseguendo la registrazione di protocollo nel caso in cui siano stati definiti dei modelli di trasmissione rapida.
- **Tipologia documento**: in cui l'utente può scegliere una tipologia da indicare. Una volta scelta la tipologia, nella sezione destra della pagina si visualizza il pannello con i campi della profilazione dinamica del documento. L'utente amministratore in fase di costruzione della "tipologia documento" o successivamente può associare, ad un ruolo specifico la visualizzazione e l'utilizzo di una determinata tipologia, per cui le informazioni relative alla tipologia documento sono visibili solo agli utenti abilitati. L'utente inserisce i dati in base alle impostazioni predefinite dall'amministratore. Se tra i dati della tipologia ci sono dei contatori con attivazione manuale all'atto della creazione compare una casella selezionabile denominata "Attiva", utilizzando la quale l'utente può determinare l'istante d'inizio del funzionamento del contatore. Per i dettagli sui campi delle tipologie documento si rimanda al paragrafo 2.7.1.1. Se alla tipologia scelta è associato un diagramma di stato, nella sezione "profilo" in automatico si visualizza il campo Stato e si popola così come descritto nel paragrafo 2.8.1 al capoverso "Stato" .
- **Note**: campo di testo in cui è possibile inserire una o più note per ciascuna delle quali si può impostare una diversa visibilità scegliendo tra le alternative proposte (per dettagli maggiori sull'utilizzo della funzionalità si veda il paragrafo 2.8.1.2);

L'oggetto ed il destinatario come sempre sono campi obbligatori.

2.16.2 Smistamento

Dopo aver popolato i campi obbligatori per la registrazione del documento, la segnatura si ottiene indicando a quale UO sia indirizzato il documento (per competenza o per conoscenza). Si possono selezionare una o più UO a cui smistare il documento che, dopo la protocollazione, verrà trasmesso al ruolo di riferimento (impostato in precedenza dall'amministratore di sistema) delle UO prescelte. Si propone di seguito l'immagine del pannello che riguarda lo smistamento.

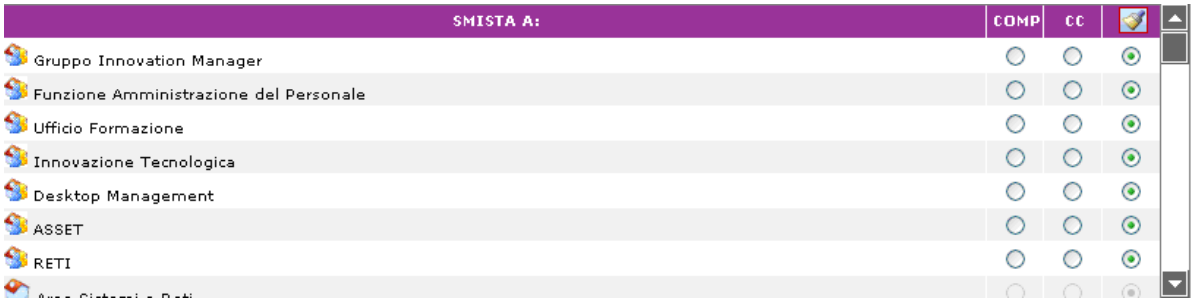


Figura 156 – Smistamento

Dopo aver inserito i dati di registrazione e selezionata l'UO a cui smistare il documento, è possibile protocollare il documento selezionando il pulsante "Protocolla" posto in basso al pannello.

Per le amministrazioni che ne abbiano fatto richiesta, lo smistamento non è obbligatorio, pertanto sarà possibile protocollare un documento anche senza aver selezionato una UO a cui smistarlo.

Figura 157 – Dettaglio pulsanti

Dalla figura precedente si evidenziano due pulsanti che propongono altre funzionalità:

- Acquisisci doc. principale e Acquisisci allegati (vedi paragrafo 2.16.3.2).
- Chiudi: consente di chiudere il pannello di protocollazione in uscita semplificata, visualizzando la pagina iniziale del sistema VTDOCS.

2.16.3 Ulteriori funzionalità

Dopo aver protocollato il documento il sistema propone in automatico, se opportunamente impostato, le seguenti operazioni:

- Stampa dell'etichetta;
- Acquisizione del documento principale;
- Acquisizione degli allegati (a seconda che sia stato acquisito il documento principale);

2.16.3.1 Stampa etichetta

Al termine dell'operazione di protocollazione viene stampata in automatico l'etichetta (se impostato dall'amministratore di sistema) su cui è impressa la segnatura del documento. Inoltre, è possibile stampare altre etichette selezionando l'icona posta a fianco al campo "Segnatura".

2.16.3.2 Acquisizione del documento principale e gestione allegati

Dopo aver prodotto la stampa dell'etichetta, se predefinito, si apre in automatico la pagina che gestisce l'acquisizione di un documento da scanner (le caratteristiche dell'acquisizione del documento sono riportate paragrafo 2.14.1). La fase di acquisizione può essere effettuata anche successivamente, operando dal sistema VTDOCS (come da indicazioni riportate sul presente manuale).
Dopo aver acquisito il documento principale, si attiva il pulsante "Acquisisci allegato", che consente di gestire gli eventuali allegati. Anche in questo caso l'operazione di acquisizione può essere effettuata in una seconda fase.
Sia per i documenti principali che per gli allegati è presente, tra parentesi, il numero di documenti che sono stati acquisiti.

Per le amministrazioni che ne abbiano fatto richiesta, l'acquisizione potrà essere effettuata anche da file system. In questo caso, cliccando sul pulsante "Acquisisci" o "Acquisisci allegati", non apparirà il pannello per l'acquisizione da scanner, ma quello classico per la scelta del tipo di acquisizione.

2.16.3.3 Pulsanti di funzione

Le icone riportate nella figura successiva consentono di effettuare le seguenti attività:

- Nuovo Protocollo: permette di creare un nuovo protocollo;
- Riproponi: predispone la sezione di protocollo con i dati obbligatori del protocollo precedente;
- Pulisci: elimina tutti i dati inseriti nella sezione prima che sia avvenuta la protocollazione.

Figura 158 – Pulsanti di funzioni

2.17 Importa documenti

La funzione “Importa documenti” attivabile dalla voce di menù: **DOCUMENTI → Imp. documenti**, consente di creare in modo rapido un numero elevato di documenti. Per ogni documento è inoltre possibile acquisire in modalità “massiva” il file ad esso relativo, prendendolo dal file system, ed inserire il codice di fascicolazione rapida.

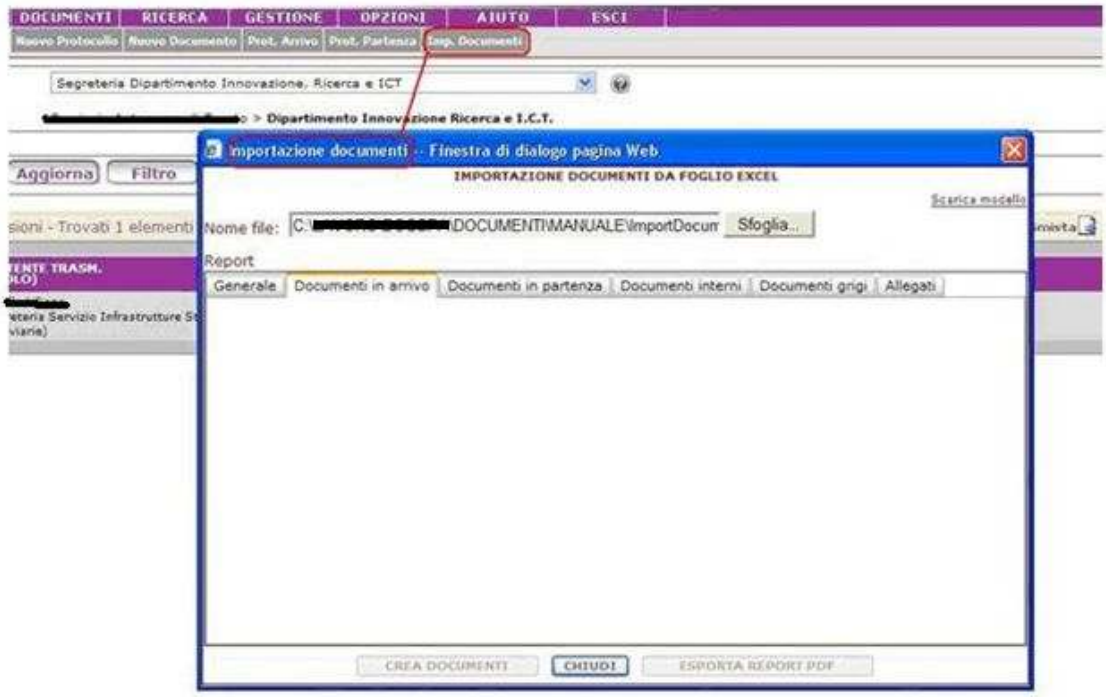


Figura 159 – Import documenti

La procedura di import fa uso di un particolare foglio excel suddiviso in tanti fogli, uno per ogni tipo di documento. Il modello da utilizzare può essere scaricato tramite il link *Scarica modello* presente nella pagina di Figura 159.

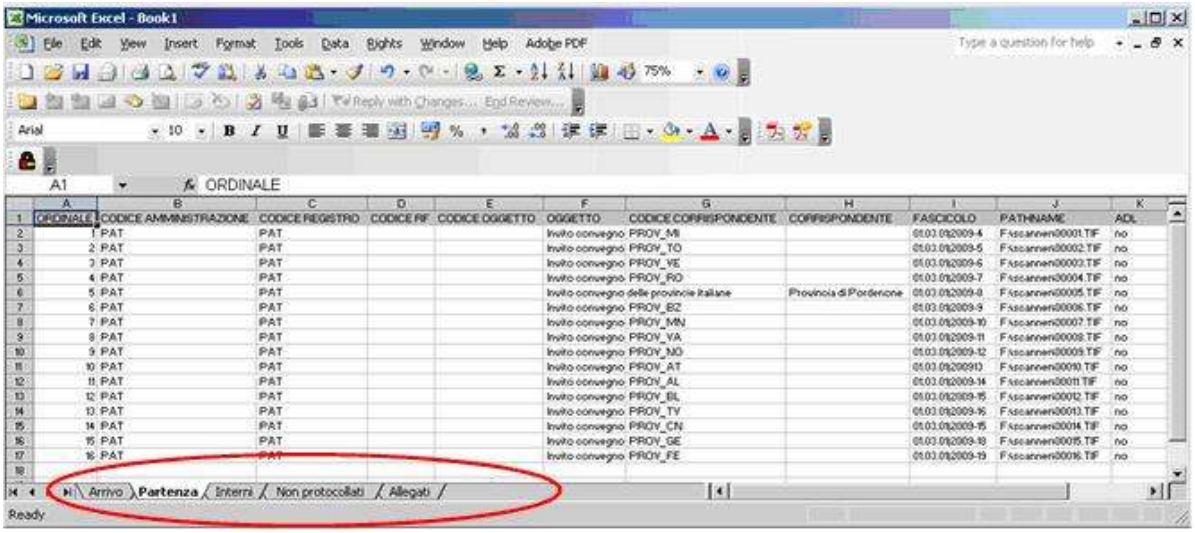


Figura 160 - Foglio excel

Dopo aver compilato il foglio excel con i dati dei documenti da creare, se ne specifica il percorso sul file system nel campo *Nome file* e si avvia la procedura di import cliccando sul pulsante CREA DOCUMENTI.

Dopo aver verificato la validità dei dati, il sistema avvia la procedura di importazione. Per ogni tipologia di documento verrà riportato il numero di documenti importati, di quelli scartati, di eventuali errori o warning. Sarà poi possibile esportare il risultato dell'operazione in un file pdf cliccando il pulsante ESPORTA REPORT PDF. Il pulsante CHIUDI consente di chiudere la pagina.

Di seguito viene descritta la struttura del foglio excel relativamente ai documenti in Arrivo, per gli altri il formato è analogo:

CAMPO	DESCRIZIONE	NOTE
ORDINALE	Ordinale da 1..N	Numero identificativo univoco della riga da importare
CODICE AMMINISTRAZIONE:	codice dell'amministrazione	Obbligatorio
CODICE REGISTRO	Codice del registro del protocollo.	Obbligatorio
CODICE RF	Codice dell'RF col il quale calcolare il codice della segnatura del protocollo	Opzionale in base al formato della segnatura
CODICE OGGETTO	Codice oggetto	Obbligatorio alternativo al campo OGGETTO. Codice in oggettario dell'oggetto da inserire.
OGGETTO	Oggetto del documento	Obbligatorio alternativo al campo CODICE OGGETTO inserimento oggetto occasionale
CODICE CORRISPONDENTE	Codice rubrica del mittente.	Obbligatorio alternativo a CORRISPONDENTE.

		Specificando questo campo il sistema ricercherà il mittente nella rubrica.
CORRISPONDENTE	Descrizione mittente occasionale	Obbligatorio alternativo a CODICE MITTENTE.
PATHNAME	Pathname completo del file da associare al documento.	Opzionale Il pathname deve essere raggiungibile condiviso (“shared”) con almeno diritti di sola lettura dai server web dove risiedono i Web Services dell’applicativo. Il nome originario del file verrà memorizzato all’interno del sistema e sarà immodificabile
ADL	Indica se il documento deve essere inserito in ADL oppure no.	Opzionale Valori possibili [si, no] Se omesso vien considerato il valore “no”
NOTE	Note generali (di tipo “Tutti”) da associare al documento	Opzionale
CODICE MODELLO TRASMISSIONE	Codici dei modelli di trasmissione, separati da “;” (punto e virgola) da utilizzare per trasmettere i documenti creati	Opzionale. Il sistema controllerà in base alle regole di visibilità ruolo creatore/registro se il modello è utilizzabile oppure no.
TIPOLOGIA DOCUMENTO	Descrizione della tipologia documento	
NOME CAMPO1	Descrizione = Valore del campo 1	In caso di campo multi valore, i diversi valori devono essere separati da “;” (punto e virgola)
..		
..		
NOME CAMPO n	Valore del campo n	
CODICE FASCICOLO	Codici, separati da “;” (punto e virgola) dei fascicoli in cui inserire il documento;	Opzionale
DESCRIZIONE FASCICOLO	Descrizione	
DESCRIZIONE SOTTOFASCICOLO	Descrizione	
TITOLARIO	Descrizione	
CODICE NODO		
TIPOLOGIA FASCICOLO	Descrizione della tipologia fascicolo profilata	Opzionale
NOME CAMPO1	Descrizione = Valore del campo 1	In caso di campo multi valore, i diversi valori devono essere separati da “;” (punto e virgola)

..		
..		
NOME CAMPO n	Valore del campo n	

Per la fascicolazione dei documenti, il sistema effettua la ricerca dei fascicoli sulla base dei valori inseriti nelle colonne dedicate alla classificazione/fascicolazione. Se viene indicato il valore puntuale del fascicolo nella colonna codice fascicolo non è necessario valorizzare i campi relativi agli altri dati di fascicolazione; se invece non si conosce il codice puntuale del fascicolo allora il sistema ricerca i fascicoli in cui inserire i documenti sulla base dei valori immessi nei campi Titolario, Descrizione fascicolo, Descrizione sottofascicolo, Tipologia fascicoli, Nome Campo 1 , campo n.
Se la classificazione del documento è obbligatoria e se l'esito della ricerca fascicoli risulta negativo il documento non viene creato.
Analogamente se la classificazione del documento è obbligatoria e non sono stati valorizzati almeno il campo nodo o campo codice fascicolo il documento non viene creato.
Se la tipologia documento è obbligatoria il sistema controlla la valorizzazione del campo Tipologia documento e se non valorizzato il documento non viene creato.

In caso i documenti abbiano degli allegati da associare è necessario utilizzare un apposito secondo foglio (work sheet) "Allegati" per descrivere ogni allegato.
Questo foglio è collegato ai documenti descritti negli altri fogli attraverso il campo ORDINALE. Nel caso un documento abbia più allegati bisogna inserire più righe con lo stesso ORDINALE

Di seguito la descrizione del formato:

CAMPO	DESCRIZIONE	NOTE
ORDINALE (allegato)	Ordinale da 1..N	Numero identificativo univoco delle riga da importare.
ORDINALE DOCUMENTO PRINCIPALE	A + ordinale documento principale (per gli allegati dei documenti protocollati in arrivo) P + ordinale principale (per gli allegati dei documenti protocollati in ingresso) I + ordinale principale (per gli allegati dei documenti interni protocollati) NP + ordinale principale (per gli allegati dei documenti non protocollati)	Poiché gli ordinali dei diversi fogli si ripetono si è reso necessario indicare in questo campo sia la lettera iniziale del foglio (A, P, I, NP) sia l'ordinale del documento principale.
DESCRIZIONE	Descrizione dell'allegato	Obbligatorio
PATHNAME	Pathname completo del file da associare al documento.	Opzionale Il pathname deve essere raggiungibile condiviso ("shared") con almeno diritti di sola lettura dai server web dove risiedono i Web

		Services dell'applicativo.

2.18 Importa Documenti Pregressi

Se l'amministrazione è opportunamente configurata, il ruolo abilitato può utilizzare la funzione "Importa documenti pregressi" (Documenti → Imp. Doc. Pregressi) che consente di inserire in modo rapido un numero elevato di documenti pregressi, associati ad uno specifico registro.

2.18.1 Nuovo import

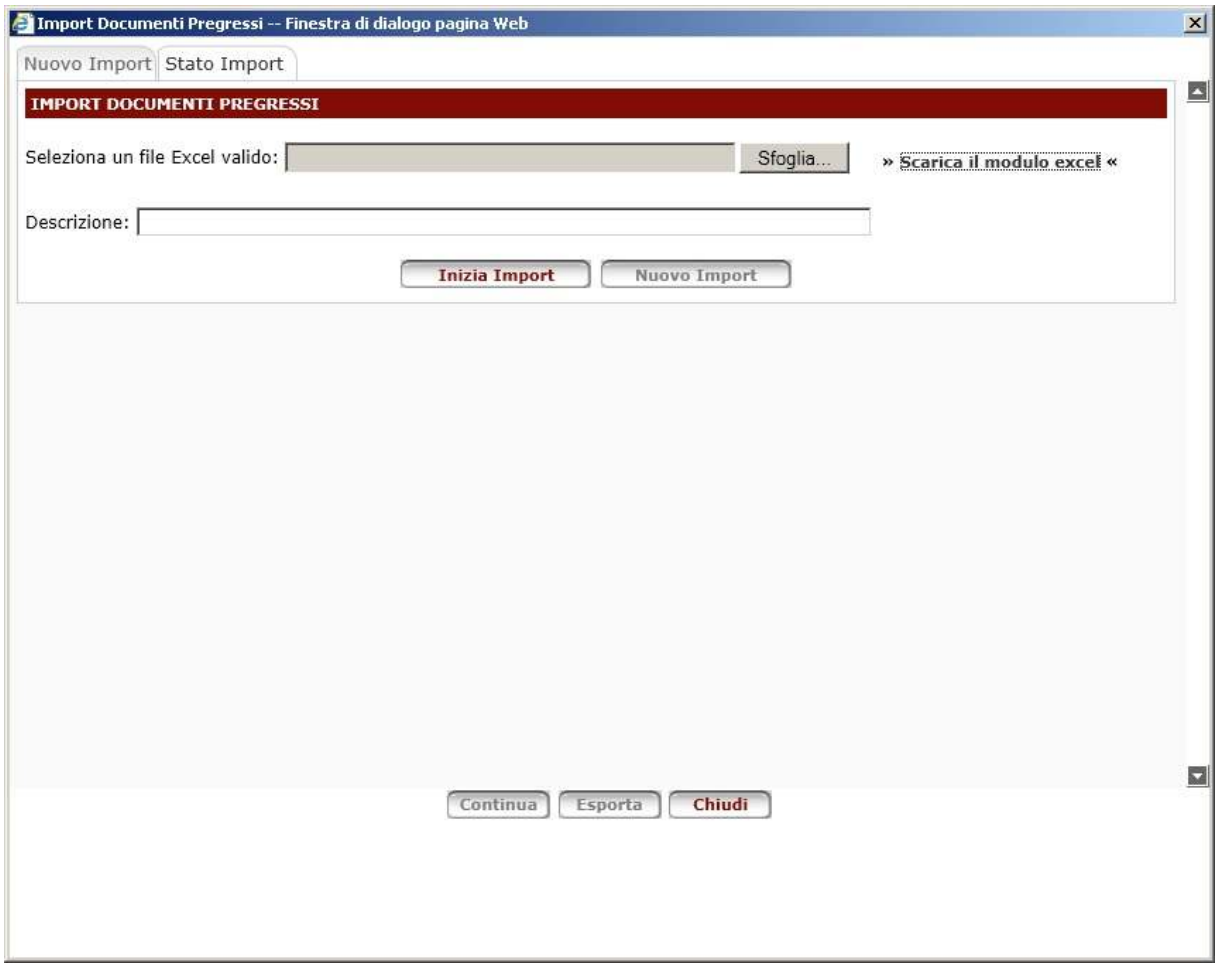


Figura 161 – Import documenti pregressi

La procedura di import fa uso di un particolare file excel (par. 2.18.1.1) contenente quatto fogli relativi a: Protocolli Pregressi, Documenti non Protocollati, Allegati ed Istruzioni di utilizzo del file. Il modello da utilizzare può essere scaricato tramite il link *Scarica il modulo excel* presente nella pagina di import documenti pregressi (Figura 161).

Dopo aver compilato il file excel con i dati dei documenti da creare:

- selezionare il file compilato nel campo “Seleziona un file Excel valido” tramite il pulsante “Sfoglia”
- indicare una descrizione che permetta successivamente di identificare l’import
- premere il pulsante Inizia Import

Prima dell’import vero e proprio il sistema verifica la validità dei dati riportati nel file excel:

✓ se l’esito è positivo, il sistema permette la selezione del pulsante Continua (Figura 162) e quindi l’avvio della procedura di importazione. Viene mostrato il messaggio “Import avviato con successo.”

✓ se l’esito è negativo, per i documenti scartati, con errori o warning il sistema descrive la tipologia di problema e per ciascuno indica l’ordinale di riferimento. Si abilita il pulsante Esporta che permette di esportare il risultato dell’operazione in un file excel che restituisce la descrizione dell’errore, e l’ordinale a cui associato, in modo che l’utente possa modificare i dati errati

Dopo aver avviato un import è possibile inoltre (Figura 162):

- predisporre un nuovo import, tramite il pulsante Nuovo Import
- chiudere la maschera di importazione selezionando il pulsante Chiudi .

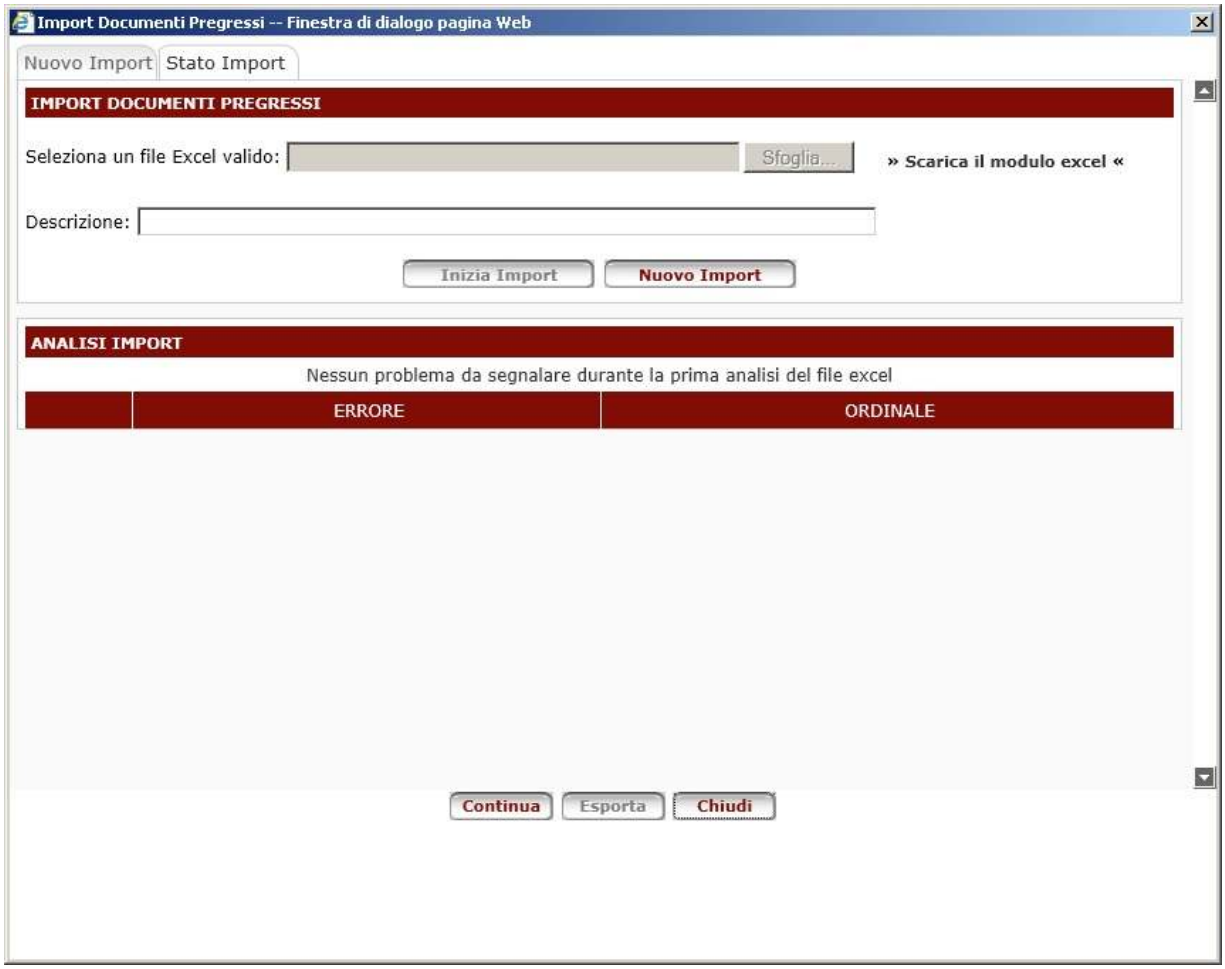


Figura 162 - Analisi del file excel per import documenti pregressi

2.18.1.1 Modulo di importazione pregressi

E' possibile scaricare il modello da compilare tramite il link "Scarica il modulo excel" (Figura 161).
Il file è costituito da quattro fogli (Figura 163):

- Protocolli Pregressi, Documenti non protocollati, Allegati: presentano dei campi obbligatori, da compilare in modo opportuno per il corretto funzionamento dell'import;
- Istruzioni: contiene le indicazioni operative per la compilazione degli altri fogli. Contiene l'elenco dei campi riportati in ciascun foglio, la relativa descrizione e le note che ne indicano l'obbligatorietà o meno.

Nel modulo di import è possibile inoltre indicare l'immagine del documento da importare. Tale immagine dovrà essere messa a disposizione su un opportuno sito ftp.

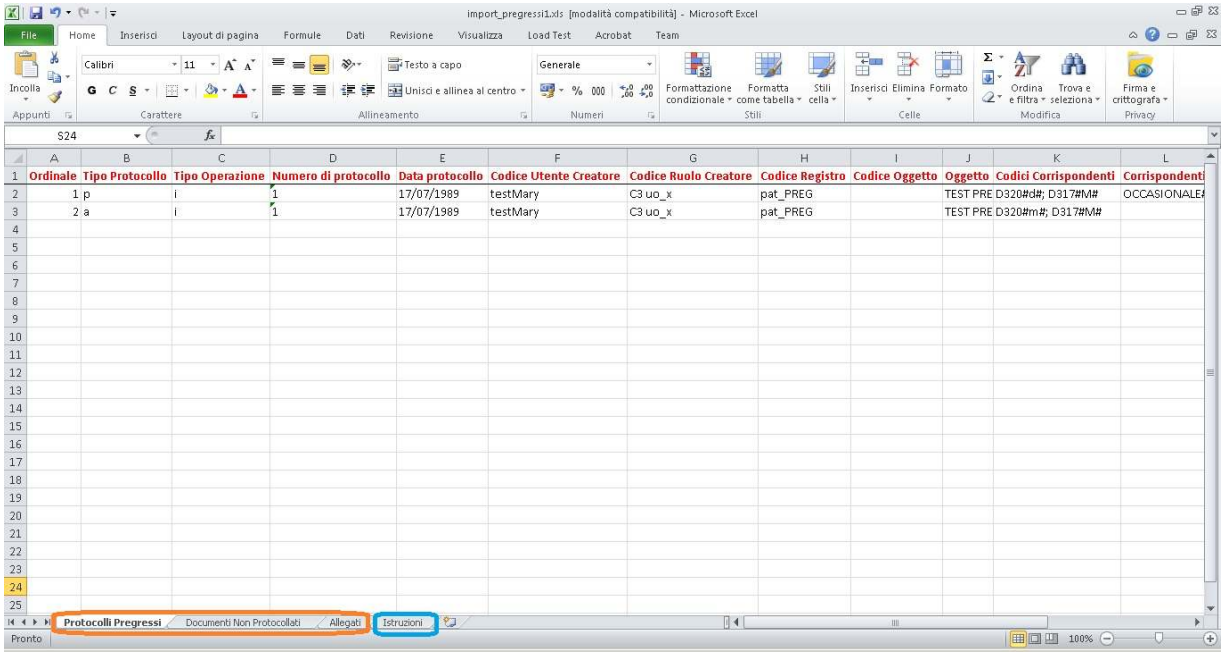


Figura 163 - File excel import documenti pregressi

2.18.2 Stato Import

Il pannello "Stato Import" permette di visualizzare lo stato di avanzamento di ciascun import avviato. Il pulsante "Ricarica lo Stato Import" permette di aggiornare i dati riportati (Figura 164):

- **Descrizione**: descrizione che è stata inserita all'atto dell'import;
- **Data inizio**: giorno ed ora di inizio import;
- **Data fine**: giorno ed ora di fine import;
- **N° documenti**: numero di documenti da importare;
- **Percetuale**: stato di avanzamento dell'import (percentuale);
- **Stato**: riflette lo stato di avanzamento dell'import. La barra inizialmente bianca, si colora via via di rosso fino a diventare verde quando l'import è stato completato;
- **Report (**): a fine import è possibile visualizzare un report dell'import effettuato (par. 2.18.2.1);
- **Elimina (**): a fine import consente la cancellazione dell'import dalla lista;
- : indica il completamento dell'import senza errori;

❖  : indica errori in fase di import. Selezionando l'immagine con il cursore, il sistema indica quanti errori vi sono nell'import.

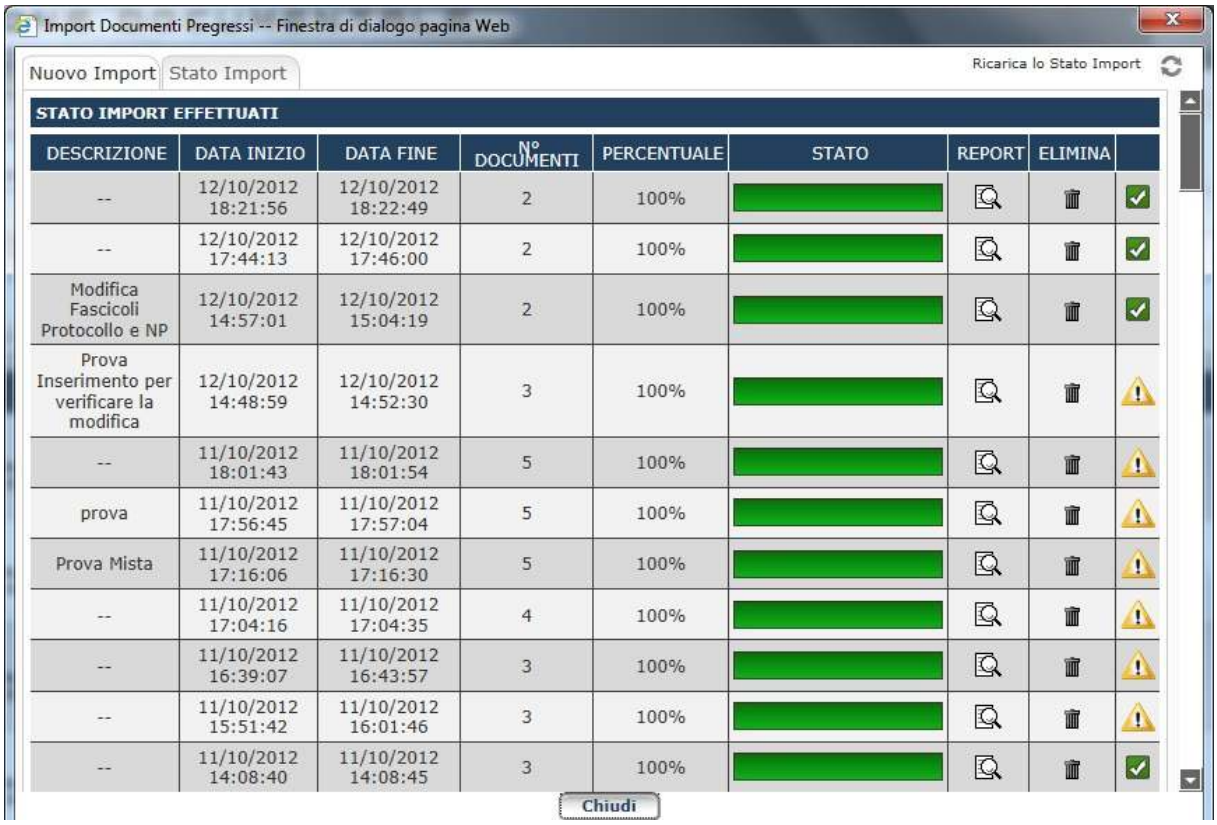


Figura 164 - Stato import documenti pregressi

2.18.2.1 Report Import Pregressi

Al termine dell'operazione di import è possibile visualizzare un report (par. 2.18.2) sull'esito dell'operazione. Il report conteine le seguenti informazioni (Figura 165):

- ✓ Data: data di creazione del documento pregresso importato;
- ✓ Esito: "S" se positivo, "W" se vi sono dei Warning (quindi crea il documento con problemi marginali), "E" se non è riuscito a creare il documento;
- ✓ Errore: descrive l'errore associato al documento con esito "W" o "E";
- ✓ Id documento: id che è stato associato al documento importato;
- ✓ Num proto/id vecchio documento: vecchio "id"/"nro protocollo" del documento importato;
- ✓ Registro: il registro[5] a cui è associato il documento importato;
- ✓ Proprietario: nome e cognome dell'utente che ha creato il documento, ed il ruolo da questi ricoperto;
- ✓ Tipo operazione: "I" per l'inserimento, "C" per la cancellazione, "M" per la modifica;
- ✓ N° allegati: numero di allegati associati al documento importato.

[5] Il registro utilizzato per l'import di documenti pregressi viene appositamente creato in amministrazione e risulta essere sempre nello stato "Chiuso"

La consultazione di questo report è consigliata soprattutto se l'import si conclude con degli errori. Inoltre è possibile esportare il report in excel attraverso la selezione del pulsante Esporta.

Figura 165 - Report relativo all'import di documenti pregressi

3 RICERCA

Tramite il pulsante ricerca è possibile selezionare i seguenti tipi di ricerche:

- dei documenti,
- dei fascicoli,
- delle trasmissioni,
- delle visibilità
- dei documenti e fascicoli in Area di lavoro.

Nelle ricerche tramite campi di testo in generale è possibile cercare:

- per frase esatta: immettendo una stringa nel campo di ricerca
- per parole tronche: tramite l'espansione a destra (es.: "comun%" per trovare comune, comunità, comunicazione, etc…)
- due o più parole in un determinato ordine: occorre inserire tali parole una dopo l'altra, utilizzando l'operatore «%» per espandere la ricerca (es.: "comun%mont%")
- due o più parole indipendentemente dall'ordine in cui compaiono: occorre inserire tali parole una dopo l'altra, utilizzando l'operatore «&&» fra le stesse. Se si inseriscono parole tronche deve essere utilizzato anche l'operatore di % per espandere la ricerca (es.: "comun%&&mont%").

Nota: non è consentita l'espansione a sinistra (es.: "%dimento" non produrrà alcun risultato). Il completamento a destra deve essere esplicitato tramite l'utilizzo del simbolo "%". Se non utilizzato la ricerca avverrà per frase esatta.

Tramite chiave di configurazione è possibile definire un valore soglia per il numero di risultati restituiti dalle ricerche di:

- documenti
- fascicoli
- trasmissioni.

Se il numero dei risultati è minore della soglia, questi vengono visualizzati, altrimenti un messaggio invita l'utente ad utilizzare criteri di ricerca più stringenti e lo informa circa il numero di risultati della ricerca corrente ed il valore impostato per la soglia.

3.1 Ricerca documenti

La funzionalità di ricerca dei documenti è ottenibile a partire dalla barra di navigazione del pannello principale selezionando la voce del menù RICERCA, premendo sul pulsante "RICERCA" e successivamente sul pulsante DOCUMENTI.
E' possibile visualizzare il seguente schema di navigazione relativo alle varie tipologie di ricerca.

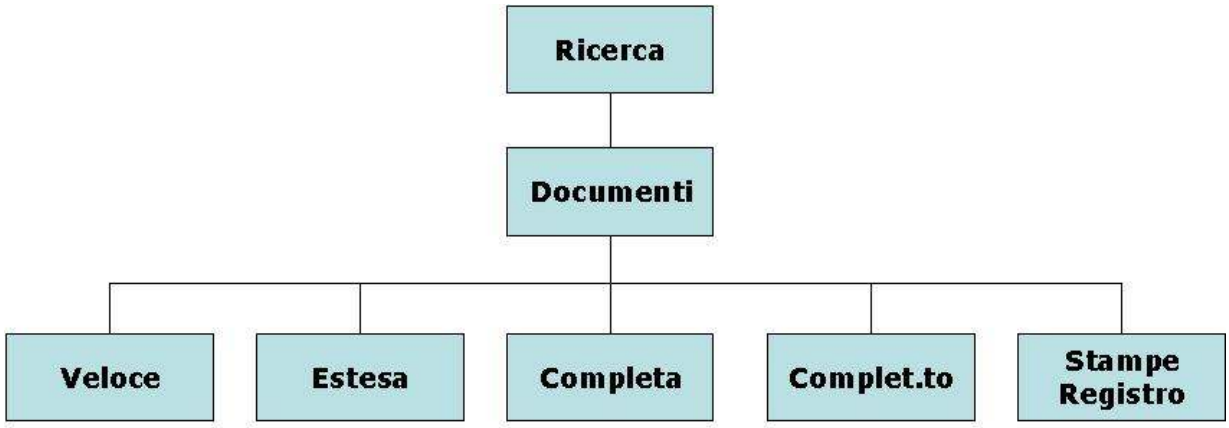


Figura 166 - Ricerca documenti: schema di navigazione

Le varie tipologie di ricerca presentano delle caratteristiche comuni principalmente per quanto riguarda la visualizzazione grafica dei risultati.

3.1.1 Risultati di ricerca

Nello schema di navigazione illustrato, la ricerca è attivata nel momento in cui si seleziona la voce di menù principale "Ricerca". I risultati di ricerca sono mostrati nella parte destra della pagina sotto forma di lista, dalla quale è possibile selezionare il documento desiderato. Nella pagina dei risultati per ciascun documento è possibile:

- visualizzare i dati di profilo del documento selezionando l'icona , che consente l'accesso alla scheda del documento;
- visualizzare il documento elettronico attraverso la selezione dell'icona corrispondente al tipo di file (per esempio). Il sistema, infatti, propone l'icona nel caso in cui il documento in questione (o

eventuali allegati) sia dotato di un file acquisito. Se il campo è vuoto il documento non ha alcun file associato. Il funzionamento del visualizzatore è descritto nel paragrafo 2.14.2.1.

- inserire il documento nell'area di lavoro, selezionando l'icona . L'operazione che prevede invece l'eliminazione dall'area di lavoro di oggetti in essa inseriti, si attiva utilizzando l'icona ;
- inserire il documento in una istanza di conservazione selezionando l'icona . Il primo documento inserito nell'area conservazione crea un'istanza di conservazione. I successivi verranno automaticamente inseriti nell'istanza creata dal primo documento. La funzionalità risulta disponibile solo per i ruoli abilitati alla gestione dell'area di conservazione.

Nella ricerca di documenti repertoriati (si veda paragrafo 2.9) se da amministrazione è stata impostata la visualizzazione della colonna contatore nelle ricerche, il sistema mostra la colonna riportante la segnatura di repertorio, come mostrato nella figura seguente.

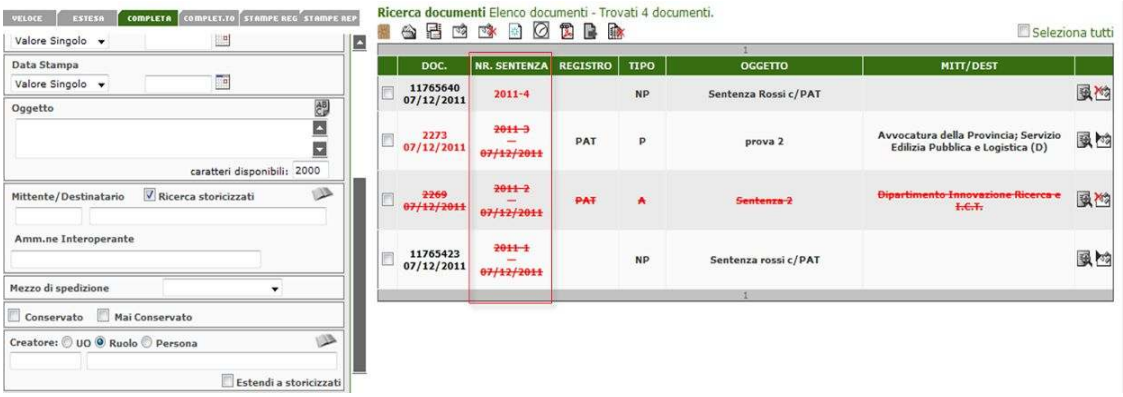


Figura 167 - Evidenza della segnatura di repertorio nella griglia dei risultati della ricerca (ruolo non abilitato all'utilizzo di griglie personalizzate)

3.1.1.1 Azioni massive

In alto, nella pagina dei risultati, sono presenti le icone per eseguire delle azioni sui documenti risultanti dalla ricerca o su una parte di essi (azioni massive).

Figura 168 - Azioni massive

In particolare:

In una sezione posta più in basso si trovano le icone che consentono di effettuare le operazioni sui documenti selezionati. La selezione può avvenire mettendo un segno di spunta accanto alla voce "Seleziona tutto", oppure scegliendo i singoli documenti, utilizzando le caselle di selezione che si trovano accanto ad ognuno di essi nell'elenco dei risultati.

La presenza di questi pulsanti è soggetta a configurazione e solo i ruoli abilitati potranno effettuare queste azioni massive (tutte o quelle per le quali sono stati abilitati).

- "Firma i documenti selezionati" , consente di firmare i documenti selezionati: cliccando su questo pulsante appare una finestra dalla quale è necessario selezionare il certificato da utilizzare per la firma. Dopo aver selezionato il certificato e aver cliccato sul pulsante "Applica firma" il sistema firma l'ultima versione dei documenti scelti e alla fine mostra l'esito dell'operazione.
  L'utente potrà anche scegliere di convertire in pdf i documenti da firmare.

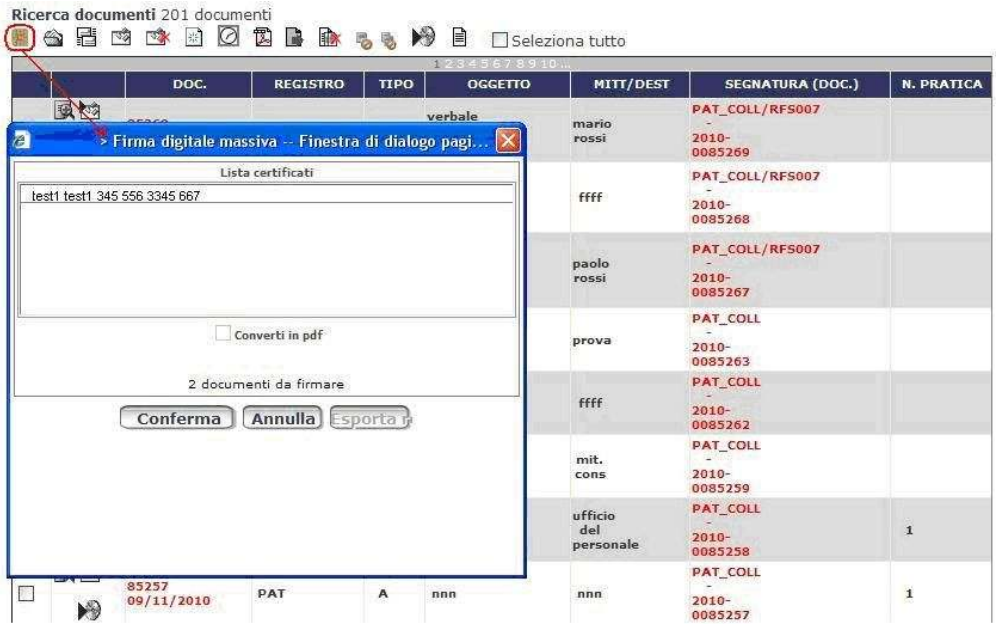


Figura 169 – Firma massiva

- "Fascicola i documenti selezionati" permette di classificare/fascicolare i documenti selezionati nel fascicolo scelto. Cliccando sul pulsante compare una finestra di dialogo per la scelta del fascicolo generale o procedimentale in cui inserire i documenti selezionati. L'operazione viene avviata mediante il pulsante "Fascicola". Alla fine viene mostrato l'esito dell'operazione e l'elenco dei documenti fascicolati. Tale risultato, come tutte le altre operazioni massive può essere esportato in formato pdf.

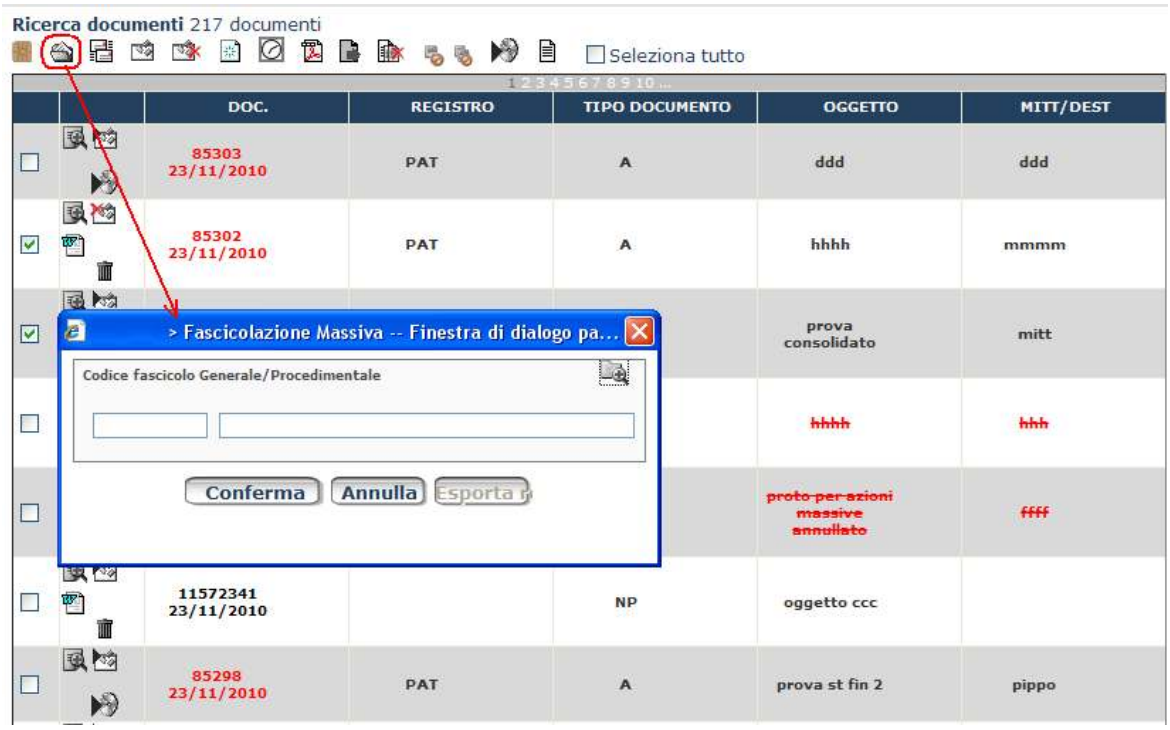


Figura 170 - Fascicolazione massiva

- "Trasmetti i documenti selezionati" consente di effettuare una trasmissione dei documenti selezionati. Dopo aver scelto i documenti da trasmettere e aver cliccato sul pulsante corrispondente all'azione massiva, si apre una finestra per la creazione della trasmissione.
  L'utente potrà utilizzare un modello di trasmissione, oppure costruirsi la trasmissione nel modo classico (selezionando la ragione di trasmissione, i destinatari, le note, …).
  - Trasmissione da modello: l'utente sceglie il modello dal menù a tendina[6] riportato in alto della pagina, aspetta che la richiesta venga elaborata e poi clicca sul pulsante "Trasmetti". Il sistema effettua le trasmissioni e ne riporta l'esito nella sezione sottostante denominata *Report*. Il risultato visualizzato può essere esportato mediante il pulsante "Esporta Report".
  - Trasmissione semplice: la sezione riporta i campi necessari per la costruzione della trasmissione. Per i dettagli sui campi si rimanda al paragrafo 2.13.1 che descrive gli stessi campi anche se in un contesto differente. Cliccando sul pulsante "Trasmetti" il sistema effettua le trasmissioni e ne riporta l'esito nella sezione sottostante. Il risultato visualizzato può essere esportato mediante il pulsante "Esporta Report".

[6] Per maggiori dettagli sui modelli di trasmissione selezionabili si veda il paragrafo 2.13.4

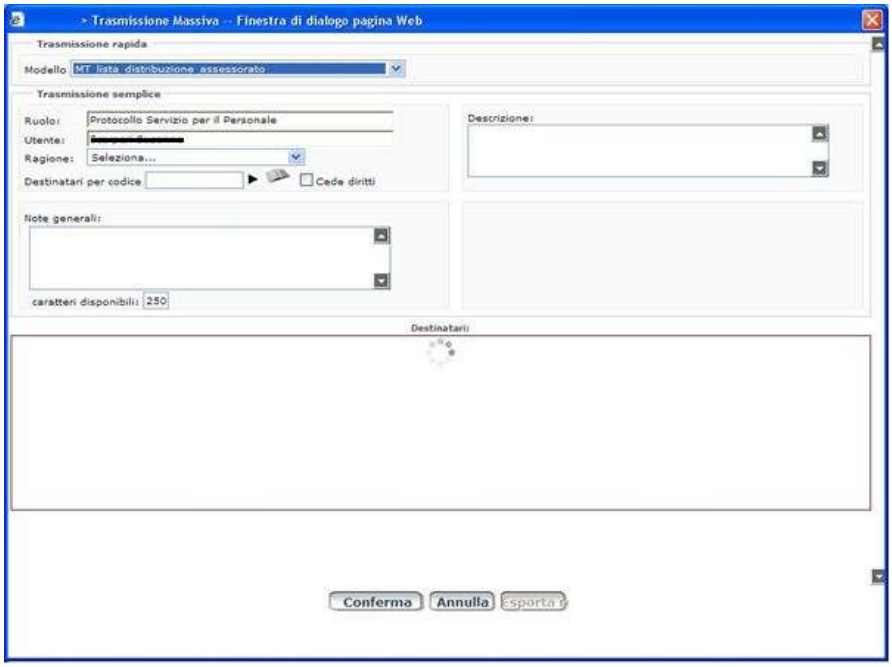


Figura 171 - Trasmissione massiva da modello

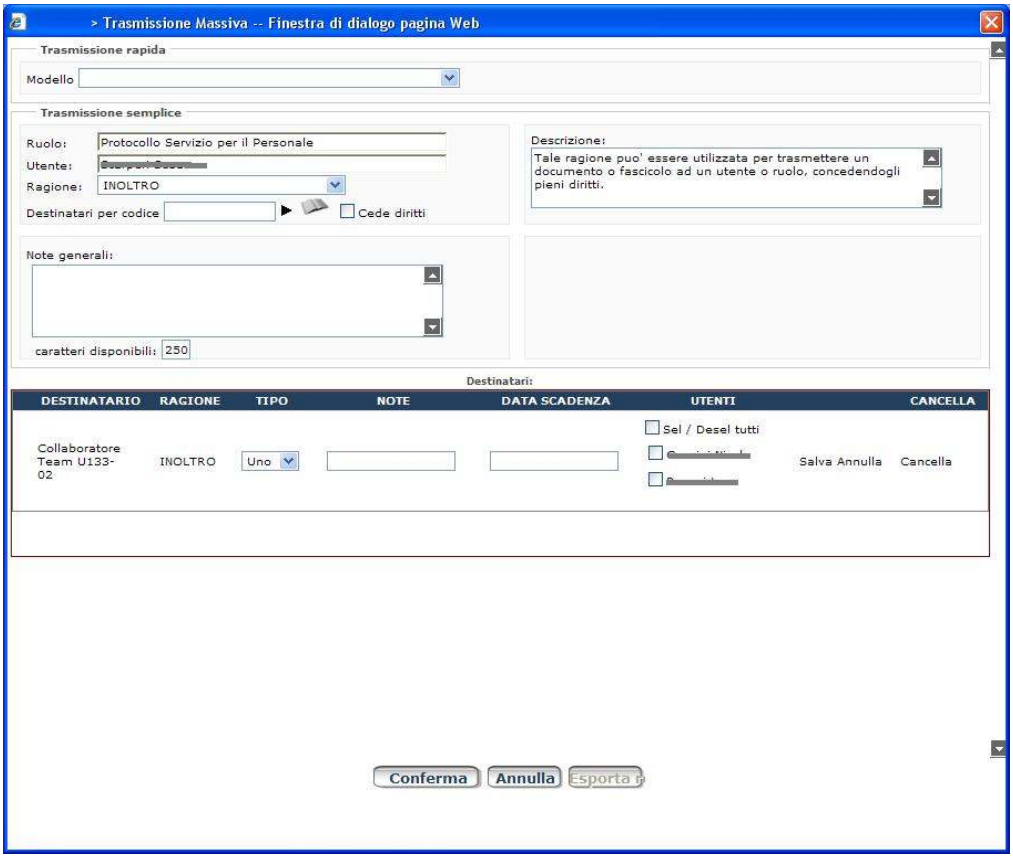


Figura 172 - Trasmissione massiva semplice

- “Esporta i documenti selezionati” che consente di esportare tutti i documenti selezionati.
  Selezionando l’icona viene visualizzata la finestra di dialogo mostrata in Figura 173, dove è possibile associare un titolo al file che si esporta e selezionare il formato del file (PDF/Excel/Calc).
  Nel caso di export in formato PDF vengono salvati campi che compaiono nella griglia standard.
  Nel caso in cui si scelga un file Excel/Calc viene abilitata l’area in cui è possibile selezionare i campi relativi ai documenti da salvare nel file. Se sono state effettuate delle ricerche con griglie personalizzate, i campi presenti nelle griglie personalizzate vengono riportati nell’elenco dei campi da esportare e sono selezionati per default. Se sono state effettuate ricerche con filtro su una tipologia i campi della tipologia selezionata eventualmente non presenti nella griglia dei risultati di ricerca verranno resi disponibili per l’export (di default non selezionati). Per l’export in formato Excel/Calc fra i campi selezionabili compare anche il “Nome originale” dell’eventuale file acquisito.

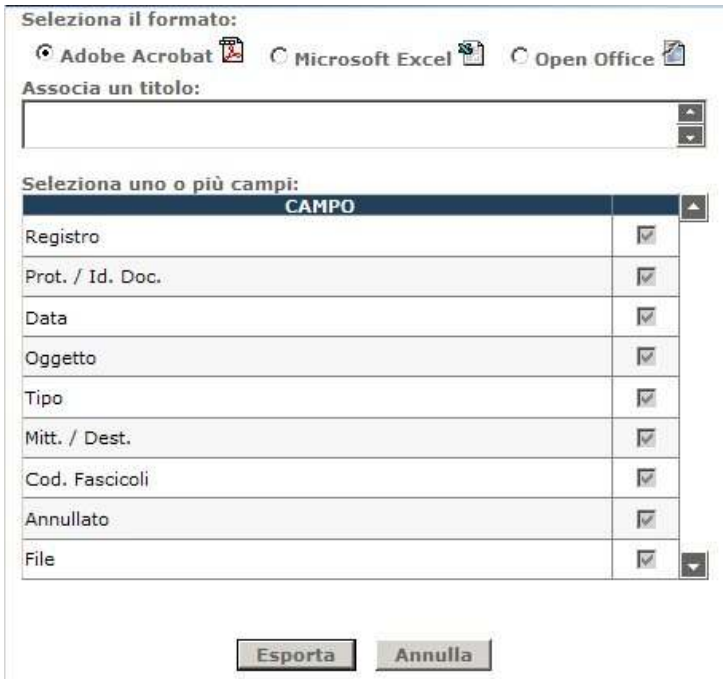


Figura 173 - Esporta risultati della ricerca

- “Salva i documenti selezionati nell‘Area Di Lavoro” , che permette di salvare contemporaneamente tutti i documenti selezionati all’interno dell’area di lavoro;

Figura 174 – Inserisci in ADL massivo

- "Rimuovi i documenti selezionati dall'area di lavoro": consente di rimuovere i documenti selezionati dall'area di lavoro ed è associato al pulsante .

- "Assegna timestamp ai documenti selezionati" permette di assegnare il timestamp all'ultima versione dei documenti selezionati.
  Dopo aver selezionato i documenti e aver cliccato sul pulsante "Applica timestamp", il sistema processa i documenti selezionati e applica il timestamp all'ultima versione di quelli che hanno un'immagine associata. Nel riquadro presente nella pagina viene riportato l'esito dell'operazione per ogni documento processato. Il risultato può essere esportato cliccando sul pulsante "Esporta Report".

- "Converti in pdf i documenti selezionati" converte in pdf l'ultima versione dei documenti selezionati:
  Dopo aver selezionato i documenti e aver cliccato sul pulsante "Converti in PDF", il sistema converte in pdf l'ultima versione di quelli che hanno un'immagine associata. Nel riquadro presente nella pagina viene riportato l'esito dell'operazione per ogni documento processato. Il risultato può essere esportato cliccando sul pulsante "Esporta Report".

- "Inoltra i documenti selezionati" : dopo aver selezionato i documenti ed aver cliccato sul pulsante "Inoltra", si apre una finestra per la conferma dell'operazione. Se viene data conferma, il sistema predispone un protocollo in uscita che ha per allegati i documenti selezionati. In particolare la descrizione dell'allegato corrisponde all'oggetto del documento ed il file associato all'allegato corrisponde all'ultima versione del documento selezionato. All'utente viene poi chiesto di chiudere la finestra e viene portato alla pagina di dettaglio del documento predisposto alla protocollazione.

- “Elimina versioni” : questa operazione può essere effettuata su
  - documenti grigi **non consolidati** (par. 2.7.1.6)
  - documenti predisposti alla protocollazione **non consolidati**
  - allegati a tali documenti

presenti nell’elenco dei risultati e selezionati dall’utente.
Attivando il pulsante “elimina versioni”, il sistema, dopo aver chiesto all’utente conferma dell’operazione e quali versioni si vogliono eliminare (tutte le vecchie versioni oppure tutte tranne la penultima e l’ultima), inizierà ad eliminare le vecchie versioni di tutti e soli i documenti grigi o predisposti alla protocollazione per i quali l’utente **possiede i diritti di rimozione**.

Alla fine dell’operazione verrà mostrato un prospetto riepilogativo delle versioni eliminate e di quelle non rimosse che potrà essere esportato in formato pdf.
Questa funzionalità è attivabile tramite chiave di configurazione.

Figura 175 – Rimuovi versioni

- “Consolida documenti” : questa operazione consente di consolidare versioni ed allegati dei documenti selezionati. Attivando il pulsante “consolida documenti”, il sistema, dopo aver chiesto all’utente conferma dell’operazione consolida i documenti selezionati. Alla fine dell’operazione verrà mostrato un prospetto riepilogativo dei documenti consolidati e di quelli che non è stato possibile consolidare. Tale prospetto potrà essere esportato in formato pdf.

- “Consolida documenti e metadati” : questa operazione consente di consolidare versioni ed allegati (se non lo si è fatto prima) ed i metadati dei documenti selezionati. La modalità è analoga al consolidamento descritto nel punto precedente.
- “Inserisci i documenti selezionati in ‘Area Conservazione’” , permette di inserire contemporaneamente nell’Area Conservazione tutti i documenti selezionati dalla lista. La funzionalità risulta disponibile solo per i ruoli abilitati alla gestione dell’area di conservazione.

- “Personalizza la griglia di ricerca”: questa funzionalità consente di personalizzare le pagine dei risultati delle ricerche e dà la possibilità di visualizzare anche i dati relativi ai campi profilati associati alle tipologie di documenti. Se la funzionalità non viene utilizzata la griglia dei risultati delle ricerche continuerà a mostrare i campi attuali.
  Cliccando sul pulsante si apre una finestra che mostra l’elenco dei campi che potranno essere inseriti nella griglia.
  L’utente può scegliere:
  - ❑ i campi da visualizzare
  - ❑ l’ordine di visualizzazione
  - ❑ la larghezza da dare alle colonne della griglia
  - ❑ il numero massimo di caratteri da visualizzare, nel caso di campi di tipo testo

  Per i dettagli si rimanda al par. 3.1.1.2

Di seguito viene mostrato il risultato di una ricerca eseguito con la tipologia di ricerca estesa.

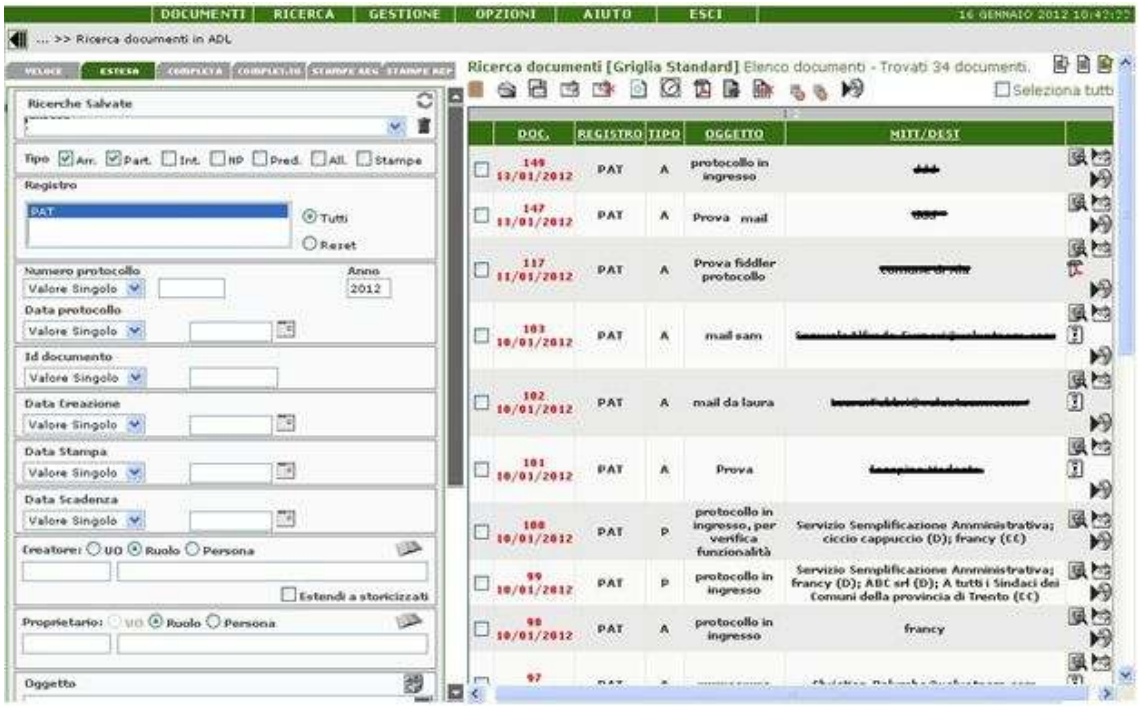


Figura 176 – Risultato della ricerca

Come detto in precedenza, selezionando l’icona è possibile accedere alla scheda di dettaglio del documento. In tale sezione in alto a destra, come evidenziato in verde nella Figura 177, sono presenti degli indicatori direzionali che consentono la navigazione delle schede presenti nel risultato della ricerca senza ritornare alla lista. Grazie ad esse è possibile visualizzare i documenti precedenti/successivi a quello selezionato. Tale funzionalità è presente nella scheda del documento solo se si accede ad essa a partire dal risultato della ricerca.

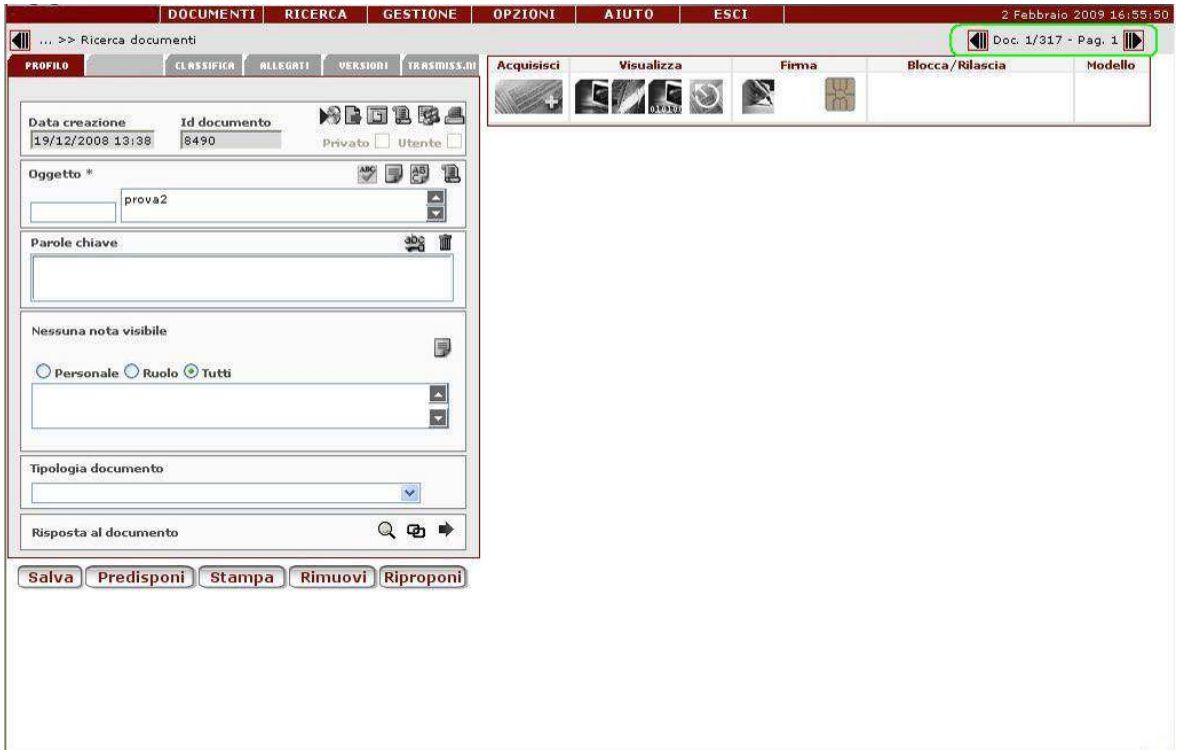


Figura 177 – Scheda di dettaglio del documento: funzioni per la navigazione tra documenti

Una volta visualizzato il dettaglio del documento è possibile ritornare alla pagina dei risultati di ricerca selezionando l'icona , che restituisce la pagina della ricerca documenti con la lista dei documenti della ricerca che si era effettuata (Figura 178).

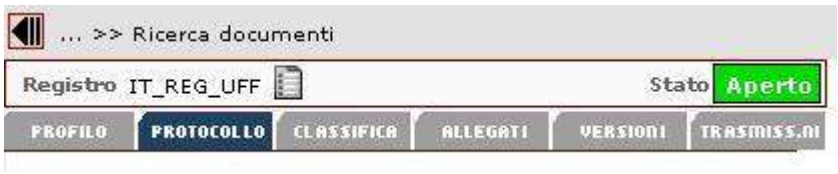


Figura 178 - Tasto per ritornare al risultato della ricerca doc. dalla pagina di dettaglio di un documento

3.1.1.2 Ricerche personalizzate

Per i ruoli opportunamente abilitati tramite tool di amministrazione, è possibile personalizzare il risultato delle ricerche visualizzando le informazioni ritenute opportune.

Nella barra delle azioni massive sono presenti tre pulsanti che permettono la gestione delle griglie di ricerca personalizzate:

- : personalizza la griglia di ricerca
- : salva o modifica griglia
- : mie griglie preferite

La gestione delle griglie personalizzate è illustrata nel dettaglio nei paragrafi successivi.

3.1.1.2.1 Personalizzazione griglie di ricerca

Premendo sul pulsante *personalizza la griglia di ricerca* apparirà una nuova maschera che permetterà di modificare la griglia al momento in uso.

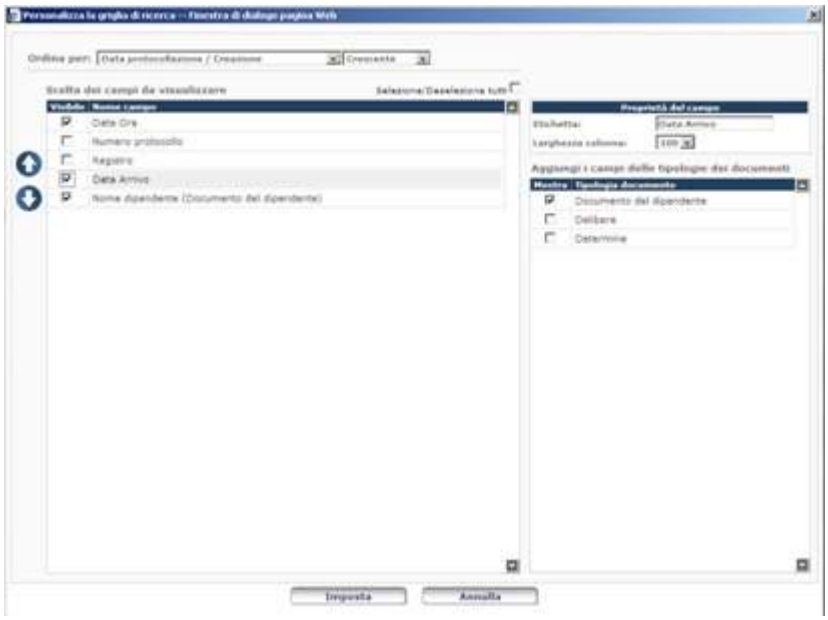


Figura 179 - Maschera di personalizzazione della griglia.

Da questa maschera è possibile:

- aggiungere o rimuovere campi alla griglia agendo sulle apposite caselle di selezione, *checkbox*
- modificare la loro posizione selezionandoli e utilizzando le frecce (verso l'alto e verso il basso)
- modificare l'etichetta di una colonna
- impostare la larghezza di una colonna
- selezionare/deselezionare tutti i campi disponibili per la pubblicazione nella griglia (ossia quelli presenti al momento nella sezione dei campi da visualizzare)
- impostare un ordinamento predefinito in base ad uno dei campi visualizzati nella griglia.

Tra i campi presenti nella maschera, è possibile selezionare il campo "Impronta – Standard" che consente di visualizzare nella griglia di ricerca l'impronta del documento (Figura 180).

Figura 180 – Selezione dell'Impronta del documento

Selezionando o deselezionando una tipologia di documento (parte destra della maschera in Figura 179), i relativi campi saranno disponibili o verranno eliminati dalla griglia.

A seconda della configurazione effettuata dal sito di amministrazione, se viene selezionato il campo' Note', verrà esportato il testo della nota o soltanto l'indicazione Si/No in base alla presenza/assenza di note per il documento.

Selezionando il contatore di una tipologia repertoriata (si veda paragrafo 2.9), fra i risultati di ricerca verrà mostrata la segnatura di repertorio.

Se invece si seleziona il contatore di una tipologia con azzeramento personalizzato, se il contatore contiene il valore dell'anno, verranno indicati l'anno di inizio e di fine del periodo di azzeramento del contatore.

Fra i campi selezionabili compare anche il "Nome originale" dell'eventuale file acquisito.

Tramite il pulsante 'Imposta' vengono apportate le modifiche richieste e viene creata una nuova griglia temporanea, come evidenziato dalla scritta riportata in cima alla griglia di ricerca: [Griglia Temporanea]. Se non si procede al salvataggio (vedi par. 3.1.1.2.2) della griglia, e si esce dalla sezione di ricerca le impostazioni effettuate andranno perse.

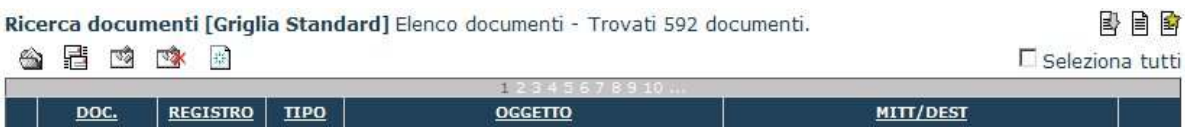


Figura 181 - Evidenza del tipo di griglia in uso nella pagina dei risultati di ricerca

3.1.1.2.2 Salvataggio griglie di ricerca

Tramite il pulsante è possibile salvare o modificare una griglia.

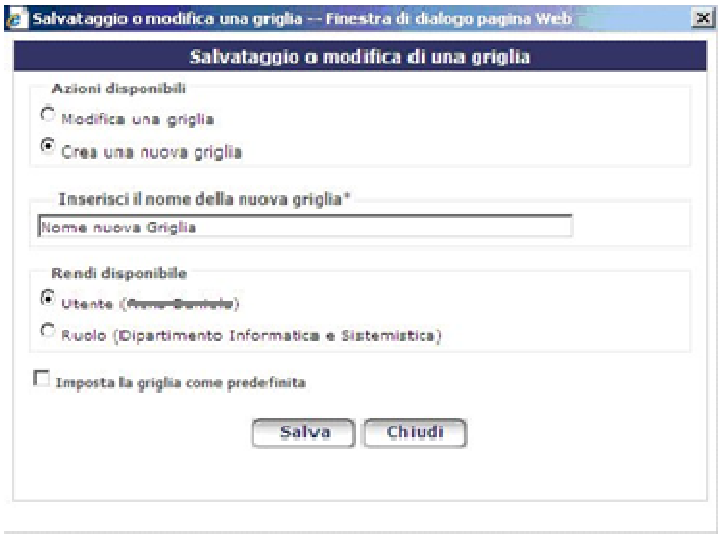


Figura 182 - Salvataggio o modifica di una griglia

Durante il salvataggio viene richiesto di inserire un nome per la griglia e di specificare se tale griglia deve essere visibile al solo utente o a tutto il ruolo cui l'utente appartiene.
È possibile inoltre impostare la griglia come *predefinita*: in tal caso. la griglia sarà utilizzata ad ogni ricerca effettuata.

Al termine del salvataggio il nome della griglia salvata viene riportato in cima alla griglia stessa fra parentesi quadre.

3.1.1.2.3 Mie griglie preferite

Ogni griglia salvata rimane a disposizione del ruolo/utente (a seconda del tipo di salvataggio effettuato) e va ad aggiungersi alla lista delle *mie griglie preferite*.

Figura 183 – Gestione delle griglie preferite e standard

In questa maschera per ogni griglia viene evidenziato:

- se la griglia è predefinita (tramite opportuna opzione)
- se la griglia è visibile al solo utente
- se la griglia è visibile anche al ruolo cui l'utente appartiene

Per ogni griglia riportata è possibile:

- renderla predefinita uilizzando l'opportuno option button
- eliminarla, tramite il pulsante relativa alla griglia in questione.

Nella lista delle mie griglie sarà sempre presente la griglia *standard* (griglia di risultati disponibile di default per gli utenti che non sono abilitati alla gestione di griglie personalizzate). La griglia *standard* non può essere eliminata o modificata in alcun modo. Rimane quindi sempre a disposizione dell'utente, che in ogni momento potrà decidere di riattivarla come *predefinit*a.

3.1.1.2.4 Modifica griglie di ricerca

Per modificare una griglia esistente, l'utente deve selezionarla dalla maschera delle griglie preferite (se non è già attiva). Quindi, tramite il pulsante dovrà aprire la maschera per la personalizzazione ed effettuare le modifiche. Al momento del salvataggio (tramite il pulsante) è possibile modificare la visibilità scegliendo tra quella al ruolo o al solo utente. Come griglia da salvare viene proposta la griglia modificata ma l'utente può comunque selezionare un altro valore, così facendo, le modifiche vengono salvate su di un'altra griglia, sovrascrivendola.

In caso di modifica o cancellazione di un griglia visibile a tutto il ruolo, il sistema all'atto delle salvataggio delle modifica o dell'avvio della cancellazione mostra un alert per ricordare all'utente che tale operazione provocherà la modifica / cancellazione della griglia attualmente in uso da parte di tutti gli utenti del ruolo. In caso di cancellazione di una griglia visibile a tutto il ruolo, l'eventuale utente che l'avesse selezionata come predefintia, avrà come griglia predefinitia quella standard.

3.1.2 Tipologie di Ricerca

L'utente di VTDOCS ha la possibilità di effettuare la ricerca sui documenti secondo differenti strutture di ricerca. Le tipologie utilizzabili sono:

- Veloce;

- Estesa;
- Completa;
- Completamento;
- Stampe Registro.

Nei paragrafi che seguono sono descritte ciascuna nel dettaglio.

Per le ricerche Estesa, Completa, Completamento oltre alla ricerca sono possibili le seguenti operazioni:

- salvataggio di una ricerca: tramite il pulsante Salva riportato a fondo pagina. L'operazione viene descritta con maggiore dettaglio nel paragrafo 3.1.2.2.2
- modifica di una ricerca salvata: tramite il pulsante Modifica riportato a fondo pagina. L'operazione viene descritta con maggiore dettaglio nel paragrafo 3.1.2.2.4
- azzerare i filtri di ricerca impostati: tramite il pulsante posto in cima alla pagina, vengono ripuliti i campi utilizzati per la ricerca.

3.1.2.1 Veloce

Tale ricerca si può effettuare sia attraverso le ricerche salvate (descritte al paragrafo 3.1.2.2.1), selezionando una modalità di ricerca dal menù a tendina, sia attraverso il criterio di ricerca oggetto, o parte di esso, contenuto nel documento.
La ricerca per oggetto, permette di limitare il numero dei risultati della ricerca specificando una delle opzioni presenti nel menù pre-impostato (ad esempio gli ultimi 10 protocolli, gli ultimi 20, ecc).

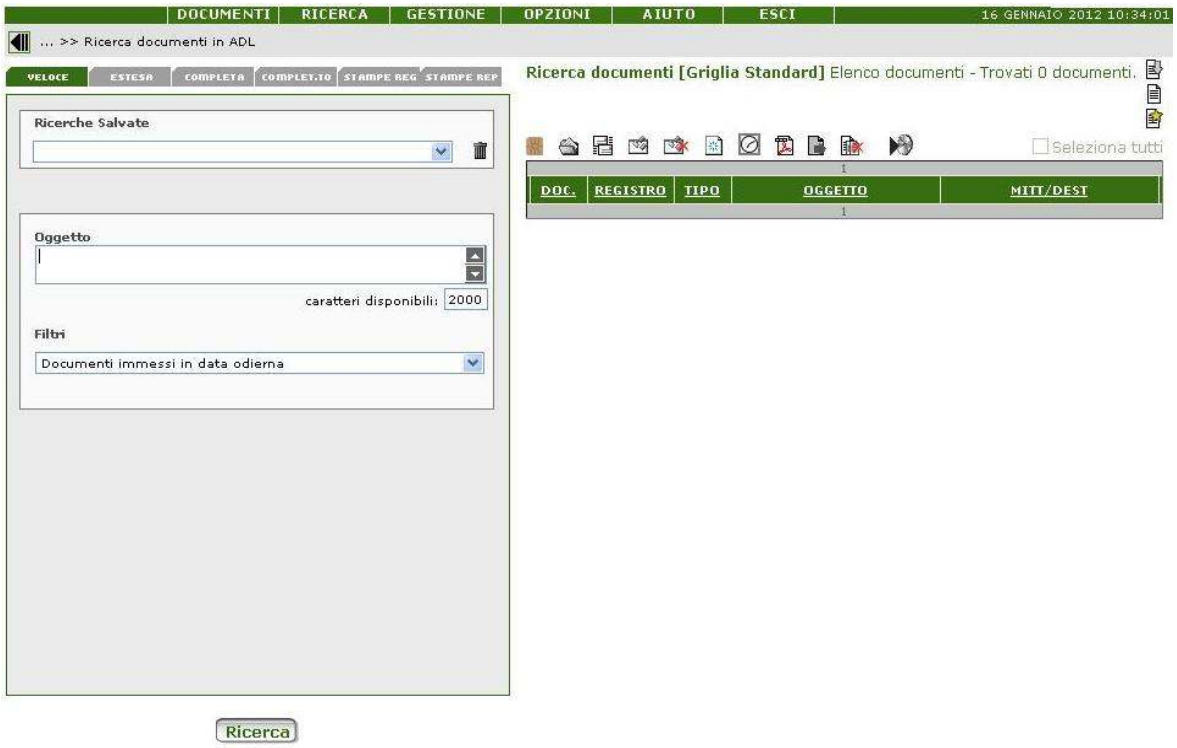


Figura 184 - Ricerca veloce di un documento

3.1.2.2 Estesa

Anche questa modalità di ricerca consente di utilizzare una modalità di ricerca salvata attraverso la selezione di una ricerca salvata dal menù a tendina (descritte al paragrafo 3.1.2.2.1).
E' inoltre possibile eseguire una ricerca in "AND" di documenti su più campi ossia attraverso una ricerca di tutti i documenti che rispondono ai criteri selezionati. I campi proposti per questo tipo di ricerca sono:

- **Tipo**[7]: utilizzato per indicare se si vuole effettuare la ricerca tra i documenti in arrivo, in partenza, non protocollati, predisposti, allegati. Con "Arr" si indicano i documenti in arrivo,con "Part" i documenti in partenza, con "Int" i documenti interni, con "NP" i documenti non protocollati, con "Pred." i documenti predisposti alla protocollazione, con "All." i documenti allegati , con "Stampe". La ricerca può essere effettuata per singolo tipo o per più tipi documento.
  La selezione di "All" consente di gestire le diverse tipologie di allegati disponibili per l'utente.Il sistema in automatico seleziona gli Allegati inseriti dall'utente, ma, mediante opportune selezioni è possibile ricercare anche:
  - gli allegati relativi alle ricevute PEC
  - tutti gli allegati del documento
  - gli allegati relativi alle ricevute PI VTDOCS, se l'amministrazione è abilitata all'utilizzo dell'interoperabilità semplificata

  gli allegati generati da sistemi esterni, se l'amministrazione è stata opportunamente abilitata
- **Registro**: selezionare il registro all'interno del quale si vuole effettuare la ricerca;
- **Numero protocollo**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo del numero di protocollo;
- **Anno protocollo**: consente di cercare i documenti per anno di protocollazione;
- **Data protocollo**: è possibile effettuare la selezione da un menù a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di protocollo. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Data Scadenza**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è scaduto il documento. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Id documento**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo dell'identificativo del documento;
- **Data creazione**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è stato creato il documento. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Creatore**: è possibile specificare se UO/Ruolo/Persona; in base a quanto selezionato, si deve inserire il codice con cui effettuare la ricerca. Se non si conosce il codice, è possibile cercarlo ed inserirlo tramite rubrica, attivabile utilizzando l'icona  (per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5). Tramite selezione del flag opportuno, è inoltre possibile estendere

[7] I nomi dei tipi documento è configurabile mediante il tool di amministrazione pertanto i documenti in Arrivo possono anche essere indicati con Ingresso o Entrata, i documenti in Uscita anche con Partenza.

la ricerca anche ai ruoli storicizzati. In tal caso verranno cercati sia i documenti creati dal ruolo indicato, che quelli creati da ruoli da cui il ruolo corrente è stato ottenuto per modifica con storicizzazione;

- **Proprietario**: di cui è possibile specificare se Ruolo/Persona; in base a quanto selezionato, si deve inserire il codice con cui effettuare la ricerca. Se non si conosce il codice, c'è la possibilità di cercarlo ed inserirlo tramite rubrica, che viene attivata utilizzando l'icona  . Per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5;
- **Oggetto**: l'oggetto può essere digitato dall'utente o ricercato nell'oggettario selezionando l'icona  ;
- **Mittente/destinatario**: l'inserimento del filtro di ricerca su mittente/destinatario può essere effettuato secondo le modalità già esposte nei paragrafi relativi all'inserimento di un nuovo documento, ovvero, inserimento del codice associato al mittente/destinatario, selezione dalla rubrica di un mittente/destinatario registrato, digitazione del nominativo nel caso di mittente/destinatario occasionale (per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5). Inoltre è possibile selezionare l'opzione ricerca storicizzati per effettuare ricerche su elementi in rubrica che hanno subito modifiche sia mediante la descrizione che mediante il codice (intero o parziale) dei corrispondenti stessi. Nel caso in cui la parte di codice inserito sia comune a più corrispondenti, il sistema mostra l'elenco di tali corrispondenti, fornendo l'informazione dell'eventuale storicizzazione dei corrispondenti.
- **Data Stampa**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è scaduto il documento. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Codice Fascicolo Generale / Procedimentale**: si inserisce nel campo a sinistra il codice del fascicolo, generale o procedimentale, in cui è stato inserito il documento, contestualmente alla ricerca. Oppure, è possibile selezionare l'icona  con cui si ricerca e si seleziona il fascicolo procedimentale/generale, in cui è stato inserito il documento.
- **Ordinamento**: è utilizzato per indicare il tipo di ordinamento. La prima finestra di selezione mostra i campi sui quali effettuare l'ordinamento (data protocollazione/creazione, oggetto, tipo, …). La seconda finestra di selezione serve per indicare il tipo di ordinamento (decrescente, crescente). Per gli utenti abilitati all'uso di griglie personalizzate è possibile ordinare i risultati di ricerca anche:
  - dalla maschera di personalizzazione della griglia in cui vengono presentati i risultati di ricerca
  - agendo direttamente sull'intestazione delle singole colonne (ove tale intestazione venga visualizzata con il arattere sottolineato). Premendo successivamente l'intestazione della colonna si passa dall'ordinamento crescente a quello decrescente e viceversa.

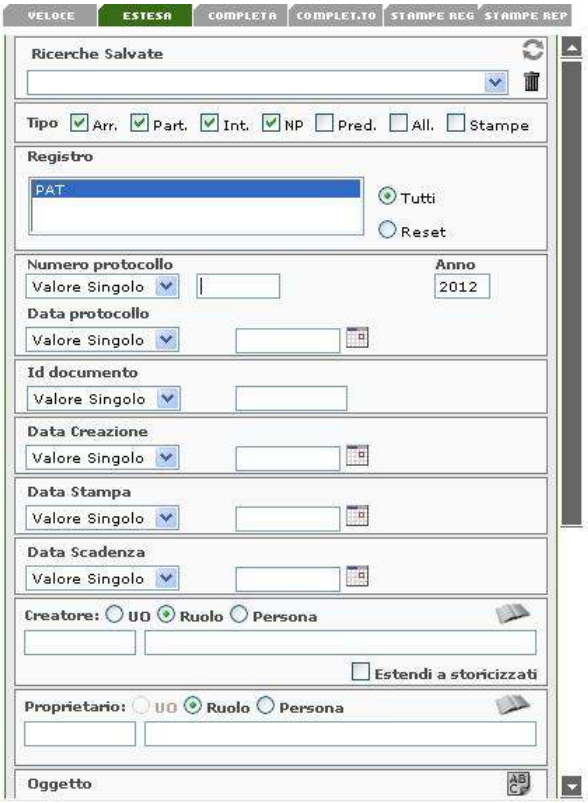


Figura 185 - Ricerca estesa di un documento (prima parte)

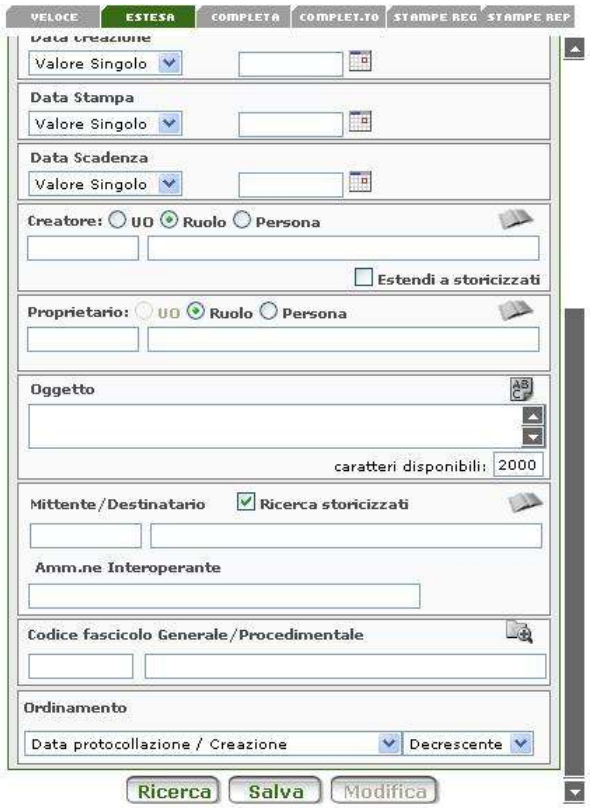


Figura 186 - Ricerca estesa di un documento (seconda parte)

3.1.2.2.1 Ricerche salvate

Le Ricerche Salvate servono per velocizzare le ricerche ripetitive di documenti. L' utente ha la possibilità di salvare, assegnando un nome, un insieme di valori che caratterizzano un filtro di ricerca per i documenti. Il salvataggio comprende tutti i campi visualizzati nella pagina di ricerca. I criteri di ricerca salvati hanno validità soltanto per la tipologia di ricerca documenti nella quale sono stati salvati ma sono tutti disponibili nella scheda "ricerca veloce".

3.1.2.2.2 Creazione nuovo criterio di ricerca

Per creare un nuovo criterio di ricerca, bisogna posizionarsi nella opportuna pagina di ricerca documenti ("estesa", "completa", "completamento"), valorizzare i campi di ricerca disponibili, e selezionare il pulsante  presente in fondo alla pagina.

La selezione del pulsante comporta l'apertura di una pagina, così come mostrato di seguito, per l'inserimento di alcuni dati obbligatori:

- **Titolo**: per inserire la descrizione del criterio di ricerca;
- **Rendi disponibile**: per assegnare il criterio di ricerca, solo all'utente creatore (proposto in automatico dal sistema) oppure all'intero ruolo di appartenenza dell'utente (ruolo attualmente in uso). In questo secondo caso anche gli eventuali altri utenti appartenenti al medesimo ruolo possono utilizzare il criterio salvato dall'utente.

Dopo aver scelto i dati con cui si desidera salvare il criterio di ricerca si seleziona il pulsante  .

L'applicativo visualizza una finestra di dialogo che comunica che "i criteri di ricerca sono stati salvati con

successo". Nel caso in cui non si voglia più salvare il criterio in esame è sufficiente selezionare il pulsante Chiudi e il sistema non salverà nessun criterio di ricerca.

Figura 187 - Creazione ricerche salvate

3.1.2.2.3 Associazione di una griglia di visualizzazione dei risultati ad un criterio di ricerca

Se l'utente è abilitato all'utilizzo di griglie personalizzate, durante il del salvataggio di un criterio di ricerca, è possibile selezionare una delle griglie personalizzate per collegarla alla ricerca.

Figura 188 - Salvataggio ricerca

Se l'utente non desidera associare una griglia personalizzata basterà selezionare quella standard nel menù a tendina "Associa la ricerca ad una mia griglia".

3.1.2.2.4 Modifica ricerca salvata

Nella pagina di ricerca, quando si seleziona una ricerca precedentemente salvata, viene abilitato il pulsante Modifica che consente di modificare tale ricerca. L'utente può modificare:

- la visibilità (ruolo/utente) della ricerca
- il nome
- le eventuali modifiche apportate ai filtri di ricerca
- la griglia associata.

Se l'utente è abilitato alla personalizzazione dei risultati di ricerca, potrà modificare anche la griglia associata alla ricerca.

Figura 189 - Modifica ricerca salvata per utente abilitato alla gestione di griglie personalizzate

3.1.2.2.5 Cancellazione criterio di ricerca

A partire da una delle pagine di ricerca documenti ("estesa", "completa", "completamento"), utilizzando il menu a tendina l'utente seleziona in sequenza il criterio di ricerca che desidera eliminare, e seleziona poi l'icona immediatamente alla destra. Ogni utente può rimuovere sia i criteri che hanno validità per l'utente stesso, sia quelli che hanno validità per l'intero ruolo (in questo caso, il sistema avvisa l'utente). Viene in ogni caso richiesta all'utente la conferma dell'operazione di cancellazione.

3.1.2.2.6 Utilizzo dei criteri di ricerca

Per utilizzare i criteri di ricerca salvati in precedenza, bisogna posizionarsi nella opportuna pagina di ricerca documenti e selezionare, dal menù a tendina, il criterio di ricerca che si intende utilizzare. Il sistema valorizzerà i corrispondenti campi. La pressione del consueto tasto di ricerca, avvierà la ricerca sulla base del criterio selezionato.
Se un criterio di ricerca risulterà non più valido (ad esempio perché riferito a tipologie documentali o campi non in uso), il sistema ne darà notifica all'utente, richiedendo la cancellazione del criterio. Un criterio non valido non sarà comunque utilizzabile.

3.1.2.3 Completa

Effettua una ricerca in AND di documenti su tutti i campi caratteristici del documento. Devono essere valorizzati i campi per i quali si vuole effettuare la ricerca nella base dati. I campi utilizzabili per questo tipo di ricerca sono i seguenti:

- **Tipo**[8]: utilizzato per indicare se si vuole effettuare la ricerca tra i documenti in arrivo, in partenza, non protocollati, predisposti, allegati. Con "Arr" si indicano i documenti in arrivo,con "Part" i documenti in partenza, con "Int" i documenti interni, con "NP" i documenti non protocollati, con "Pred." i documenti predisposti alla protocollazione, con "All." i documenti allegati , con "Stampe". La ricerca può essere effettuata per singolo tipo o per più tipi documento.
  La selezione di "All" consente di gestire le diverse tipologie di allegati disponibili per l'utente.Il sistema in automatico seleziona gli Allegati inseriti dall'utente, ma, mediante opportune selezioni è possibile ricercare anche:
  - gli allegati relativi alle ricevute PEC
  - tutti gli allegati del documento

[8] Il nome dei tipi documento è configurabile mediante il tool di amministrazione pertanto i documenti in Arrivo possono anche essere indicati con Ingresso o Entrata, i documenti in Uscita anche con Partenza.

- gli allegati relativi alle ricevute PI VTDOCS, se l'amministrazione è abilitata all'utilizzo dell'interoperabilità semplificata

gli allegati generati da sistemi esterni, se l'amministrazione è stata opportunamente abilitata

- **Registro:** per selezionare il registro all'interno del quale si vuole effettuare la ricerca;
- **Numero protocollo**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo del numero di protocollo;
- **Anno protocollo**: consente di cercare i documenti per anno di protocollazione;
- **Data protocollo**: è possibile effettuare la selezione da un menù a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di protocollo. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Data Scadenza**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è scaduto il documento. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Id documento**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo dell'identificativo del documento;
- **Data creazione**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è stato creato il documento. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Data Stampa**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è scaduto il documento. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Mezzo di spedizione**: lista a tendina per la selezione del mezzo di spedizione dei documenti su cui si vuole filtrare la ricerca;
- **Conservato**: se selezionato ricerca i soli documenti sottoposti a conservazione sostitutiva;
- **Mai conservato**: se selezionato ricerca i documenti che non hanno subito il processo di conservazione;
- **Creatore**: è possibile specificare se UO/Ruolo/Persona; in base a quanto selezionato, si deve inserire il codice con cui effettuare la ricerca. Se non si conosce il codice, è possibile cercarlo ed inserirlo tramite rubrica, attivabile utilizzando l'icona  (per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5). Tramite selezione del flag opportuno, è inoltre possibile estendere la ricerca anche ai ruoli storicizzati. In tal caso verranno cercati sia i documenti creati dal ruolo indicato, che quelli creati da ruoli da cui il ruolo corrente è stato ottenuto per modifica con storicizzazione;
- **Proprietario**: di cui è possibile specificare se Ruolo/Persona; in base a quanto selezionato, si deve inserire il codice con cui effettuare la ricerca. Eventualmente, se non si conosce il codice, c'è la possibilità di cercarlo ed inserirlo tramite rubrica, attivata attraverso la selezione dell'icona  ; Per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5;
- **Stato del documento**: indica lo stato del documento, ovvero se esso è stato annullato o meno, è anche possibile ricercare tra tutti quelli disponibili;
- **Segnatura**: é la stringa assegnata dal sistema al documento protocollato, in base a regole pre-impostate e costruite attraverso l'applicazione di amministrazione.

- **Tipologia Documento**: indica la tipologia del documento che si vuol ricercare selezionando la voce da un menù pre-impostato. Se la tipologia scelta è profilata, si attiva l'icona , che propone il pannello della profilazione dinamica del documento. E' necessario che l'utente amministratore in fase di costruzione della tipologia abbia specificato che l'informazione possa essere utilizzata per le ricerche.
  Per le ricerche sono disponibili anche le tipologie al momento sospese tramite interfaccia di amministrazione. Nelle griglie di risultato delle ricerche oltre al numero di protocollo o al id documento è possibile visualizzare anche il campo contatore della tipologia documento ad esso associata.
  Nel pannello dell'Anteprima della Profilazione Dinamica sono presenti tre pulsanti:
  - "Resetta": che reimposta i dati inseriti;
  - "Conferma": salva i dati che successivamente saranno utilizzati nella ricerca;
  - "Chiudi": chiude il pannello.

  Se la tipologia comprenda campi di tipo corrispondente, gli eventuali corrispondenti storicizzati verranno restituiti dalla ricerca in rubbrica e saranno opportunamente evidenziati con carattere barrato. Per i campi di tipo corrispondente è comunque possibile la selezione da codice. Nel caso in cui la parte di codice inserito sia comune a più corrispondenti censiti in rubriche diverse, il sistema mostra l'elenco di tali corrispondenti, da cui l'utente potrà selezionare quello di interesse in base alla rubrica di appartenenza.
  La lista a tendina che mostra i tipi documento configurati e disponibili presenta, inoltre, un valore denominato "Campi comuni" selezionando il quale si ha la possibilità di ricercare tutti i documenti di qualsiasi tipo in cui è stato profilato anche il campo comune sul quale si sta effettuando la ricerca.
  Selezionando questa voce si attiva l'icona ,che propone il pannello della profilazione dinamica che riporta i campi comuni configurati con il tool di amministrazione e utilizzabili nelle ricerche, come spiegato nella sezione relativa alla *Tipologia Documento* nel paragrafo 2.7.1.
- **Stato**: la visualizzazione di tale campo nella pagina di ricerca e i valori disponibili nel corrispondente menù a tendina dipendono dalla scelta che viene effettuata sul campo "tipologia documento". Se viene selezionata una tipologia alla quale è associato un "diagramma di stato", il sistema mostra un menù a tendina contenente tutti gli stati possibili per la tipologia selezionata ovvero gli stati che non sono stati dichiarati 'non ricercabili' da interfaccia di amministrazione e per cui esista almeno un documento in tale stato;
- **Oggetto**: l'oggetto può essere digitato dall'utente o ricercato nell'oggettario selezionando l'icona ;
- **Mittente/destinatario**: l'inserimento del filtro di ricerca sul campo mittente/destinatario può essere effettuato secondo le modalità già esposte nei paragrafi relativi all'inserimento di un nuovo documento, ovvero, inserimento del codice associato al mittente/destinatario o mediante la selezione dalla rubrica di un mittente/destinatario registrato, oppure digitando il nominativo nel caso di mittente/destinatario occasionale. Per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5. Inoltre è possibile selezionare l'opzione ricerca storicizzati per effettuare ricerche su elementi in rubrica che hanno subito modifiche sia mediante la descrizione che mediante il codice (intero o parziale) dei corrispondenti stessi. Nel caso in cui la parte di codice inserito sia comune a più corrispondenti, il sistema mostra l'elenco di tali corrispondenti, fornendo l'informazione dell'eventuale storicizzazione dei corrispondenti;
- **Mittente intermedio**: indicare il nominativo del mittente intermedio per un documento in ingresso, è possibile farlo anche mediante l'icona della rubrica;
- **Codice Fascicolo Generale / Procedimentale**: si inserisce nel campo a sinistra il codice del fascicolo, generale o procedimentale, in cui è stato inserito il documento, contestualmente alla

ricerca. Oppure, è possibile selezionare l'icona  con cui si ricerca e si seleziona il fascicolo procedimentale/generale, in cui è stato inserito il documento.

- **Protocollo mittente**: il numero di protocollo che è stato assegnato dall'amministrazione che ha inviato il documento;
- **Data protocollo mittente**: si inserisce la data in cui tale documento è stato protocollato dall'amministrazione. E' possibile effettuare la selezione da un menù a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di protocollazione mittente. Inoltre, la data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Data arrivo**: è possibile effettuare la selezione da un menù a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di arrivo del documento. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Parole chiave**: consente di indicare le parole chiave da ricercare nei documenti selezionandole dall'archivio delle parole chiave tramite l'icona  ;
- **Note**: permette di cercare nel campo note associato al documento; è possibile ricercare i documenti in base al tipo di nota *a:*
  - ✓ *Tutti*: visibile a tutti gli utenti che hanno la visibilità sul documento*;*
  - ✓ *Ruolo:* visibile solamente agli utenti del ruolo dell'utente creatore della nota*;*
  - ✓ *Rf* (se gli RF sono configurati nel sistema): visibile ai soli ruoli appartenenti all'RF*;*
  - ✓ *Personale:* visibile solamente all'utente che l'ha creata*;*
  - ✓ *Qualsiasi:* comprende tutte le tipologie di note precedentemente descritte.
- **Documenti in completamento**: Tale funzionalità può essere vista come una ricerca rapida di documenti che mancano di alcune delle informazioni caratterizzanti. I campi utilizzabili per questo tipo di ricerca sono i seguenti:
  - *Senza immagine*: se selezionato la ricerca è effettuata tra i documenti per i quali non è stato acquisito il formato digitale del documento;
  - *Con immagine*: se selezionato la ricerca è effettuata tra i documenti per i quali è stato acquisito il formato digitale del documento;
  - *Senza fascicolazione*: se selezionato la ricerca è effettuata tra i documenti non inseriti in un fascicolo;
  - *Con fascicolazione*: se selezionato la ricerca è effettuata tra i documenti inseriti in un fascicolo;
- **Trasmesso**: se selezionato la ricerca è effettuata tra i documenti per i quali è stata effettuata una trasmissione; è possibile anche specificare la ricerca su una particolare ragione di trasmissione selezionandola dall'apposita lista a tendina;
- **Trasmesse senza**: se selezionato la ricerca è effettuata tra i documenti che non sono stati mai trasmessi oppure, se si specifica la ricerca su una particolare ragione di trasmissione selezionandola dall'apposita lista a tendina, si possono ricercare tutti i documenti che non sono stati trasmessi con la ragione selezionata;
- **Segnatura di emergenza**: consente di cercare un documento in base al numero di registrazione assegnato in emergenza;
- **Data segn. di emergenza**: consente di cercare un documento in base alla data di registrazione assegnata in emergenza. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Evidenza**: permette di cercare tra i soli documenti posti in evidenza, nell'insieme complementare o fra tutti i documenti.

- **Tipo file acquisito**: consente di ricercare il documento indicando l'estensione del file che è stato acquisito(.bmp, .doc, .docx, .gif, ec…). Inoltre possiamo fornire in fase di ricerca dettagli relativi alla presenza della firma sul file acquisito oppure no.
- **Versioni** : consente di ricercare il documento in base al "Numero di versioni del documento" che può essere maggiore, minore o esattamente eguale al numero inserito dall'utente;
- **Allegati**: consente di ricercare il documento in base al "Numero di allegati al documento" che può essere maggiore, minore o esattamente eguale al numero inserito dall'utente. Per default il sistema cerca tutti i tipi di allegati, l'utente può, se necessario, scegliere gli allegati di tipo "Utente", "PEC" o "Sist. Esterno" (se l'amministrazione è stata opportunamente abilitata);
- **Ordinamento**: è utilizzato per indicare il tipo di ordinamento. La prima finestra di selezione mostra i campi sui quali effettuare l'ordinamento (data protocollazione/creazione, id documento, oggetto, tipo documento, data annullamento, autore, numero protocollo). La seconda finestra di selezione serve per indicare il tipo di ordinamento (decrescente, crescente). Per gli utenti abilitati all'uso di griglie personalizzate è possibile ordinare i risultati di ricerca anche:
  - dalla maschera di personalizzazione della griglia in cui vengono presentati i risultati di ricerca
  - agendo direttamente sull'intestazione delle singole colonne (ove tale intestazione venga visualizzata con il arattere sottolineato). Premendo successivamente l'intestazione della colonna si passa dall'ordinamento crescente a quello decrescente e viceversa.

Alternativamente, la ricerca è effettuabile in maniera rapida attraverso la selezione del menù a tendina delle ricerche salvate (descritte al paragrafo 3.1.2.2.1).

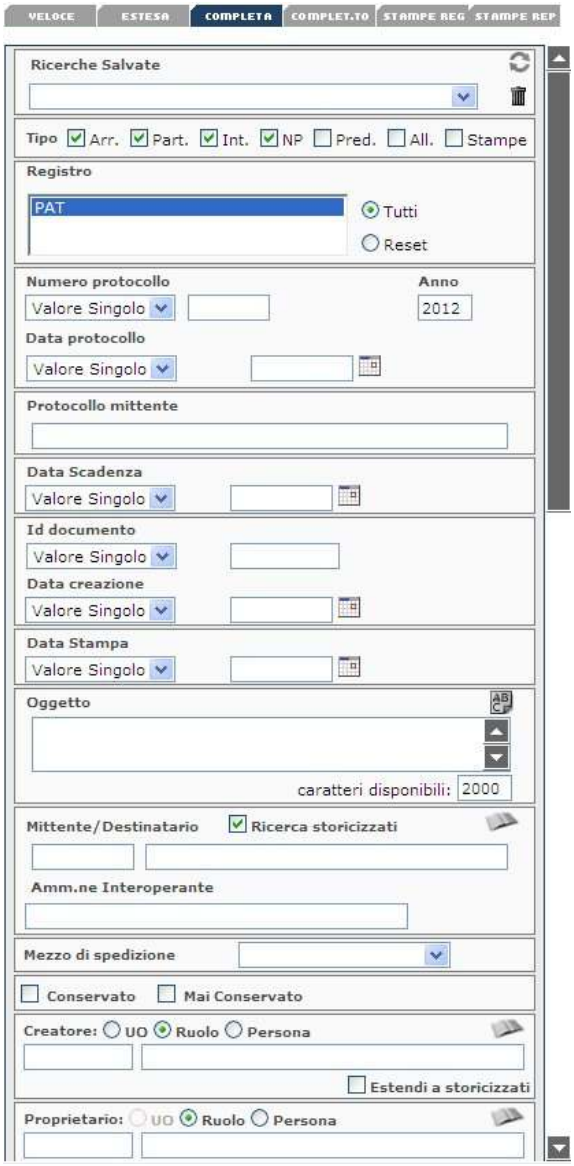


Figura 190 - Ricerca completa (prima parte)

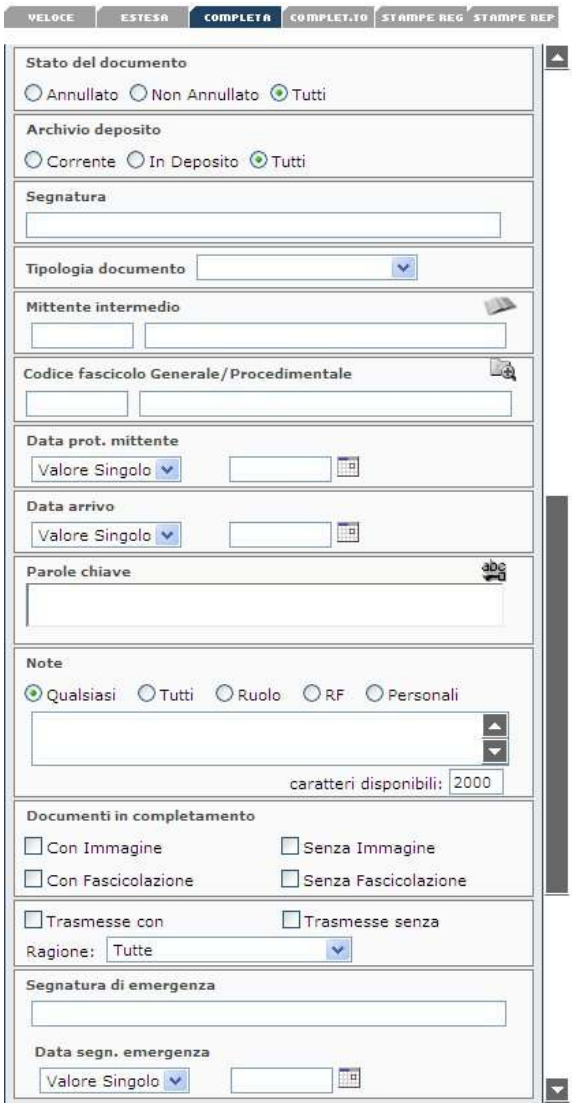


Figura 191 - Ricerca completa (seconda parte)

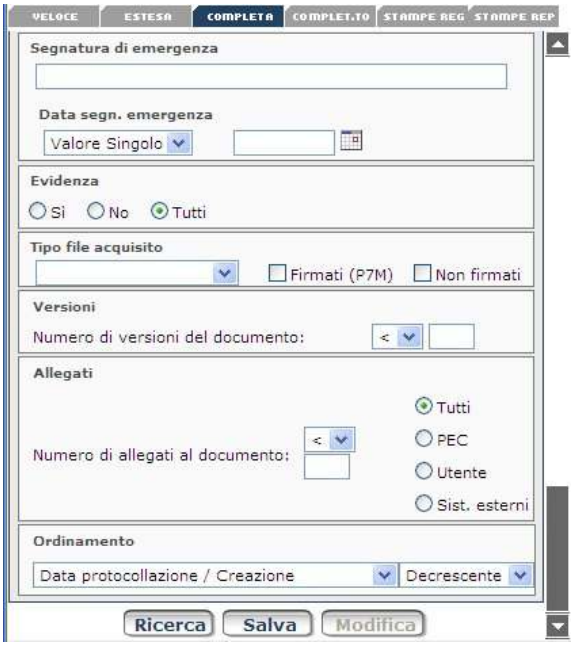


Figura 192 - Ricerca completa (terza parte)

3.1.2.4 Completamento

Tale funzionalità può essere vista come una ricerca rapida di documenti che mancano di alcune delle informazioni caratterizzanti. I campi utilizzabili per questo tipo di ricerca sono i seguenti:

- **Tipo**[9]: utilizzato per indicare se si vuole effettuare la ricerca tra i documenti in arrivo, in partenza, non protocollati, predisposti, allegati. Con "Arr" si indicano i documenti in arrivo,con "Part" i documenti in partenza, con "Int" i documenti interni, con "NP" i documenti non protocollati, con "Pred." i documenti predisposti alla protocollazione, con "All." i documenti allegati". La ricerca può essere effettuata per singolo tipo o per più tipi documento.
  La selezione di "All" consente di gestire le diverse tipologie di allegati disponibili per l'utente.Il sistema in automatico seleziona gli Allegati inseriti dall'utente, ma, mediante opportune selezioni è possibile ricercare anche:
  - gli allegati relativi alle ricevute PEC
  - tutti gli allegati del documento
  - gli allegati relativi alle ricevute PI VTDOCS, se l'amministrazione è abilitata all'utilizzo dell'interoperabilità semplificata

  gli allegati generati da sistemi esterni, se l'amministrazione è stata opportunamente abilitata
- **Senza immagine**: se selezionato la ricerca è effettuata tra i documenti per i quali non è stato acquisito il formato digitale del documento;
- **Con immagine**: se selezionato la ricerca è effettuata tra i documenti per i quali è stato acquisito il formato digitale del documento;
- **Senza fascicolazione**: se selezionato la ricerca è effettuata tra i documenti non inseriti in un fascicolo;
- **Con fascicolazione**: se selezionato la ricerca è effettuata tra i documenti inseriti in un fascicolo;

9 I nomi dei tipi documento è configurabile mediante il tool di amministrazione pertanto i documenti in Arrivo possono anche essere indicati con Ingresso o Entrata, i documenti in Uscita anche con Partenza.

- **Senza timestamp**: se selezionato la ricerca è effettuata tra i documenti ai quali non è stato applicato alcun timestamp;
- **Con timestamp**: se selezionato la ricerca è effettuata tra i documenti ai quali è stato applicato almeno un timestamp;
- **Trasmesse con**: se selezionato la ricerca è effettuata tra i documenti per i quali è stata effettuata una trasmissione; è possibile anche specificare la ricerca su una particolare ragione di trasmissione selezionandola dall'apposita lista a tendina;
- **Trasmesse senza**: se selezionato, la ricerca è effettuata tra i documenti che non sono stati mai trasmessi oppure, se si specifica la ricerca su una particolare ragione di trasmissione, selezionandola dall'apposita lista a tendina, si possono ricercare tutti i documenti che non sono stati trasmessi con la ragione selezionata;
- **Registro**: si seleziona il registro all'interno del quale si vuole effettuare la ricerca, è possibile selezionare tutti i fascicoli spuntando l'icona "tutti";
- **Oggetto**: l'oggetto può essere digitato dall'utente o ricercato nell' oggettario selezionando l'icona  ;
- **Mittente/destinatario**: l'inserimento del filtro sul campo mittente/destinatario può essere effettuato secondo le modalità già esposte nei paragrafi relativi all'inserimento di un nuovo documento, ovvero, inserimento del codice associato al mittente/destinatario, selezione dalla rubrica di un mittente/destinatario registrato, digitazione del nominativo nel caso di mittente/destinatario occasionale Inoltre è possibile selezionare l'opzione ricerca storicizzati per effettuare ricerche su elementi in rubrica che hanno subito modifiche. Per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5;
- **Data protocollo**: per questo campo è possibile effettuare la selezione da un menù a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di protocollo. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Id documento**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo dell'identificativo del documento;
- **Data creazione**: per questo campo può essere selezionata la ricerca per valore singolo o per intervallo di valori, in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è stato creato il documento. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola;
- **Creatore**: è possibile specificare se UO/Ruolo/Persona; in base a quanto selezionato, si deve inserire il codice con cui effettuare la ricerca. Se non si conosce il codice, è possibile cercarlo ed inserirlo tramite rubrica, attivabile utilizzando l'icona  (per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5). Tramite selezione del flag opportuno, è inoltre possibile estendere la ricerca anche ai ruoli storicizzati. In tal caso verranno cercati sia i documenti creati dal ruolo indicato, che quelli creati da ruoli da cui il ruolo corrente è stato ottenuto per modifica con storicizzazione;
- **Proprietario**: di cui è possibile specificare se Ruolo/Persona, in base a quanto selezionato, si deve inserire il codice con cui effettuare la ricerca. Se non si conosce il codice, c'è la possibilità di cercarlo ed inserirlo tramite rubrica, attivata tramite la selezione dell'icona  . Per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5;
- **Protocollo mittente**: il numero di protocollo che è stato assegnato dall'amministrazione che ha inviato il documento;

- **Data protocollo mittente**: si inserisce la data in cui tale documento è stato protocollato dall'amministrazione. E' possibile effettuare la selezione da un menù a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di protocollazione del mittente. La data può essere inserita attraverso la selezione da calendario  o semplicemente editandola.
- **Tipo file acquisito**: consente di ricercare il documento indicando l'estensione del file che è stato acquisito(.bmp, .doc, .docx, .gif, ec…). Inoltre possiamo fornire in fase di ricerca dettagli relativi alla presenza della firma sul file acquisito oppure no.
- **Documenti spediti**: consente di ricercare i documenti in base alle informazioni relative alla spedizione del documento per interoperabilità (PEC o PI) ad altre amministrazioni/enti. E' possibile filtrare la ricerca per documenti con ricevuta, in attesa di risposta (anche a fronte di ricevuta di eccezione), tutti i documenti spediti; altresì è possibile eseguire una ricerca per intervallo di date di spedizione.
- **Ricevute PEC**: questa sezione è presente solo se è stata attivata la funzionalità che gestisce le ricevute PEC e consente di ricercare i documenti spediti ai quali è associata una notifica PEC. In particolare i possibili valori tra cui scegliere sono:
  - avvenuta accettazione
  - avvenuta consegna
  - mancata accettazione
  - mancata consegna
  - con errori

  E' anche possibile eseguire la ricerca per data o intervallo di date di ricezione della notifica.
- **Ricevute PI**: questa sezione è presente solo se l'amministrazione è abilitata all'utilizzo dell'interoperabilità semplificata e consente di ricercare i documenti spediti ai quali è associata una notifica automatica inviata dal sistema a fronte di una spedizione. In particolare i possibili valori tra cui scegliere sono:
  - avvenuta consegna
  - mancata consegna

  E' anche possibile eseguire la ricerca per data o intervallo di date di ricezione della notifica.
- **Stato consolidamento:** questa sezione è presente solo se è stata attivata la funzionalità che gestisce il consolidamento dei documenti. In particolare è possibile ricercare:
  - documenti non consolidati
  - documenti consolidati
  - documenti con metadati consolidati

  E' inoltre possibile ricercare per data di consolidamento inserendo
  - un singolo valore
  - un intervallo di date
  - oggi
  - la settimana corrente
  - il mese corrente

  E' infine possibile ricercare per utente e ruolo che hanno effettuato il consolidamento.
- **Ordinamento**: è utilizzato per indicare il tipo di ordinamento. La prima finestra di selezione mostra i campi sui quali effettuare l'ordinamento (data protocollazione/creazione, id documento, oggetto, tipo documento, data annullamento, autore, numero protocollo). La seconda finestra di selezione serve per indicare il tipo di ordinamento (decrescente, crescente). Per gli utenti abilitati all'uso di griglie personalizzate è possibile ordinare i risultati di ricerca anche:
  - dalla maschera di personalizzazione della griglia in cui vengono presentati i risultati di ricerca

- agendo direttamente sull'intestazione delle singole colonne (ove tale intestazione venga visualizzata con il arattere sottolineato). Premendo successivamente l'intestazione della colonna si passa dall'ordinamento crescente a quello decrescente e viceversa.

Alternativamente, la ricerca è effettuabile in maniera rapida attraverso la selezione del menù a tendina delle ricerche salvate (descritte al paragrafo 3.1.2.2.1).

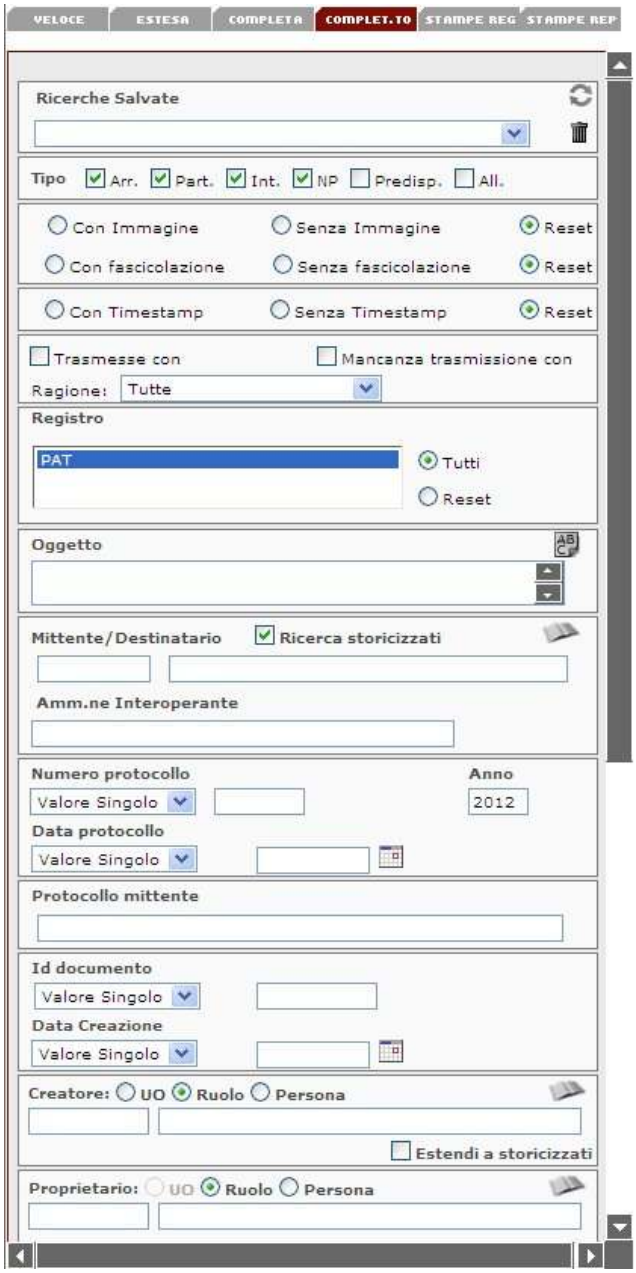


Figura 193 - Ricerca completamento (prima parte)

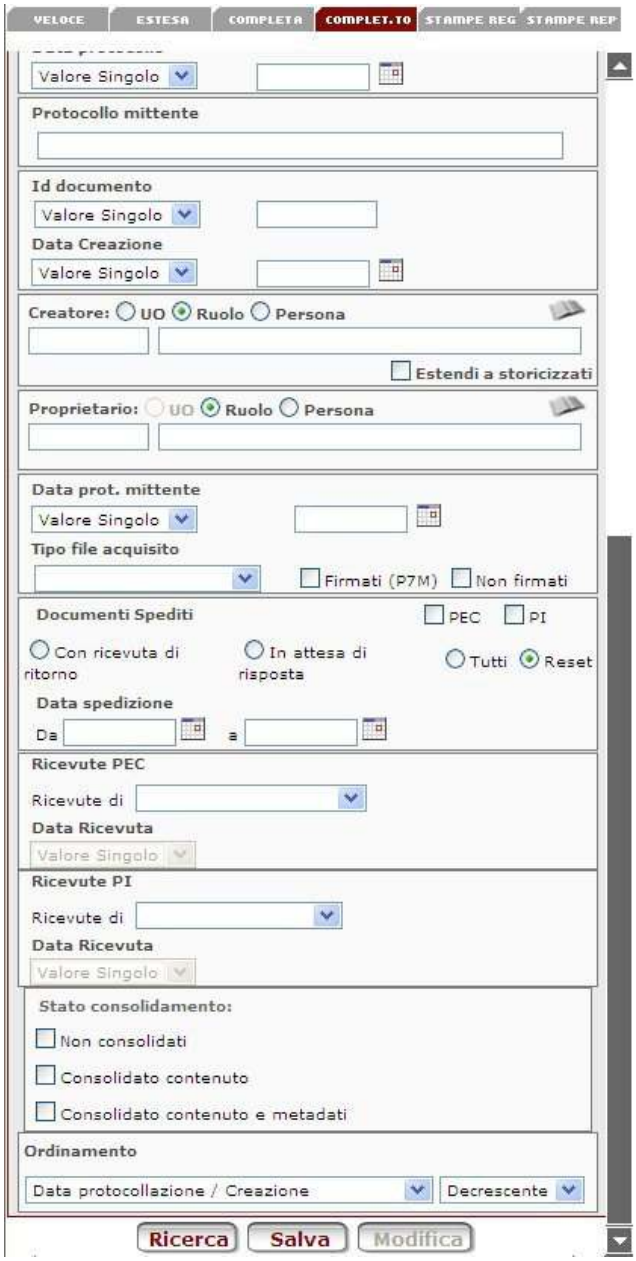


Figura 194 - Ricerca completamento (seconda parte)

3.1.2.5 Stampe Registri

Tale funzionalità consente di ricercare tutte le stampe dei registri (vedi paragrafo 4.3) effettuate in precedenza. Tale ricerca è attivabile attraverso la selezione del registro di cui si vuole visualizzare la stampa effettuata. Per velocizzare la ricerca è possibile applicare un ulteriore filtro rispetto ai seguenti criteri di ricerca:

- Numero protocollo o intervallo di numeri di protocollo;
- Anno di protocollo;
- Data stampa: è possibile effettuare la selezione da un menù a tendina che visualizza “valore singolo” ed “intervallo”. Può essere quindi effettuata la selezione per valore singolo o per intervallo

di valori. In questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di protocollo. La data può essere inserita attraverso la selezione da calendario o semplicemente editandola.

Per ogni documento presente nella pagina dei risultati sono mostrate le seguenti informazioni: l'identificativo del documento, la data di creazione, l'oggetto (da cui si desume l'insieme dei numeri di protocolli contenuti nella stampa) e l'icona dei dettagli che permette di visualizzare il contenuto del documento prodotto con la stampa del registro.

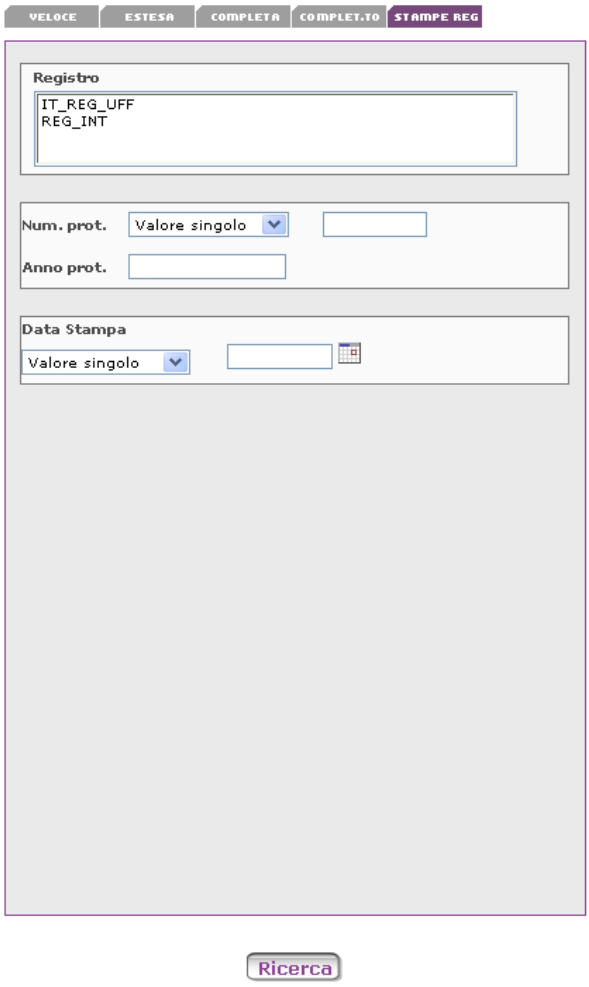


Figura 195 - Stampe registri

3.1.2.6 Stampe Repertori

Se è stata abilitata la gestione dei documenti repertoriati, nella sezione *Stampa rep* è possibile ricercare tutte le stampe (automatiche e manuali) dei registri di repertorio.
I ruoli che hanno visibilità sulle stampe dei registri di repertorio possono ricercarle selezionando in sequenza il menù *Ricerca*, la voce *Documenti* e la sezione *Stampe rep.*

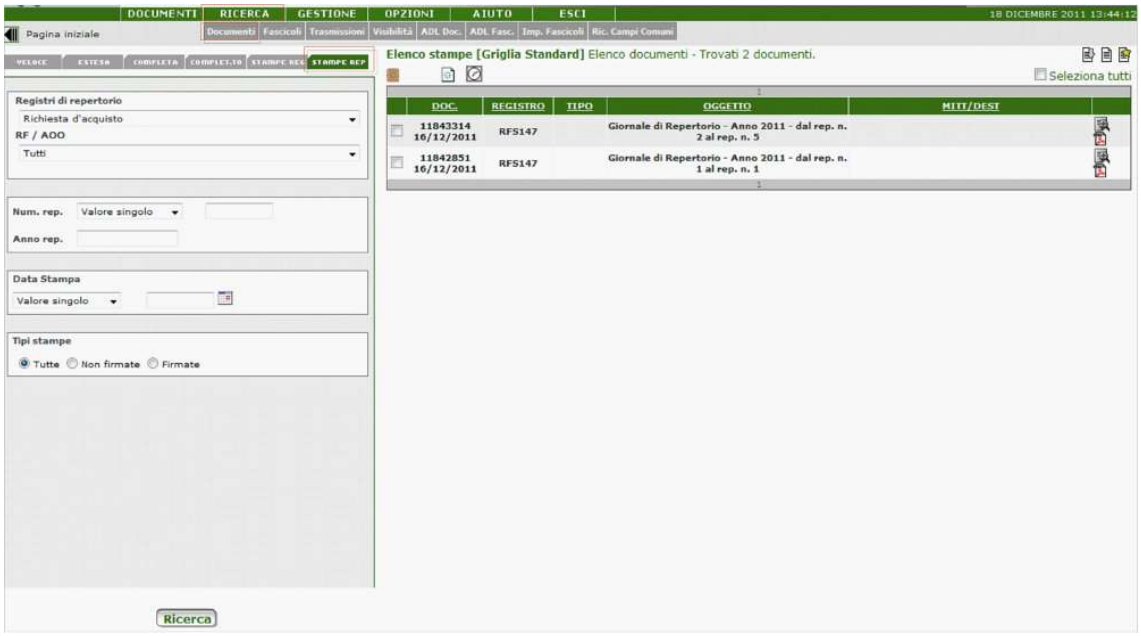


Figura 196 - *Ricerca delle stampe del registro di repertorio*

Si seleziona il registro di repertorio che si intende ricercare. Se il contatore di repertorio conta sull'RF o sull'AOO è possibile raffinare la ricerca grazie al menù a tendina "RF / AOO.

Figura 197 - Filtri Registri di repertorio e RF/AOO

Come mostrato nella figura seguente, gli altri filtri della ricerca permettono di:

- indicare il numero di repertorio (valore singolo o intervallo di valori);
- digitare l'anno di repertorio;
- indicare la data della stampa del registro (valore singolo o intervallo di valori);
- selezionare la tipologia delle stampe da ricercare (Tutte, Non firmate, Firmate).

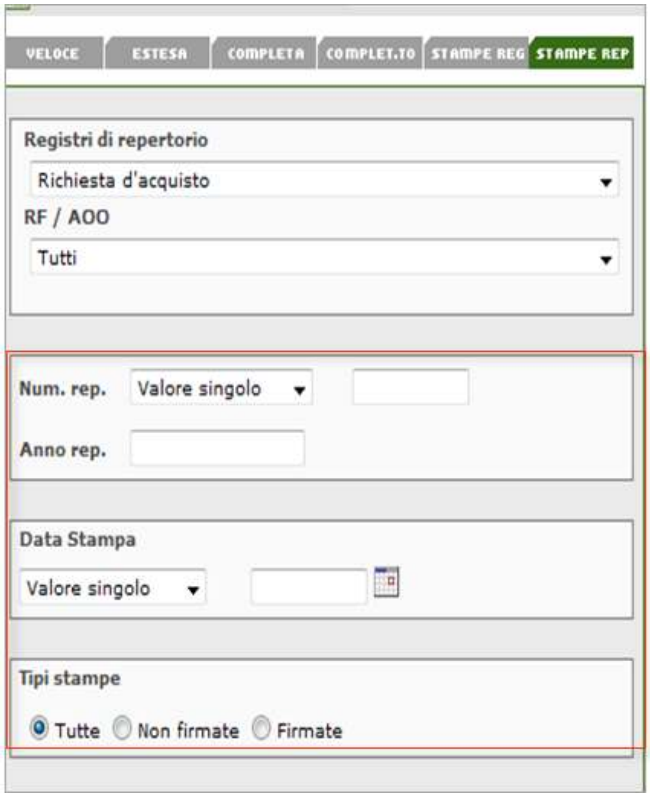


Figura 198 - *Filtri Numero di repertorio, Anno di repertorio, Data Stampa, Tipi stampe*

Dopo aver impostato i filtri di ricerca premere il pulsante 'Ricerca' ottenendo così l'elenco delle stampe che rispondono ai filtri impostati.

Cliccando sull'icona di dettaglio  (*Figura* 196) si visualizza il documento di stampa del registro di repertorio: si tratta di un documento grigio che ha come immagine principale un file pdf contenente l'elenco dei nuovi documenti repertoriati su quel particolare registro e dei documenti repertoriati che hanno subito modifiche al campo oggetto o ai campi storicizzati o che sono stati annullati, dall'ultima stampa fino al momento in cui viene effettuata la stampa (*Figura* 199). Sono attive le sole maschere Profilo e Versioni.

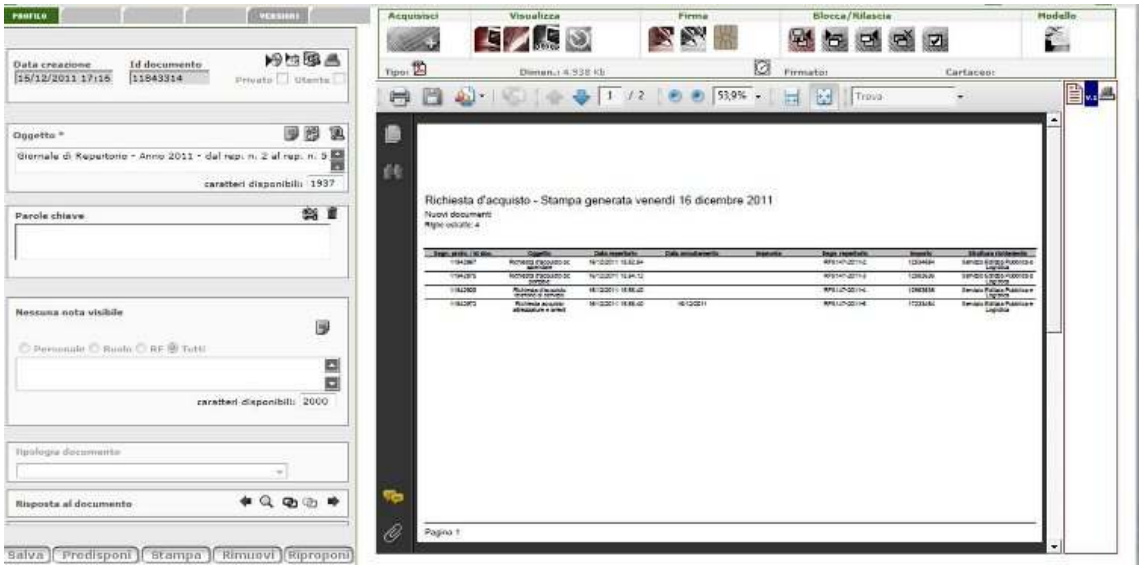


Figura 199 - *Dettaglio del documento di stampa di repertorio*

La prima sezione della stampa del registro di repertorio riporta:

- la denominazione del registro di repertorio;
- la data in cui viene effettuata la stampa del registro;
- l'elenco dei nuovi documenti repertoriati su quel particolare registro con i campi standard ed i campi storicizzati.

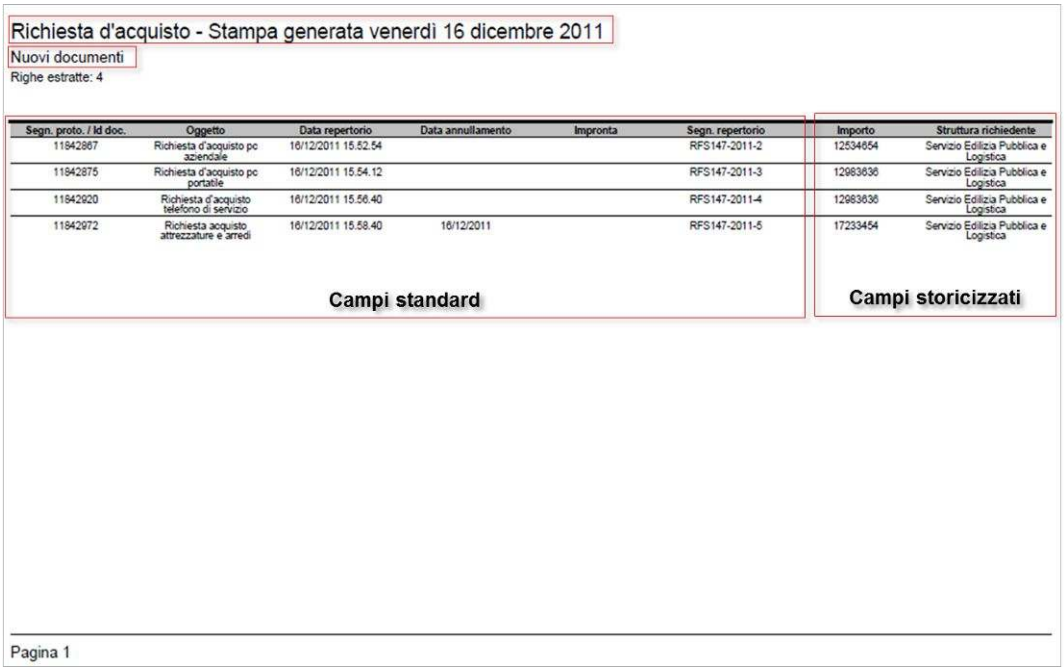
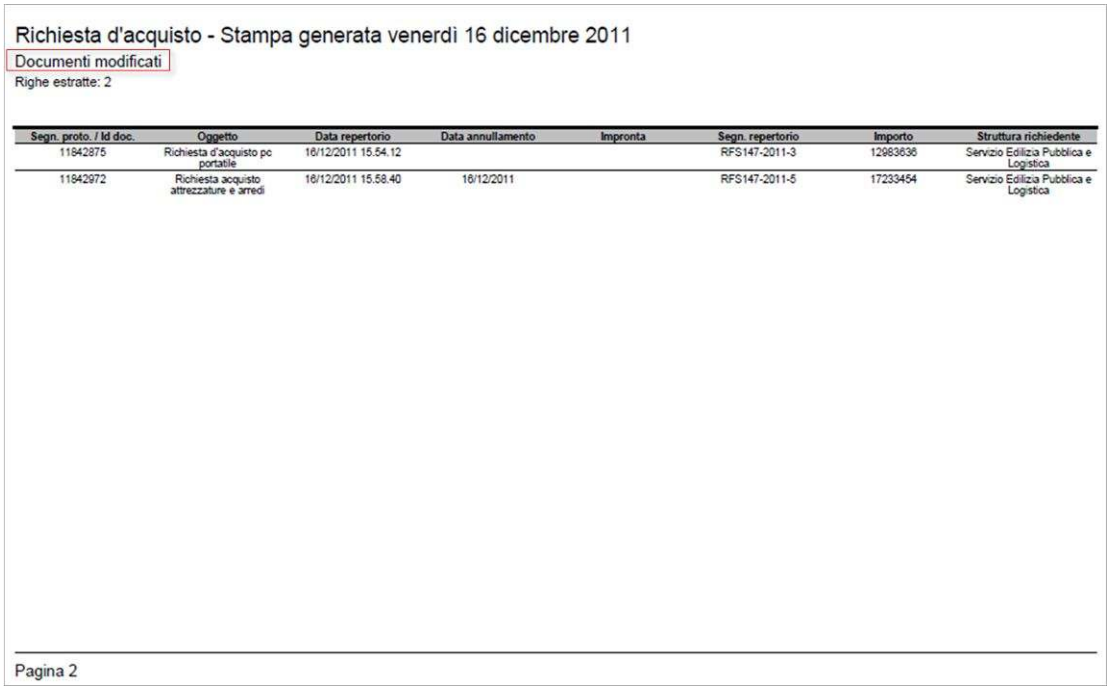


Figura 200 - *Stampa del registro di repertorio – Nuovi documenti repertoriati*

La seconda sezione della stampa del registro di repertorio riporta:

- la denominazione del registro di repertorio;
- la data in cui viene effettuata la stampa del registro;
- l'elenco dei documenti repertoriati che hanno subito modifiche all'oggetto oppure ai campi soggetti a storicizzazione e i documenti che sono stati annullati.


Richiesta d'acquisto - Stampa generata venerdì 16 dicembre 2011

Documenti modificati

Righe estratte: 2

Segn. proto. / Id doc.	Oggetto	Data repertorio	Data annullamento	Impronta	Segn. repertorio	Importo	Struttura richiedente
11842875	Richiesta d'acquisto pc portatile	16/12/2011 15.54.12			RFS147-2011-3	12983636	Servizio Edilizia Pubblica e Logistica
11842972	Richiesta acquisto attrezzature e arredi	16/12/2011 15.58.40	16/12/2011		RFS147-2011-5	17233454	Servizio Edilizia Pubblica e Logistica

Pagina 2

Figura 201 - *Stampa del registro di repertorio – Documenti repertoriati modificati*

3.2 Ricerca Fascicoli

La funzionalità di ricerca fascicoli è ottenibile a partire dalla barra di navigazione del pannello principale selezionando la voce del menù RICERCA, premendo sul pulsante "RICERCA" e successivamente su quello dei FASCICOLI.

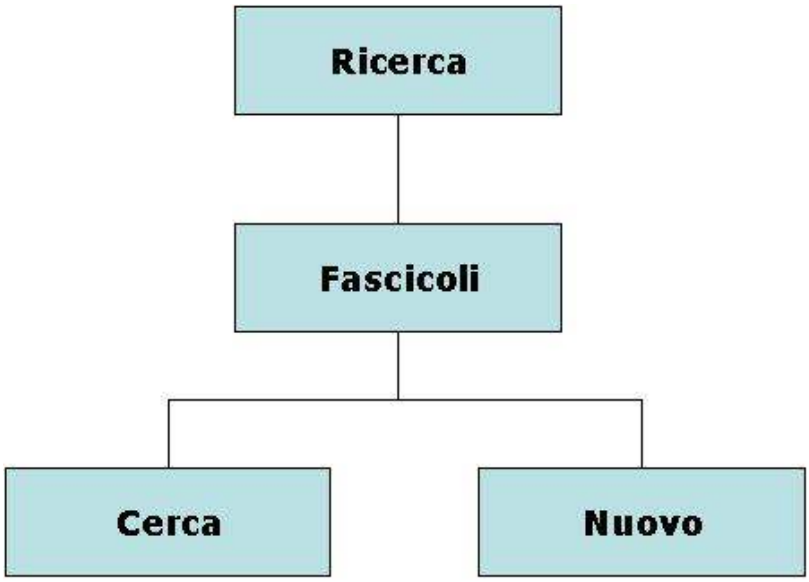


Figura 202 - Ricerca fascicoli: schema di navigazione

Il pannello che consente di effettuare tali operazioni è quello riportato nella Figura 202

E' possibile popolare il campo 'Codice' con differenti modalità:

- Selezionando la casella di selezione accanto alla voce "codice" ed editando direttamente un codice di titolario;
- Selezionando la casella di selezione accanto alla voce "livello" e scegliendo i valori dei 6 livelli di catalogazione con l'ausilio di menu pre-impostati presenti nella pagina;
- accedendo al titolario di classificazione tramite la selezione dell'icona . Viene visualizzato un pannello con la struttura del titolario nel quale è possibile selezionare il livello da riportare nel pannello di classificazione. Il titolario è visualizzato a partire dal livello digitato dall'utente nel campo 'Codice' o per intero qualora l'utente non abbia specificato alcun codice prima di selezionare l'icona.

Una volta popolato questo campo è possibile:

- tramite il pulsante **Cerca**, ottenere l'elenco dei fascicoli contenuti nel nodo scelto;
- tramite il pulsante **Nuovo**, creare un nuovo fascicolo(così come descritto nel paragrafo 2.10);
- tramite il pulsante **Salva**, salvare una ricerca effettuata (analogamente a quanto avviene per i documenti)
- tramite il pulsante **Modifica** (abilitato quando viene selezionata una ricerca salvata), modificare una ricerca precedentemente salvata (analogamente a quanto avviene per i documenti)
- tramite il pulsante **Riclassifica** (abilitato in fase di modifica, per gli utenti appartenenti ad un ruolo con opportuno profilo funzionale), modificare il dato relativo alla classificazione del fascicolo. Alla pressione del pulsante, un'opportuna maschera consente infatti di scegliere, nel titolario attivo, il nuovo nodo in cui spostare il fascicolo. Dopo essere usciti dalla maschera di selezione del nodo, sul tab fascicolo confermare l'operazione premendo il pulsante "Salva".

Una volta effettuata una ricerca, tramite il pulsante (posto in cima alla pagina di ricerca) è possibile azzerare tutti i filtri di ricerca impostati.

Per la visualizzazione dei fascicoli l'utente può impostare i filtri di ricerca proposti nella parte inferiore del pannello:

- **Titolario**: permette la selezione tra il titolario attivo ed eventuali titolari chiusi;
- **Codice**: permette all'utente di editare il codice del fascicolo di interesse;
- **Aperto**: permette di specificare la data di apertura del fascicolo. Il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è stato aperto il fascicolo. Questi valori possono essere inseriti attraverso la selezione da calendario  o semplicemente editandoli;
- **Chiuso**: permette di specificare la data di chiusura del fascicolo. Il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è stato chiuso il fascicolo. Questi valori possono essere inseriti attraverso la selezione da calendario  o semplicemente editandoli;
- **Creato**: permette di specificare la data di creazione del fascicolo. Il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è stato creato il fascicolo. Questi valori possono essere inseriti attraverso la selezione da calendario  o semplicemente editandoli;
- **Numero**: è il numero progressivo del fascicolo che si vuole cercare;
- **Anno**: consente di indicare l'anno di creazione del fascicolo;
- **Stato**: permette di specificare lo stato (aperto o chiuso) del fascicolo;
- **Tipo**: permette di effettuare ricerche per fascicoli procedimentali o generali. Se si seleziona l'opzione 'Generali' vengono disabilitati i filtri "Stato", "Numero", "Anno";
- **Descrizione**: consente di effettuare ricerche in base a parole presenti nella descrizione del fascicolo;
- **Note**: permette di cercare nel campo note associato al documento; è possibile ricercare i documenti in base al tipo di nota *a:*
  - ✓ *Tutti*: visibile a tutti gli utenti che hanno la visibilità sul documento*;*
  - ✓ *Ruolo:* visibile solamente agli utenti del ruolo dell'utente creatore della nota*;*
  - ✓ *Rf* (se gli RF sono configurati nel sistema): visibile ai soli ruoli appartenenti all'RF*;*
  - ✓ *Personale:* visibile solamente all'utente che l'ha creata*;*
  - ✓ *Qualsiasi:* comprende tutte le tipologie di note precedentemente descritte.
- **Data scadenza**: permette di specificare la data di scadenza del fascicolo. Il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di scadenza del fascicolo. Questi valori possono essere inseriti attraverso la selezione da calendario  o semplicemente editandoli;
- **Data collocazione**: permette di specificare la data di collocazione fisica del fascicolo. Il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data in cui è stato creato il documento. Questi valori possono essere inseriti attraverso la selezione da calendario  o semplicemente editandoli;
- **Collocazione fisica**: permette di specificare l'esatta collocazione del fascicolo (selezionabile attraverso la rubrica o mediante digitazione del codice nel primo dei due campi);
- **Tipo fasc.**: permette di selezionare una delle tipologie fascicolo (se presenti) a cui è associata l'icona  , che propone il pannello della profilazione dinamica del fascicolo. E' necessario che l'utente amministratore in fase di costruzione della tipologia abbia specificato che l'informazione possa essere utilizzata per le ricerche.

  Nel menu a tendina verranno proposte anche le tipologie di fascicolo al momento sospese. Nel pannello dell'Anteprima della Profilazione Dinamica sono presenti tre pulsanti:
  - *"Resetta"*: che reimposta i dati inseriti;

- *"Conferma"*: salva i dati che successivamente saranno utilizzati nella ricerca;
- *"Chiudi":* chiude il pannello.

Se la tipologia comprenda campi di tipo corrispondente, gli eventuali corrispondenti storicizzati verranno restituiti dalla ricerca in rubbrica e saranno opportunamente evidenziati con carattere barrato. Per i campi di tipo corrispondente è comunque possibile la selezione da codice. Nel caso in cui la parte di codice inserito sia comune a più corrispondenti censiti in rubriche diverse, il sistema mostra l'elenco di tali corrispondenti, da cui l'utente potrà selezionare quello di interesse in base alla rubrica di appartenenza.

La lista a tendina che mostra i tipi fascicolo configurati e disponibili presenta, inoltre, un valore denominato "Campi comuni" selezionando il quale si ha la possibilità di ricercare tutti i fascicoli procedimentali di qualsiasi tipo in cui è stato profilato anche il campo comune sul quale si sta effettuando la ricerca. Il risultato della ricerca così impostata rappresenta l'iperfascicolo ovvero l'insieme dei fascicoli, anche di diversa tipologia, che si riferiscono ad un medesimo soggetto/oggetto aggregante. Per ottenere un iperfascicolo sarà quindi necessario poter specificare la query ovvero selezionare tutti i fascicoli procedimentali, di qualunque tipologia essi siano ed a qualunque nodo di titolario appartengano, che hanno valorizzato un determinato campo comune con un determinato valore. L'iperfascicolo viene estratto e presentato quindi come elenco dei fascicoli (anche di tipi diversi) che rispettano la condizione impostata. Esportando il risultato della ricerca su un file esterno è possibile effettuare ulteriori elaborazioni con programmi di produttività personale e/o stamparne il contenuto.

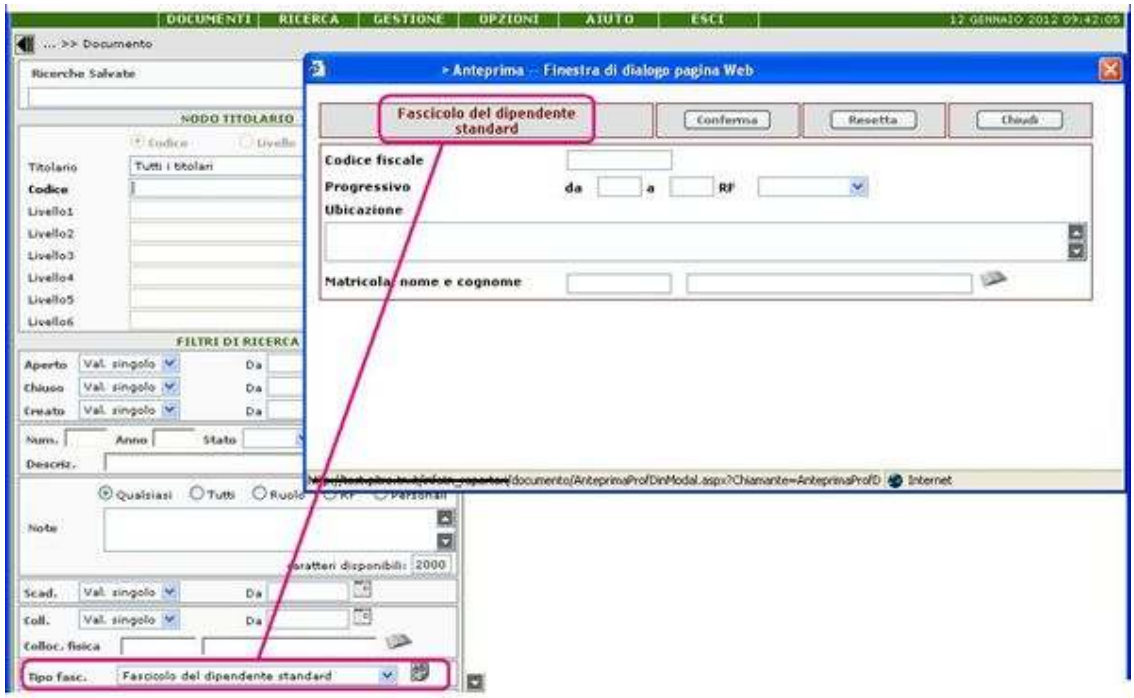


Figura 203 - Ricerca fascicolo tramite selezione tipologia fascicolo

- **Stato**: dopo aver selezionato il campo Tipo fascicolo, se a questo è stato associato un "diagramma di stato", immediatamente sotto il menù a tendina compare:

- un ulteriore menù a tendina con l'elenco degli stati del tipo fascicolo. Sono visibili gli stati che non sono stati dichiarati 'non ricercabili' da interfaccia di amministrazione e per cui esista almeno un fascicolo per tali stati;
- una data di scadenza; la scadenza di un tipo fascicolo viene definita in numero di giorni entro cui il fascicolo procedimentale deve raggiungere uno stato finale. Il sistema invia delle trasmissioni a tutti i destinatari del fascicolo quando si avvicina la data di scadenza o quando la data di scadenza è spirata senza che il fascicolo abbia raggiunto uno stato finale.

Ad ogni successivo accesso al documento, nel menu a tendina "Stato", se l'utente ne ha visibilità, sarà possibile selezionare lo stato successivo a quello corrente. Nel caso in cui lo stato corrente sia uno stato di sistema, lo stato successivo non è disponibile e verrà raggiunto al verificarsi di un determinato evento relativo al documento.

- **Sottofasc.**: se in tale campo si edita la descrizione del sottofascicolo la ricerca restituisce i fascicoli che contengono un sottofascicolo, a qualunque livello, la cui descrizione contiene il testo specificato;
- **Conservato**: se selezionato ricerca tutti i fascicoli sottoposti a conservazione sostitutiva;
- **Non conservato**: se selezionato ricerca tutti i fascicoli non sottoposti al processo di conservazione;
- **Creatore**: è possibile specificare se UO/Ruolo/Persona; in base a quanto selezionato, si deve inserire il codice con cui effettuare la ricerca. Se non si conosce il codice, è possibile cercarlo ed inserirlo tramite rubrica, attivabile utilizzando l'icona  (per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5). Tramite selezione del flag opportuno, è inoltre possibile estendere la ricerca anche ai ruoli storicizzati. In tal caso verranno cercati sia i fascicoli creati dal ruolo indicato, che quelli creati da ruoli da cui il ruolo corrente è stato ottenuto per modifica con storicizzazione;
- **Proprietario**: di cui è possibile specificare se Ruolo/Persona; in base a quanto selezionato, si deve inserire il codice con cui effettuare la ricerca. Se non si conosce il codice, c'è la possibilità di cercarlo ed inserirlo tramite rubrica selezionando l'icona  . Se viene selezionata la tipologia UO, è possibile effettuare ricerche sui fascicoli creati dalle UO sottoposte. Per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5;
- **Ordinamento:** è utilizzato per indicare il tipo di ordinamento. La prima finestra di selezione mostra i campi sui quali effettuare l'ordinamento (data creazione, codice, tipo, …). La seconda finestra di selezione serve per indicare il tipo di ordinamento (decrescente, crescente).
- **Mostra tutti i fascicoli**: attivando l'opzione sul 'SI', verranno presentati tutti i fascicoli procedimentali e generali associati sia al nodo titolario selezionato che a tutti i suoi figli.

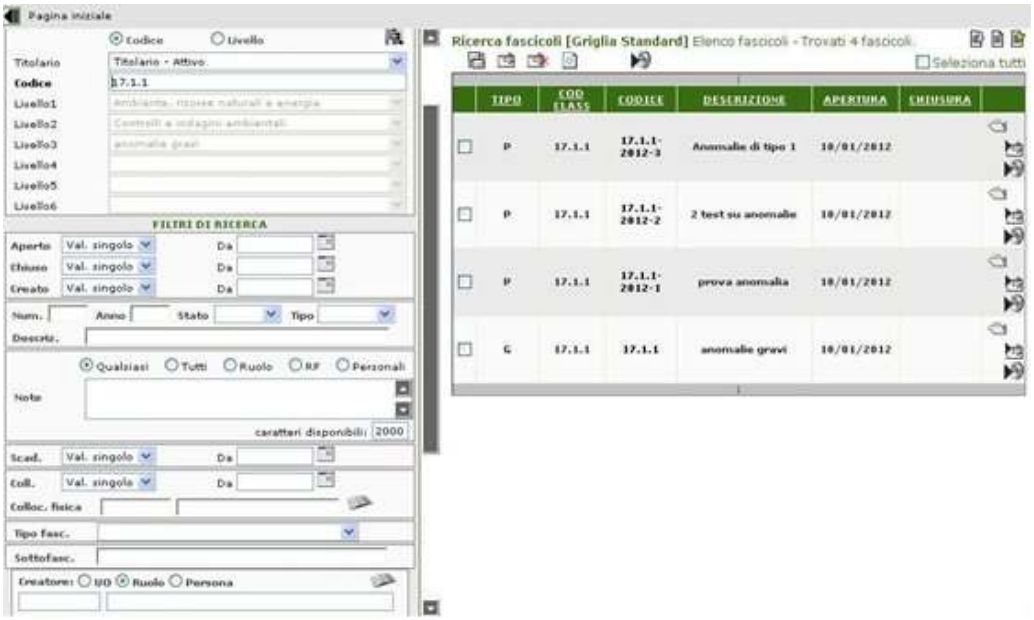


Figura 204 - Risultato della ricerca fascicoli

Nelle pagine di ricerca dei fascicoli è possibile salvare i criteri di ricerca per poi utilizzarli nelle ricerche future. La modalità di funzionamento è analoga a quella presente nelle ricerche dei documenti anche per quanto riguarda l'associazione con griglie di ricerca personalizzate (vedere i paragrafi da 3.1.2.2.1 a 3.1.2.2.6).

In alto, nella pagina dei risultati, sono presenti le icone per eseguire delle azioni sui fascicoli risultanti dalla ricerca o su una parte di essi (azioni massive).

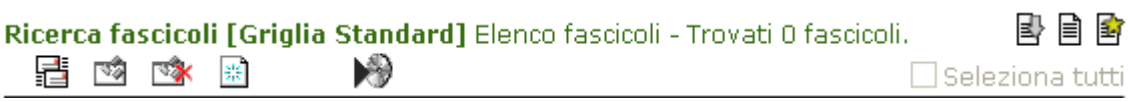


Figura 205 - Azioni massive

La selezione può avvenire mettendo un segno di spunta accanto alla voce "Seleziona tutto", oppure scegliendo i singoli fascicoli, utilizzando le caselle di selezione che si trovano accanto ad ognuno di essi nell'elenco dei risultati.
La presenza di questi pulsanti è soggetta a configurazione e solo i ruoli abilitati potranno effettuare queste azioni massive (tutte o quelle per le quali sono stati abilitati).

- "Esporta i fascicoli selezionati" che consente di esportare tutti i fascicoli selezionati.
  Selezionando l'icona viene visualizzata la finestra di dialogo mostrata in Figura 206, dove è possibile associare un titolo al file che si esporta, selezionare il formato del file (PDF/Excel/Calc).
  Nel caso di export in formato PDF vengono salvati campi che compaiono nella griglia standard.
  Nel caso in cui si scelga un file Excel/Calc viene abilitata l'area in cui è possibile selezionare i campi relativi ai documenti da salvare nel file. Se sono state effettuate delle ricerche con griglie personalizzate, i campi presenti nelle griglie personalizzate vengono riportati nell'elenco dei campi

da esportare e sono selezionati per default. Se sono state effettuate ricerche con filtro su una tipologia i campi della tipologia selezionata eventualmente non presenti nella griglia dei risultati di ricerca verranno resi disponibili per l'export (di default non selezionati).;

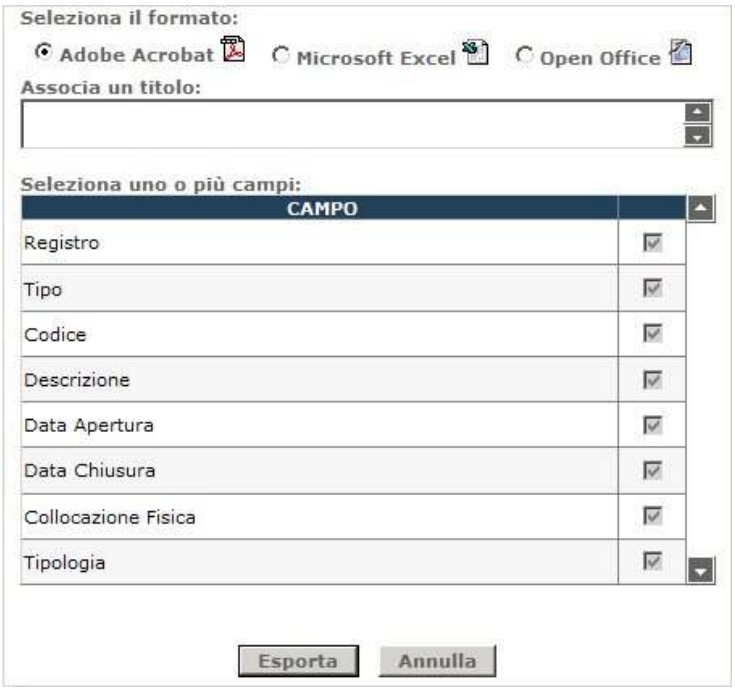


Figura 206 - Esporta risultati della ricerca

- "Trasmetti i fascicoli selezionati" consente di effettuare una trasmissione dei fascicoli selezionati. Dopo aver scelto i fascicoli da trasmettere e aver cliccato sul pulsante corrispondente all'azione massiva, si apre una finestra per la creazione della trasmissione.
  L'utente potrà utilizzare un modello di trasmissione, oppure costruirsi la trasmissione nel modo classico (selezionando la ragione di trasmissione, i destinatari, le note, …).
  - Trasmissione da modello: scegliere il modello dal menu a tendina[10] riportato in alto della pagina, attendere che la richiesta venga elaborata e poi cliccare sul pulsante "Trasmetti". Il sistema effettua le trasmissioni e ne riporta l'esito nella sezione sottostante denominata *Report*. Il risultato visualizzato può essere esportato mediante il pulsante "Esporta Report".
  - Trasmissione semplice: è la sezione che riporta i campi necessari per la costruzione della trasmissione. Per i dettagli sui campi si rimanda al paragrafo 2.13.1 che descrive gli stessi campi anche se nel contesto dei documenti. Cliccando sul pulsante "Trasmetti" il sistema effettua le trasmissioni e ne riporta l'esito nella sezione sottostante. Il risultato visualizzato può essere esportato mediante il pulsante "Esporta Report".
- "Salva i fascicoli selezionati nell'Area Di Lavoro": permette di salvare contemporaneamente nell'area di lavoro tutti i fascicoli selezionati;
- Rimuovi i fascicoli selezionati dall'Area Di Lavoro, che permette di eliminare i fascicoli selezionati dall'area di lavoro;

[10] Per maggiori dettagli sui modelli di trasmissione selezionabili si veda il paragrafo 2.13.4

- “Inserisci i fascicoli selezionati in ‘Area Conservazione’” , permette di inserire contemporaneamente nell’Area Conservazione tutti i fascicoli selezionati dalla lista.

In modo del tutto analogo a quanto avviene per i documenti, nel caso in cui l’utente sia abilitato alla personalizzazione delle griglie di ricerca:

- “Personalizza le griglie di ricerca” : in modo del tutto analogo a quanto avviene per i documenti, nel caso in cui l’utente sia abilitato alla personalizzazione delle griglie di ricerca, il pulsante consente di accedere alla maschera di personalizzazione delle griglie di ricerca (vedere paragrafo 3.1.1.2.1);
- “Salva o modifica griglie” : consente di accedere alla maschera di salvataggio delle modifiche apportate alle griglie personalizzate (vedere paragrafo 3.1.1.2.2 e 3.1.1.2.4);
- “Mie griglie preferite” : consente di accedere alla maschera di selezione della griglia di riferimento (vedere paragrafo 3.1.1.2.3).

Dopo aver effettuato la ricerca, sulla parte sinistra del pannello è possibile visualizzare il dettaglio di un fascicolo tramite la selezione della corrispondente icona come riportato in Figura 204.
Il fascicolo visualizzato è suddiviso in 3 differenti parti:

- la gerarchia di classificazione del fascicolo ;
- i dati del fascicolo;
- i sotto fascicoli contenuti dal fascicolo;

Nella gerarchia di classificazione del fascicolo selezionato, il sistema mostra le voci di titolario sotto le quali si trova il fascicolo a partire dal nodo di più alto livello.
Per quanto riguarda i dati del fascicolo (Figura 207) in particolare, vi è una serie di icone presenti nel pannello che consentono di effettuare le seguenti operazioni (se il fascicolo è di tipo generale alcune delle icone non sono attive):

- : consente di visualizzare la storia del processo di conservazione a cui è stato sottoposto il fascicolo;
- : visualizza la storia delle operazioni avvenute nel fascicolo, indicando: data, operatore (nome e ruolo), azione effettuata;
- : consente di modificare il campo note relativo al fascicolo;
- : inserisce il fascicolo selezionato nell’area di lavoro;
- : permette di stampare le etichette del fascicolo;
- : permette di chiudere e riaprire un fascicolo procedimentale;
- : mostra i ruoli/utenti che hanno la visibilità sul fascicolo selezionato. Per un maggiore dettaglio si veda il paragrafo 2.8.1.1.

Nella scheda del fascicolo sono inoltre presentati i dati di dettaglio del fascicolo: la classifica, il codice, la data apertura, la data chiusura, il tipo di fascicolo, lo stato attuale (se aperto o chiuso), la descrizione, le note, la collocazione fisica, la data della collocazione.
La sezione per la gestione dei sottofascicoli consente:

- attraverso la selezione dell’icona , la ricerca dei sottofascicoli contenuti nel fascicolo attraverso l’inserimento della loro descrizione o una parte di essa, e la selezione della lentina della ricerca, così come descritto nel paragrafo 2.8.1.3;
- la visualizzazione della struttura dei sotto fascicoli contenuti nel fascicolo scelto.

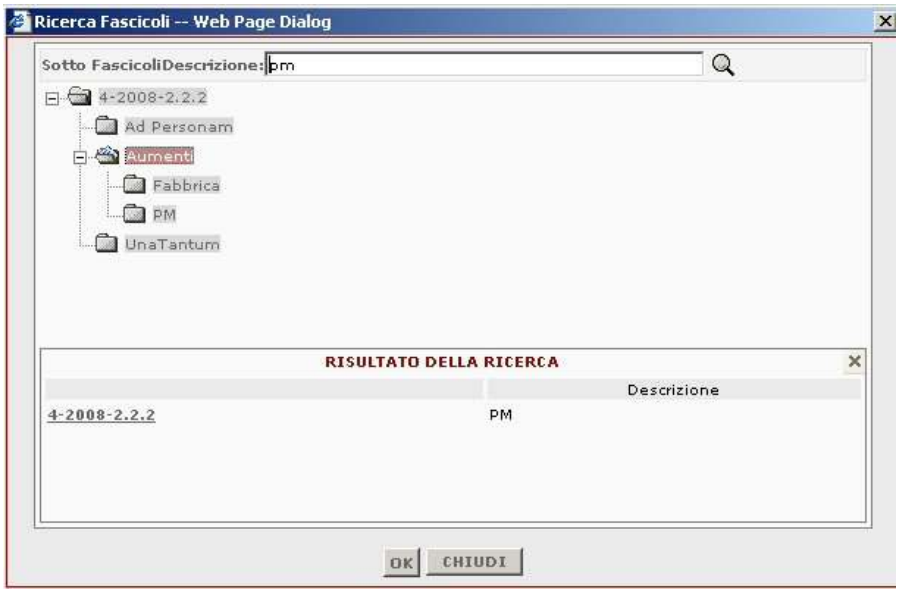


Figura 207 - Ricerca sotto fascicoli

Infine, sulla pulsantiera posta in basso alla finestra sono disponibili i seguenti comandi:

- **Modifica:** consente di modificare il nome del sottofascicolo selezionato;
- **Aggiungi**: consente di aggiungere un nuovo sottofascicolo;
- **Rimuovi**: consente la rimozione del sottofascicolo selezionato.

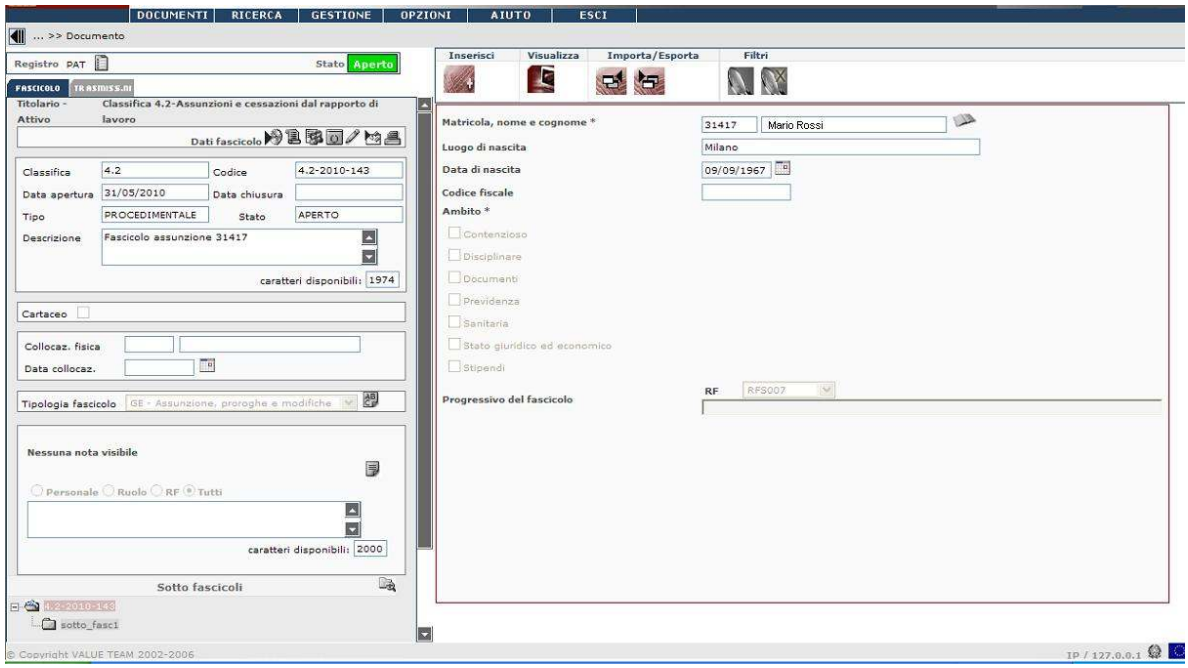


Figura 208 - Dettaglio fascicolo- dati tipologia fascicolo

Sulla parte destra della scheda di dettaglio del fascicolo per default vengono visualizzati i campi profilati associati alla tipologia scelta per il fascicolo.
Per le amministrazioni che ne abbiano fatto richiesta, è possibile tener traccia delle modifiche effettuate sui campi della tipologia fascicolo (ad eccezione dei campi contatore, oggetti esterni e link) . In tal caso in alto a destra della sezione relativa ai campi profilati è presente il pulsante  . Cliccando su tale pulsante si apre una finestra che mostra le eventuali modifiche apportate ai campi con l'indicazione dell'utente e del ruolo che ha effettuato la modifica, della data e del valore precedente alla modifica. Verrà data evidenza anche della cancellazione/modifica di un corrispondente che compare in un campo di tipo corrispondente di una tipologia di fascicolo.

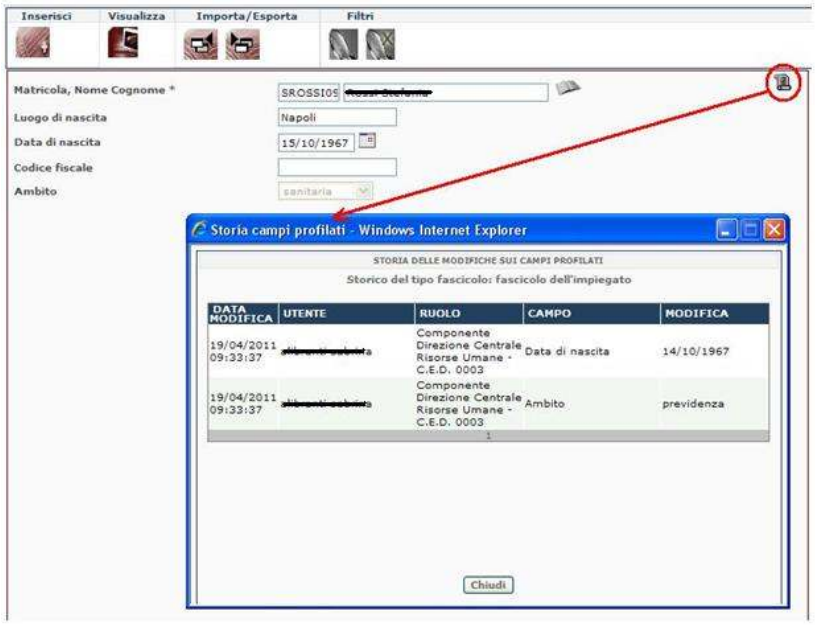


Figura 209 Storia delle modifiche dei campi profilati

Se non è stata scelta alcuna tipologia la pagina mostra l'elenco dei documenti contenuti eventualmente nel fascicolo.
Nella parte superiore della pagina di destra sono presenti una serie di pulsanti che servono ad effettuare delle operazioni sul fascicolo. Di seguito la descrizione di tali pulsanti:


Inserisci documento


Visualizza elenco documenti


Importa documenti


Esporta documenti


Filtra documenti


Elimina filtri

Inserisci documento: il tasto è attivo quando vengono visualizzati i documenti presenti nel fascicolo. Selezionando tale pulsante viene visualizzato il pannello mostrato nell'immagine qui di seguito, in cui è possibile cercare:

- Documenti protocollati: utilizzando come possibili criteri di ricerca il "Numero Protocollo" (esatto) o un determinato intervallo di numeri protocollo, l "anno" di protocollazione dei documenti ricercati, la "Data del protocollo" (esatta) o l'intervallo di data in cui si ritiene vi sia il documento ;
- Documenti non protocollati: utilizzando come possibili criteri di ricerca l'"Identificativo Documento" (esatto) o un determinato intervallo di numeri identificativi di documento, la "Data di creazione" (esatta) o l'intervallo di data in cui si ritiene sia stato creato il documento;
- Documenti Predisposti: utilizzando come possibili criteri di ricerca l'"Identificativo Documento" (esatto) o un determinato intervallo di numeri identificativi di documento, la "Data di creazione" (esatta) o l'intervallo di data in cui si ritiene sia stato creato il documento;
- Documenti in Area di Lavoro.

Dopo aver selezionato il documento di interesse, per effettuare un maggiore filtro sui documenti è possibile digitare per intero o solo una parte dell'oggetto contenuto nei documenti ricercati, oppure selezionandoli attraverso l'oggettario (così come descritto nel paragrafo 2.7.1.3.1).

La ricerca di tali documenti avviene attraverso la selezione del pulsante **"Cerca".**

A questo punto si visualizzano i documenti ricercati, si scelgono quelli a cui si è interessati, e si preme il pulsante "OK" . I documenti sono inseriti nel fascicolo su cui si sta operando.

Figura 210 - Dettaglio funzione Inserisci documenti in fascicolo

Visualizza documenti: il tasto è attivo quando nella pagina sono mostrati i dati della tipologia fascicolo (Figura 208). Cliccando su tale pulsante nella pagina di destra, vengono mostrati, se presenti, i documenti contenuti nel fascicolo. Per tornare alla visualizzazione dei campi associati alla tipologia fascicolo, bisogna cliccare sul pulsante .

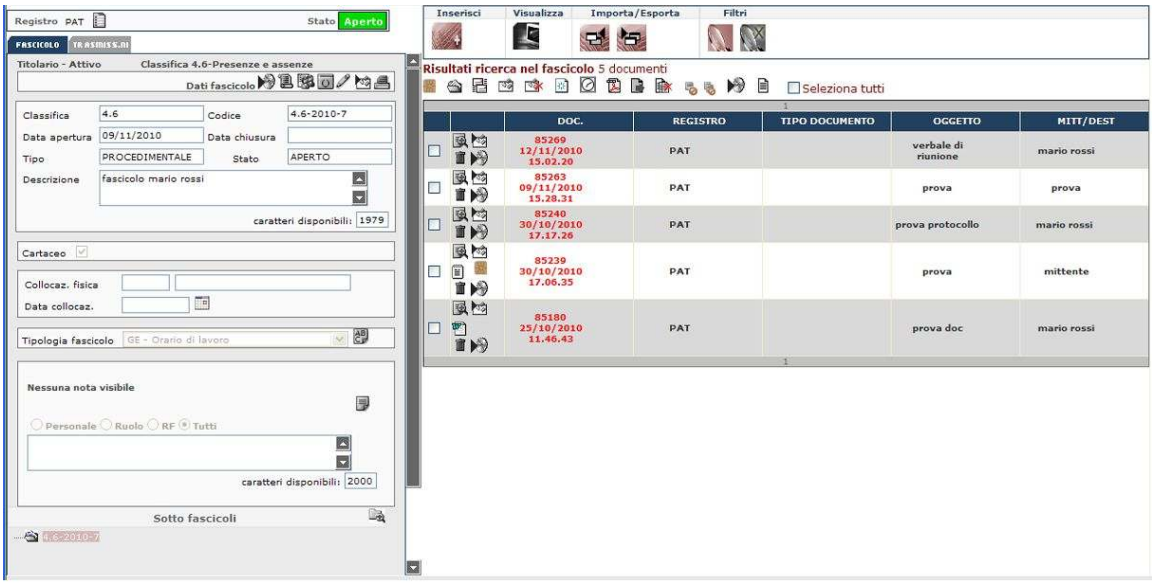


Figura 211 – Fascicolo – Dettaglio documenti

La lista dei documenti contenuti nel fascicolo indica:

- **Doc.:** il numero del documento (id documento per i documenti grigi e numero di protocollo per i documenti protocollati);
- **Registro**: il registro a cui è associato il protocollo;
- **Tipo:** il tipo di protocollo associato che può essere: “A” = “protocollo in arrivo”, “P”= “Protocollo in partenza”, “I”=”Protocollo interno” e “NP”= “documento non protocollato”;
- **Oggetto:** oggetto del documento presente nel fascicolo;
- **Mitt./Dest.:** il mittente e/o gli eventuali destinatari del documento;

in corrispondenza di ciascun documento sono inoltre presenti i seguenti pulsanti d’azione:

- **Dett.:** selezionando l’icona è possibile accedere alla scheda di dettaglio del documento. Dalla scheda di dettaglio del documento, attraverso le freccette in alto a destra, evidenziate in verde nella Figura 171, è possibile visualizzare gli altri documenti presenti nel fascicolo, precedenti o successivi al documento selezionato, senza ritornare all’elenco iniziale;
- **Visualizza:** per ogni documento di cui sia stata acquisita l’immagine o a cui sia stato associato un documento elettronico, è possibile visualizzare tale immagine/documento elettronico selezionando l’icona che rappresenta il formato del file acquisito. Nel caso di documenti senza file elettronico associato, l’icona non appare dando così anche l’informazione di “assenza di documento elettronico”. Il funzionamento del visualizzatore è descritto nel paragrafo 2.14.2.1.
- **Area di lavoro:** selezionando l’icona è possibile inserire il documento presente nel fascicolo nell’Area di lavoro documenti; il pulsante consente invece eliminare il documento presente nel fascicolo dall’area di lavoro.
- **Area** Conservazione: è possibile inserire ciascun documento presente nel fascicolo in una istanza di conservazione selezionando l’icona corrispondente;

- **Elimina**: la selezione dell'icona consente di eliminare il documento dal fascicolo.

Sopra l'elenco dei documenti (fig. 170) compaiono inoltre una serie di pulsanti che permettono di effettuare alcune azioni in modo massivo sull'insieme dei documenti selezionati (tali azioni sono descritte nel dettaglio nel paragrafo 3.1.1.1).
Per gli utenti opportunamente abilitati, insieme a tali pulsanti sono presente anche le icone , e che consentono di gestire le griglie personalizzate, analogamente a quanto descritto circa i documenti nel par. 3.1.1.2.

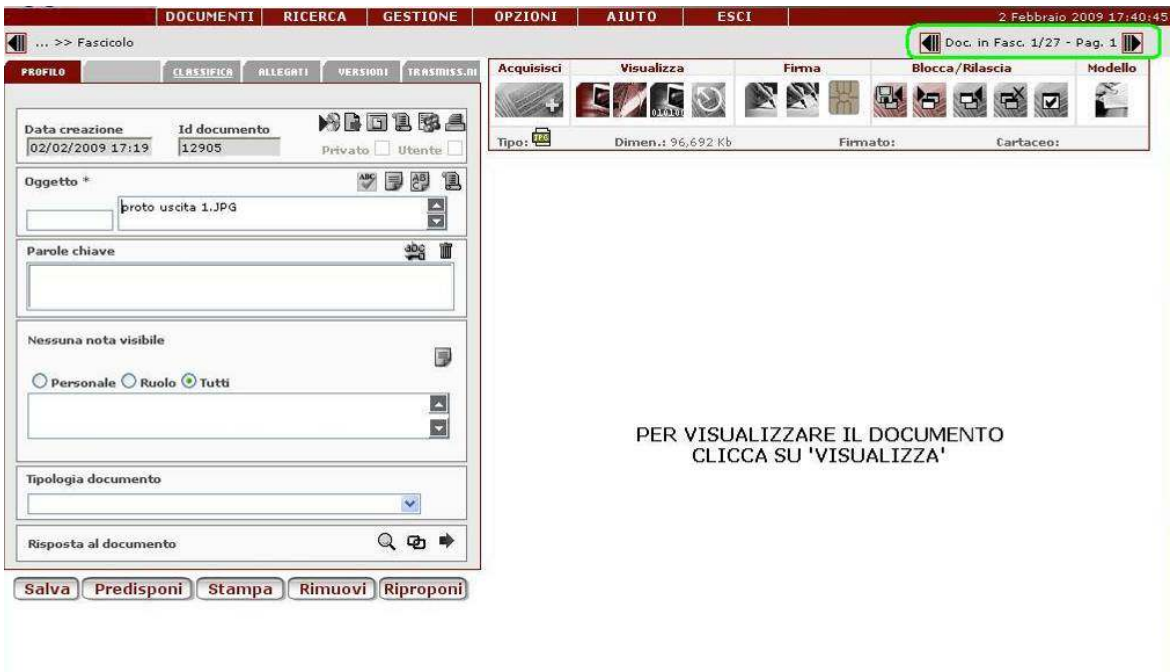


Figura 212 – Scheda documento: funzioni di navigazione dei documenti all'interno di un fascicolo

Importa documenti: consente di importare in maniera massiva nel fascicolo (o in un sottofascicolo) documenti presenti su file system o in dispositivi di memoria esterni.
All'attivazione della funzione il sistema presenta una finestra di dialogo da cui è possibile ricercare e selezionare la cartella sorgente contenente i documenti da importare e inserire nel fascicolo; una volta selezionata la cartella, si avvia l'operazione di importazione attraverso il pulsante "Invia".
Conclusa l'operazione il sistema restituisce nella medesima finestra il log dell'importazione ossia l'elenco dei documenti importati e inseriti nel fascicolo. Il sistema memorizza il nome dei file importati. Tale nome risulta immodificabile e viene visualizzato all'interno del visualizzatore (par. 2.14.1, 2.14.2.1).

Esporta documenti: consente di esportare i documenti contenuti nel fascicolo, o parte di essi, inviandoli ad una cartella selezionata.
All'attivazione della funzione il sistema presenta una finestra di dialogo che consente di selezionare la cartella di destinazione a cui inviare i file dei documenti che si intende esportare; selezionata la cartella si avvia l'operazione mediante il pulsante "Invia".

Al termine dell'operazione il sistema restituisce nella medesima finestra di dialogo il log dei documenti esportati. Per l'export vengono utilizzati i nomi originari dei file (ossia quelli memorizzati all'acquisizione).

Filtra documenti: tale pulsante consente di ricercare specifici documenti nell'insieme dei documenti presenti nel fascicolo; all'attivazione della funzione il sistema propone come possibili filtri di ricerca quelli mostrati nella Figura 172.

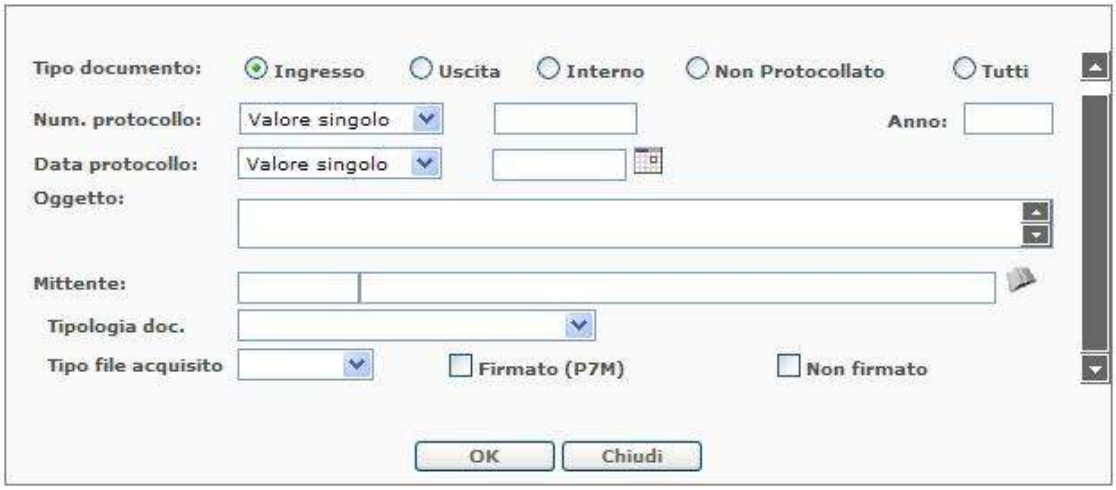


Figura 213 - Filtro documenti

I parametri disponibili sono:

- **Tipo Documento**: permette di selezionare documenti protocollati in ingresso, in uscita, con protocollo interno, non protocollati o tutti;
- **Numero Protocollo**: permette di indicare un singolo numero o un intervallo di numeri di protocollo;
- **Anno**: permette di selezionare l'anno di creazione del/dei documento/i a cui si è interessati;
- **Data Protocollo**: permette di utilizzare come filtro di ricerca un "valore singolo" o un "intervallo" di valori selezionando l'opzione che interessa dall'apposito menu a tendina; nel caso si scelga l'opzione "intervallo" il sistema restituisce sulla stessa riga due campi in cui devono essere inseriti rispettivamente i valori minimo e massimo della data di protocollo.
  La data può essere inserita in tali campi digitandola manualmente o attraverso la selezione da calendario ;
- **Oggetto**: permette l'inserimento di una o più parole presenti nell'oggetto del documento che si intende cercare;
- **Mittente/Destinatario**: tale campo non è visibile se nel campo "Tipo documento" è selezionata una delle due opzioni "Non protocollati" o "Tutti"; viene visualizzato solamente a seguito della scelta di una delle opzioni "Arrivo" oppure "Partenza" o "Interno"; a seconda del tipo selezionato compare rispettivamente il campo "Mittente" o "Destinatario".
  E' possibile valorizzare il campo richiamando un corrispondente dalla rubrica a cui si accede attraverso l'icona : si apre una schermata che mette a disposizione le diverse possibilità (codice, descrizione, città e/o località) per la ricerca di uffici, utenti o ruoli; una volta effettuata la ricerca si può valorizzare il campo "Mittente/Destinatario" selezionando dai risultati della ricerca il valore desiderato (per maggiori dettagli sull'utilizzo della rubrica si veda il paragrafo 4.5).

E' possibile valorizzare il campo "Mittente/Destinatario" anche digitando nello spazio breve il codice rubrica associato al corrispondente; una ulteriore possibilità è quella di digitare nello spazio lungo una parte della descrizione del corrispondente che interessa.

- **Tipologia documento:** indica la tipologia del documento che si vuol ricercare selezionando la voce da un menu pre-impostato. Se la tipologia scelta è profilata (Figura 214, evidenziata in rosso) si attiva l'icona , che propone il pannello della profilazione dinamica del documento. E' necessario che l'utente amministratore in fase di costruzione della tipologia abbia specificato che l'informazione possa essere utilizzata per le ricerche. Nel menu a tendina verranno mostrate solamente le tipologie in esercizio (non sospese).
  Nel pannello dell'Anteprima della Profilazione Dinamica sono presenti tre pulsanti:
  - "Resetta": che reimposta i dati inseriti;
  - "Conferma": salva i dati che successivamente saranno utilizzati nella ricerca;
  - "Chiudi": chiude il pannello.
- **Tipo file acquisito:** consente di filtrare l'elenco dei documenti presenti nel fascicolo per tipologia di file acquisito.
- **Firmato / Non firmato:** consente di estrarre dall'elenco dei documenti presenti nel fascicolo i documenti firmati digitalmente.

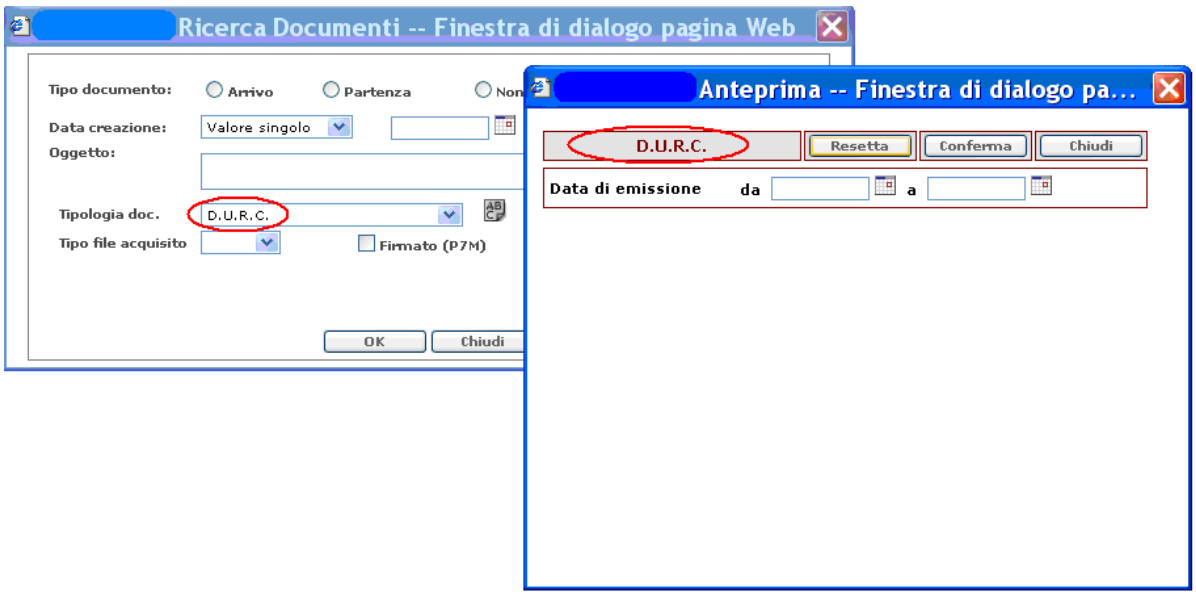


Figura 214 - Filtro documenti: tipologia documenti

Rimuovi filtro: permette di rimuovere un filtro precedentemente creato tornando così a visualizzare l'elenco completo dei documenti presenti nel fascicolo.

Se l'Amministrazione è abilitata alla gestione dei documenti repertoriati e se il ruolo che effettua la ricerca è abilitato all'uso di griglie personalizzate, è possibile includere la segnatura di repertorio nella griglia dei documenti contenuti nel fascicolo. Per fare ciò è sufficiente selezionare il contatore di una tipologia repertoriata (si veda paragrafo 2.9) fra i campi di una griglia personalizzata. Fra i risultati di ricerca verrà mostrata la segnatura di repertorio (Figura 215).

Figura 215 - Evidenza della segnatura di repertorio nel contenuto di un fascicolo (ruolo abilitato all'utilizzo di griglie personalizzate)

3.2.1 Trasmissione fascicolo

Nella pagina di dettaglio relativa ad un fascicolo è presente la sezione 'Trasmissioni' da cui è possibile vedere le trasmissioni effettuate e ricevute relative al fascicolo selezionato. Sulle trasmissioni è possibile effettuare le seguenti operazioni:

- **Nuova**: consente di creare una nuova trasmissione per un fascicolo secondo quanto visto in 2.13. Analogamente a quanto avviene per i documenti è possibile usufruire delle funzionalità relative ai modelli. Pertanto oltre al salvataggio (**Salva**) o trasmissione (**Trasmetti**) del fascicolo è possibile anche creare dei modelli di trasmissione (**Salva Mod.**) in modo analogo a quanto mostrato nel paragrafo relativo alla trasmissione dei documenti 2.13.4. Per l'utilizzo di modelli di trasmissione già definiti si veda il paragrafo 2.13.4;
- **Modifica**: consente di modificare i dati di una trasmissione precedentemente salvata;
- **Trasmetti**: consente di trasmettere un fascicolo i cui dati di trasmissione erano stati precedentemente preparati;
- **Trasmissione rapida**: è possibile effettuare una trasmissione utilizzando un modello di trasmissione precedentemente definito, selezionandolo dal menu a tendina delle trasmissioni rapide. Se il modello di trasmissione scelto contiene una UO fra i destinatari, al momento della trasmissione viene fatto un controllo sull'esistenza dei ruoli di riferimento per la UO stessa. Se non ve ne sono, il sistema mostra un opportuno messaggio e la trasmissione alla specifica UO non viene effettuata
- **Stampa**: consente di visualizzare un report PDF relativo alle trasmissioni effettuate sul fascicolo. Vengono visualizzate le stesse informazioni proposte nell'analogo report sui documenti.

3.3 Ricerca Trasmissioni

La funzionalità di ricerca di trasmissioni è ottenibile a partire dalla barra di navigazione del pannello principale selezionando la voce del menu RICERCA, premendo sul pulsante "RICERCA" e successivamente sul pulsante TRASMISSIONI. Il menu delle trasmissioni consente all'utente di effettuare ricerche relative alle trasmissioni effettuate o ricevute.

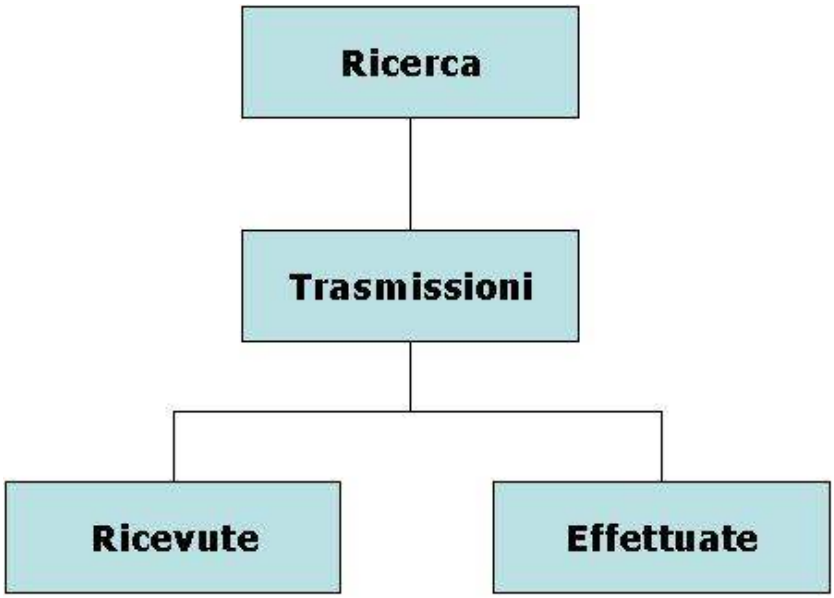


Figura 216 - Ricerca trasmissioni: schema di navigazione

3.3.1 Trasmissioni ricevute

La pagina di ricerca delle trasmissioni ricevute (opzione “Ricevute”) contiene:
- un menù a tendina contenente eventuali ricerche salvate in precedenza. Tramite il pulsante si può eliminare una ricerca già salvata;
- un insieme di parametri utilizzabili per la ricerca di documenti o fascicoli.

I criteri di ricerca utilizzabili sia per i documenti che per i fascicoli, sono:

- **Destinatario trasmissione**: consente di specificare il destinatario delle trasmissioni ricevute che si vogliono ricercare, proponendo per default “utente” e “ruolo” relativi all’utenza al momento connessa al sistema. Utente e ruolo sono selezionabili/deselezionabili attraverso la spunta nella casella corrispondente. Se si mette la spunta alla casella “ruolo”, è possibile modificare tramite codice o rubrica il ruolo a cui è destinata la trasmissione. Il sistema permette di selezionare da un menu a tendina il nominativo dell’utente a cui è stata notificata la trasmissione. La selezione del ruolo può avvenire indicandone il codice o tramite ricerca nella rubrica (si veda par. 4.5.4).Se si seleziona il flag “Estendi a storicizzati”, nel menu a tendina che permette di selezionare gli utenti a cui è stata notificata la trasmissione, vengono proposti anche gli utenti che non sono più presenti nel ruolo selezionato.
  E’ inoltre possibile ricercare trasmissioni ricevute dai ruoli sottoposti al ruolo a cui appartiene chi sta effettuando la ricerca e anche in questo caso si può specificare il nominativo dell’utente che ha ricevuto la notifica.(Per maggiori dettagli si veda oltre il paragrafo 3.3.1.1).
- **Oggetto trasmesso**: consente di creare una ricerca per “Documento” o per “Fascicolo”. Nel caso di ricerca documenti (valore di default), un ulteriore menù a tendina permette di scegliere fra protocollato, protocollato in arrivo, protocollato in partenza, interno, non protocollato o tutti.
- **Tipologia documento**: tale campo è presente solamente se nel campo “Oggetto trasmesso” è stata selezionata la voce “Documento”.

Consente di specificare la tipologia dei documenti ricevuti che si intende ricercare selezionandola da un menu a tendina; una volta selezionata una specifica tipologia, agendo sull'icona si ha la possibilità di valorizzare i campi propri della tipologia scelta, purché questi siano visibili all'utente.

- **Tipologia fascicolo**: tale campo è presente solamente se nel campo "Oggetto trasmesso" è stata selezionata la voce "Fascicolo".
  Consente di specificare la tipologia dei fascicoli ricevuti che si intende ricercare. Successivamente alla selezione di una determinata tipologia fascicolo è inoltre possibile impostare i valori relativi agli specifici campi della tipologia che sono visibili all'utente.
- **Documenti in completamento**: tale sezione permette di selezionare una tra le seguenti opzioni: "Predisposti alla Protocollazione", "Mancanza immagine", "Con immagine" ,"Mancanza fascicolazione".
- Se si seleziona l'opzione "Con immagine", il sistema consente di filtrare ulteriormente la ricerca discriminando tra documenti "firmati" e "non firmati" e/o specificando un determinato formato del file acquisito (selezione da menu a tendina).
- **Mittente** (selezionabile per UO, Ruolo, Persona): permette l'inserimento da rubrica, per cui è necessario selezionare l'icona associata al campo "mittente". Nella finestra che si apre a seguito della selezione dell'icona, sono presenti i campi per la ricerca, e quindi per la successiva valorizzazione del campo mittente, di utenti, ruoli o UO. Inoltre è possibile valorizzare il campo mittente anche attraverso la semplice digitazione del codice rubrica associato all'utente, al ruolo o all'UO di interesse;
- **Data di trasmissione**: è possibile effettuare la selezione da un menu a tendina che visualizza "valore singolo" ed "intervallo", quindi può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di protocollo. Inoltre, la data può essere inserita attraverso la selezione da calendario o semplicemente editandola;
- **Ragione Trasmissione**: è possibile selezionare tramite menu a tendina una delle ragioni di trasmissione proposte dal sistema;
- **Accettate/Rifiutate/Pendenti**: se selezionate, attivano un menu a tendina che visualizza "valore singolo" ed "intervallo", quindi se possibile può essere effettuata la selezione per valore singolo o per intervallo di valori; in questo secondo caso il sistema visualizza sulla riga due campi nei quali inserire il valore minimo e massimo della data di protocollo. Inoltre, la data può essere inserita attraverso la selezione da calendario o semplicemente editandola;
- **Altri Filtri** (selezionabili tra quelli proposti dal sistema).: tale sezione permette di effettuare una ricerca ancora più puntuale popolando i seguenti campi "Note Generali", "Note Individuali", "Data scadenza dal al"
- **Ordinamento:** consente di ordinare i risultati della ricerca in base alla data di invio/creazione dell'oggetto ricercato o in base alla ragione di trasmissione; i risultati di ricerca inoltre possono essere ordinati in modo *crescente* o *decrescente*.

Tramite il pulsante **Cerca** viene visualizzato il risultato della ricerca nella parte destra della pagina.

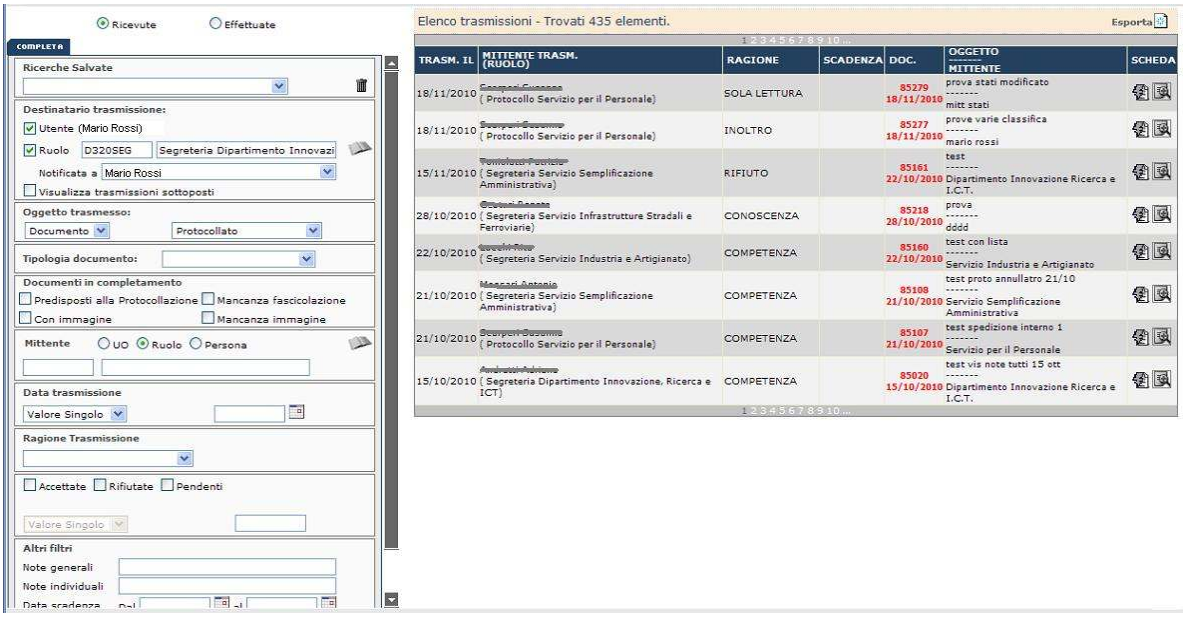


Figura 217 - Ricerca trasmissioni ricevute

Per ogni trasmissione trovata vengono riportate le seguenti informazioni:

- La data in cui è stata effettuata la trasmissione;
- Il mittente, che una volta stabilito se si intenda utilizzare tale parametro facendo riferimento a un mittente di tipo UO, ruolo o persona, può essere valorizzato o scrivendo il valore manualmente o selezionandolo dalla rubrica a cui si accede tramite l'icona ;
- La ragione della trasmissione;
- La scadenza di tale trasmissione;
- L'icona per visualizzare i dettagli della trasmissione del documento, comprendenti i seguenti dati: note generali, note individuali, data vista, data risposta, data accettazione, data riferimento, note accettazione/rifiuto; nella stessa scheda in basso è presente anche il dettaglio dei destinatari che aggiunge ai dati precedenti l'elenco dei destinatari della trasmissione (ruoli e utenti a cui è stata data la notifica), la ragione e il tipo di trasmissione;
- Il numero di protocollo/ID del documento;
- L'oggetto ed il mittente della trasmissione;
- L'icona che consente il collegamento al documento oggetto della trasmissione.
  Accedendo alla scheda di dettaglio del documento/fascicolo trasmesso è possibile navigare nei documenti/fascicoli precedenti e successivi utilizzando le freccette poste in alto a destra come mostrato nella figura seguente.

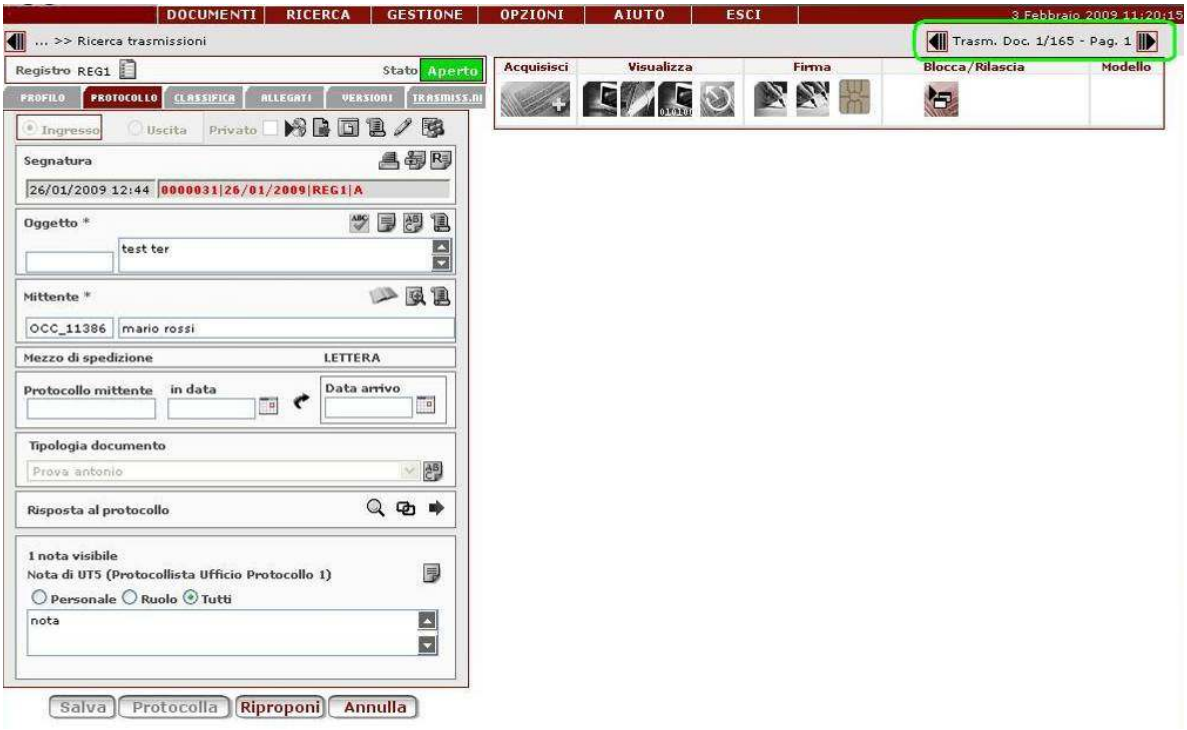


Figura 218 – Funzioni per la navigazione tra documenti presenti in una ricerca trasmissioni

In alto a destra, nella pagina dei risultati, è presente l'icona che consente di creare un file in formato pdf o xls con la lista delle trasmissioni ricevute.

Oltre al comando Ricerca, è possibile salvare i criteri di ricerca per poi utilizzarli nelle ricerche future selezionando il pulsante Salva. Anche in questa fase sarà possibile salvare la ricerca solo per l'utente o estendere la ricerca salvata al tutto il ruolo.

3.3.1.1 Filtro Destinatario trasmissioni ricevute

Tale sezione presenta due caselle di selezione:

- ☐ Utente
- ☐ Ruolo

Entrambe le caselle risultano selezionate di default.
La prima permette di ricercare le trasmissioni che abbiano come destinatario l'utente che sta effettuando la ricerca (trasmissioni ad utente); la seconda invece consente di ricercare le trasmissioni che siano state effettuate verso il ruolo specificato nei campi posti accanto al flag (codice e descrizione) che risultano valorizzati per default con i dati del ruolo corrente con cui l'utente sta realizzando la ricerca.
Quando il campo ruolo è valorizzato, è possibile specificare anche il nominativo di uno degli utenti del ruolo al quale sia stata notificata la trasmissione selezionando tale valore da un menu a tendina; tale menu propone i nominativi di tutti gli utenti inseriti nel ruolo; è impostato per default il nominativo dell'utente che sta effettuando la ricerca. Nel menu a tendina compaiono anche gli utenti che non fanno più parte del ruolo contraddistinti ~~con~~ dal colore rosso.

Pertanto, mantenendo i filtri impostati di default, l'utente ricerca sia le trasmissioni che sono state effettuate a lui come utente sia quelle che sono state effettuate al ruolo corrente con il quale l'utente sta effettuando la ricerca e notificate all'utente stesso.
Il menu a tendina da cui è possibile selezionare il nominativo dell'utente che ha ricevuto la notifica, oltre al nome di tutti gli utenti del ruolo, presenta anche le voci:

- "<<qualsiasi utente>>" : se selezionata permette di ricercare le trasmissioni effettuate al ruolo indipendentemente dagli utenti a cui sia stata data la notifica;
- "<<gli altri utenti>>": se selezionata vengono ricercate le trasmissioni effettuate al ruolo e per le quali sia stata data notifica ad utenti diversi rispetto all'utente che sta effettuando la ricerca.
  Questa voce compare solamente se il ruolo selezionato coincide con il ruolo corrente dell'utente che sta effettuando la ricerca.

Se il campo "Notificata a " viene valorizzato con il nome di un utente, vengono ricercate le trasmissioni effettuare al ruolo specificato e per le quali sia stata data notifica all'utente selezionato, indipendentemente dalle notifiche date eventualmente anche ad altri utenti del ruolo.

Se si lascia selezionata la sola casella "Utente" (togliendo la spunta alla casella "Ruolo"), si ricercano esclusivamente le trasmissioni che abbiano come destinatario personalmente l'utente che sta effettuando la ricerca.

Selezionando la casella "Ruolo" e valorizzando il campo corrispondente si ha anche la possibilità di visualizzare le trasmissioni ricevute dai ruoli sottoposti al ruolo impostato aggiungendo una spunta nella casella "Visualizza trasmissioni sottoposti". La selezione del ruolo può avvenire indicandone il codice o tramite ricerca nella rubrica (si veda par. 4.5.4).

Togliendo la spunta della selezione alla casella "Ruolo", i campi corrispondenti (codice, descrizione, notificata a) risultano disabilitati.
In questo caso inoltre, se si seleziona la casella "Visualizza trasmissioni sottoposti", si ricercano le trasmissioni ricevute dai soli ruoli sottoposti al ruolo corrente dell'utente che sta effettuando la ricerca.

Almeno una delle tre opzioni "Utente", "Ruolo", "Visualizza trasmissioni sottoposti" deve essere selezionata per poter effettuare la ricerca.

3.3.2 Trasmissioni effettuate

E' ottenibile selezionando l'opzione 'Effettuate' come mostrato in Figura 219.
Il funzionamento della sezione 'Completa' è quasi del tutto analogo a quanto illustrato nel paragrafo precedente. Si differenzia solo per la parte riguardante i solleciti delle trasmissioni. Tale funzionalità è stata implementata per effettuare più velocemente il sollecito (quindi la ritrasmissione) di una o più trasmissioni effettuate e di cui non si è avuta ancora nessuna risposta o risultato. Come si può vedere nella Figura 219, è possibile selezionare una o più trasmissioni e quindi effettuare il sollecito attraverso il pulsante Sollecita selezionati; in alternativa, se si è interessati ad effettuare il sollecito per tutte le trasmissioni si può selezionare direttamente il pulsante Sollecita tutti.

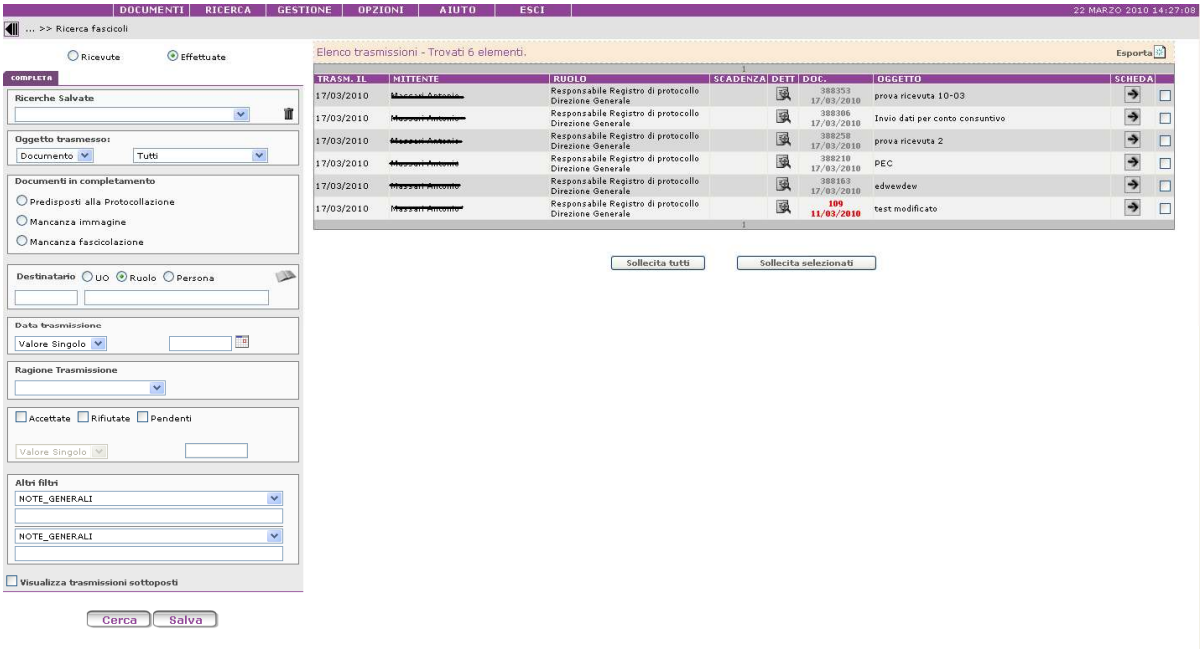


Figura 219 - Ricerca trasmissioni effettuate

Nella ricerca delle trasmissioni effettuate è presente il campo “Mittente trasmissione” che funziona in modo analogo a quanto visto per il “Destinatario trasmissione” nella ricerca delle trasmissioni ricevute.
In particolare si ha la possibilità di selezionare la casella “Ruolo” (per default la casella risulta già selezionata e i campi corrispondenti sono valorizzati con il ruolo corrente e l’utente che sta effettuando la ricerca); è possibile selezionare anche la casella “Visualizza trasmissioni sottoposti”: nel caso sia selezionato e valorizzato anche il campo ruolo, si ricercano in tal modo sia le trasmissioni effettuate dal ruolo impostato sia quelle effettuate dai ruoli ad esso sottoposti; se invece la casella ruolo non è selezionata, la sola selezione della casella “Visualizza trasmissioni sottoposti” consente di ricercare le trasmissioni effettuate dai ruoli gerarchicamente sottoposti al ruolo corrente dell’utente che sta effettuando la ricerca. La selezione del ruolo può avvenire indicandone il codice o tramite ricerca nella rubrica (si veda par. 4.5.4).

Un insieme di criteri di ricerca è memorizzabile selezionando il pulsante “Salva”: ciò permetterà il rapido riutilizzo dei parametri ogni qualvolta se ne presenti la necessità. L’utente può decidere di condividere con tutti i componenti del ruolo la ricerca salvata oppure di renderla disponibile solo a se stesso. Se sono state utilizzate le ricerche personalizzate (3.1.1.2), vengono salvate anche le scelte effettuate.

Se l’Amministrazione è abilitata alla gestione dei documenti repertoriati, nella griglia dei risultati della ricerca delle trasmissioni ricevute/effettuate sarà presente la nuova colonna ‘Repertorio’ in cui sarà possibile visualizzare la segnatura di repertorio dei documenti repertoriati, come mostrato nella seguente figura.

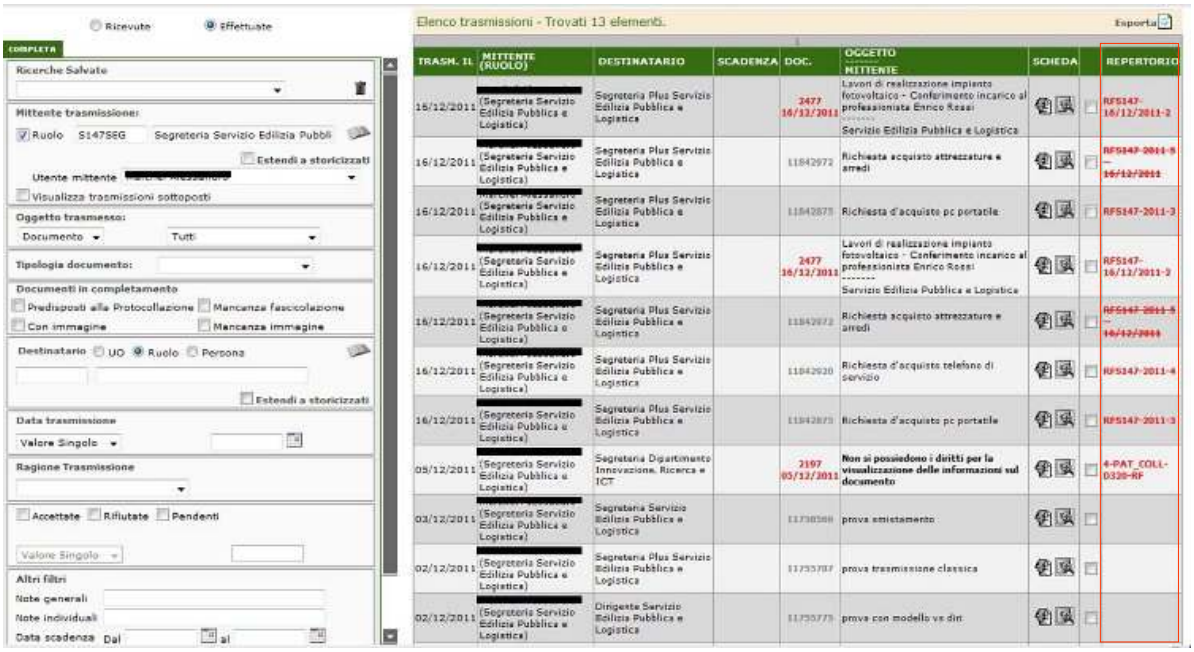


Figura 220 - *Segnatura di repertorio nella ricerca trasmissioni*

3.4 Ricerca Visibilità

La funzione “Ricerca Visibilità” è ottenibile a partire dalla barra di navigazione del pannello principale selezionando la voce del menu RICERCA, premendo sul pulsante “RICERCA” e successivamente sul pulsante VISIBILITA’.
Il sistema visualizza una finestra di dialogo che riporta la tipologia di documenti per i quali si sta ricercando la visibilità:

- **protocollati:** alla selezione di questa tipologia il sistema propone i seguenti capi di ricerca:
  - **Menu a tendina da cui è possibile selezionare il registro**: il sistema visualizza la lista dei registri con cui l’utente può operare o su cui ha visibilità (il documento cercato è comunque protocollato da altre strutture ma su registri visibili dall’operatore); VTDOCS imposta automaticamente il registro predefinito;
  - **Anno di protocollo:** è impostato automaticamente all’anno corrente. Naturalmente è modificabile in base alle esigenze dell’utente;
  - **Numero di protocollo:** si inserisce il numero di protocollo relativo al documento di cui si vuole conoscere la visibilità.
- **non protocollati:** alla selezione di questa voce il sistema propone il campo ID documento per eseguire la ricerca;
- **tipologia documento**: alla selezione di questa voce il sistema propone una lista a tendina dalla quale selezionare il tipo documento desiderato.

A questo punto, il sistema restituisce una finestra che indica la visibilità corrente. Tale finestra è la stessa che si ottiene richiedendo la visibilità di un documento di cui si ha l’accesso.
Tale funzionalità permette una maggiore flessibilità perché non limita l’informazione al solo utente proprietario, ma dà la possibilità di rivolgersi a chiunque abbia in qualche modo visibilità sul documento.

3.5 Ricerca Area di lavoro documenti e Area di lavoro fascicoli

L'Area di Lavoro (ADL) è uno spazio di memoria persistente associato a ciascuna coppia <utente, ruolo>. In una ADL è possibile inserire dei "collegamenti" a documenti (ADL Documenti) e a fascicoli (ADL Fascicoli).
Ciascun utente ha la possibilità di gestire la propria Area di Lavoro ed utilizzarla come modalità di accesso rapido agli oggetti ivi memorizzati.
Le funzionalità associate all'Area di Lavoro (AdL) per i Documenti e i Fascicoli sono accessibili a partire dalla barra di navigazione del pannello principale selezionando la voce del menu RICERCA e successivamente quella "ADL Doc.", per i documenti, oppure "ADL Fasc." per i fascicoli
L'ambiente dell'Area di Lavoro è del tutto analogo agli ambienti di ricerca dei documenti e dei fascicoli e si differenzia da questi ultimi solo per l'immediata visualizzazione dei documenti e dei fascicoli presenti in quest'area al momento dell'accesso.

3.5.1 Area di Lavoro documenti

Selezionando dal menu principale il pulsante "RICERCA" e successivamente quello "ADL Doc." si visualizzano i documenti presenti nell'AdL.
Per distinguerlo dall'analogo ambiente relativo alle ricerche dei documenti, l'intestazione dell'elenco dei documenti è "AREA DI LAVORO" con le stesse icone visualizzate per la ricerca dei documenti.

La lista dei documenti presenti nell'AdL riporta le seguenti informazioni:

- **Doc.**: il numero del documento e la data di creazione;
- **Registro**: per i documenti protocollati, il registro su cui è stato protocollato il documento;
- **Tipo:** per i documenti protocollati, l'indicazione del tipo di protocollo: A = in Arrivo, P = in Partenza;
- **Oggetto**: oggetto del documento;
- **Mitt/dest**: per i documenti protocollati, il mittente/i destinatari del documento;
- **Dett**:contiene le seguenti icone:
  - ✓  permette la visualizzazione del dettaglio dei documenti;
  - ✓  consente di eliminare dall'area di lavoro il documento a cui è associato;
  - ✓  inserisce il documento associato nell'area di conservazione.

Il nuovo ambiente per l'Area di Lavoro estende a quest'ultima le capacità di ricerca offerti dalla funzione "RICERCA/Documenti". in particolare, l'utente ha la possibilità di effettuare una ricerca sui documenti presenti in AdL attraverso i seguenti ambienti:

- Veloce;
- Estesa;
- Completa;
- Complet.to;.

Gli ambienti di ricerca ed il funzionamento relativo sono del tutto analoghi al normale ambiente di ricerca dei documenti e dei fascicoli. Si rimanda pertanto al paragrafo 3.1.2 - Tipologie di Ricerca e ai relativi sottoparagrafi.

3.5.2 Area di Lavoro fascicoli

La funzionalità di Area di lavoro Fascicoli è ottenibile a partire dalla barra di navigazione del pannello principale selezionando la voce del menu RICERCA e successivamente “ADL Fasc.”.
Nella parte destra del pannello l’applicativo visualizza immediatamente i fascicoli presenti nell’ADL.
Sopra l’elenco dei fascicoli presenti in AdL è presente l’icona che permette l’esportazione della lista dei fascicoli visualizzati su file di formato Pdf o Excel.

Per i fascicoli presenti nell’elenco dell’AdL sono riportate le seguenti informazioni:

- **TIPO**: G (se il fascicolo è generale) o P (se il fascicolo è procedimentale);
- **CODCLASS**: codice di classificazione del fascicolo;
- **CODICE**: codice del fascicolo;
- **DESCRIZIONE**: descrizione del fascicolo;
- **APERTURA**: la data in cui è stato creato il fascicolo;
- **CHIUSURA**: data in cui è stato chiuso il fascicolo; se il fascicolo è aperto questo campo e vuoto;
- **DETT**: riporta l’icona , che permette la visualizzazione del dettaglio del fascicolo;
- **ADL**: riporta l’icona , che permette l’eliminazione del singolo fascicolo dall’area di lavoro.

L’ambiente per l’Area di Lavoro estende a quest’ultima le capacità di ricerca offerte dalla funzione “RICERCA/Fascicoli”. L’utente ha la possibilità di effettuare una ricerca sui fascicoli presenti in AdL in maniera del tutto analoga alla normale ricerca dei fascicoli, alla quale si rimanda per la descrizione dell’operatività.

3.6 Ricerca campi comuni

La funzione “Ricerca Campi Comuni” attivabile dalla voce di menu: RICERCA → Ric. Campi Comuni, consente di effettuare delle ricerche su documenti e fascicoli utilizzando i campi comuni definiti ed utilizzati nel sistema.

Figura 221 - Voce di menu “Ricerca campi comuni”

Selezionando la voce “Ric. Campi Comuni” viene aperta una nuova pagina di ricerca, in cui sarà possibile inserire come filtri i campi comuni rispettivamente di documenti e fascicoli visualizzati in due diverse sezioni. Impostando i criteri e cliccando sul pulsante Ricerca, nella parte destra della pagina verrà mostrato l’elenco dei documenti e dei fascicoli che soddisfano i criteri impostati.

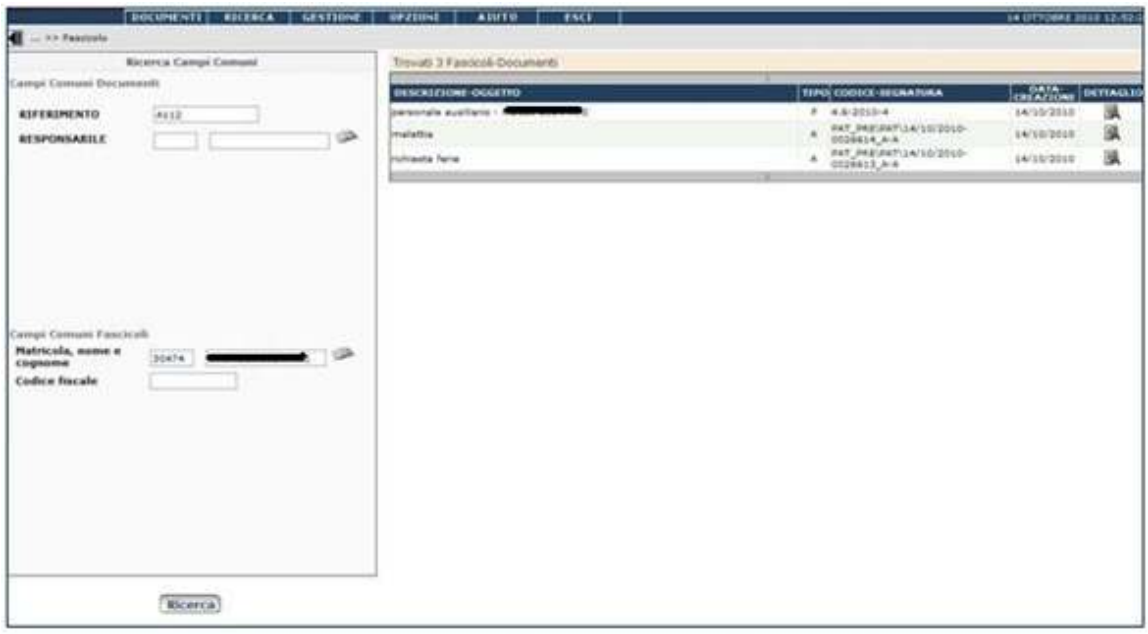


Figura 222 - Ricerca campi comuni

3.7 Importa fascicoli

La funzione “Importa fascicoli” attivabile dalla voce di menu: **RICERCA → Imp. Fascicoli**, consente di creare in modo rapido un numero elevato di fascicoli procedimentali.

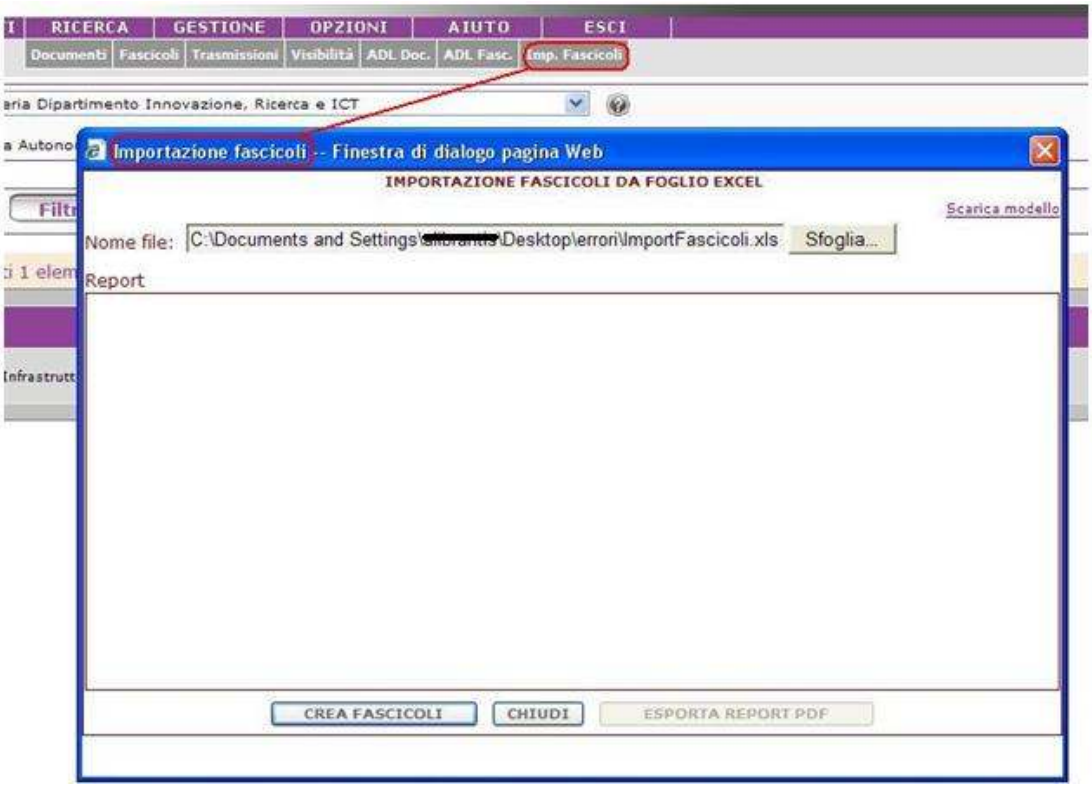


Figura 223 – Import fascicoli

La procedura di import fa uso di un particolare foglio excel opportunamente strutturato. Il modello da utilizzare può essere scaricato tramite il link *Scarica modello* presente nella pagina di Figura 223.
Dopo aver compilato il foglio excel con i dati dei fascicoli da creare, se ne specifica il percorso sul file system nel campo *Nome file* e si avvia la procedura di import cliccando sul pulsante CREA FASCICOLI.
Dopo aver verificato la validità dei dati, il sistema avvierà la procedura di importazione e alla fine verrà mostrato l'esito dell'operazione e il numero dei fascicoli importati, di quelli scartati, di eventuali errori o warning. Sarà poi possibile esportare il risultato dell'operazione in un file pdf cliccando il pulsante ESPORTA REPORT PDF. Il pulsante CHIUDI consente di chiudere la pagina.

4 GESTIONE

4.1 Registri

La funzione di gestione dei registri consente, a partire dal pannello proposto in Figura 224, di effettuare alcune operazioni sui registri visibili all'utente. Le operazioni di gestione del registro sono disponibili soltanto per gli utenti opportunamente abilitati. L'icona dettaglio permette di visualizzare tutti i dati relativi a quel registro: descrizione, e-mail associata, data apertura, data chiusura, data dell'ultimo protocollo e prossimo numero di protocollo.
Nel caso in cui l'amministrazione sia abilitata alla gestione multicasella ed il ruolo dell'utente connesso sia abilitato alla consultazione di più di una casella di posta fra quelle associate al Registro/RF selezionato, tramite opportuno menu a tendina l'utente può scegliere quale casella di posta consultare (Figura 224).
Per ogni registro selezionato le funzioni disponibili sono le seguenti:

- **Cambia stato**: consente di cambiare lo stato del registro, ovvero di chiudere un registro aperto o di aprirne uno chiuso;
- **Casella Ist/Ie**: interroga la casella di posta istituzionale relativa al registro; i messaggi di posta elettronica presenti nella casella istituzionale, in arrivo o in partenza, sono elaborati;
- **Stampa**: consente di stampare il registro di protocollo selezionato. La stampa del registro include tutti i documenti protocollati successivamente all'ultima stampa effettuata e tutti i documenti protocollati che successivamente all'ultima stampa effettuata sono stati modificati o annullati. Il formato stampa registro contiene anche l'indicazione del numero degli allegati e se il documento è stato protocollato in emergenza. La segnatura di emergenza compare sulla stampa stessa nella stessa colonna del numero di protocollo.
- **Modifica**: consente all'utente amministratore di modificare i dati di dettaglio del registro.

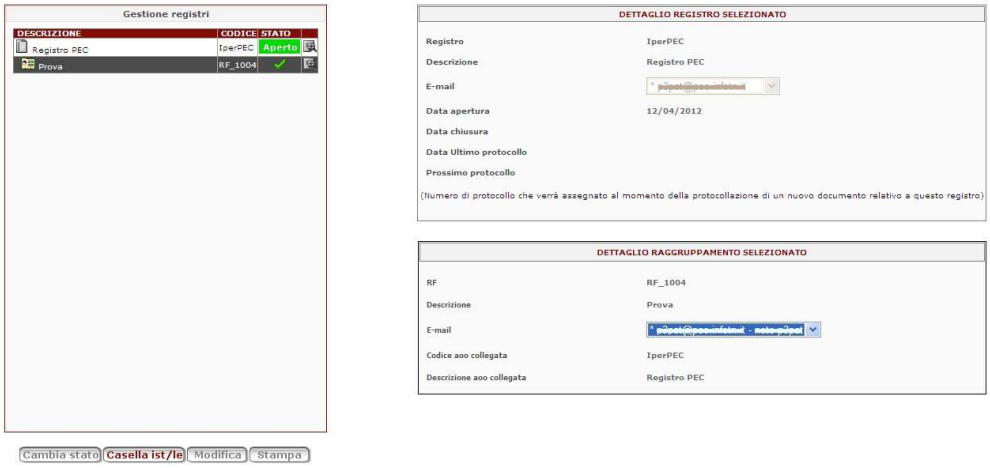


Figura 224 - Gestione registri

4.1.1 Interrogazione casella istituzionale

All'atto dell'interrogazione della casella istituzionale, il sistema avvia lo scarico dei messaggi pervenuti sulla casella e contestualmente richiama il servizio esterno di verifica[11] del formato. Questo accerta che il formato del file sia conforme alla sua estensione e rispetto ai formati ammessi per la gestione documentale.
In caso di esito positivo della verifica di conformità, il sistema crea tanti documenti predisposti alla protocollazione quanti sono i messaggi ricevuti e associa ai documenti stessi i rispettivi file; in caso di esito negativo – formato del file non valido o corrotto - il sistema restituisce un avviso e non elabora il messaggio di posta.

Una volta terminata l'operazione di controllo della casella istituzionale, la maschera relativa all'esito del controllo della casella istituzionale mostra due riquadri:

1. il primo riporta il riepilogo dell'interrogazione, che contiene la tipologia di documenti elaborati e la numerosità dichiarando l'esito delle singole elaborazioni effettuate. È possibile applicare dei filtri a tale report selezionando uno dei valori numerici presenti nella griglia posta in alto

[11] Tale verifica fa parte delle funzionalità relative alla conservazione dei documenti e deve essere opportunamente abilitate tramite intrefaccia di amministrazione

2. il secondo contiene la tipologia del documento, il mittente, l'oggetto, la data di invio, il numero degli allegati,e l'esito del controllo del messaggio.

L'esito del controllo sarà "OK. Eccezione non bloccante nella segnatura informatica" (Figura 225) nei seguenti casi:

- eccezione relativa alla verifica della descrizione del destinatario
- eccezione relativa alla verifica della struttura del documento
- eccezione relativa alla conformità della segnatura informatica alla DTD

Il mittente del documento riceverà quindi una ricevuta di eccezione che illustra il problema riscontrato ma avvisa che non è necessario rispedire il documento inviato. In questo caso, inoltre:

- il documento viene inserito nel sistema con mezzo di spedizione MAIL (e non INTEROPERABILITÀ)
- di conseguenza, il mittente non riceverà alcuna ricevuta di conferma della protocollazione del documento predisposto.

Figura 225 - Interrogazione casella istituzionale – Esempio eccezione non bloccante

L'utente, tramite il pulsante Esporta (Figura 226), ha la possibilità di esportare in locale in formato PDF, Excel o Open Office l'esito del controllo della casella istituzionale; il titolo del documento da esportare presenta le indicazioni relative all'utente che ha effettuato il controllo, la struttura a cui è associata la casella interrogata, data e ora del controllo.

Nella maschera relativa all'esito di controllo casella istituzionale è presente il pulsante Crea doc (Figura 226) che consente all'utente di inserire nel sistema un documento non protocollato avente come immagine il PDF del report complessivo dell'interrogazione e nell'oggetto l'indicazione dell'utente che ha effettuato il controllo, la struttura a cui è associata la casella interrogata, data e ora del controllo. Tale documento ha come proprietario l'utente che ne ha richiesto la creazione e segue le regole standard di visibilità.
Si evidenzia, infine, che nel caso in cui nell'elaborazione sia presente una ricevuta di eccezione, di errore nella spedizione o di mancata elaborazione (relativa ad una precedente spedizione), il sistema crea in automatico il documento non protocollato relativo al controllo effettuato. La creazione automatica del report viene notificata mediante trasmissione nell'elenco delle cose da fare dell'utente che ha effettuato il controllo della casella istituzionale. Nel caso di rilevazione di eccezioni non bloccanti, il report non viene creato in automatico.

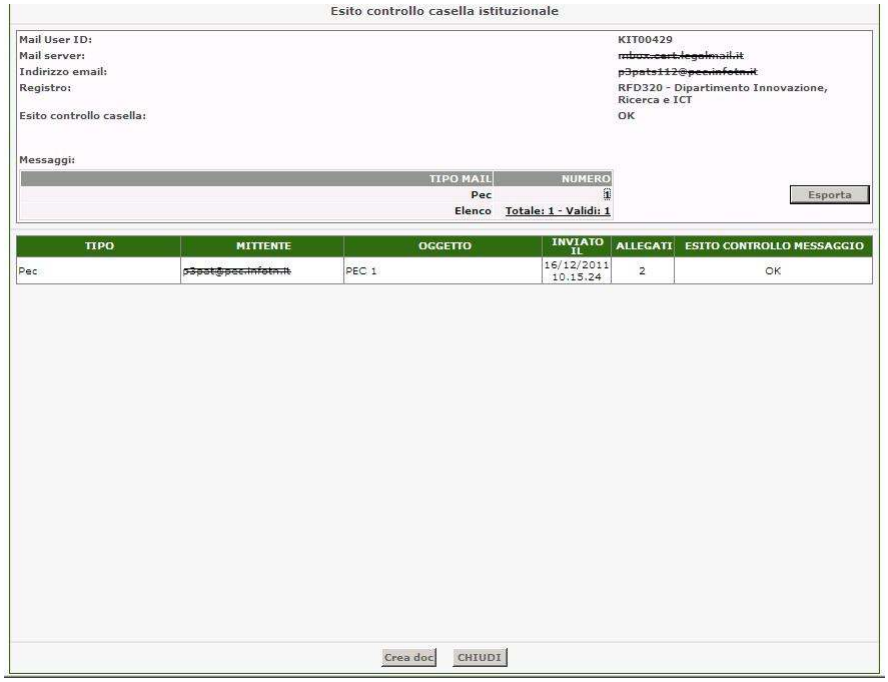


Figura 226 - Interrogazione casella istituzionale – Esempio esito positivo

4.2 Gestione registri di repertorio

Se l'Amministrazione è abilitata alla gestione dei documenti repertoriati e se è stato configurato il ruolo di Responsabile delle stampe di repertorio, quest'ultimo dal menù 'Gestione', selezionando la voce 'Reg. repertorio' può visualizzare l'elenco dei registri di repertorio per cui è Responsabile delle stampe.

Per il registro di repertorio selezionato (tramite il pulsante) sono disponibili le seguenti funzionalità:

- **Cambia stato**: consente di cambiare lo stato del registro, ovvero di chiudere un registro aperto o di aprirne uno chiuso;
- **Stampa**: consente di stampare il registro di repertorio selezionato. La stampa del registro include tutti i nuovi documenti repertoriati su quel particolare registro ed i documenti repertoriati che hanno subito modifiche al campo oggetto o ai campi storicizzati o che sono stati annullati, dall'ultima stampa fino al momento in cui viene effettuata la stampa.

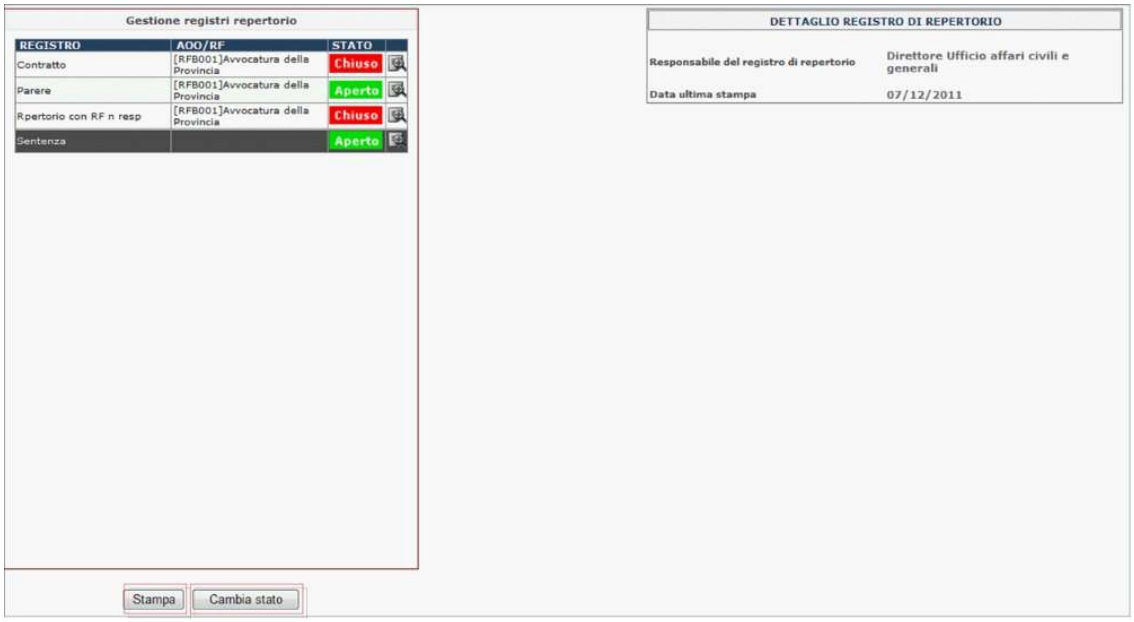


Figura 227 - Stampa manuale del registro di repertorio

4.3 Gestione stampe e rapporti

Sono disponibili i seguenti report:

- **Stampa titolario**: consente di visualizzare il titolario appartenente al registro in esame;
- **Stampa corrispondenti esterni**: consente di visualizzare i corrispondenti esterni;
- **Stampa trasmissioni UO**: consente di visualizzare un elenco di trasmissioni documenti o fascicoli effettuate e ricevute dalla struttura di appartenenza. Riporta le informazioni seguenti: Id del documento, data di trasmissione, oggetto del documento, l'utente Mittente, il Ruolo Mittente, il Destinatario, la ragione di trasmissione e le note generali;
- **Stampa Documenti Registro**: consente di visualizzare un elenco delle stampe documenti registri effettuate. Il sistema permette di selezionare l'elenco delle stampe di interesse attraverso differenti parametri: si può valorizzare un determinato numero di protocollo o un intervallo di numeri; una data o un intervallo di date di protocollo; una certa Unità Organizzativa, il cui valore è editabile o manualmente tramite codice o selezionando il valore desiderato dalla rubrica, a cui si accede attraverso l'icona ; una spunta nell'apposita casella di selezione consente di estendere la selezione alle UO sottoposte; è possibile infine selezionare per tipologia documento.
- **Stampa Documenti**: consente di stampare tutti i documenti non protocollati di un'amministrazione; per generare la stampa è sufficiente utilizzare i filtri su data creazione, id documento e tipologia se associata.
- **Stampa buste**: consente di visualizzare tutti i destinatari (compresi quelli in cc) dei protocolli in uscita che soddisfano i criteri di ricerca. I parametri di ricerca sono anno, numero protocollo e data di protocollazione;
- **Stampa Fascette Fascicolo**: consente di visualizzare la stampa della fascetta del fascicolo questo rispetto ad un determinato Codice Fascicolo.

La stampa di ciascuna voce sopra indicata fornisce l'output in una nuova finestra di dialogo.
Le stampe dei corrispondenti riportano le seguenti informazioni:

- **Tipo**: indica se si tratta di una UO o di un utente,
- **Codice**: il codice associato al corrispondente,
- **Descrizione**: la descrizione del corrispondente,
- **E-mail**: l'indirizzo di posta elettronica del corrispondente,
- **I/E**: indica se il corrispondente è interno o esterno.

4.4 Prospetti riepilogativi

Tali prospetti sono stati sviluppati per poter far avere all'utente, in maniera chiara e sintetica, una visione statistica e globale dell'andamento della lavorazione della documentazione. Per documentazione redatta si intende: documenti Grigi, protocolli, fascicoli, trasmissioni. Tali documenti sono redatti in base a parametri e filtri, che andremo ad indicare nel dettaglio qui di seguito.

I prospetti a disposizione dell'utente sono:

- **Report annuale sui documenti,** che effettua il filtro rispetto ai seguenti parametri (quelli contrassegnati dall'asterisco sono obbligatori):
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;
  - Sede: per le amministrazioni in cui vi sono più sedi è selezionabile la sede di appartenenza, o la sede di interesse, rispetto al prospetto che si vuole effettuare;
  - Anno*: selezionabile mediante menu a tendina;
  - Mese: selezionabile mediante menu a tendina.
- **Report annuale sui documenti per sede**
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;
  - Anno*: selezionabile mediante menu a tendina.
- **Report annuale sui documenti protocollati per Unità Organizzativa**
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;
  - Anno*: selezionabile mediante menu a tendina.
- **Report sui documenti classificati**
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;
  - Titolario*: selezionabile dall'utente mediante un menu a tendina;
  - Sede: per le amministrazioni in cui vi sono più sedi è selezionabile la sede di appartenenza, o la sede di interesse, rispetto al prospetto che si vuole effettuare;
  - Anno*: si sceglie l'anno di interesse mediante menu a tendina;
  - Modalità: compatta o estesa; nel primo caso il report mostra solo il 1° livello del titolari di classificazione; nel secondo caso produce il report con il dettaglio di tutti i livelli.
- **Report annuale sui documenti trasmessi ad altre amministrazioni**
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;

- Anno*: si sceglie mediante menu a tendina l'anno di interesse.

- **Report annuale sui fascicoli su titolario attivo**
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;
  - Anno*: si sceglie l'anno di interesse mediante menu a tendina;
  - Mese: selezionabile mediante menu a tendina.
- **Report annuale sui fascicoli per voce di titolario**
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;
  - Titolario*: selezionabile dall'utente mediante un menu a tendina;
  - Anno*: si sceglie l'anno di interesse mediante menu a tendina;
  - Modalità: compatta o estesa; nel primo caso il report mostra solo il 1° livello del titolari di classificazione; nel secondo caso produce il report con il dettaglio di tutti i livelli.
- **Tempi medi di lavorazione fascicoli**
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;
  - Titolario*: selezionabile dall'utente mediante un menu a tendina;
  - Sede: per le amministrazioni in cui vi sono più sedi è selezionabile la sede di appartenenza, o la sede di interesse, rispetto al prospetto che si vuole effettuare;
  - Anno*: si sceglie l'anno di interesse mediante menu a tendina;
  - Modalità: compatta o estesa; nel primo caso il report mostra solo il 1° livello del titolari di classificazione; nel secondo caso produce il report con il dettaglio di tutti i livelli.
- **Report contatori documento**
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;
  - Anno*: si sceglie l'anno di interesse mediante menu a tendina;
- **Report contatori fascicolo**
  - Amministrazione*: Nome amministrazione di competenza dell'utente che sta richiedendo il prospetto. Tale valore viene inserito in automatico dal sistema;
  - Registro*: selezionabile dall'utente mediante un menu a tendina;
  - Anno*: si sceglie l'anno di interesse mediante menu a tendina;
- **Report conteggio fascicoli procedimentali**
  - Proprietario*: permette di indicare una UO o un RF. Il report conterrerrà i fascicoli appartenenti a tutti i ruoli che fanno riferimento alla UO o al RF selezionato. Nel primo caso è possibile effettuare il conteggio anche sui fascicoli creati dalle UO sottoposte selezionando la voce 'sottoposti';
  - Data creazione: può essere indicato un giorno o un intervallo di date e rappresenta la data di creazione dei fascicoli procedimentali;
  - Data chiusura: può essere indicato un giorno o un intervallo di date e rappresenta la data di chiusura dei fascicoli;
  - Titolario*: possono essere considerati i fascicoli presenti su tutti i titolari dell'amministrazione, oppure di uno specifico titolario (attivo o storicizzato);

  Questo report può essere effettuato solo dai ruoli abilitati.
- **Report fascicoli procedimentali e documenti contenuti**

- Proprietario*: permette di indicare una UO o un RF. Il report conterrerrà i fascicoli appartenenti a tutti i ruoli che fanno riferimento alla UO o al RF selezionato. Nel primo caso è possibile effettuare il conteggio anche sui fascicoli creati dalle UO sottoposte selezionando la voce 'sottoposti';
- Data creazione: può essere indicato un giorno o un intervallo di date e rappresenta la data di creazione dei fascicoli procedimentali;
- Data chiusura: può essere indicato un giorno o un intervallo di date e rappresenta la data di chiusura dei fascicoli;
- Titolario*: possono essere considerati i fascicoli presenti su tutti i titolari dell'amministrazione, oppure di uno specifico titolario (attivo o storicizzato);

Questo report può essere effettuato solo dai ruoli abilitati.

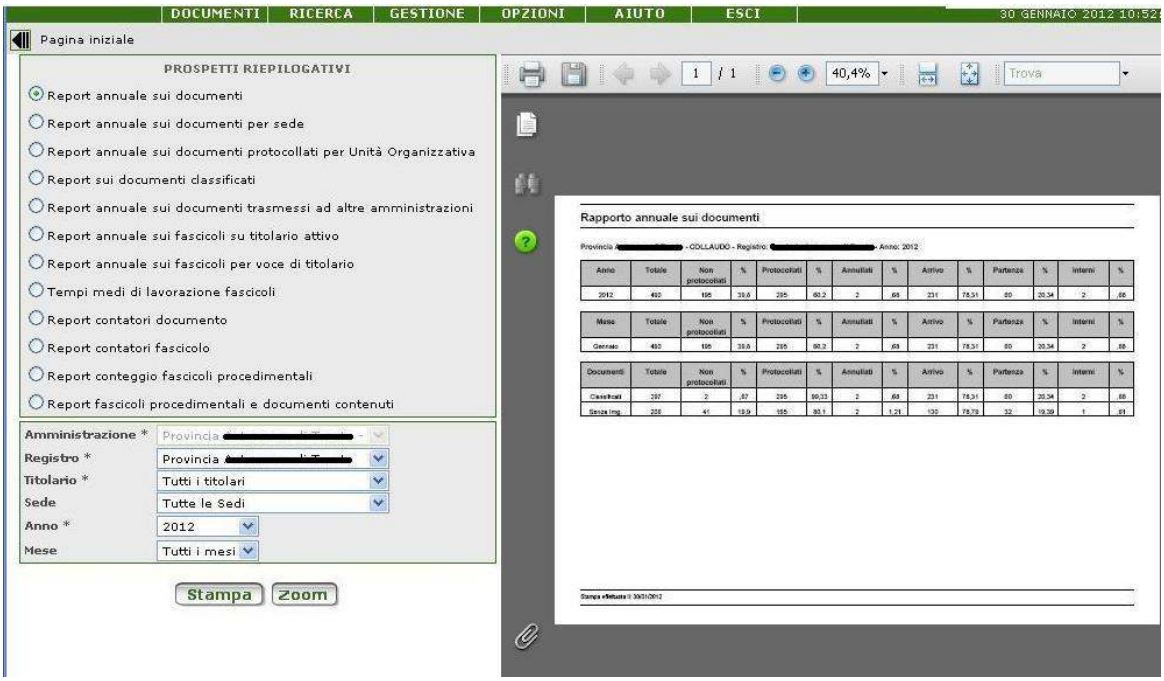


Figura 228 - Prospetti Riepilogativi (es. report annuale sui documenti)

4.5 Gestione Rubrica

La funzione di gestione della rubrica consente, a partire dalla finestra presente nella Figura 229, di effettuare alcune operazioni sui soli corrispondenti esterni all'amministrazione. Le operazioni di gestione della rubrica sono disponibili soltanto per gli utenti opportunamente abilitati. Esse sono:

- **Inserimento:** consente all'utente abilitato di inserire nuovi corrispondenti
- **Modifica**: consente all'utente abilitato di modificare i dati di dettaglio del corrispondente.
- **Cancellazione**: consente all'utente abilitato di cancellare il corrispondente dalla rubrica o di disabilitarlo, nel caso in cui risultasse mittente o destinatario di qualche documento.

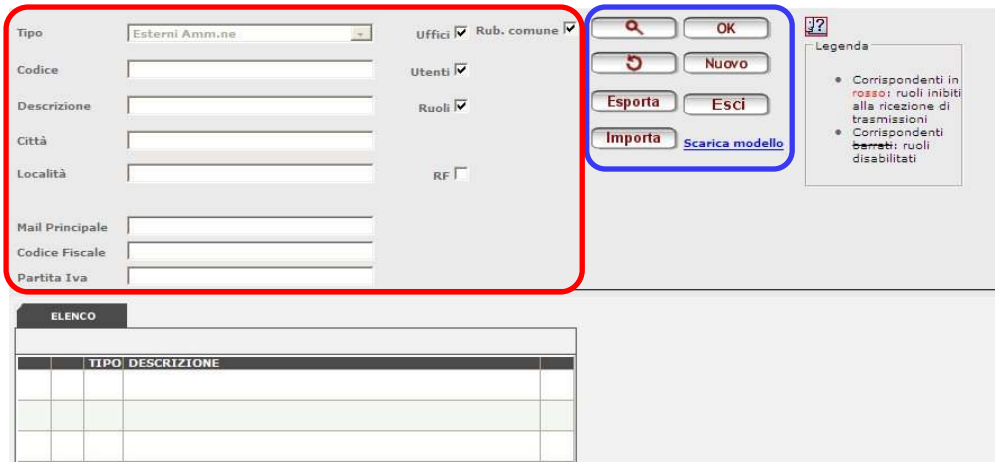


Figura 229 - Gestione rubrica: pagina di ricerca del corrispondente

Dopo aver ricercato il corrispondente con le usuali operazioni presenti nella rubrica (si veda Figura 229 sezione evidenziata in blu), selezionando l'icona posta accanto al corrispondente ricercato, si visualizzano i dati di dettaglio (Figura 230). Da questa schermata si possono effettuare le operazioni di Modifica e/o di Cancellazione. L'icona presente in alto sulla parte destra della pagina, consente di rendere i campi editabili e quindi di modificarli, a meno del codice rubrica che non può essere modificato.

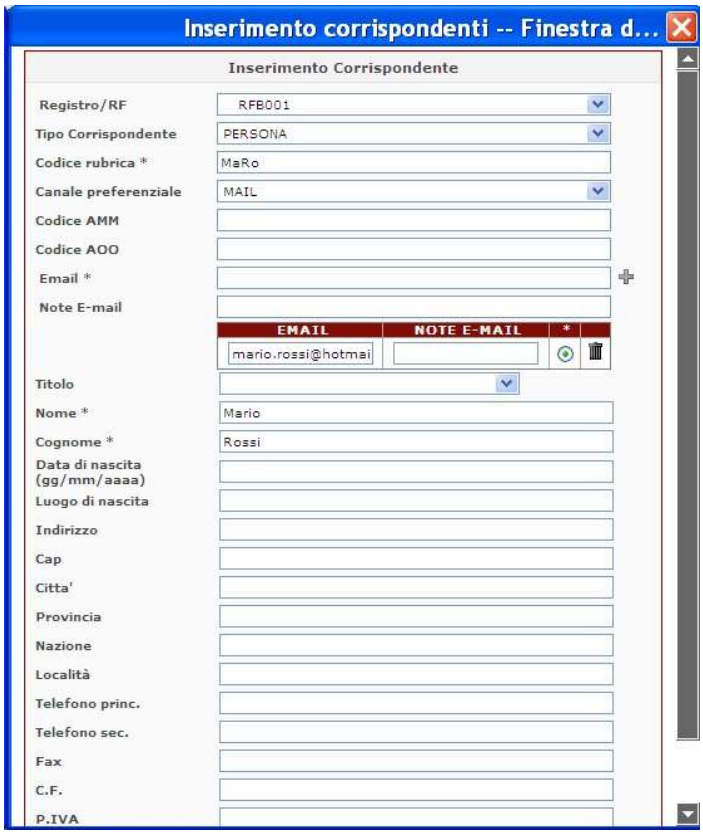


Figura 230 - Gestione rubrica: pagina di dettaglio e di modifica/cancellazione del corrispondente

La rubrica, presente nel sistema di protocollo informatico, consente di ricercare sia i corrispondenti interni/esterni ad una determinata Area Organizzativa Omogenea, sia quelli esterni all'Amministrazione corrente. La ricerca può essere effettuata utilizzando dei filtri che sono presenti nella parte alta della pagina, come mostrato nella Figura 229 e dettagliato nel paragrafo 4.5.2.

L'aspetto grafico della rubrica è uguale in tutte le parti del sistema, la differenza è nel filtraggio dei dati a seconda del contesto da cui essa è richiamata. Ad esempio, nella pagina delle trasmissioni di un protocollo la rubrica consente solamente la ricerca di corrispondenti interni alla AOO (ovvero al registro su cui il documento è stato protocollato), disabilitando il menu relativo al tipo corrispondente; mentre nella selezione del mittente per il protocollo in ingresso o del destinatario per il protocollo in uscita, è possibile specificare qualsiasi tipologia di corrispondenti (sia interni, sia esterni, sia interni/esterni).

Per aprire la rubrica è sufficiente selezionare l'icona  , dove presente, nelle pagine di VTDOCS.
La rubrica presenta una sezione superiore la cui parte sinistra contiene i campi valorizzabili con i parametri che si intende utilizzare come filtri per la ricerca; la parte destra propone invece una serie di pulsanti che consentono di dare avvio alla ricerca, di gestire le funzionalità di inserimento di nuovi corrispondenti, o di uscire dalla rubrica stessa (pulsanti evidenziati da un rettangolo di colore blu).
La sezione inferiore è suddivisa in due parti: in quella di sinistra compare l'elenco dei risultati della ricerca o eventualmente la porzione di organigramma in cui è inserito il corrispondente che è stato ricercato; quella di destra per inserire in VTDOCS il/i corrispondente/i (a seconda che sia un mittente o uno/più destinatari) selezionato/i dall'elenco dei risultati di ricerca.
Sono disponibili diversi diritti funzionali che abilitano i ruoli all'inserimento nella rubrica dei corrispondenti esterni:

- abilitazione inserimento rubrica su Registro;
- abilitazione inserimento rubrica su RF;
- abilitazione inserimento rubrica su Amministrazione.

4.5.1 Rubrica comune per corrispondenti esterni

E' possibile creare rubriche comuni a diverse amministrazioni. Questa tipologia di rubrica contiene i corrispondenti esterni che possono essere così condivisi da AOO di diverse amministrazioni. La rubrica comune può essere importata attraverso un foglio excel. È possibile pubblicare una UO interna ad una specifica amministrazione nella rubrica comune. La rubrica comune è attivabile attraverso un parametro di configurazione.

4.5.2 Filtri di ricerca

La ricerca di corrispondenti in rubrica può essere filtrata mediante l'uso di campi di testo, campi di opzione e selezione, consentendo sia la velocizzazione dell'operazione stessa sia una più facile individuazione del/dei corrispondente/i ricercato/i. La figura successiva riporta il dettaglio della sezione di ricerca.

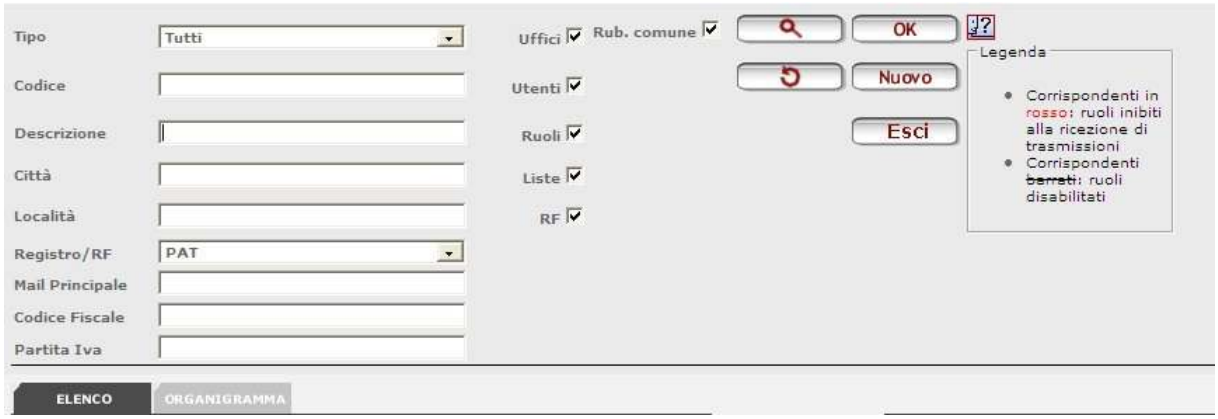


Figura 231 – Filtri di ricerca

4.5.2.1 Codice, Descrizione, Città, Località, Mail Principale

I campi da popolare per eseguire una ricerca sono:

- Codice: il codice univoco associato al corrispondente nella rubrica;
- Descrizione: completa o parziale della descrizione del corrispondente;
- Città: la città indicata al momento dell'inserimento del corrispondente in rubrica (se esterno) o dell'utente (se interno), inserito nell'applicazione di amministrazione
- Località: la località indicata al momento dell'inserimento del corrispondente in rubrica (se esterno)
- Mail principale: indirizzo di posta elettronica (o parte di esso) associato al corrispondente. In caso di corrispondente multicasella la ricerca viene effettuata per mail principale.
- Codice Fiscale: codice fiscale (o parte di esso) associato al corrispondente (di tipo UO o Persona). Il filtro di ricerca inserito deve avere una lunghezza minima di quatrro caratteri
- Partita Iva: numero di partita IVA (o parte di esso) associato al corrispondente (di tipo UO o Persona). Il filtro di ricerca inserito deve avere una lunghezza minima di quatrro caratteri

I risultati forniti dalla ricerca saranno quei corrispondenti che soddisfano tutti i criteri di ricerca specificati.

4.5.2.2 Uffici, Utenti, Ruoli, Rubrica comune

I campi di opzione filtrano il tipo di corrispondente da ricercare, in particolare:

- Uffici: consente di ricercare tutte le Unità Organizzative;
- Utenti: consente di trovare tutti gli utenti;
- Ruoli: consente di ricercare tutti i ruoli presenti in organigramma;
- Rubrica comune: consente di ricercare tutti i corrispondenti presenti nella rubrica comune.
- RF (se configurati): se selezionato, consente di cercare un RF[12] in base ai criteri di ricerca indicati.

4.5.2.3 Tipo corrispondente

Uno dei principali dati da specificare per la ricerca è il tipo corrispondente. Le voci selezionabili sono tre:

[12] Utilizzare un RF come destinatario consente, ad esempio, di effettuare una trasmissione a tutti i ruoli facenti parte del RF scelto.

- **Interni**: in tal caso la ricerca viene effettuata nell'ambito dei corrispondenti interni alla AOO sulla quale si sta effettuando il protocollo o interni nell'ambito dei corrispondenti interni ad un determinato RF (raggruppamento funzionale);
- **Esterni**: in tal caso la ricerca viene effettuata tra i corrispondenti esterni alla AOO sulla quale si sta effettuando il protocollo, tra i corrispondenti esterni all'Amministrazione corrente e tra i corrispondenti esterni ad un determinato RF (raggruppamento funzionale);
- **Tutti**: in tal caso la ricerca è effettuata tra tutti i corrispondenti presenti in rubrica, interni ed esterni associati ad un determinato registro o ad un determinato RF (raggruppamento funzionale di ruoli in UO).

4.5.2.4 Registro/RF

Il menù a tendina[13] mostra l'elenco dei Registri e dei Raggruppamenti Funzionali di ruoli in UO su cui si è attestati. La selezione della ricerca per Raggruppamento funzionale consentirà di ottenere i corrispondenti esterni presenti in rubrica che sono stati associati al Raggruppamento Funzionale selezionato. Nel caso in cui venga selezionato un Registro, la ricerca avverrà su tutti gli elementi presenti in rubrica per il Registro selezionato.

4.5.3 Inserimento corrispondenti e annullamento operazioni

In alto a destra in Figura 229 sono presenti dei pulsanti (cerchiati in blu) necessari allo svolgimento di alcune importanti funzionalità della Rubrica.
Tali pulsanti sono:

- **Esci**: chiude la pagina delle Rubrica senza riportare nessun corrispondente in VTDOCS, anche se in precedenza è stato correttamente selezionato;
- **Ok**: si attiva dopo aver selezionato il/i corrispondente/i dall'elenco. Effettua l'inserimento nel campo mittente/destinatario in CC/destinatario di una trasmissione a seconda del contesto in cui è stata aperta;
- **Nuovo**: permette di inserire un nuovo corrispondente (UO, Ruolo, Utente) esterno all'Amministrazione. In questo caso è sufficiente riempire i campi del pannello "Inserimento Corrispondenti", proposto nella Figura 232 in cui sono obbligatori solamente i dati contraddistinti dal carattere asterisco;
- **Esporta**: il pulsante "Esporta" permette di eseguire l'esportazione dell'elenco dei corrispondenti presenti nella rubrica nel formato "Microsoft Excel" così come descritto nel paragrafo 4.5.3.1. Il pulsante è presente soltanto nella rubrica raggiungibile tramite le voci di menù 'Gestione' → 'Rubrica'
- **Importa**: il pulsante "Importa" permette di eseguire l'importazione dei corrispondenti effettuando l'inserimento, la cancellazione, e la modifica di quelli presenti nella rubrica nel attraverso un file in formato "Microsoft Excel"così come descritto nel paragrafo 4.5.3.2. Oltre ai campi che definiscono i corrispondenti l foglio contiene una colonna che permette di specificare quale azione il sistema deve attuare sul corrispondente: inserimento, modifica, cancellazione. Il pulsante è presente soltanto nella rubrica raggiungibile tramite le voci di menù 'Gestione' → 'Rubrica'
- **Scarica modello**: tale link consente di scaricare il template Excel da utilizzare per l'import dei corrispondenti. Tale link è presente soltanto nella rubrica raggiungibile tramite le voci di menù 'Gestione' → 'Rubrica'.

[13] E' visibile, da parte di utenti abilitati. Non è presente nella rubrica raggiungibile tramite le voci di menu 'Gestione' → 'Rubrica', bensì nelle altre rubriche

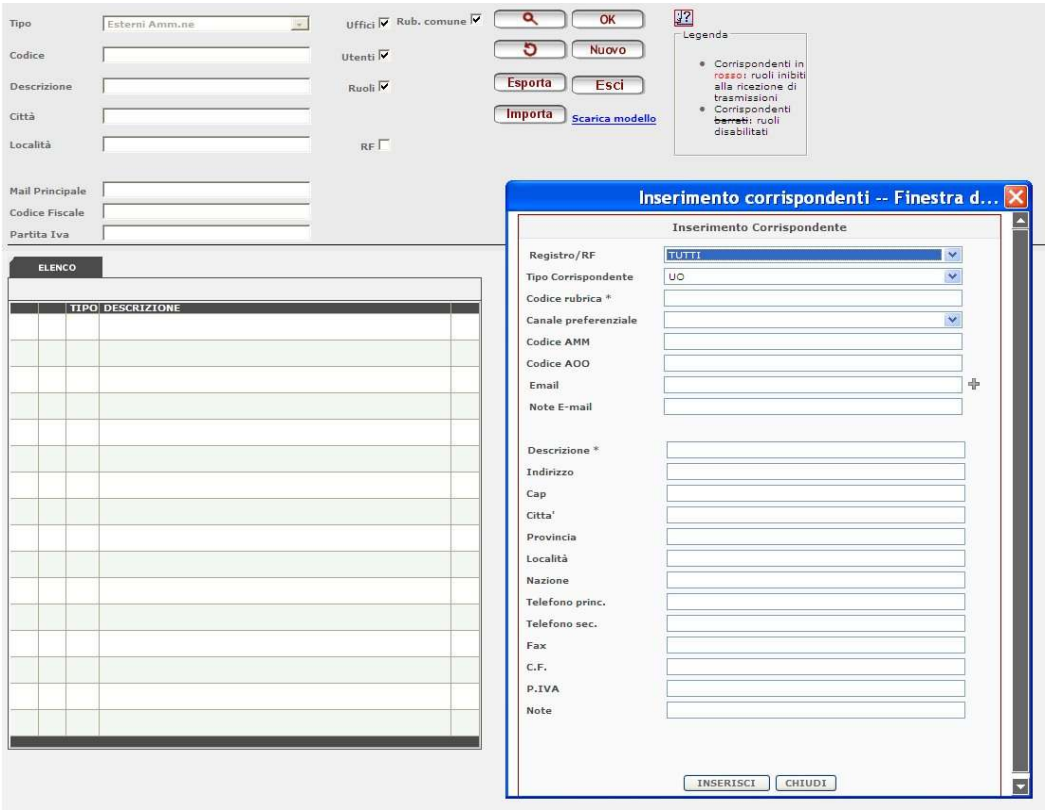


Figura 232 – Inserimento di un corrispondente esterno

I dati necessari per l'inserimento di un nuovo corrispondente variano a seconda che si voglia inserire una Unità Organizzativa, un Ruolo o una Persona. In Figura 232 è mostrata la schermata per l'inserimento di un nuovo corrispondente.

Alcuni campi sono obbligatori, come:

- **Registro/RF**: indica l'AOO nella quale si vuole creare il nuovo corrispondente ovvero il Raggruppamento funzionale di Ruoli in UO (RF) a cui si vuole associare il corrispondente;
- **Codice rubrica**: sequenza di caratteri che identifica univocamente il corrispondente all'interno dell'Amministrazione. Tale codice può essere utilizzato per la selezione diretta del corrispondente in fase di creazione di un documento senza passare per la rubrica;
- **Nome**: il nome del corrispondente (campo presente solo per l'inserimento di una Persona);
- **Cognome**: il cognome del corrispondente (campo presente solo per l'inserimento di una Persona);
- **Descrizione**: è una descrizione estesa del corrispondente (campo presente solo per UO e Ruolo);
- **E-mail**: indica l'indirizzo e-mail del corrispondente. E' obbligatorio se come Canale preferenziale è stata specificata l'e-mail o l'interoperabilità, altrimenti è facoltativo. Se l'amministrazione è abilitata alla gestione multicasella, è possibile specificare più indirizzi di posta elettronica ad un unico corrsipondente ed inserire delle note ('Note email', max 20 caratteri) di utilizzo per ricordare per quale scopo possono essere utilizzate le differenti caselle di posta elettronica. Dopo aver inserito l'indirizzo di posta ed eventuali note di utilizzo premere il pulsante . La prima (eventualmente unica) casella di posta verrà considerata come principale, digitando altri indirizzi e utilizzando

sempre il pulsante  è possibile aggiungere ulteriori indirizzi di posta elettronica. E' possibile successivamente modificare o eliminare gli indirizzi di posta inseriti;

Campi non obbligatori:

- **Canale preferenziale**: è il canale di comunicazione tramite cui il corrispondente vuole ricevere comunicazioni ad esso indirizzate. Il valore corrispondente è selezionabile da un menu a tendina;
- **Codice AMM**: è il codice dell'amministrazione a cui appartiene il corrispondente;
- **Codice AOO**: è il codice della AOO a cui appartiene il corrispondente;
- **Titolo**: menu a tendina da cui selezionare il titolo (Avv, Dott, Ing, …) del corrispondente (campo presente solo per l'inserimento di una Persona);
- **Data nascita**: data di nascita del corrispondente (campo presente solo per l'inserimento di una Persona);
- **Luogo nascita**: luogo di nascita del corrispondente (campo presente solo per l'inserimento di una Persona);
- **Indirizzo:** è l'indirizzo del corrispondente (campo presente solamente per i corrispondenti di tipo UO e Persona)
- **Cap**: è il Codice di Avviamento Postale appartenente all'indirizzo del corrispondente (campo presente solo per UO e Persona);
- **Città**: è la città appartenente all'indirizzo del corrispondente (campo presente solo per UO e Persona);
- **Provincia**: provincia a cui appartiene corrispondente (campo presente solo per UO e Persona);
- **Località**: località a cui appartiene il corrispondente;
- **Nazione**: è la nazione a cui appartiene corrispondente (campo presente solo per UO e Persona);
- **Telefono princ**.: è il numero telefonico principale con il quale è possibile contattare il corrispondente (campo presente solo per UO e Persona);
- **Telefono sec.**: è il numero di telefono secondario con il quale è possibile contattare il corrispondente (campo presente solo per UO e Persona);
- **Fax**: è il numero di fax con il quale è possibile contattare il corrispondente (campo presente solo per UO e Persona);
- **C.F.**: è il codice fiscale del corrispondente (il campo non è presente se si seleziona il valore Ruolo nel campo "tipo corrispondente"). Al momento della creazione del corrispondente viene effettuato un controllo di validità del valore inserito. Se il controllo fallisce non sarà possibile creare il nuovo corrispondente. Per le UO è possibile indicare un codice di 11 o 16 caratteri:
  - nel caso di 11 caratteri verranno applicati gli stessi controlli della partita IVA
  - nel caso di 16 caratteri verranno applicati gli stessi controlli del CF di una persona fisica e ne verrà dato avviso all'utente tramite un opportuno messaggio;
- **P.IVA**: è il numero di partita iva del corrispondente (il campo non è presente se si seleziona il valore Ruolo nel campo "tipo corrispondente"). Al momento della creazione del corrispondente viene effettuato un controllo di validità del valore inserito. Se il controllo fallisce non sarà possibile creare il nuovo corrispondente;
- **Note**: è un campo disponibile per eventuali annotazioni relative al corrispondente (campo presente solo per UO e Persona). Nel caso di modifica di un corrispondente esistente, il campo potrebbe essere popolato con i dati relativi a codice fiscale/partita IVA precedentemente inseriti per il corrispondente ma che non rispettano il formato previsto per tali informazioni.

Una volta inseriti i campi obbligatori, mediante la selezione del pulsante "Inserisci", il corrispondente viene creato e riportato automaticamente nella parte destra della rubrica, pronto per essere utilizzato nel

contesto corrente. E' possibile quindi utilizzarlo come corrispondente esterno nei documenti, ad esempio come destinatario di un protocollo in uscita.

4.5.3.1 Esportazione dei corrispondenti

Nella pagina di gestione della rubrica il pulsante "Esporta" consente di creare un foglio Excel con il contenuto della rubrica relativo ai corrispondenti esterni. Il foglio presenta le seguenti colonne:

- Storicizza
- Codice registro
- Codice rubrica
- Codice amministrazione
- Codice AOO
- Tipo
- Descrizione
- Cognome
- Nome
- Indirizzo
- CAP
- Città
- Provincia
- Nazione
- Cod. Fiscale
- P. Iva
- Telefono 1
- Telefono 2
- Fax
- Email
- Località
- Note
- Nuovo registro
- Canale preferenziale

La colonna Storicizza è vuota e viene utilizzata nella fase di importazione.
Il pulsante "Esporta" fa aprire una finestra di dialogo in cui è possibile indicare il nome e la directory di destinazione del file Excel in cui viene inserito il contenuto della rubrica.

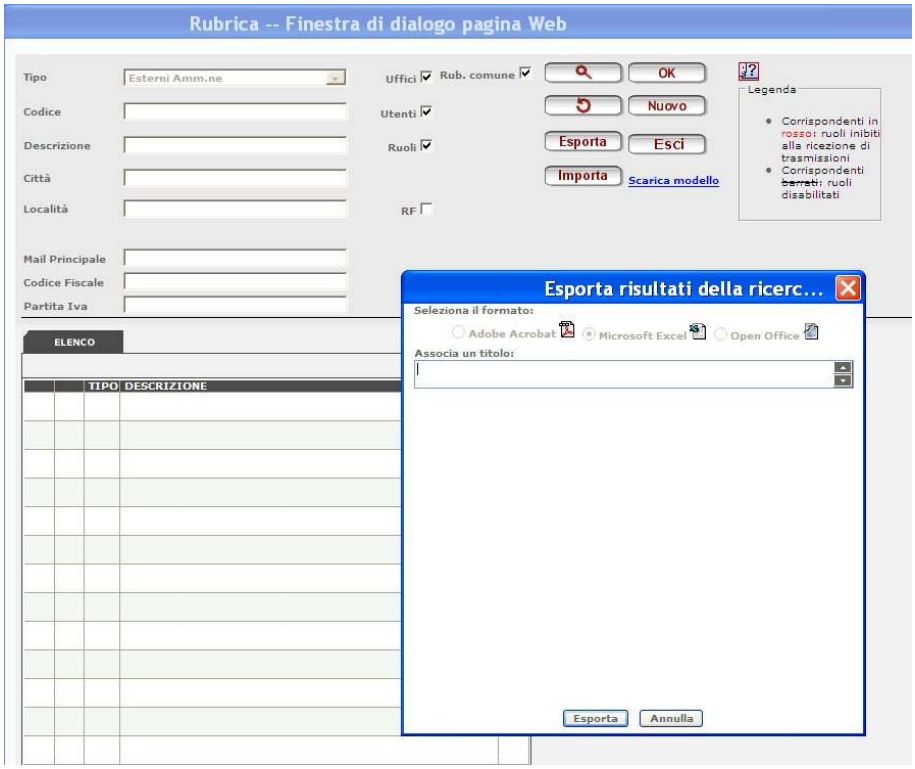


Figura 233 – Export corrispondenti

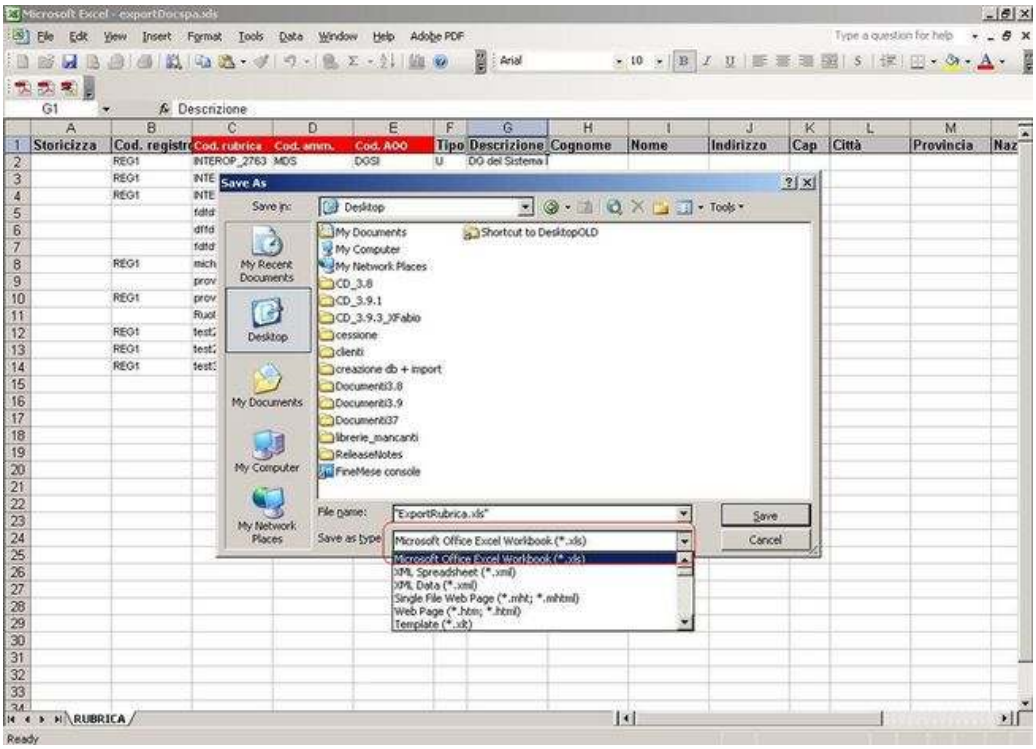


Figura 234 – Foglio Excel con i dati della rubrica dei corrispondenti

4.5.3.2 Importazione dei corrispondenti

Analogamente a quanto illustrato per l'operazione di esportazione delle rubrica, il pulsante "Importa" fa aprire una finestra di dialogo analoga a quella mostrata nella figura precedente che consente di selezionare il foglio Excel (compilato come descritto nel paragrafo 4.5.3.2.1) per aggiornare la Rubrica con il suo contenuto.
Il termine dell'operazione è segnalato con un opportuno messaggio dinamico che indica il numero di corrispondenti eliminati, il numero di corrispondenti modificati ed il numero di corrispondenti inseriti. Se nell'importazione si riscontrano dei problemi, l'applicativo mostra un messaggio a video. Sia nel caso che l'importazione vada a buon fine sia nel caso che ci siano dei problemi, tramite la selezione del pulsante "Log", si visualizza quanto accaduto all'atto dell'importazione (Figura 236).

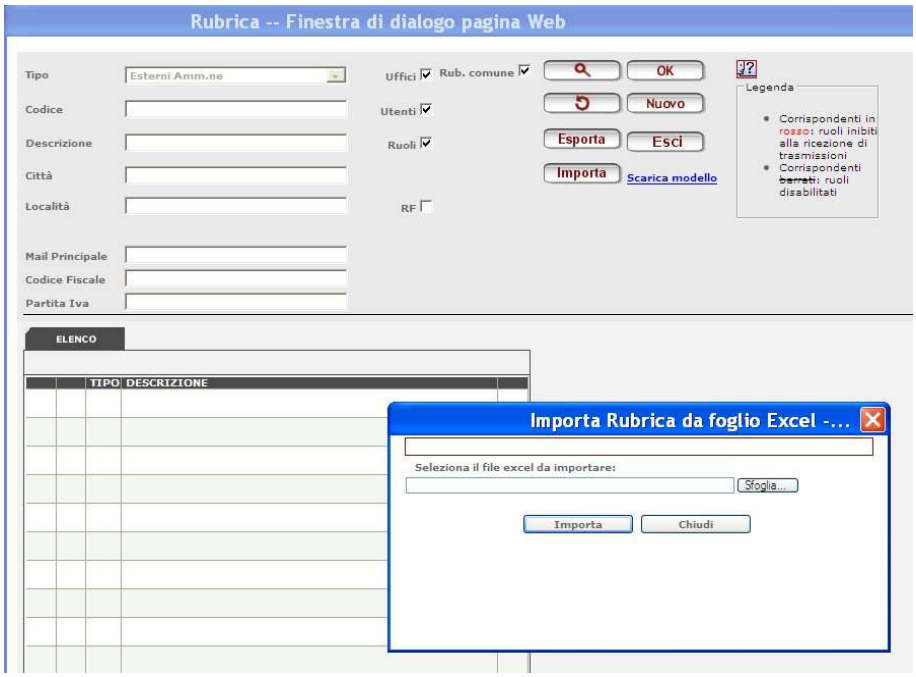


Figura 235 – Import corrispondenti

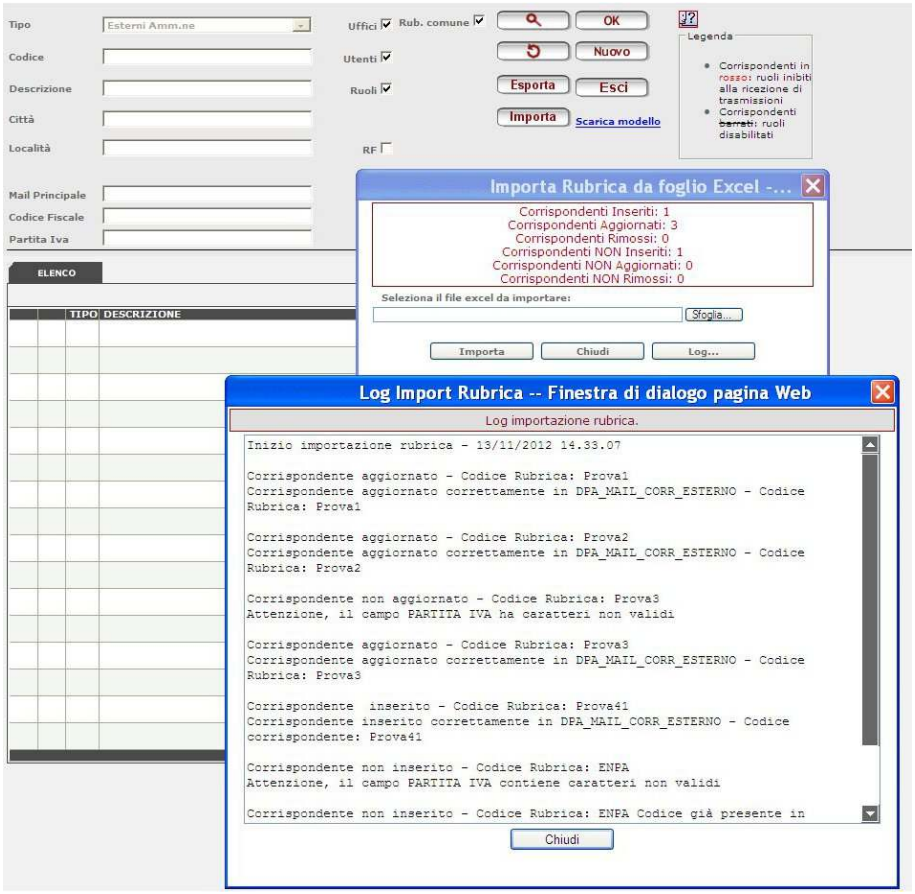


Figura 236 – Log relativo ad import corrispondenti

4.5.3.2.1 Preparazione del foglio Excel per l'importazione

Tramite il link 'Scarica modello' è possibile salvare in locale il template del file Excel da utilizzare per l'import dei corrispondenti. Per modificare il foglio Excel si devono seguire le indicazioni riportate nel file stesso all'interno del foglio 'Istruzioni'.
La colonna "Storicizza" permette l'inserimento, la modifica o la cancellazione dei corrispondenti, in base al carattere inserito. Tramite l'import è possibile indicare anche il canale preferenziale del corrispondente e gestire corrispondenti con più indirizzi di posta elettronica associati (vedere foglio 'Istruzioni' del template di import).

4.5.4 Risultati della Ricerca

Una volta impostati i parametri di ricerca si seleziona il pulsante "Ricerca"  , il risultato viene mostrato nella Figura 237.
Il risultato della ricerca può essere mostrato in due differenti sezioni:

- Elenco: presenta i risultati della ricerca sotto forma di elenco (un esempio in Figura 237).
  A seconda del caso, i corrispondenti trovati potrebbero essere evidenziati in modo particolare:

- in rosso: se si tratta di ruolo inibiti alla ricezione di trasmissioni o modificati con storicizzazione[14]
- in nero barrato: se si tratta di ruoli disabilitati.

Sulla sinistra di ciascun risultato sono presenti due icone:

- attraverso la quale è possibile visualizzare il dettaglio ovvero tutti i dati che caratterizzano il corrispondente, valori inseriti in fase di creazione del corrispondente (mediante VTDOCS se esterno all'Amministrazione o mediante l'applicazione di Amministrazione se interno all'Amministrazione);
- , , : attraverso le quali è possibile visualizzare la porzione di organigramma relativa al corrispondente a cui tali immagini si riferiscono. L'organigramma è visualizzabile solamente per i corrispondenti interni all'Amministrazione. Per gli esterni tali immagini sono disabilitate.

Per gli utenti aventi più ruoli quello principale verrà evidenziato con un asterisco.

- Organigramma: attivo solo per la ricerca dei corrispondenti interni quando si richiama la rubrica dalla protocollazione, dalla trasmissione di un documento o fascicolo, dalla creazione di un modello di trasmissione, dalla creazione di una lista di distribuzione. Evidenzia la porzione di organigramma di cui fa parte il corrispondente selezionato, o tutto l'organigramma se nessun corrispondente è stato selezionato prima della selezione del pannello Organigramma. É possibile navigare all'interno dell'organigramma e selezionare il corrispondente, UO, Ruolo, Persona, che si desidera durante tale navigazione. Un esempio è mostrato in Figura 238.

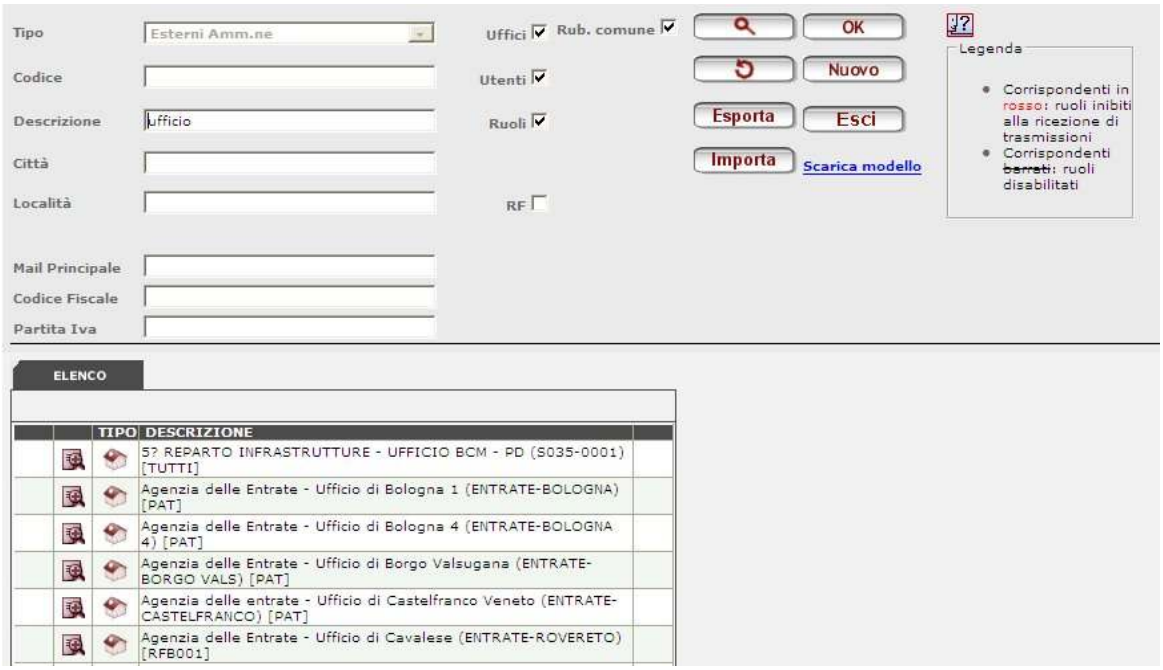


Figura 237 – Rubrica pannello "Elenco": risultati della ricerca

[14] Se è stata abilitata da amministrazione la gestione avanzata dei ruoli

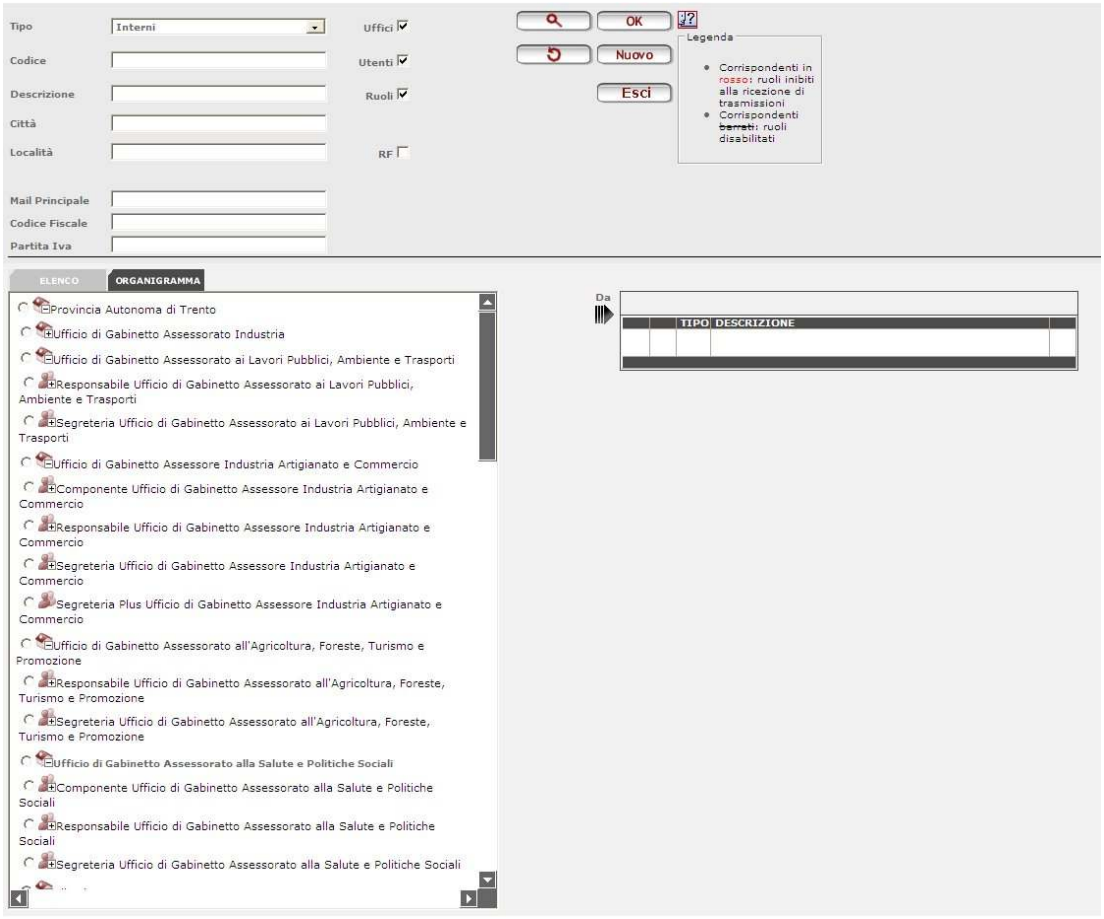


Figura 238 – Rubrica pannello "Organigramma": esempio di navigazione

Solamente i corrispondenti autorizzati in un particolare contesto potranno essere selezionati in Rubrica. Ad esempio se si sta protocollando in uscita sul registro REG1 e si vuole selezionare un corrispondente per il campo mittente, la rubrica renderà selezionabili solamente quei corrispondenti che sono memorizzati su quel particolare registro. Tutti gli altri, poiché considerati esterni alla AOO del protocollo non saranno selezionabili.

Da entrambi i pannelli mostrati in Figura 237 e Figura 238 è possibile selezionare il corrispondente di interesse e utilizzarlo nel contesto da cui la rubrica stessa è stata richiamata.

4.6 Gestione allineamento archivio elettronico / cartaceo

Questa funzionalità permette agli archivisti di mantenere allineato l'archivio cartaceo con quello elettronico. È possibile, attraverso la voce di menu "Gestione → Archivio cartaceo", visualizzare una lista di tutte le ultime versioni dei documenti con l'immagine acquisita e fascicolata in elettronico ma ancora da archiviare in fascicolo cartaceo.

Figura 239 – Funzione "Archivio cartaceo"

Le informazioni visualizzate per ciascun documento sono:

- Num. Prot./Data Prot. (in caso di documento protocollato).
- Id Doc./Data Creazione (in caso di documento non protocollato).
- Tipologia del documento.
- Numero della versione del documento visualizzata (sempre l'ultima).
- Codice del registro di protocollo (in caso di documento protocollato).
- Fascicolo (nodo di titolario e descrizione fascicolo).

Per ciascun documento è possibile effettuare le seguenti operazioni:

- Impostare lo stato in "Cartaceo", nel caso in cui al documento elettronico corrisponde un documento cartaceo da archiviare (punto (a) della Pagina gestione cartaceo).
- Impostare lo stato come "Inserito in archivio cartaceo" (funzione attiva solamente se il documento è impostato come "Cartaceo") (punto (b) della Pagina gestione cartaceo).
- Visualizzare il documento selezionato (punto (c) della Pagina gestione cartaceo).
- Verificare la presenza del documento in altri fascicoli dell'archivio cartaceo (punto (d) della Pagina gestione cartaceo).

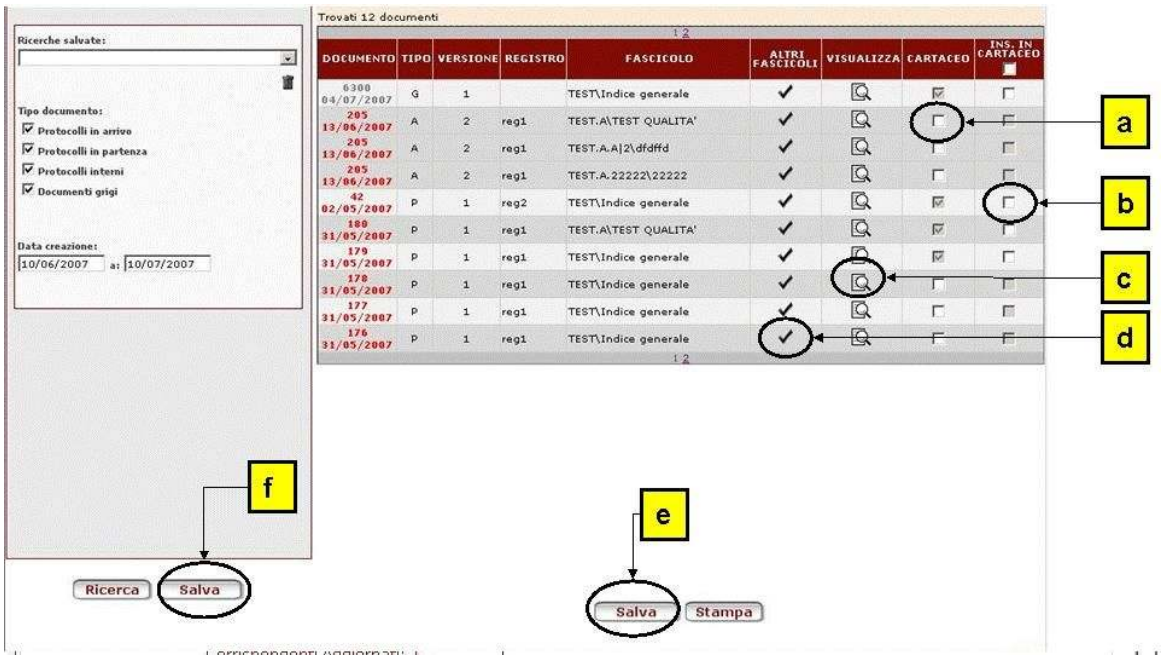


Figura 240 – Pagina gestione cartaceo

La funzione "Salva" (punto (e) della Pagina gestione cartaceo) permette di confermare tutte le eventuali modifiche effettuate.

La funzione “Inserito in archivio cartaceo” (ovvero il campo di selezione denominato, “Ins. cartaceo”, punto (b) della Pagina gestione cartaceo) è quella che permette di allineare l’archivio cartaceo a quello elettronico.
Tutti i documenti che sono stati contrassegnati come “Inserito in archivio cartaceo” non saranno più visualizzati. La funzione “Stampa” consente di esportare in formato “PDF” (Acrobat) o “XLS” (Excel) l’intera lista dei documenti visualizzati.
Nella parte sinistra della Pagina Gestione Cartaceo sono riportate le funzioni di ricerca.
È possibile applicare i seguenti filtri per la ricerca dei documenti:

- Sulla tipologia del documento
  - Protocolli in arrivo
  - Protocolli in partenza
  - Protocolli interni
  - Documenti grigi
- Sulla data di creazione del documento.

Per impostazione predefinita sono visualizzati tutti i documenti creati nell’ultimo mese. Per ripristinare esattamente la stessa “vista” generata in una fase successiva, è possibile salvare tramite il pulsante Salva (punto (f) della Pagina gestione cartaceo), i criteri di filtro di ricerca con i tutti documenti visualizzati. Per ciascuna ricerca è salvato il nome dell’utente che l’ha generata con data e ora.

In fase di acquisizione dei file immagine è possibile stabilire se, per il documento, è presente un corrispondente cartaceo. L’informazione è evidenziata nel dettaglio del documento/protocollo. È possibile impostare la stessa informazione anche per il fascicolo.

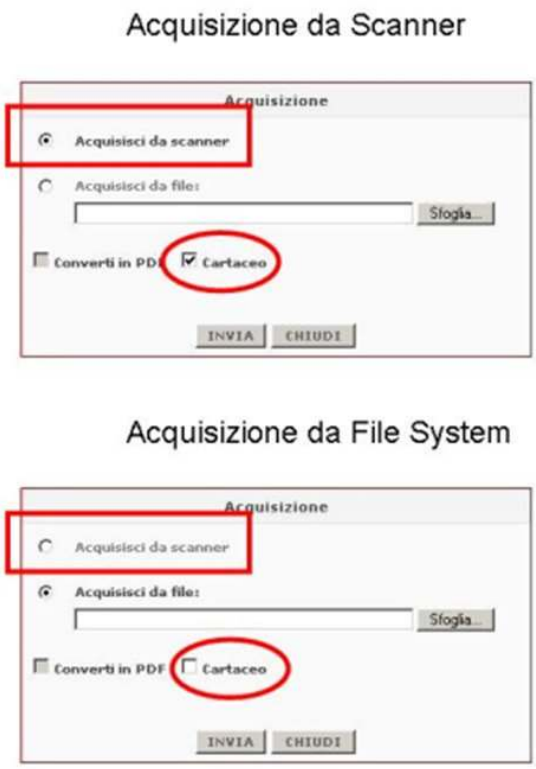


Figura 241 – Acquisizione file immagine: impostazione cartaceo

Nel caso di acquisizione da scanner, il campo selezionabile “cartaceo” sarà selezionato automaticamente dall’applicativo, mentre per l’acquisizione da file system dovrà essere selezionato dall’utente.

Nella prossima immagine viene mostrato il dettaglio di un documento in cui si fornisce evidenza della presenza del cartaceo associato al documento.

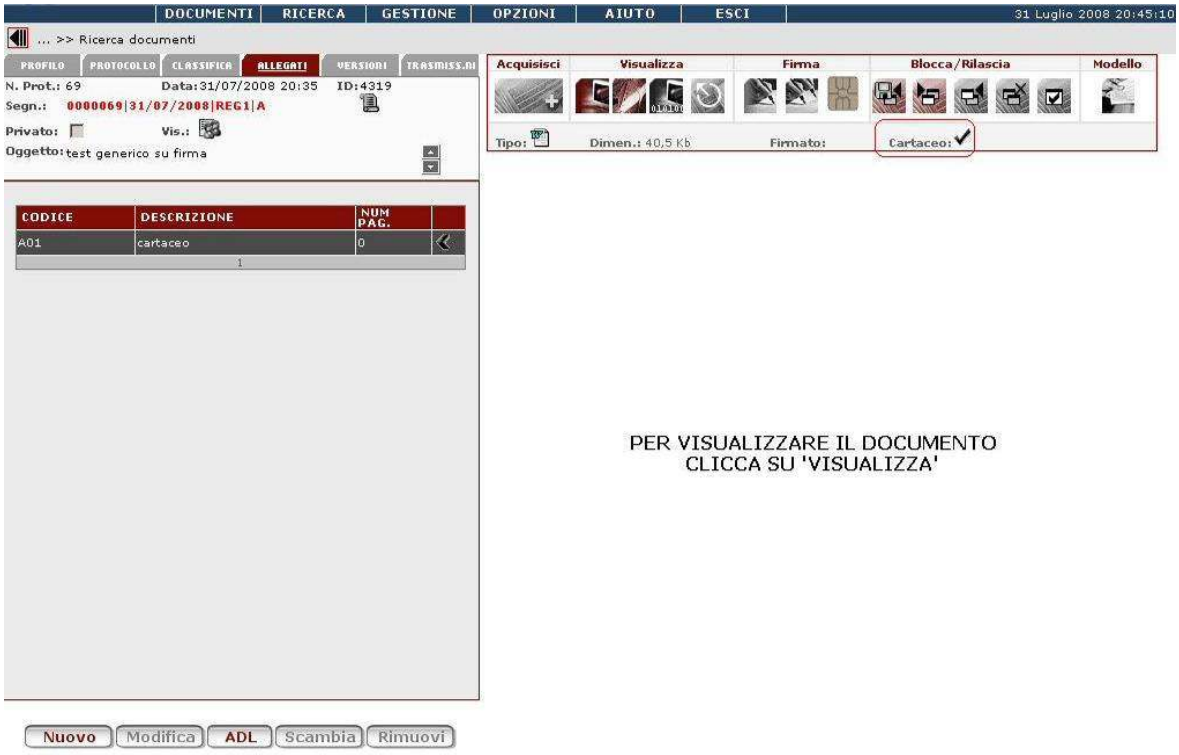


Figura 242 – Dettaglio documento: evidenza della presenza dell'originale cartaceo

Creando un fascicolo elettronico, che è già presente nell'archivio cartaceo, è possibile impostare questa ulteriore informazione attraverso l'apposito tasto selezione presente nella pagina di creazione di un fascicolo, come riportato qui di seguito.

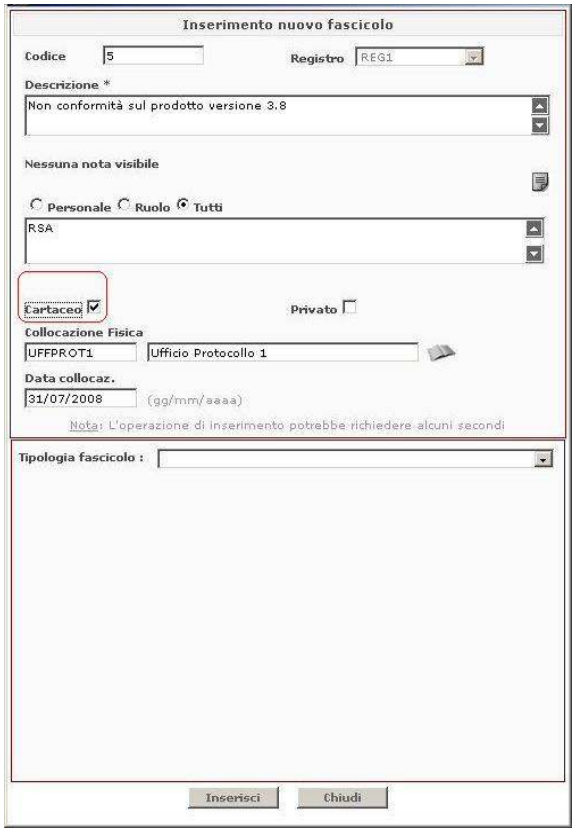


Figura 243 – Creazione fascicolo: impostazione cartaceo

4.7 Gestione Liste di distribuzione

Questa funzionalità consente di creare dei gruppi di destinatari associati ad un nome, denominati *Liste di distribuzione* da poter utilizzare nell'operazione di protocollazione in uscita e di trasmissione interna dei documenti. Le liste di distribuzione potranno essere utilizzate con modalità analoghe alle Unità Organizzative, ai Ruoli e agli utenti. Ogni utente potrà creare delle liste di distribuzione che potranno essere disponibili solo a se stesso o a tutto il ruolo. Un'analoga funzionalità presente nell'applicazione di amministrazione consentirà all'amministratore del sistema di creare delle liste di distribuzione pubbliche che tutti gli utenti potranno utilizzare.
L'esecuzione del comando "Gestione/Liste" visualizza un pannello per la gestione delle liste: creazione, visualizzazione, modifica, cancellazione (Figura 244).

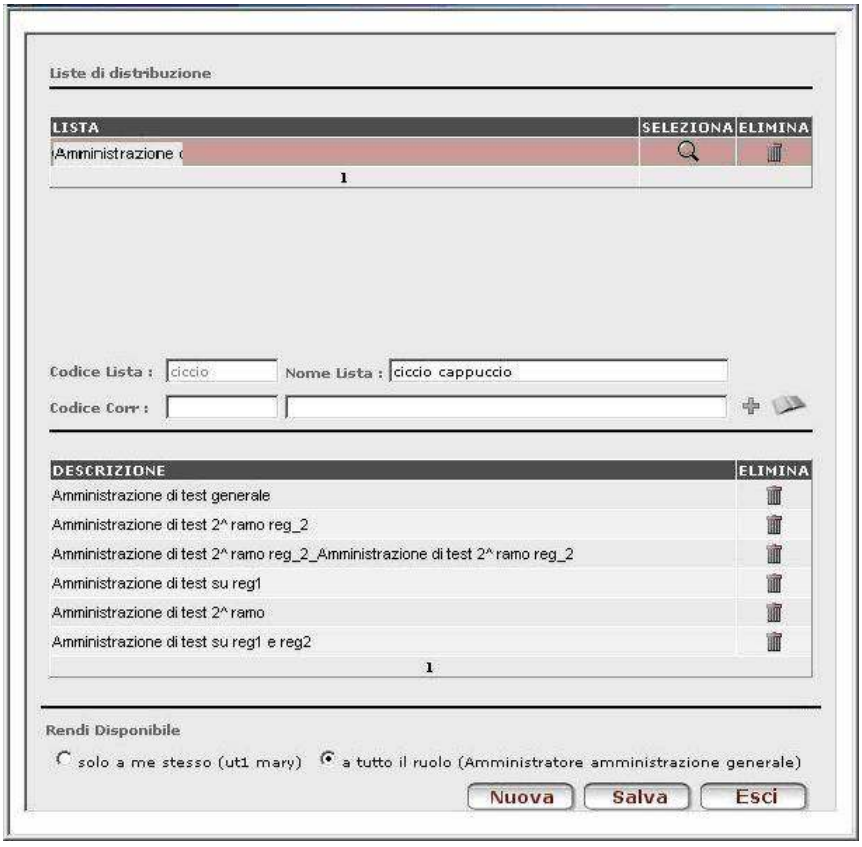


Figura 244 - Gestione Liste

In tale pannello è disponibile:

- l'elenco delle liste di distribuzione già definito (inizialmente tale elenco sarà vuoto). Le liste contenenti ruoli inibiti alla ricezione di trasmissioni verranno evidenziate in colore rosso e con carattere barrato. Sarà possibile modificare tali liste per sostituire i ruoli inibiti: in tal modo la lista tornerà ad essere utilizzabile nelle trasmissioni e nella selezione dei destinatari di un protocollo;
- il pulsante "*Nuova*" per la creazione di una nuova lista di distribuzione;
- il comando "*Seleziona*" per la visualizzazione o la modifica di una lista di distribuzione precedentemente definita;
- il pulsante "*Salva*" per il salvataggio delle eventuali modifiche apportate alla lista selezionata;
- il comando "*Elimina*" per la rimozione di una lista di distribuzione precedentemente definita;
- il comando "*Rendi disponibile*" per salvare la lista e renderla visibile solo all'utente che la sta creando o a tutto il ruolo dell'utente creatore.

L'esecuzione del comando "*Nuova*", tramite selezione del relativo pulsante, richiede il nome della lista di distribuzione che si vuole creare e consente la selezione dei componenti singolarmente, attraverso il codice di un corrispondente censito in rubrica, o attraverso l'utilizzo della rubrica stessa, in questo caso è possibile una selezione multipla dei corrispondenti.

Una lista di distribuzione può contenere indistintamente:

- Unità organizzative;
- Ruoli;

- Persone;
- Corrispondenti esterni.

Non è possibile inserire una lista di distribuzione in un'altra lista.
Una volta creata una lista di distribuzione, è possibile modificarla aggiungendo o togliendo elementi dalla lista. La modifica della lista di distribuzione ha effetto solo per le protocollazioni in uscita o le trasmissioni effettuate successivamente alla modifica della lista di distribuzione.
Una lista di distribuzione può anche essere cancellata.

4.8 Gestione Modelli di trasmissione

Questa funzionalità consente di creare dei modelli da poter utilizzare nell'operazione di trasmissione interna di documenti e fascicoli. Ogni utente può creare i propri modelli di trasmissione e decidere se renderli disponibili anche alle altre persone del proprio ruolo.
L'esecuzione del comando "Gestione/Modelli di trasmissione" fa apparire un pannello per la gestione dei modelli da cui si ha la possibilità di creare nuovi modelli, cercare, visualizzare ed eventualmente modificare o cancellare modelli già esistenti. Figura 245

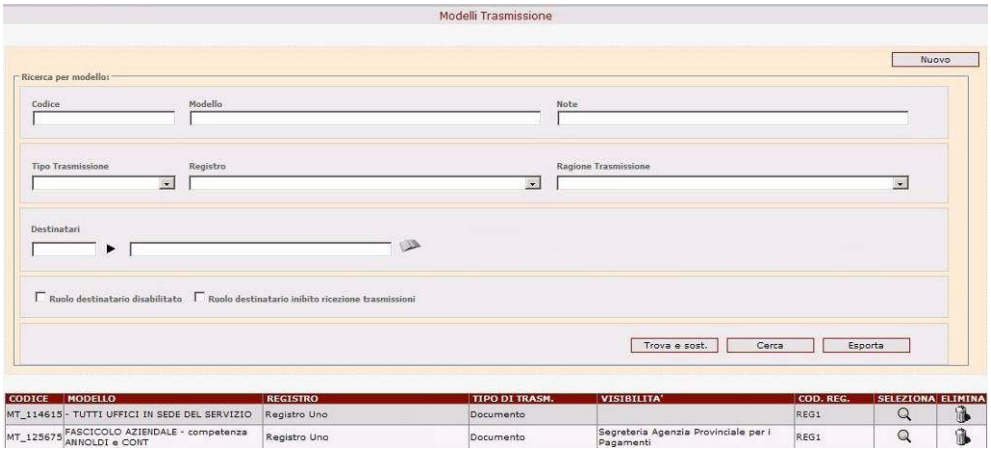


Figura 245 - Gestione Modelli di trasmissione

In tale pannello è disponibile:

- la ricerca per codice e descrizione del modello di trasmissione;
- l'elenco dei modelli di trasmissione già definiti (inizialmente tale elenco sarà vuoto);
- il comando "*Nuovo*" per la creazione di un nuovo modello di trasmissione;
- il comando "*Salva*" per il salvataggio delle eventuali modifiche apportate al modello.

Accanto ad ogni modello in elenco sono presenti:

- il comando "Seleziona" per la visualizzazione o la modifica di un modello precedentemente definito;
- il comando "Elimina" per la rimozione di un modello precedentemente definito.

E' possibile effettuare ricerche di modelli di trasmissione in base ai seguenti criteri (Figura 245):

- codice: codice del modello di trasmissione;

- modello: nome del modello;
- note: note di trasmissione;
- tipo trasmissione: documento o fascicolo;
- registro: registro di protocollo;
- ragione di trasmissione: è possibile indicare al massimo una ragione di trasmissione e il sistema ritornerà tutti i modelli di trasmissione che contengono almeno la ragione di trasmissione eventualmente indicata dall'utente;
- destinatario: è possibile indicare soltanto un destinatario e il sistema ritornerà tutti i modelli di trasmissione che contengono almeno quel destinatario;

Tramite opportune checkbox è inoltre possibile ricercare modelli di trasmissione che contengano, fra i destinatari, almeno un ruolo inibito alla ricezione di trasmissioni.
Premendo il pulsante Cerca viene avviata la ricerca dei modelli di trasmissione in base ai criteri indicati.

Fra i modelli trovati a valle di una ricerca, vengono evidenziati in rosso quelli contenenti:
- ruoli inibiti alla ricezione di trasmissione
- ruoli disabilitati
- ruoli storicizzati[15].

Dalla pagina di gestione dei modelli di trasmissione (Figura 245), tramite il pulsante 'Esporta', è possibile esportare su file:
- i risultati delle ricerche di modelli di trasmissione
- l'elenco dei ruoli disabilitati/inibiti.

Una volta premuto il pulsante 'Esporta' è possibile selezionare (Figura 246):
- il tipo di dati da esportare: elenco ruoli disabilitati e dei ruoli inibiti alla ricezione di trasmissioni o risultati delle ricerche effettuate
- il tipo di file di output (excel o pdf)
- i campi da esportare a scelta fra (solo nel caso di export di risultati di ricerca):
    - nel caso di export di risultato di ricerca, a scelta fra:
        - Codice
        - Descrizione
        - Visibilità
        - Documento/Fascicolo
        - Registro
        - Ragione
        - Ruoli Disabilitati
        - Ruoli inibiti alla ricezione trasmissioni.

[15] La storicizzazione dei ruoli è possibile se è stata abilitata la gestione avanzata dei ruoli tramite interfaccia di amministrazione.

Figura 246 - Export ricerche modelli di trasmissione

Dalla pagina di gestione dei modelli di trasmissione (Figura 245), tramite il pulsante 'Trova e sost.', è possibile sostituire all'interno dei modelli di ricerca trovati un ruolo destinatario con un altro ruolo. Occorre quindi specificare:

- ruolo da ricercare
- ruolo con cui sostituire
- copia note di trasmissione. è un flag che consente di copiare le note di trasmissione nella sostituzione del ruolo destinatario.

Tale funzionalità consente in particolare di aggiornare in modo massivo modelli in cui, ad esempio, compaiono ruoli inibiti alla ricezione di trasmissione, disabilitati o storicizzati[16] al fine di renderli nuovamente utilizzabili nel menu delle trasmissioni rapide.

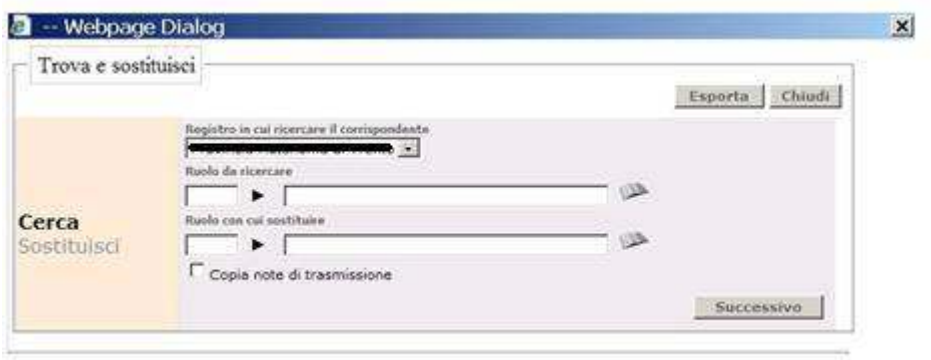


Figura 247 - Trova e sostituisci

[16] La storicizzazione dei ruoli è possibile se è stata abilitata la gestione avanzata dei ruoli tramite interfaccia di amministrazione.

La sostituzione viene effettuata in base alle seguenti regole:

- l'attributo "uno/tutti" presente per il ruolo "X" sarà riportato sul ruolo "Y";
- tutti gli utenti del ruolo "Y" saranno oggetto di notifica della trasmissione, indipendentemente dalle corrispondenti impostazioni presenti sugli utenti del ruolo "X" dei modelli coinvolti nella sostituzione.
- qualora esistano ragioni di trasmissioni che prevedono limiti sui destinatari (solo superiori, solo sottoposti), il sistema effettuerà le sostituzioni soltanto nel caso in cui il nuovo ruolo destinatario "Y" sia coerente con le limitazioni della ragione di trasmissione e del mittente;
- qualora siano presenti modelli di trasmissione indirizzati sia al Ruolo "X" sia al ruolo "Y", la sostituzione non verrà eseguita;
- qualora siano presenti modelli di trasmissione non indirizzati al Ruolo "X", non verrà eseguita alcuna operazione sui modelli;
- i campi "ruolo X" e "ruolo Y" sono obbligatori: se non valorizzati, l'operazione non può essere avviata.

Selezionando il pulsante 

presente nella Figura 245 viene visualizzato un pannello (Figura 248) suddiviso in due parti distinte. Nella prima è presente un campo definito Lista Modelli contenente 4 pulsanti: "Lista Modelli", "Salva", "Nuovo"; "Chiudi"; la seconda parte è rappresentata dalla sezione in cui si crea il modello di trasmissione vero e proprio con l'inserimento dei seguenti campi (quelli con l'asterisco [*] si intendono obbligatori) quali:

- **Nome** [*]: nome con cui verrà individuato il modello dall'utente per effettuare la trasmissione documento/fascicolo dal sistema documentale VTDOCS;
- **Note**: eventuali note per individuare o utilizzare al meglio i modelli di trasmissione;
- **Codice**: è un campo popolato automaticamente dall'applicativo composto da una sigla iniziale "MT_" più un numero progressivo. Tale campo non è modificabile dall'utente amministratore;
- **Tipo trasmissione** [*]: si visualizza il menu a tendina, riportato di seguito che permette di specificare se la tipologia di modello di trasmissione che si sta creando è legata ad un documento o ad un fascicolo;

- **Registro** [*]: si visualizza il menu a tendina, riportato di seguito, che permette di specificare per quale registro stiamo creando il modello di trasmissione;

- **Rendi disponibile**: per rendere disponibile il modello solo all'utente creatore o a tutti gli utenti che appartengono al suo ruolo;
- **Seleziona la Ragione Trasmissione**: si sceglie, attraverso il menu a tendina, la ragione di trasmissione che si vuole inserire all'interno del modello di trasmissione;
- **Seleziona i Destinatari**: si effettua la scelta dei destinatari attraverso la selezione dell'icona rubrica  , che permetterà la ricerca degli utenti interni all'amministrazione in base a tre criteri: il registro selezionato, il mittente scelto (ovviamente dipendente dal registro selezionato) e la ragione di trasmissione selezionata. Come ruolo destinatario non potrà essere selezionato (pur se visualizzato in rubrica evidenziato in colore rosso) un ruolo inibito alla ricezione di trasmissioni.

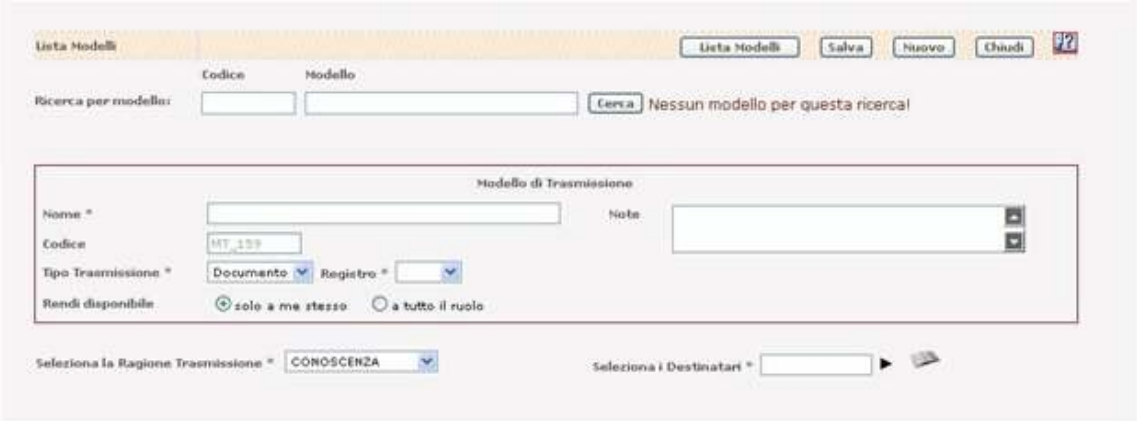


Figura 248 – Pagina per l'inserimento di un modello di trasmissione

A questo punto, se il modello di trasmissione che si sta creando è quello desiderato, si seleziona il pulsante Salva.
Se la trasmissione si effettua a ruolo e/o a persone, il sistema apre una nuova finestra di dialogo, visibile in Figura 249. Tale finestra mostra un elenco di utenze (se si sono selezionati solo utenti), o, per ogni ruolo selezionato, l'elenco delle utenze presenti nel ruolo.
Accanto a ciascuna utenza vi sono due caselle selezionabili, una per la notifica ed una per la cessione:

- la casella della notifica è sempre attiva e selezionabile, è necessario selezionare almeno un'utenza;
- la casella della cessione è attiva solo per le ragioni di trasmissione che prevedono cessione. Nel caso la casella fosse attiva, permetterà la selezione di un'unica utenza per un unico ruolo.

Figura 249 – Gestione notifiche e cessione diritti

Per salvare l'inserimento del nuovo modello di trasmissione, selezionare i ruoli e cliccare sul pulsante "Salva". In tal modo il sistema crea il modello di trasmissione aggiungendolo alla lista dei modelli disponibili.

Inoltre per le amministrazioni che abbiano attivato la funzionalità di consolidamento, accanto ad ogni destinatario è presente una casella di selezione per effettuare delle trasmissioni nella modalità 'nascondi versioni precedenti' (2.13.2).

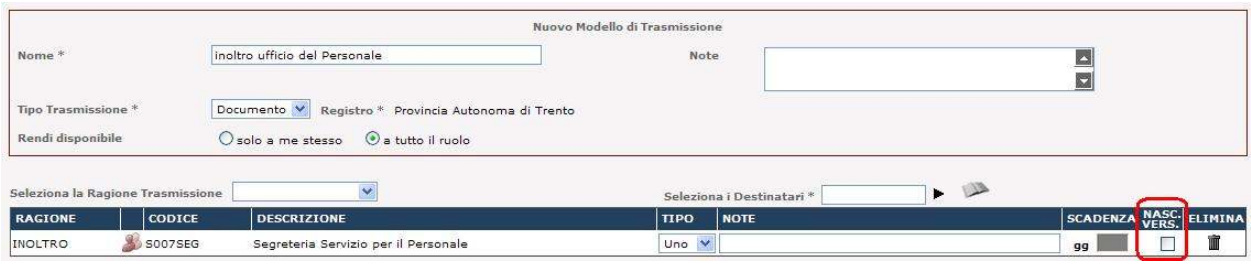


Figura 250 – Modello di trasmissione con l'opzione nascondi versioni precedenti

Durante la creazione di un modello (ma anche durante la sua modifica – vedi Figura 248) sono inoltre disponibili tre pulsanti (posizionati in alto a destra):

- Lista Modelli : per visualizzare la lista dei modelli di trasmissione presenti nell'amministrazione;
- Salva : per salvare e quindi creare e/o modificare dei modelli di trasmissione;
- Nuovo : per creare un nuovo modello di trasmissione.

Una volta creato un modello di trasmissione, è possibile modificarne il nome, aggiungere o rimuovere destinatari, modificare le note, modificare il tipo di trasmissione. Se si modifica il registro i dati precedentemente immessi verranno persi.
Un modello di trasmissione può anche essere eliminato mediante la selezione dell'icona che è presente in corrispondenza di ciascun modello nella visualizzazione dell'elenco dei modelli disponibili.
I modelli di trasmissione possono essere creati anche direttamente in fase di trasmissione di un documento o di un fascicolo. Si rimanda alle pagine del manuale che trattano le trasmissioni per avere ulteriori dettagli al riguardo (paragrafo 2.13.4).

4.9 Gestione Organigramma

Questa funzionalità permette la ricerca e la navigazione all'interno dell'organigramma e consente stampe dell'organigramma visualizzato.
L'esecuzione del comando "Gestione/Organigramma" visualizza il pannello mostrato di seguito:

Figura 251 - Gestione Organigramma

E' possibile ricercare l'unità organizzativa di cui si vuole stampare l'organigramma attraverso:

- Codice della UO;
- Descrizione della UO;
- Codice Ruolo;
- Descrizione Ruolo;
- Lista RF;
- Nome utente;
- Cognome Utente.

E' possibile richiedere la visualizzazione, e quindi la stampa, dell'organigramma nelle seguenti modalità:

- Solo Unità Organizzative;
- UO e Ruoli;
- UO, Ruoli e Utenti.

E' possibile ricercare:

- una UO: in tal caso apparirà la porzione di Organigramma ad essa relativa;
- un Ruolo: in tal caso verrà visualizzata la porzione di Organigramma in cui tale ruolo è collocato;
- un Raggruppamento funzionale di ruoli in UO;
- un Utente: in tal caso verranno visualizzati, in un'opportuna finestra di dialogo, i ruoli da lui ricoperti, e selezionandone uno, verrà visualizzata la porzione di Organigramma in cui tale ruolo è collocato.

Se la ricerca ha come risultato un unico dato, questo verrà rappresentato direttamente a video, mentre se la ricerca produce più risultati (come nel caso della ricerca di un utente che ha più ruoli), questi saranno elencati in una finestra di dialogo secondaria dove saranno selezionabili a scelta dall'utente.
E' possibile chiudere rami dell'organigramma visualizzato.

La selezione del'icona "stampa" consente di esportare in forma testuale su un file in formato pdf l'organigramma visualizzato per poterne poi eseguire la stampa .
Descrizione dei pulsanti:

Permette la ricerca nell'organigramma rispetto ai criteri inseriti dall'utente

Pulisce i dati a video e ripristina la condizione iniziale di ricerca

Riporta alla pagina iniziale

Riporta alla UO padre di quella visualizzata come radice

Imposta la UO selezionata nell'albero di visualizzazione come radice

Visualizza tutto l'organigramma partendo dalla UO radice (l'operazione di visualizzazione potrebbe richiedere qualche secondo)

I dati visualizzati ad albero vengono esportati in un file con formato pdf dal quale si effettua la stampa.

4.10 Gestione Doc. Rimossi

La funzionalità per la visualizzazione e la gestione dei documenti cancellati è ottenibile a partire dalla barra di navigazione del pannello principale selezionando la voce del menu Gestione, premendo sul pulsante "GESTIONE" e successivamente su quello dei "Doc. rimossi" , che apre un'altra finestra in cui si visualizzerà immediatamente la lista dei documenti che sono stati rimossi.

Figura 252 - Gestione Doc Rimossi

L'intestazione dell'elenco dei documenti trovati riporta il numero di elementi presenti in *"Documenti in cestino"*. In questa vi sono anche due icone:

- : permette la cancellazione di tutti i documenti presenti nei "Documenti in Cestino" ;
- : permette l'esportazione dell'elenco su file di formato Pdf o Excel. Il file è costituito dai seguenti campi:
  - Registro;
  - Prot./Id. Doc.;
  - Data Creazione;
  - Oggetto;
  - Tipo, Mitt./Dest.;
  - Motivo Rimozione.

Dopo aver visualizzato l'elenco esportato tramite l'applicazione proprietaria, l'utente può stampare, modificare o salvare il file.

Ogni documento nella lista dei documenti che sono stati rimossi è descritto dalle seguenti informazioni:

- **Doc.Data**: Numero documento e data creazione del documento;

- **Registro**: per i documenti predisposti alla protocollazione riporta il nome del registro su cui è predisposto;
- **Oggetto**: oggetto del documento;
- **Tipo**: specifica se è un documento non protocollato o un predisposto alla protocollazione;
- **Mitt/Dest**: mittenti o destinatari per i documenti predisposti alla protocollazione;
- **Motivo**: motivo della cancellazione;
- **Dett**: la selezione dell'icona permette la sola visualizzazione del documento;
- **Attiva**: selezionando l'icona , è possibile ripristinare il documento;
- **Elimina**: attraverso la selezione dell'icona , è possibile cancellare in maniera definitiva il documento a cui è associato.

Su questa lista, attraverso il pulsante "Filtro", è possibile visualizzare solo i documenti con determinati requisiti. Tale filtro permette di vedere la lista dei documenti in cestino rispetto ad una serie di parametri:

- **Tipo documento**: indica il tipo di documento che si vuole visualizzare, attraverso dei campi a selezione esclusiva che permettono di effettuare una scelta tra le varie opzioni:
  - Pred. Arrivo (predisposto alla protocollazione in arrivo);
  - Pred. Partenza (predisposto alla protocollazione in partenza);
  - Non Protocollato;
  - Tutti.
- **Data Creazione**: per indicare, il giorno o l'intervallo di tempo in cui è stata effettuata la creazione del documento;
- **Oggetto**: ricerca i documenti che contengono nel testo dell'oggetto il testo specificato.

Una volta impostati i parametri di interesse, si seleziona il pulsante "OK" oppure se non si è più interessati a filtrare i documenti si seleziona il pulsante "Chiudi".

Una volta attivato un filtro, questo può essere ridefinito attraverso il pulsante "Filtro" o rimosso attraverso il pulsante "Rimuovi Filtro".

Figura 253 - Visualizzazione dei documenti in cestino

4.10.1 Recupero dei documenti cancellati

Dalla lista dei documenti è possibile ripristinare i documenti cancellati. Tale operazione può essere effettuata mediante la selezione dell'icona : a seguito della selezione il sistema mostra il seguente messaggio:

"Sei sicuro di voler ripristinare il documento?"

Se si vuole confermare l'operazione si deve selezionare il pulsante "Ok", in tal modo il sistema ripristina il documento; altrimenti l'operazione viene annullata.

4.10.2 Cancellazione fisica dei documenti

La cancellazione fisica e definitiva di tutti i documenti presenti nei "Documenti in cestino" avviene attraverso la selezione dell'icona . L'operazione deve essere esplicitamente confermata selezionando "Ok" su un messaggio di conferma dell'operazione.
Selezionando "Ok", tutti i documenti presenti nel cestino vengono cancellati.
Selezionando "Annulla", si annulla l'operazione.

La cancellazione fisica e definitiva del singolo documento presente nella pagina "Documenti in cestino" avviene attraverso la selezione dell'icona associata ad ogni documento. Anche in questo caso l'operazione deve essere ulteriormente confermata.
Selezionando Ok, il documento in questione viene cancellato.
Selezionando "Annulla", si annulla l'operazione.

4.11 Gestione area conservazione

Dal menu "Gestione > Area conservazione" [17], mostrato in Figura 254, gli utenti abilitati all'utilizzo delle funzionalità legate alla conservazione dei documenti digitali, possono accedere all'area di gestione delle istanze di conservazione; tali istanze, che hanno come fine la conservazione dei documenti e dei fascicoli, possono essere create dagli utenti abilitati nei modi illustrati nei paragrafi successivi.

Figura 254 - Area conservazione

Premessa sulla conservazione sostitutiva
L'essenza del sistema è costituita dai documenti elettronici, documenti che spesso sono rilevanti ai fini amministrativi e legali, pertanto una particolare attenzione è dedicata alla loro corretta conservazione nel tempo.
Gli strumenti realizzati nell'ambito sistema sono indirizzati a coprire le seguenti esigenze:

- Backup/disaster recovery/conservazione
- Produzione di ulteriori copie informatiche dei documenti (oltre a quelle gestite nel sistema di gestione documentale), indipendenti dalla tecnologia usata per produrre e gestire documenti e

[17] Le funzionalità relative alla conservazione dei documenti devono essere opportunamente abilitate tramite intrefaccia di amministrazione

informazioni connesse, al fine di meglio supportare i processi e le responsabilità di conservazione a lungo termine.
- Esibizione dei documenti attraverso la produzione di copie su supporti rimuovibili dei documenti e/o fascicoli richiesti da un soggetto interessato

E' inoltre necessario ricordare che, secondo la normativa vigente, un documento potrà assumere lo stato di "documento conservato" solo se adeguatamente collocato in "sistema archivio". Tale "sistema archivio" deve essere inteso sia come un sistema tecnologico sia come una struttura organizzativa dove esistano dei processi di gestione e dove siano definiti dei ruoli e siano attribuite delle responsabilità; un luogo dove il patrimonio documentale elettronico possa essere "sorvegliato e protetto" non solo contro i fenomeni accidentali o fraudolenti che ne possono determinare la indisponibilità, ma soprattutto contro l'obsolescenza tecnologica e l'impossibilità di verificarne l'integrità ed autenticità.

Il sistema di protocollazione informatica e di gestione documentale è basato su un modello organizzativo che, ai fini della conservazione, prevede la presenza di uno o più centri servizi che gestiscono ed hanno in carico i processi legati a tale funzione:
- delega del ruolo di responsabile della conservazione per l'apposizione della firma digitale;
- produzione e archiviazione e verifica di leggibilità dei supporti;
- monitoraggio dei fenomeni di obsolescenza tecnologica di sistemi, formati e supporti;
- esecuzione del processo di riversamento diretto;
- consegna dei supporti al soggetto interessato richiedente.

I paragrafi successivi illustrano nel dettaglio le funzionalità disponibili per gli utenti del sistema applicativo per la gestione documentale, mentre nel paragrafo **Errore. L'origine riferimento non è stata trovata.** sono illustrate le funzionalità disponibili per gli utenti del centro servizi attraverso il modulo applicativo "Gestione conservazione".

4.11.1 Indicazione dei documenti e/o fascicoli per la conservazione

All'interno dell'interfaccia di lavoro di VTDOCS sono state realizzate delle funzionalità che consentono la costruzione di un'istanza di conservazione.
Un'istanza di conservazione è una collezione di "item di conservazione" che possono essere documenti (protocollati o no) e/o fascicoli procedimentali. Un documento o un fascicolo possono appartenere a più istanze di conservazione. Un'istanza di conservazione rappresenta, pertanto, l'insieme dei documenti e dei fascicoli che devono essere trasferiti su un supporto di conservazione (ottico o di altro tipo) secondo le modalità previste dalla normativa vigente. Un'istanza di conservazione può essere creata dagli utenti dell'applicativo "VTDOCS – Gestione documentale" nell'esercizio del proprio ruolo. Solo i ruoli abilitati hanno la possibilità di definire istanze di conservazione.

4.11.1.1 Creazione di un'istanza di conservazione

L'utente abilitato, per creare una istanza di conservazione, ricerca i documenti/fascicoli da inserire nell'istanza, utilizzando una delle modalità di ricerca presenti in VTDOCS. Selezionando successivamente l'icona  posta a sinistra del documento/fascicolo, ed evidenziata in rosso in nella figura seguente, verrà creata una nuova istanza di conservazione, come viene messo in evidenza dalla finestra che compare Figura 256.

L'istanza creata sarà visibile al solo utente creatore dell'istanza stessa.

Figura 255 – Documenti/Fascicoli da inserire nell'istanza di conservazione

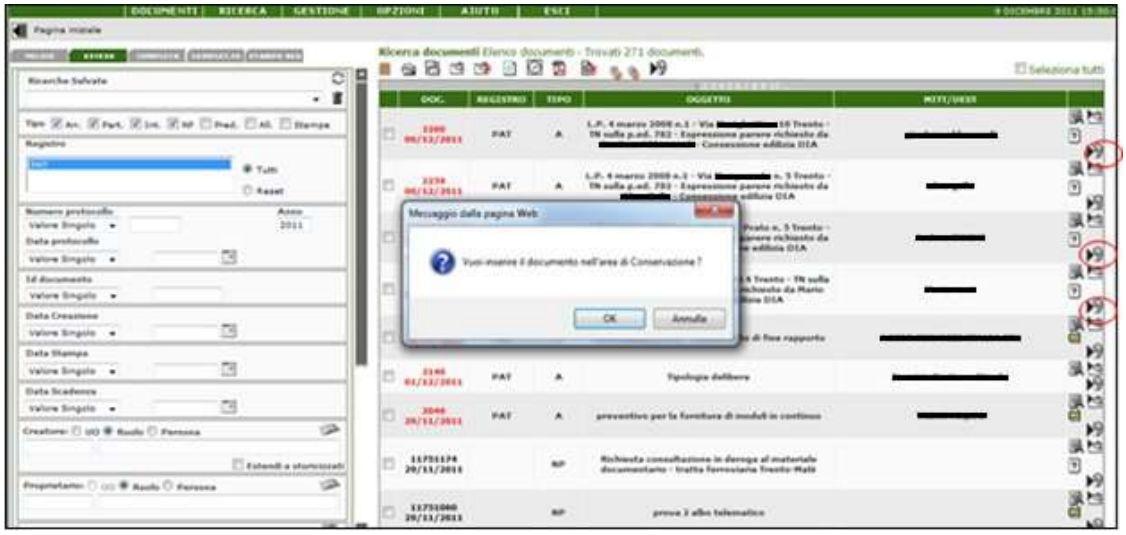


Figura 256 - Creazione di una nuova istanza di conservazione

Per inserire altri documenti all'interno di una istanza è necessario selezionare l'icona . Il sistema provvederà a cambiare l'icona in corrispondenza del documento/fascicolo selezionato in (Figura 257) e ad aggiornare la lista dei documenti/fascicoli da conservare (istanza).

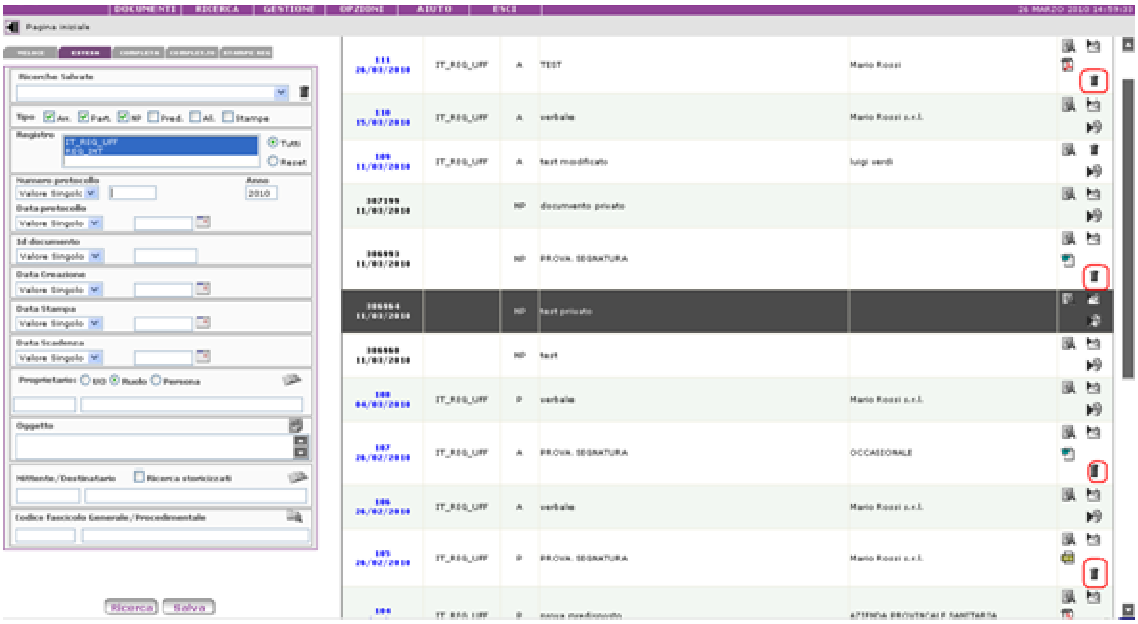


Figura 257 – Documenti/Fascicoli inseriti nell'istanza

4.11.1.2 Trasmissione di un'istanza per la conservazione

Gli utenti abilitati possono gestire le istanze di conservazione create accedendo all'area conservazione; tale accesso si effettua a partire dal menu "Gestione > Area conservazione", come in Figura 258.

Accedendo a tale "Area conservazione", l'utente ha la possibilità di visualizzare la lista delle istanze di conservazione create. La schermata presenta la lista delle istanze di conservazione con le seguenti informazioni:

- Id istanza: indica il numero identificativo dell'istanza;
- Stato: indica lo stato di transizione in cui si trova l'istanza di conservazione. Tale campo presenta uno dei seguenti valori: *nuova, in lavorazione, firmata, chiusa, rifiutata, conservata, errore.*
- Note: riporta eventuali note inserite dall'utente all'atto di invio dell'istanza;
- Descrizione: viene visualizzata la descrizione dell'istanza di conservazione;
- Data apertura: indica la data di creazione dell'istanza da parte dell'utente o l'eventuale data di creazione automatica dell'istanza
- Data invio: indica la data di invio dell'istanza al centro Servizi;
- Data conservazione: indica la data di chiusura dell'istanza;
- Tipo cons: indica se l'istanza è finalizzata alla *conservazione consolidata, conservazione non consolidata o esibizione;*
- Note rifiuto: vengono visualizzate le motivazioni del rifiuto nel caso in cui una istanza venga rifiutata dal Centro Servizi;
- A/M: indica la modalità di creazione dell'istanza stessa: manuale (M) o automatica (A);
- Dett.: consente di visualizzare i dettagli dell'istanza;
- Elimina: consente di eliminare l'istanza.

È possibile, inoltre, utilizzare i filtri di ricerca presenti nella parte superiore della schermata al fine di visualizzare solamente i tipi di istanze desiderati.

Figura 258 - Lista istanze di conservazione

La finestra con i dettagli dell'istanza presenta la lista con i documenti/fascicoli da conservare con i relativi dettagli che, nel caso di istanza contenente documenti, sono:

- Tipo documento: A: Protocollo in Ingresso, P: Protocollo in Uscita, NP: Documento non protocollato;
- Oggetto: breve descrizione del documento;
- Codice fascicolo: codice del fascicolo in cui è inserito il documento;
- Data di inserimento: è la data dell'inserimento del documento nell'istanza;
- ID/Segnatura Data: é l'id nel caso di un documento grigio, o la segnatura nel caso di un documento protocollato e la relativa data;
- Size byte: è la dimensione del documento;
- Tipo file: estensione del file;
- Numero allegati: numero degli allegati (se presenti);
- Visualizza: consente di visualizzare l'immagine del documento e degli eventuali allegati;
- Elimina: selezionando l'icona consente di eliminare il documento dall'istanza.

Sono presenti una serie di campi, alcuni dei quali obbligatori:

- Inserisci descrizione(*): è necessario inserire una descrizione dell'istanza;
- Inserisci note: è possibile inserire delle note;
- Tipologia conservazione(*):dal menu a tendina è possibile scegliere la tipologia di istanza che si intende creare (Figura 260):
  - Conservazione consolidata: prevede il consolidamento automatico dei documenti, file e metadati, inseriti nell'istanza. L'istanza chiusa viene sempre memorizzata almeno sullo *storage* di rete;
  - Conservazione non consolidata: non prevede il consolidamento automatico dei documenti. L' istanza chiusa viene sempre memorizzata almeno sullo *storage* di rete;
  - Esibizione: non prevede il consolidamento dei documenti. L'istanza viene memorizzata sullo *storage* di rete.
- Valida l'istanza con una policy (vedi par. 4.10.1.3): consente di selezionare una policy dal menù a tendina per verificare che i documenti contenuti nell'istanza siano conformi alla policy stessa (Figura 261).

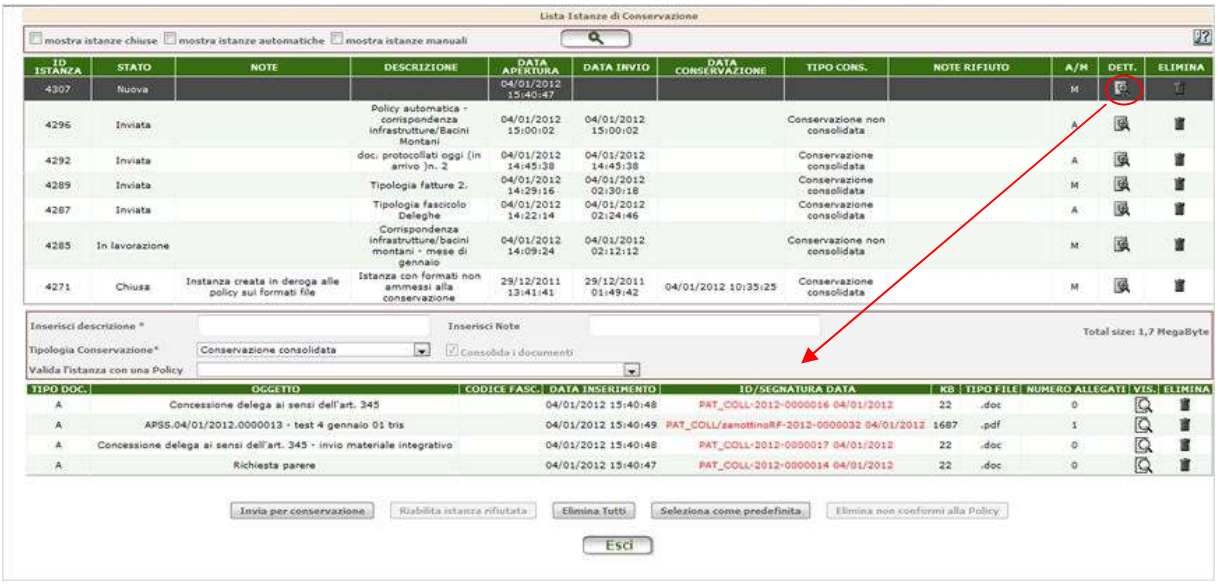


Figura 259- *Dettagli istanza di conservazione*

Figura 260 - *Selezione tipologia di conservazione*

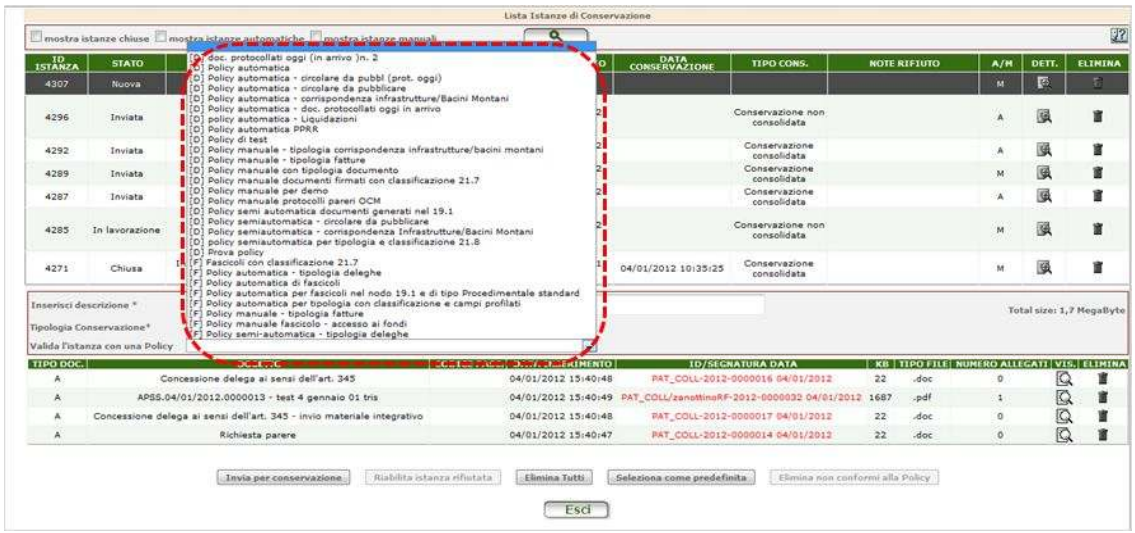


Figura 261 – *Selezione policy per la validazione dell'Istanza*

Dopo aver compilato i campi obbligatori è possibile inviare l'istanza di conservazione al Centro servizi selezionando il pulsante Invia per conservazione.
E' possibile altresì eliminare tutti i documenti/fascicoli dall'istanza selezionando il pulsante Elimina Tutti.

In caso di generazione automatica delle istanze sarà possibile avere più istanze aperte contemporaneamente in "area conservazione", in particolare un'istanza creata manualmente e 1-n istanze create in modo automatico attraverso le policy e per le quali non sia stato previsto l'invio automatico al Centro Servizi. Per la gestione di tali istanze, in particolare per consentire eventualmente agli utenti di modificare il contenuto delle istanze generate attraverso le policy, in "area conservazione", selezionando il pulsante Seleziona come predefinita è possibile definire l'istanza in cui devono essere inseriti eventuali documenti/fascicoli selezionati a partire dalle funzionalità di ricerca.

4.11.1.3 Validazione dell'istanza con una policy

Dalla maschera di dettaglio dell'istanza è possibile verificare che i documenti contenuti nella stessa siano conformi alla policy selezionata (Figura 261).
Dopo aver selezionato una policy dal menù a tendina il sistema effettua in automatico i controlli di conformità dei documenti inseriti nell'istanza rispetto ai criteri definiti nella policy selezionata.
Solo in caso di esito negativo il sistema barra in rosso i documenti che non rispettano i parametri della policy (Figura 262) e contemporaneamente si abilita il pulsante Elimina non conformi alla Policy che consente all'utente di eliminare i documenti non conformi alla policy selezionata.
L'utente può comunque procedere all'invio dell'istanza in conservazione anche senza eliminare i documenti non conformi alla policy, infatti, l'esito negativo della verifica di conformità non preclude tale operazione.

Figura 262 – *Risultato verifica di conformità alla policy*

4.11.2 Gestione del processo di produzione dei supporti legati ad un'istanza

Le istanze di conservazione vengono sottomesse al Centro servizi a cui è associato l'ente richiedente (ogni ente può essere associato ad un centro servizi differente) che provvederà a produrre uno o più supporti per la conservazione.

4.12 Deleghe

La gestione delle deleghe consente ad un utente abilitato detto "Delegante", di delegare un'altra persona definita "Delegato" a svolgere le proprie mansioni e quindi ad avere la sua stessa visibilità e diritti funzionali all'interno del sistema documentale. Il Delegato avrà la facoltà di effettuare operazioni del Delegante ma a proprio nome accedendo al sistema con le proprie credenziali. Con Delegante si intende quindi il titolare di uno specifico ruolo organizzativo che assegna la delega, mentre con Delegato si intende l'utente che riceve la delega ad agire per conto del Delegante.
Un Delegato erediterà le prerogative proprie di un Delegante e potrà sostituirlo per un determinato periodo temporale in tutte le funzioni assegnate al ruolo delegante.
Con delega impostata si intende la delega immessa nel sistema, ma non ancora attiva in quanto ci si trova al di fuori del periodo di validità fissato; con delega attiva si intende invece la delega già impostata e nel periodo di validità ad essa associato.
Un Delegante potrà assegnare più deleghe ma per periodi temporali diversi e non sovrapposti, in modo da assicurare l'univoca assegnazione della responsabilità ad un solo utente di uno specifico ruolo organizzativo.
Per poter gestire casi di assenza non prevista, una terza persona può attivare la delega per conto del Delegante: l'amministratore di sistema potrà gestire le deleghe attivandole, revocandole o modificando quelle esistenti. In questo caso, l'attivazione di una delega sarà possibile indicando l'utente Delegante, l'utente Delegato e le date di decorrenza e di scadenza.

L'utente accede alla sezione dedicata alle deleghe a partire dalla voce di menu principale "Gestione" e selezionando dal sottomenu la voce ""Deleghe.
La finestra dialogo "Gestione deleghe" mostra un elenco riassuntivo delle deleghe ricevute e assegnate.
Da questa finestra è possibile visualizzare le deleghe, Ricevute o Assegnate, che sono: Attive, Impostate, Scadute oppure tutte.
Per delega **Attiva** s'intende la delega in vigore al momento attuale.
Per delega **Impostata** s'intende la delega immessa nel sistema, ma non ancora attiva in quanto ci si trova al di fuori del periodo di validità fissato ovvero con data/ora di decorrenza successiva alla data/ora odierna.
Per delega **Scaduta** s'intende la delega immessa nel sistema ma non attiva in quanto ci si trova in un periodo successivo all'intervallo di validità.

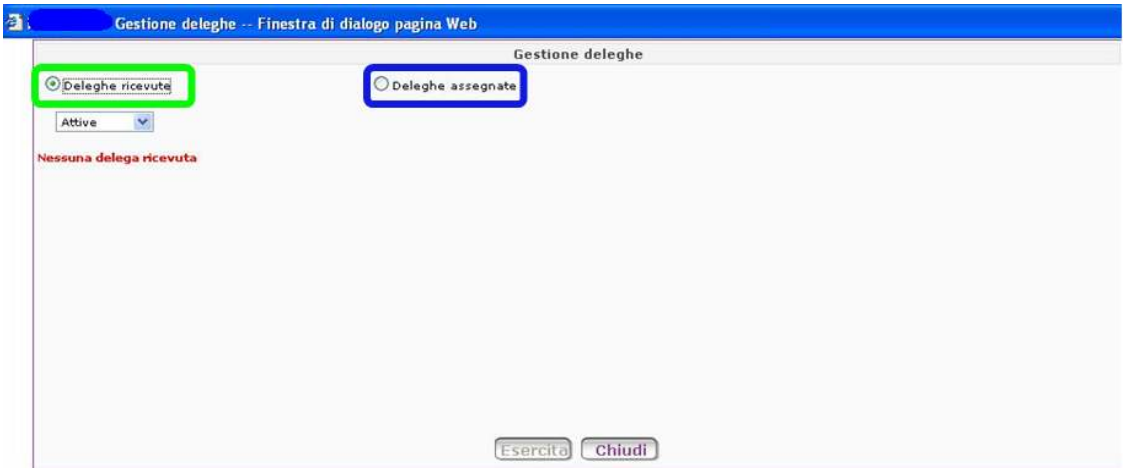


Figura 263 – Gestione deleghe

4.12.1 Assegnazione di una delega

Per assegnare una delega è necessario selezionare la voce Deleghe assegnate all'interno dell'area di gestione delle deleghe, come evidenziato nella figura successiva in verde. Per creare una nuova delega è necessario selezionare il pulsante Nuova.

Figura 264 – Assegnazione nuova delega

Il sistema restituisce i campi da utilizzare per la creazione di una nuova delega. I campi presenti sono:

- **seleziona ruolo delegante:** lista a tendina per attivare la delega su uno o più ruoli rivestiti dall'utente delegante;
- **seleziona delegato:** il sistema propone la navigazione dell'organigramma dell'amministrazione nonché alcuni filtri di visualizzazione degli elementi in organigramma (ricerca tra UO, ruoli, utente);
- **data decorrenza**: campo data per indicare la data di decorrenza della delega;
- **ora**: per indicare l'ora di decorrenza della delega nella data indicata
- **data scadenza**: campo data per indicare la data di scadenza della delega;

- **ora**: per indicare l'ora di scadenza della delega nella data indicata.

La selezione del pulsante Conferma permette il salvataggio della delega e aggiorna l'elenco delle deleghe assegnate.

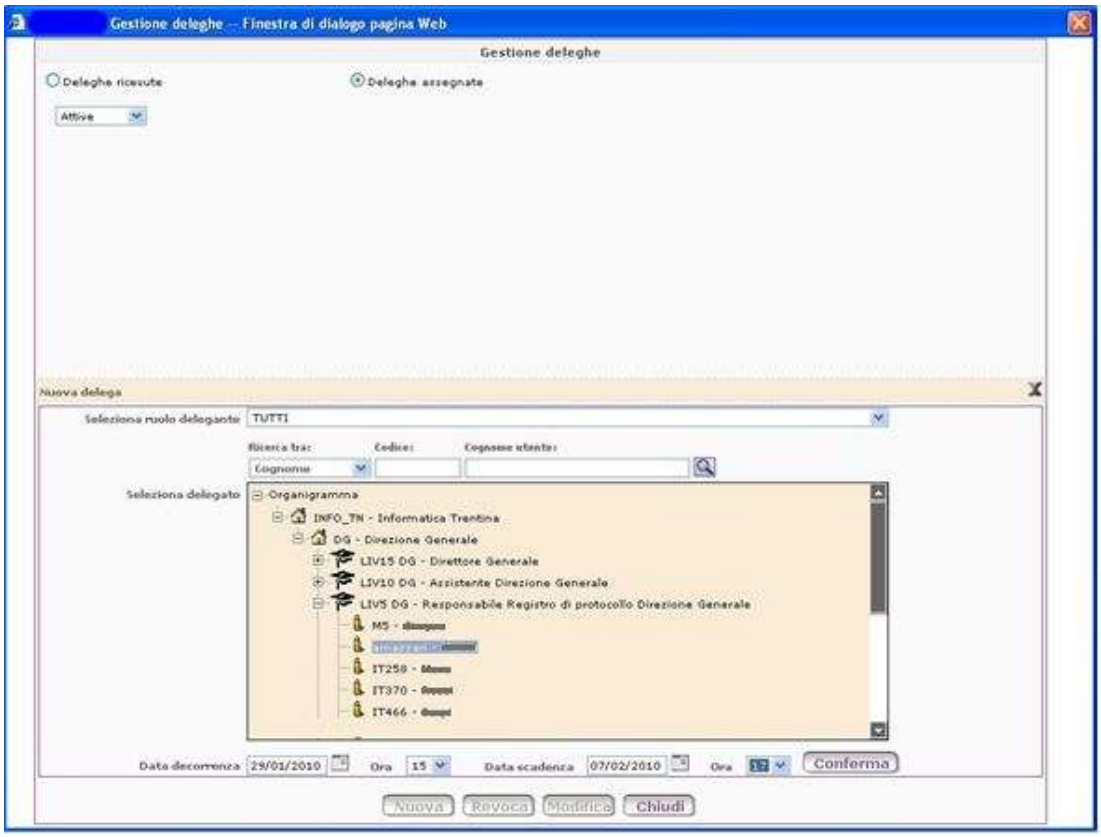


Figura 265 – Dettaglio assegnazione nuova delega

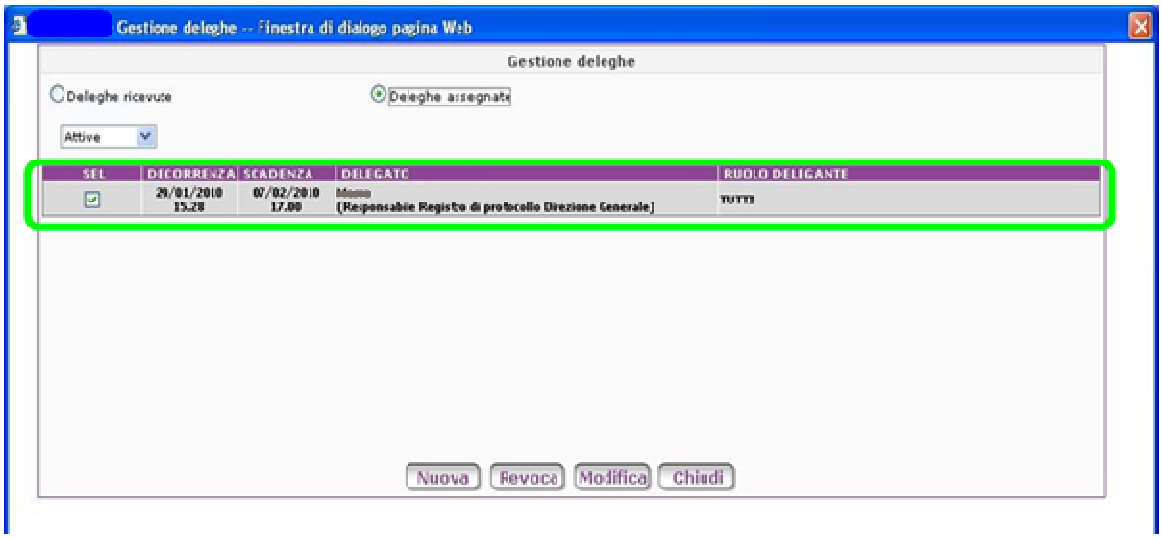


Figura 266 – Elenco deleghe assegnate

Un delegante potrà assegnare più deleghe ma per periodi temporali diversi e non sovrapposti, in modo da assicurare l'univoca assegnazione della responsabilità, ad uno e solo utente, di uno specifico ruolo organizzativo.
Se si creano deleghe sovrapposte il sistema restituisce il seguente avviso:

Figura 267 – Avviso di impossibilità crazione delega sovrapposta

4.12.2 Revoca di una delega

Nella pagina di gestione Deleghe è possibile revocare una o più deleghe create. Selezionando la delega da revocare si abilita il pulsante Revoca (in rosso).
Selezionando tale pulsante compare il messaggio di conferma, a seguito del quale il sistema revoca immediatamente le deleghe selezionate e aggiorna l'elenco delle deleghe assegnate nella pagina di Gestione Deleghe.

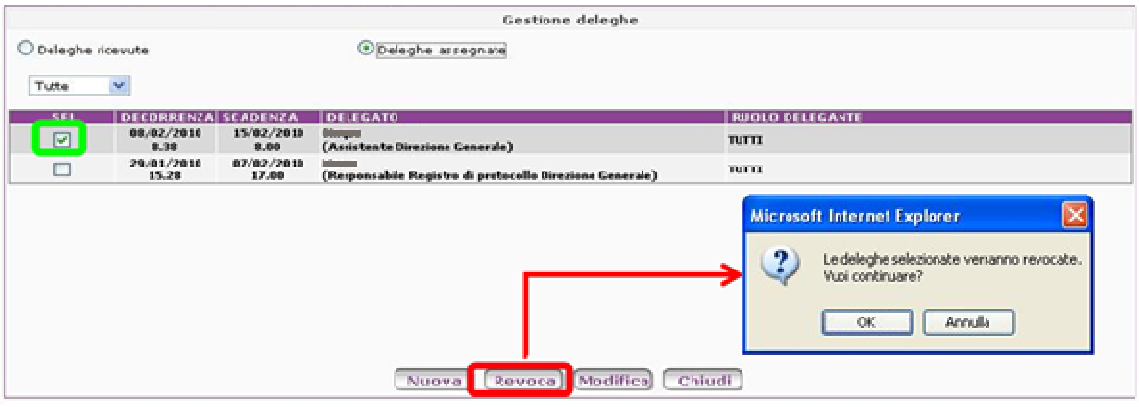


Figura 268 – Revoca della delega

Per tutte le deleghe Impostate il sistema elimina completamente la delega come se questa non fosse mai esistita.
Per tutte le deleghe Attive il sistema imposta la data e l'ora di scadenza al momento della revoca.

4.12.3 Modifica di una delega

Nella pagina Gestione Deleghe è possibile modificare le deleghe assegnate.
E' consentita la modifica di una delega alla volta. Il pulsante Modifica Delega è attivo solo se si seleziona una ed una sola delega assegnata, attiva o impostata.
La selezione del pulsante Modifica sulla delega selezionata attiva la possibilità di modificare i seguenti campi:

- **organigramma**: presenta l'indicazione del ruolo delegato con evidenza dell'utente delegato;
- **data decorrenza**: per l'inserimento della data e ora di decorrenza della delega;
- **data di scadenza**: per l'inserimento della data e ora di scadenza delle delega.

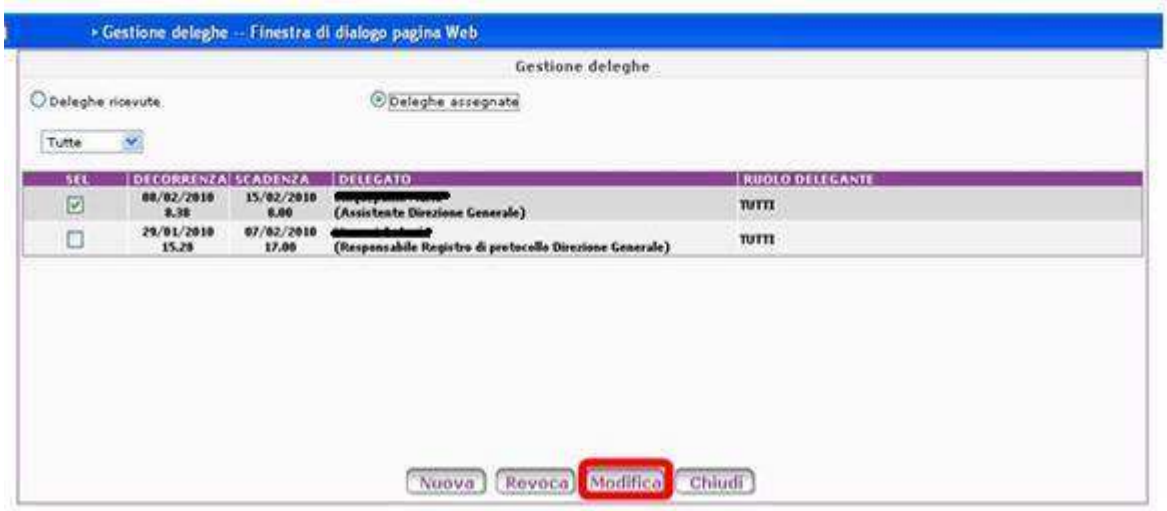


Figura 269 – Modifica della delega

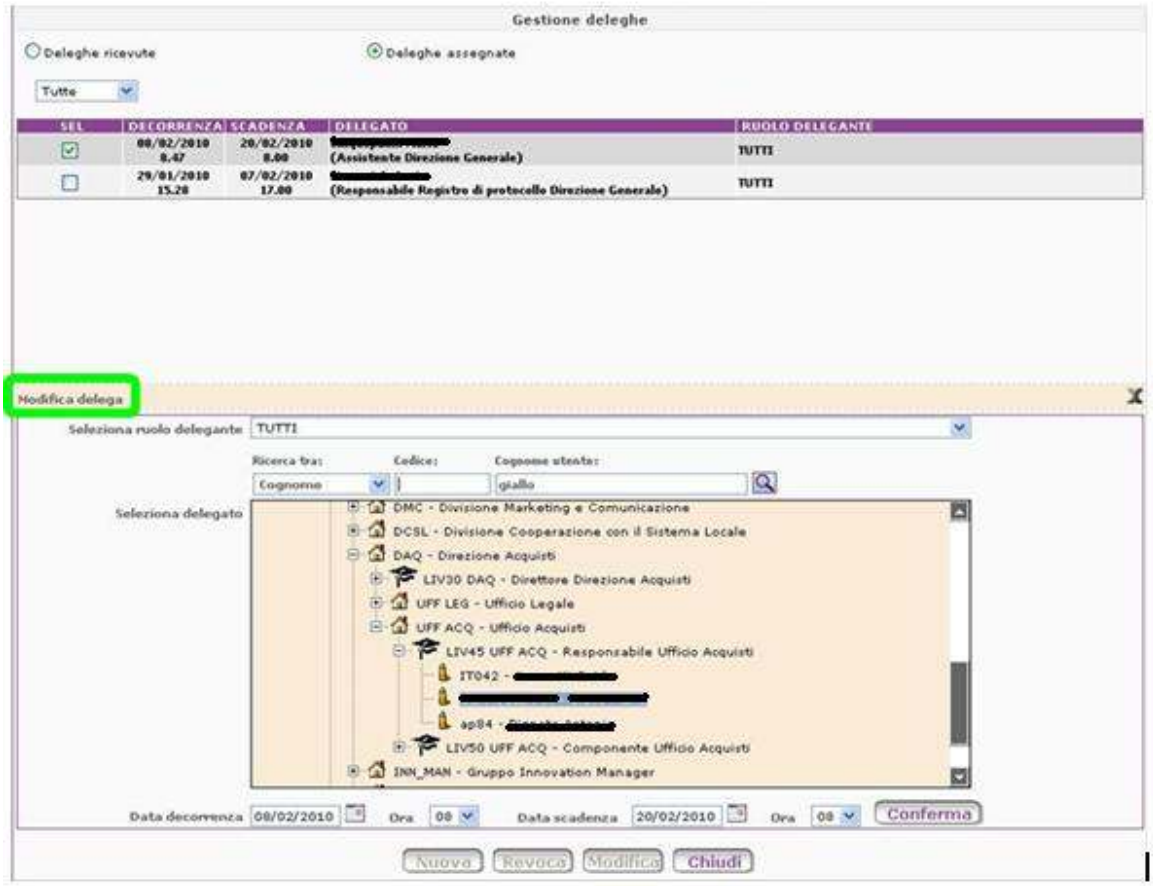


Figura 270 – Modifica della delega: dettaglio campi disponibili

4.12.4 Esercizio della delega

L'utente che riceve la delega ad agire per conto del Delegante può operare con i soli ruoli assegnati dal Delegante e può sostituirlo per un determinato periodo temporale in tutte le funzioni assegnate ai ruoli del Delegante.
Effettuando il login si visualizza la finestra che avverte l'utente che ha ricevuto una o più deleghe.

Figura 271 – Login dell'utente delegato: avviso assegnazione delega

Alla selezione del pulsante OK, il sistema conduce l'utente nella finestra "Gestione deleghe" dove sono visualizzate in automatico le deleghe ricevute attive.

Figura 272 – Esercita delega

Accettando la delega ricevuta il delegato avrà l'accesso esclusivamente ai ruoli che gli sono stati assegnati dal delegante. Selezionando il pulsante "esercita" in automatico il delegato accede alla "lista delle cose da fare" del delegante. L'utente delegato visualizza in alto a destra nella pagina principale del sistema il suo nome seguito da quello del delegante; nella lista a tendina Scelta ruolo visualizza tutti i ruoli delegati all'utente.
Il delegato visualizza nella pagina principale l'elenco delle trasmissioni ricevute del Delegante.
Accedendo ad uno degli elementi potrà effettuare tutte le "mansioni" del delegante; il sistema traccia tali azioni ed eventi come eseguiti dal delegato.

4.12.5 Dismissione di una delega

Per dismettere la delega ricevuta ed espletata l'utente delegato accede alla sezione "Gestione deleghe", e dopo aver spuntato dall'elenco la delega da dimettere seleziona il pulsante Dismetti. Il sistema propone la pagina principale con l'elenco delle cose da fare del ruolo rivestito dall'utente all'interno del sistema.

Figura 273 – Dismetti delega

4.12.6 Modelli delega

Per le amministrazioni che la richiedano, è possibile utilizzare la funzionalità "Modelli delega" che consente di creare dei modelli di delega da utilizzare poi nel momento in cui si voglia creare una nuova delega.

La creazione di un modello prevede:

- la scelta di un nome da dare al modello
- la scelta del ruolo e dell'utente delegante
- la scelta di chi può utilizzare il modello: solo il ruolo che sta creando il modello o tutti i ruoli che ricopre l'utente
- la data di inizio validità
- la definizione di un intervallo di validità della delega creata a partire da quel modello (l'intervallo è espresso in giorni) o in alternativa la definizione di una data di fine.

Una volta definito uno o più modelli di delega, ogni volta che un utente ha bisogno di delegare qualcuno per un periodo di tempo e quindi ha bisogno di creare una delega, può semplicemente scegliere il modello con le caratteristiche di cui ha bisogno, in particolare il modello a cui corrisponde la persona che vuole delegare.
Se è attiva questa funzionalità, la voce "Modelli delega" comparirà accanto alle voci "Deleghe ricevute" e "Deleghe effettuate" come mostrato nella Figura 274

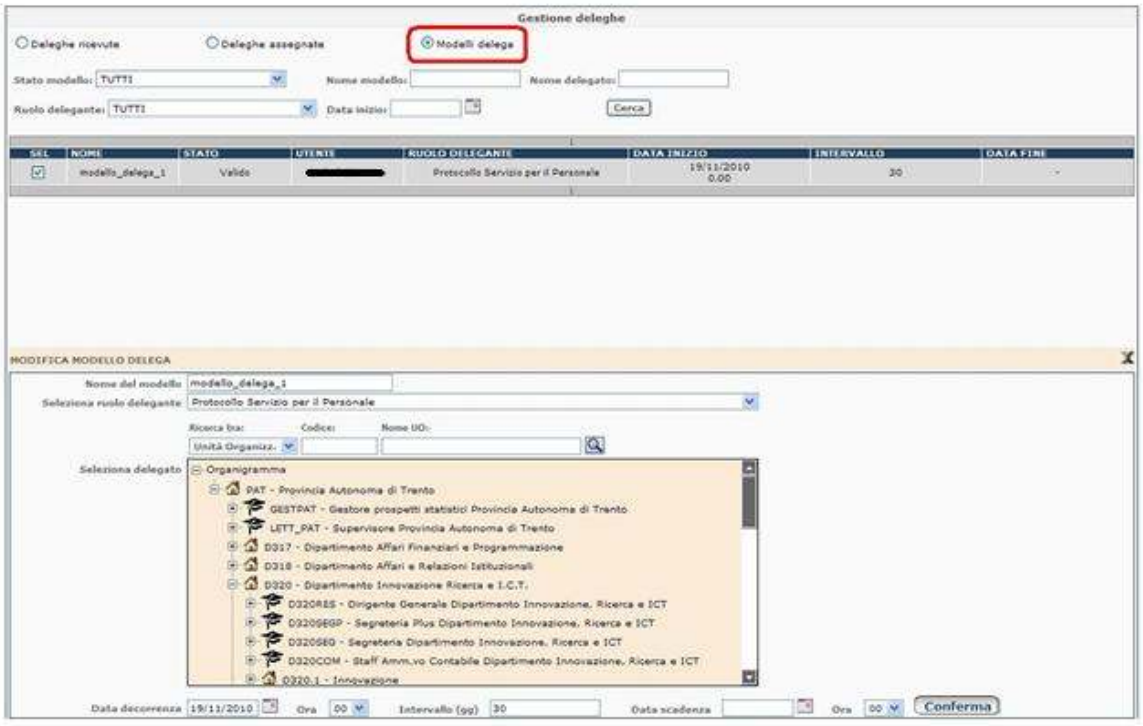


Figura 274 - Modelli delega

4.13 Elenco note

Selezionando la voce di menù **Gestione → Elenco note**, si apre il pannello proposto in Figura 275 che consente di effettuare l'inserimento, la modifica e la cancellazione manuale delle note.
Solo i ruoli autorizzati, con opportuno profilo funzionale possono accedere a tale pannello ed effettuare le operazioni suddette.

Tramite questa maschera è anche possibile inserire note importandole da un foglio excel. Per far questo è necessario selezionare la voce "*Inserimento da excel"*, selezionare il file .xls, caricarlo in locale ed effettuare l'inserimento.
Il modello da utilizzare può essere scaricato mediante il link *Scarica modello.*
I dati da impostare per l'inserimento delle note (manuale o con foglio excel) sono il codice dell'RF ed il testo della nota.

Figura 275 – Elenco note

Per ogni registro selezionato la funzioni disponibile è la seguente:

- **Cambia stato**: consente di cambiare lo stato del registro, ovvero di chiudere un registro aperto o di aprirne uno chiuso;

4.14 Importa documenti di emergenza

La funzione "Importa documenti d'emergenza" attivabile dalla voce di menù: **GESTIONE → Imp. RDE**, consente di importare i protocolli effettuati in emergenza tramite un apposito foglio excel.

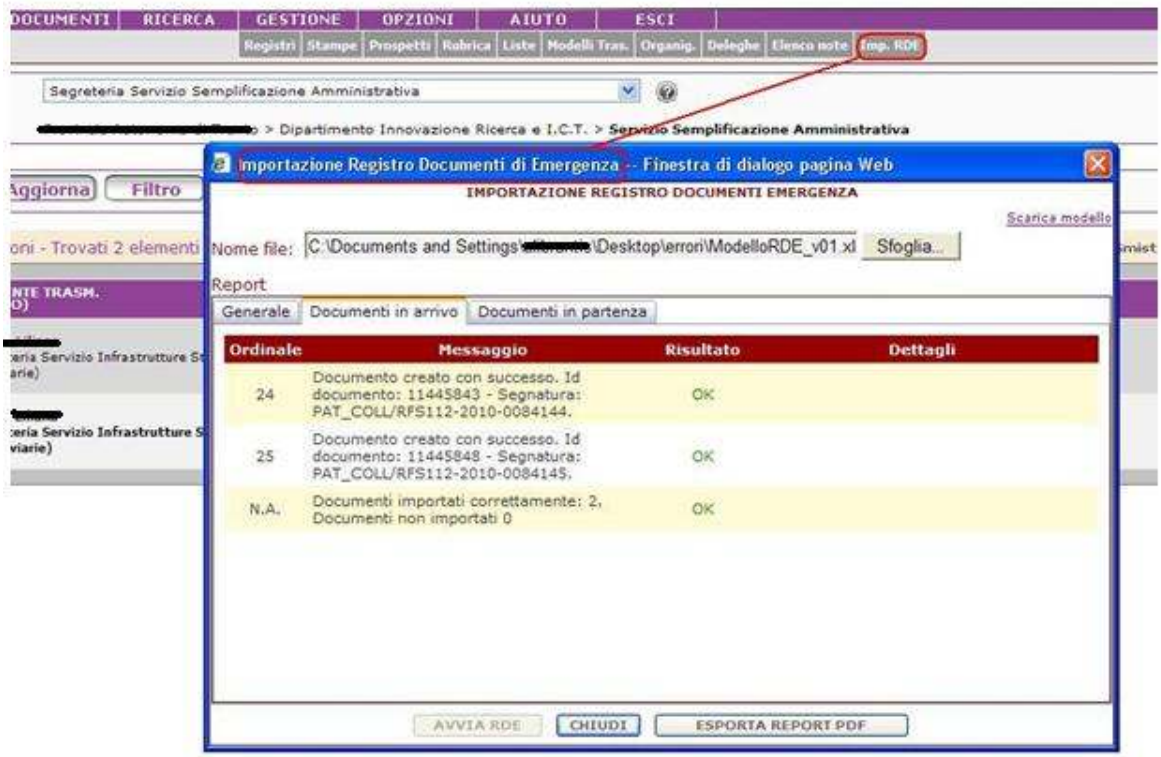


Figura 276 – Import documenti d'emergenza

La procedura di import fa uso di un particolare foglio excel. Il modello da utilizzare può essere scaricato tramite il link *Scarica modello* presente nella pagina di Figura 276.
Il foglio da utilizzare per l'importazione dei protocolli effettuati in emergenza ha le seguenti colonne:

CAMPO	DESCRIZIONE	ESEMPIO
Data protocollo emergenza	Data del protocollo emergenza	22/04/2010
Ora protocollo emergenza	Ora del protocolo di emergenza	13.45
Numero protocollo emergenza	Numero di protocollo emergenza	1
Stringa protocollo emergenza	Segnatura del protocollo emergenza	AMM/AOO/PR40577/0000001
Tipo protocollo	Tipolgia protocollo (A/P/I)	P
Oggetto		Progetto per le persone migranti che hanno sviluppato dipendenza da alcool e sostanze stupefacenti e progetto di prevenzione selettiva in materia di nuove droghe - richiesta posticipo data fine progetti
Mittente	Mittente del protocollo;	Presidenza del Consiglio
Destinatari	Destinatari del protocollo. Separati da ";"	Ministero dell'Interno; Ministero della salute
Destinatari_CC	Destinatari in cc del protocollo. Separati da ";"	
Codice amministrazione		
Codice Registro		
Data protocollo mittente		
Numero protocollo mittente		
Data arrivo		
Codice classifica	Codice del titolo o del fascicolo	4.10.2

Dopo aver compilato il foglio excel con i dati dei documenti da creare, se ne specifica il percorso sul file system nel campo *Nome file* e si avvia la procedura di import cliccando sul pulsante 

.
Dopo aver verificato la validità dei dati, il sistema avvierà la procedura di importazione. Per ogni tipologia di protocollo verrà riportato il numero di documenti importati, di quelli scartati, di eventuali errori o warning. Sarà poi possibile esportare il risultato dell'operazione in un file pdf cliccando il pulsante 

. Il pulsante 

consente di chiudere la pagina.
La funzionalità sarà disponibile solo per i ruoli autorizzati.

4.15 Stampa unione

La funzione "Stampa Unione" attivabile dalla voce di menù: **GESTIONE → Stampa Unione**, simula la 'stampa unione' di word consentendo così la creazione e la protocollazione di documenti a partire da un foglio excel (contenente i dati dei documenti da creare) e da un modello word da riempire con i valori presenti nel foglio. Il modello Word per la stampa unione è un modello rtf da associare (a cura dell'amministratore del sistema) alla tipologia del documento. Nel foglio excel deve essere specificata la tipologia del documento. Se non indicata, il documento verrà creato, ma ad esso non verrà associato alcun file. Tale procedura non tratta gli allegati.

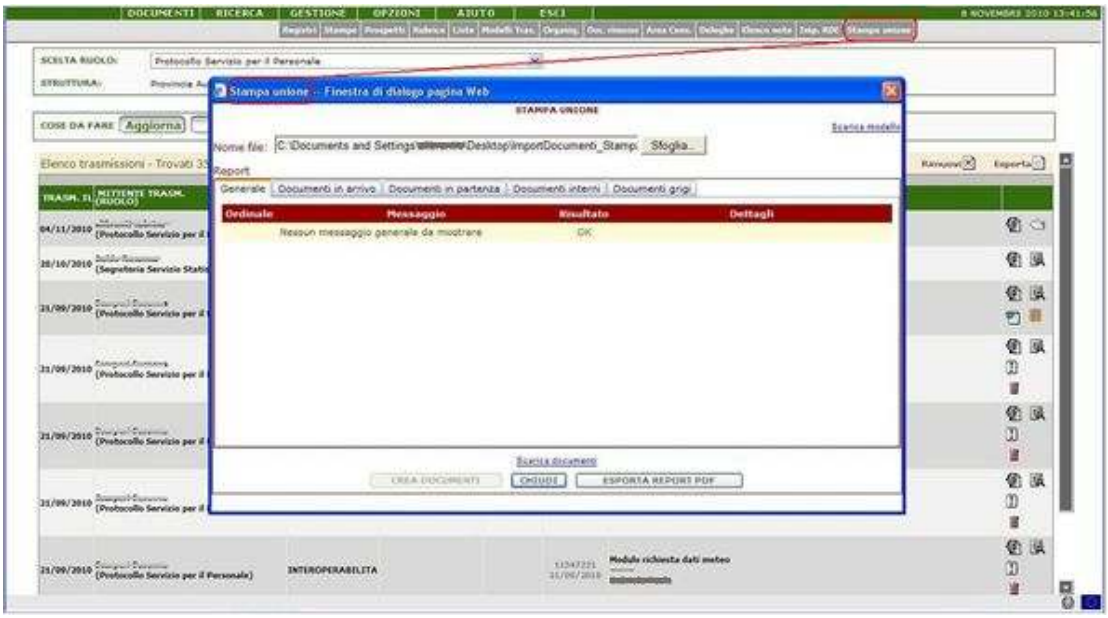


Figura 277 – Stampa unione

La procedura di stampa unione fa uso di un particolare file excel suddiviso in tanti fogli, uno per ogni tipo di documento. Il modello da utilizzare è simile a quello usato per l'import dei documenti e può essere scaricato tramite il link *Scarica modello* presente nella pagina di Figura 277.

Dopo aver compilato il foglio excel con i dati dei documenti da creare, si avvia la procedura di import cliccando sul pulsante CREA DOCUMENTI.
Dopo aver verificato la validità dei dati, il sistema avvia la procedura di importazione. Per ogni tipologia di documento verrà riportato il numero di documenti importati, di quelli scartati, di eventuali errori o warning. Sarà poi possibile esportare il risultato dell'operazione in un file pdf cliccando il pulsante ESPORTA REPORT PDF. Il pulsante CHIUDI consente di chiudere la pagina.
Il link *Scarica documenti* consente di scaricare in locale un file zip contenente i file creati a partire dal modello rtf e dai dati presenti nel foglio excel.

5 OPZIONI

La funzione "Cambia password" permette a ciascun utente di modificare la propria password di accesso all'applicativo.

6 AIUTO

La funzione "Aiuto" permette all'utente di visualizzare il Manuale utente (in formato pdf) all'interno di una finestra di dialogo. Il manuale utente è direttamente consultabile dall'interfaccia utente. Aprendo il manuale da una particolare area funzionale del sistema, questo si posiziona sul paragrafo o capitolo relativo.

7 ESCI

Permette di chiudere la sessione di lavoro.

8 LEGENDA DELLE ICONE

In questo capitolo viene riportata una sintetica descrizione delle icone utilizzate nel prodotto VTDOCS

ICONA	DESCRIZIONE	AZIONE
	Seleziona un oggetto dall'oggettario	Visualizza il pannello dell'oggettario per la selezione di un oggetto per la creazione di un nuovo documento o protocollo.
	Stampa	Stampa l'oggetto visualizzato
	Stampa Segnatura A4	Stampa su un foglio A4 la segnatura del documento, la posizione e le coordinate sono scelte dall'utente.
	Descrizione campo dell'oggetto	Consente di visualizzare per intero il testo contenuto nel campo oggetto
	Modifica	Consente di modificare i dati visualizzati del documento e/o fascicolo.
	Storia	Mostra la storia delle modifiche effettuate su un oggetto
	Seleziona mittente/destinatario nella rubrica	Visualizza il pannello della rubrica per la selezione di un mittente o destinatario. La ricerca può essere effettuata per utente interno, esterno o tutti e per Unità Organizzativa, ruolo o nominativo.
	Dettagli	Visualizza i dettagli di un oggetto
	Seleziona documenti protocollati da area di lavoro	Consente di selezionare un documento o un fascicolo tra quelli precedentemente inseriti nell'Area di Lavoro
	Mostra visibilità	Mostra l'elenco dei ruoli che hanno visibilità sul documento
	Seleziona parola chiave	Visualizza il pannello delle parole chiave inserite nella base dati utilizzate nei documenti
	Aggiungi	Aggiunge un oggetto (mittente, destinatario, parola chiave, etc.) in una lista (rubrica, oggettario, etc.)
	Cancella	Toglie un oggetto (mittente, destinatario, parola chiave, etc.) da una lista (rubrica, oggettario, etc.)
	Inserisci tra i destinatari per conoscenza	Sposta i nominativi selezionati dalla casella destinatari alla casella dei destinatari per conoscenza.
	Inserisci tra i destinatari	Sposta i nominativi selezionati dalla casella dei destinatari per conoscenza alla casella dei destinatari.
	Cerca / Avvia ricerca	Ricerca un oggetto nella base dati
	Acquisisci	Acquisisce da scanner un documento cartaceo o un file elettronico.
	Titolario	Visualizza il pannello del titolario di classificazione
	Inserisci documento/fascicolo in Area di Lavoro	Inserisce il documento/fascicolo selezionato nell'Area di Lavoro

ICONA	DESCRIZIONE	AZIONE
	Ricerca Fascicoli	Ricerca un fascicolo generale/procedimentale nella base dati
	Chiudi/riapri fascicolo	Chiude e riapre un fascicolo procedimentale
	Seleziona	Seleziona l'oggetto della riga
	Copia in locale	Copia in locale non attiva
	Copia in locale	Copia in locale attiva
	Controllo Ortografico	Consente di effettuare il controllo ortografico sul testo digitato nel campo oggetto
	Calendario	Il calendario è stato inserito in ogni campo legato alla data per la selezione di questa.
	Storia	Mostra la storia delle modifiche effettuate sul documento
	Multiclassificazione	Classifica il documento nei fascicoli selezionati dall'Area di Lavoro.
	Conservazione	Visualizza la storia del processo di conservazione a cui è stato sottoposto il documento.
	Inoltra	Crea un documento predisposto alla protocollazione in uscita con lo stesso oggetto del documento protocollato in ingresso che si vuole inoltrare.
	Visualizza	Visualizza l'immagine associata al documento e ai suoi eventuali allegati.
	Stampa ricevuta	Stampa la ricevuta di protocollo.
	Rispedizione ricevuta di ritorno	Rispedisce la ricevuta di ritorno al mittente del documento ricevuto per interoperabilità.
		Consente di inserire documenti e fascicoli risultanti da una ricerca in 'Area Conservazione'".
	Estensione	L'attivazione dell'icona mostra l'estensione del file acquisito e la visualizzazione del documento.
	Dettaglio documento	Permette di accedere al dettaglio documento (profilo, protocollo, classifica, allegati, trasmissioni) dai pulsanti di azione in un'unica colonna.
	Contenuto Fascicoli	Permette di visualizzare il contenuto del fascicolo dai pulsanti di azione in un'unica colonna.

ICONA	DESCRIZIONE	AZIONE
	Crea documento di risposta	Permette di creare un documento di risposta (*catena nera* per i documenti dello stesso tipo - grigio con grigio, protocollato con protocollato -, *catena grigia* per i documenti di tipo diverso)
	Documento arrivato per interoperabilità	E' solo un'icona che mette in evidenza i documenti arrivati per interoperabilità da una casella di posta non certificata
	Documento arrivato per interoperabilità	E' solo un'icona che mette in evidenza i documenti arrivati per interoperabilità da una casella di posta certificata
	Applica il timestamp ai documenti	il documento ha un timestamping valido (verde) il documento non ha timestamping (grigio) il documento ha un timestamping scaduto (rosso)
	Consolida contenuto	Consente di consolidare le versioni e gli allegati di un documento
	Consolida contenuto e metadati	Consente di consolidare le versioni, gli allegati ed i metadati di un documento
	Rimuovi versioni	Permette di rimuovere le vecchie versioni di documenti grigi o predisposti alla protocollazione e consolidati
	Ricerca personalizzata	Consente di personalizzare il risultato delle ricerche di documenti e fascicoli
	Rimuovi dall'area di lavoro	Rimuove documenti o fascicoli dall'area di lavoro
	Crea fascicolo da fascicolazione rapida	Consente di creare un nuovo fascicolo direttamente durante la fascicolazione rapida