



CITTÀ DI CHIOGGIA

MANUALE DI GESTIONE DEL

PROTOCOLLO INFORMATICO,

DEI **DOCUMENTI** e DEGLI **ARCHIVI**
DELLA **CITTA' DI CHIOGGIA**

Area Organizzativa Omogenea Città di Chioggia

Sommario

PRINCIPI GENERALI

1.1. Premessa	5
1.2. Ambito di applicazione del manuale	5
1.3. Definizioni e norme di riferimento	5
1.4. Area Organizzativa Omogenea	6
1.5. Servizio per la gestione informatica del protocollo	6
1.6. Conservazione delle copie di riserva	6
1.7. Firma digitale	7
1.8. Tutela dei dati personali	7
1.9. Caselle di Posta Elettronica.....	7
1.10. Sistema di classificazione dei documenti	7
1.11. Formazione	7
1.12. Accreditalamento dell'AOO all'IPA	7

2. ELIMINAZIONE DEI REGISTRI DI PROTOCOLLO DIVERSI DAL REGISTRO UFFICIALE DI PROTOCOLLO INFORMATICO8

2.1. Piano di attuazione	8
--------------------------------	---

3. GESTIONE DEI DOCUMENTI INFORMATICI

3.1. Gestione dei documenti informatici	8
3.2. Trasmissione e interscambio dei documenti informatici	8
3.2.1 Interoperabilità dei sistemi di protocollo informatico	8
3.3. Accesso ai documenti informatici	9
3.3.1. Utenti interni alla AOO	9
3.3.2. Accesso al registro di protocollo per utenti interni alla AOO	9
3.3.3. Utenti esterni alla AOO - Altre AOO/Amministrazioni	10
3.4. Conservazione dei documenti informatici	10
3.4.1. Servizio archivistico	10
3.4.2. Conservazione del registro giornaliero di protocollo	10

4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI..... 11

4.1. Documento ricevuto	12
4.2. Documento inviato	12
4.3. Documento interno formale	12
4.4. Documento interno informale	13
4.5. Il documento analogico - cartaceo	13
4.6. Formazione dei documenti - Aspetti operativi	13
4.7. Sottoscrizione di documenti informatici	14
4.8. Requisiti degli strumenti informatici di scambio	14
4.9. Firma digitale	14
4.10. Verifica delle firme nel SdP per i formati .p7m	14
4.11. Uso della posta elettronica certificata	14

5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI15

5.1. Generalità	15
5.2. Flusso dei documenti in ingresso alla AOO	15
5.2.1. Provenienza esterna dei documenti	15
5.2.2. Provenienza di documenti interni formali	16
5.2.3. Ricezione di documenti informatici sulla casella di posta istituzionale	16
5.2.4. Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale	16
5.2.5. Ricezione di documenti informatici su supporti rimovibili	16
5.2.6. Ricezione di documenti cartacei a mezzo posta convenzionale	17

5.2.7. Errata ricezione di documenti digitali	17
5.2.8. Errata ricezione di documenti cartacei	17
5.2.9. Attività di protocollazione dei documenti	17
5.2.10. Rilascio di ricevute attestanti la ricezione di documenti informatici	17
5.2.11. Rilascio di ricevute attestanti la ricezione di documenti cartacei	17
5.2.12. Conservazione dei documenti informatici	18
5.2.13. Conservazione delle copie per immagine di documenti cartacei	18
5.2.14. Assegnazione, presa in carico dei documenti e classificazione.	18
5.2.15. Conservazione dei documenti nell'archivio corrente	18
5.2.16. Conservazione dei documenti e dei fascicoli nella fase corrente	18
5.3. Flusso dei documenti in uscita dalla AOO	18
5.3.1. Sorgente interna dei documenti	19
5.3.2. Registrazione di protocollo e segnatura	19
5.3.3. Trasmissione di documenti informatici	19
5.3.4. Trasmissione di documenti cartacei a mezzo posta	19
5.3.5. Affrancatura dei documenti in partenza	19
5.3.6. Documenti in partenza per posta convenzionale con più destinatari	19
5.3.7. Inserimento delle ricevute di trasmissione nel fascicolo	20
6. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI	20
6.1. Regole disponibili con il SdP	20
6.2. Attività di assegnazione	20
6.3. Corrispondenza di particolare rilevanza.....	20
6.4. Assegnazione dei documenti ricevuti in formato digitale	20
6.5. Assegnazione dei documenti ricevuti in formato cartaceo	21
6.6. Modifica delle assegnazioni	21
7. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI INVIATI	21
8. UO RESPONSABILE DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, ORGANIZZAZIONE E TENUTA DEI DOCUMENTI	21
8.1. Servizio archivistico	22
9. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE	22
9.1. Documenti esclusi	22
9.2. Documenti soggetti a registrazione particolare	22
10. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE.....	22
10.1. Protezione e conservazione degli archivi pubblici	22
10.1.1. Caratteristiche generali	22
10.1.2. Misure di protezione e conservazione degli archivi pubblici	22
10.2. Titolario o piano di classificazione	23
10.2.1. Titolario	23
10.2.2. Classificazione dei documenti	23
10.3. Fascicoli e dossier	23
10.3.1. Fascicolazione dei documenti	24
10.3.2. Apertura del fascicolo	24
10.3.3. Chiusura del fascicolo	24
10.3.4. Processo di assegnazione dei fascicoli	24
10.3.5. Repertorio dei fascicoli	24
10.4. Consultazione e movimentazione dell'archivio corrente, di deposito e storico	25
10.4.1. Principi generali	25
10.4.2. Consultazione ai fini giuridico-amministrativi	25

10.4.3. Consultazione da parte di personale esterno all'amministrazione	26
10.4.4. Consultazione da parte di personale interno all'amministrazione	26

**11. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI
DI PROTOCOLLO INFORMATICO26**

11.1. Unicità del protocollo informatico	27
11.2. Registro giornaliero di protocollo	27
11.3. Registrazione di protocollo	27
11.3.1. Documenti informatici	28
11.3.2. Documenti analogici (cartacei e supporti rimovibili)	28
11.4. Elementi facoltativi delle registrazioni di protocollo	28
11.5. Segnatura di protocollo dei documenti	28
11.5.1. Documenti informatici	28
11.5.2. Documenti cartacei	29
11.6. Annullamento delle registrazioni di protocollo.....	29
11.7. Livello di riservatezza	30
11.8. Casi particolari di registrazioni di protocollo.....	30
11.8.1. Circolari e disposizioni generali.....	30
11.8.2. Documenti cartacei in uscita con più destinatari	30
11.8.3. Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio	30
11.8.4. Fatture, assegni e altri valori di debito o credito	30
11.8.5. Protocollazione di documenti inerenti gare di appalto confezionate su supporti cartacei.....	30
11.8.6. Protocolli urgenti.....	30
11.8.7. Documenti non firmati	31
11.8.8. Protocollazione dei messaggi di posta elettronica convenzionale	31
11.8.9. Protocollazione di documenti digitali pervenuti erroneamente	31
11.8.10. Ricezione di documenti cartacei pervenuti erroneamente	31
11.8.11. Copie per "conoscenza"	31
11.8.12. Differimento delle registrazioni	31
11.8.13. Corrispondenza personale o riservata	31
11.8.14. Integrazioni documentarie	32
11.9. Gestione delle registrazioni di protocollo con il SdP	32
11.10. Registrazioni di protocollo	32
11.10.1. Attribuzione del protocollo	32
11.10.2. Registro informatico di protocollo	32
11.10.3. Tenuta delle copie del registro di protocollo	32

**12. DESCRIZIONE DELLE FUNZIONI E DELLE MODALITÀ' OPERATIVE DEL
SISTEMA DI PROTOCOLLO INFORMATICO.....32**

12.1. Descrizione funzionale ed operativa	32
---	----

13. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA 32

13.1. Il registro di emergenza.....	33
13.2. Modalità di apertura del registro di emergenza	33
13.3. Modalità di utilizzo del registro di emergenza	34
13.4. Modalità di chiusura e di recupero del registro di emergenza	34

**14. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE
E FINALI 34**

14.1. Modalità di approvazione e aggiornamento del manuale.....	34
14.2. Regolamenti abrogati	34
14.3. Pubblicità del presente Manuale	35
14.4. Operatività del presente manuale	35

PRINCIPI GENERALI

1.1. Premessa

Il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico", articolo 3, comma 1, lettera d), prevede l'adozione del manuale di gestione per tutte le amministrazioni di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale. Il manuale di gestione, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi". In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 50 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000).

Obiettivo del Manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili per gli addetti al servizio e per i soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'attività dell'amministrazione. Il manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

Il presente documento, pertanto, si rivolge non solo agli operatori di protocollo, ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

Il manuale è articolato in due parti: nella prima vengono indicati l'ambito di applicazione, le definizioni usate e i principi generali del sistema, nella seconda sono descritte analiticamente le procedure di gestione dei documenti e dei flussi documentali.

1.2. Ambito di applicazione del manuale

Il presente manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'articolo 3, comma 1, lettera d) del decreto del Presidente del Consiglio del 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico".

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'Amministrazione Comunale della Città di Chioggia.

Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e della spedizione di un documento.

1.3. Definizioni e norme di riferimento

Ai fini del presente manuale si intende per:

"amministrazione", il Comune di Chioggia

"Testo Unico", il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

"Regole tecniche", il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico";

"Codice", il decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale.

Per la definizione di AOO vedasi l'allegato 1.

Di seguito si riportano gli acronimi utilizzati più frequentemente:

AOO - Area Organizzativa Omogenea;

MdG - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;

RPA - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;

RSP - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;

SdP – Servizio di protocollo informatico;

UOP - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo (tutti gli uffici per protocolli in uscita – Protocollo Generale, Urbanistica, Polizia Locale per protocolli in ingresso);

UOR - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;

UU - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal servizio di protocollo informatico; ovvero il soggetto, destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Per le norme ed i regolamenti di riferimento vedasi le norme in atto delle leggi su protocollo informatico, archivi e flussi documentali.

1.4. Area Organizzativa Omogenea

Per la gestione dei documenti l'amministrazione ha istituito un'unica Area Organizzativa Omogenea (AOO) dove è istituito un unico servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

All'interno dell'amministrazione il sistema archivistico è unico.

All'interno della AOO il sistema di protocollazione è organizzato con postazioni di protocollo in ingresso: Protocollo Generale, Urbanistica e Polizia Locale mentre per le postazioni di protocollo in uscita tutti gli utenti dell'Amministrazione sono abilitati a protocollare corrispondenza in uscita.

La corrispondenza sia in ingresso che in uscita è gestita da una sola UOP e precisamente dal Servizio di Protocollo Generale.

1.5. Servizio per la gestione informatica del protocollo

Nella AOO è istituito il servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Al suddetto servizio è preposto il responsabile del servizio di protocollo informatico.

In relazione alla modalità di fruizione del servizio di protocollo adottata dalla AOO, è compito del servizio:

- predisporre lo schema del manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;

- provvedere alla pubblicazione del manuale sul sito istituzionale dell'amministrazione;

- abilitare gli utenti dell'AOO all'utilizzo del SdP e definire per ciascuno di essi il tipo di funzioni più appropriate tra quelle disponibili;

- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;

- garantire la corretta conservazione della copia del registro giornaliero di protocollo;

- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;

- garantire il buon funzionamento degli strumenti interni all'AOO e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno;

- autorizzare le eventuali operazioni di annullamento della registrazione di protocollo;

- vigilare sull'osservanza delle disposizioni delle norme vigenti da parte del personale autorizzato e degli incaricati;

- curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza con gli strumenti e le funzionalità disponibili nel SdP.

1.6. Conservazione delle copie di riserva

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, nella giornata lavorativa successiva, il contenuto del registro informatico di protocollo, viene inviato in conservazione.

1.7. Firma digitale

Per l'espletamento delle attività istituzionali l'amministrazione fornisce la firma digitale ai soggetti da essa delegati a rappresentarla. Nell'allegato 10 viene riportato l'elenco delle persone titolari di firma digitale (fornito dai Servizi Informatici - Ced).

1.8. Tutela dei dati personali

L'amministrazione titolare dei dati di protocollo e dei dati personali, comuni, sensibili e/o giudiziari, contenuti nella documentazione amministrativa di propria competenza ha ottemperato al dettato del decreto legislativo 30 giugno 2003, n.196 con atti formali aventi rilevanza interna ed esterna.

1.9. Caselle di Posta Elettronica

L'AOO si dota di una casella di posta elettronica certificata istituzionale per la corrispondenza, sia in ingresso che in uscita. Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UOR) che ad essa fanno riferimento.

In attuazione di quanto previsto dalla Direttiva del Ministro per l'Innovazione e le Tecnologie 18 novembre 2005 sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione munisce i propri dipendenti di una casella di posta elettronica convenzionale.

1.10. Sistema di classificazione dei documenti

Con l'inizio dell'attività operativa del protocollo informatico viene adottato un unico titolare di classificazione per l'archivio centrale unico dell'amministrazione.

Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base dell'organizzazione funzionale dell'AOO, consentendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.

La definizione del sistema di classificazione è stata effettuata prima dell'avvio del sistema di protocollo informatico.

Al fine di agevolare e normalizzare, da un lato la classificazione archivistica e dall'altro l'assegnazione per competenza, sul SdP è stato predisposto un elenco degli Uffici Utente e dei dipendenti unitamente a quello di classificazione. L'elenco è una guida rapida di riferimento, in ordine alfabetico che, sulla base del titolare, permette l'immediata individuazione della classificazione e delle competenze.

1.11. Formazione

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni sulla formazione e la valorizzazione del personale delle pubbliche amministrazioni, l'amministrazione stabilisce percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.

1.12. Accreditamento dell'AOO all' IPA

L'AOO, come accennato si è dotata di una casella di posta elettronica certificata – chioggia@pec.chioggia.org attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della UOP incaricata; quest'ultima procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta. La ricezione della corrispondenza inviata con la P.E.C. in ingresso è in capo al SdP, mentre per la spedizione della corrispondenza in uscita con l'utilizzo della P.E.C. ogni UOP protocolla ed invia direttamente la propria corrispondenza. L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'indice delle pubbliche amministrazioni (IPA). Il codice identificativo dell'amministrazione è stato generato e attribuito dall'IPA.

L'indice delle pubbliche amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa, in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività l'amministrazione comunica la soppressione, ovvero la creazione di una AOO.

2. ELIMINAZIONE DEI REGISTRI DI PROTOCOLLO DIVERSI DAL REGISTRO UFFICIALE DI PROTOCOLLO INFORMATICO

Il presente capitolo riporta la pianificazione, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli diversi dal protocollo informatico.

2.1. Piano di attuazione

In coerenza con quanto previsto e disciplinato dal presente manuale, tutti i documenti inviati e ricevuti dalla AOO sono registrati all'interno del registro ufficiale di protocollo informatico. Pertanto, tutti gli eventuali registri di protocollo, interni agli UOR e/o agli UU, diversi dal registro ufficiale di protocollo informatico, sono aboliti ed eliminati con l'entrata in vigore del manuale stesso.

3. GESTIONE DEI DOCUMENTI INFORMATICI

3.1. Gestione dei documenti informatici

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente. Il sistema operativo del *server* che ospita i *file* utilizzati come deposito dei documenti è configurato in maniera da consentire:

l'accesso esclusivamente al *server* del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;

la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;

assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;

consente il reperimento delle informazioni riguardanti i documenti registrati;

consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili e giudiziari;

garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

3.2. Trasmissione e interscambio dei documenti informatici

Gli addetti della AOO alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il *server* di posta certificata del fornitore esterno (*provider*) di cui si avvale l'AOO, oltre alle funzioni di un *server* SMTP tradizionale, svolge anche le seguenti operazioni:

accesso all'indice dei gestori di posta elettronica certificata, allo scopo di verificare il gestore mittente;

mantenere l'integrità del messaggio e del suo contenuto;

archivio di sicurezza;

gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

3.2.1. Interoperabilità dei sistemi di protocollo informatico

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo

mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

Il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal Codice dell'Amministrazione Digitale.

3.3. Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso, UserID e Password ed un sistema di autorizzazione basato sulla profilazione degli utenti.

La profilazione consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale. Queste, in sintesi, sono:

consultazione, per visualizzare in modo selettivo, le registrazioni di protocollo eseguite da altri;

inserimento, per inserire gli estremi di protocollo e effettuare una registrazione di protocollo ed associare i documenti;

modifica, per modificare i dati opzionali di una registrazione di protocollo;

annullamento, per annullare una registrazione di protocollo autorizzata dal RSP.

Le regole per la composizione delle *password* e il blocco delle utenze valgono sia per gli amministratori della AOO che per gli utenti della AOO.

Le relative politiche di composizione, aggiornamento e, in generale di sicurezza, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.

Il SdP fruito dall'AOO:

consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente, o gruppi di utenti;

assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una *Access Control List* (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

Considerato che il SdP segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.

Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca *full text*.

3.3.1. Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RSP dell'AOO. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti principi operativi:

gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta esplicita dell'amministratore dell'AOO o per errori di inserimento)

la credenziale privata degli utenti e dell'amministratore AOO non transita in chiaro sulla rete, né al momento della prima generazione, né successivamente al momento del *login*.

3.3.2. Accesso al registro di protocollo per utenti interni alla AOO

L'autorizzazione all'accesso ai registri di protocollo è regolata tramite i seguenti strumenti:

ruoli degli utenti, gestiti dall'amministratore di ente (amministrazione), per la specificazione delle macrofunzioni alle quali vengono abilitati;

protocollazione "*particolare o riservata*", gestita dall'amministratore di ente, relativa a documenti sottratti alla consultazione da parte di chi non sia espressamente abilitato.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di "Responsabile del registro" e limitatamente al registro dell'AOO sul quale è stato abilitato ad operare. L'utente assegnatario dei documenti protocollati è invece abilitato ad una vista parziale sul registro di protocollo. Tale vista è definita dalle voci di titolare associate alla lista di competenza in cui l'utente è presente (sia come singolo, sia come ufficio).

L'operatore che gestisce lo smistamento dei documenti può definire riservato un protocollo ed assegnarlo per competenza ad un utente assegnatario.

Nel caso in cui sia effettuata una protocollazione riservata la visibilità completa sul documento è possibile solo all'utente a cui il protocollo è stato assegnato per competenza e ai protocollatori che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo).

Tutti gli altri utenti (seppure inclusi nella giusta lista di competenza) possono accedere solo ai dati di registrazione (ad esempio: progressivo di protocollo, data di protocollazione) mentre vedono mascherati i dati relativi al profilo del protocollo (ad esempio: classificazione).

3.3.3. Utenti esterni alla AOO

Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.

3.4. Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene sulla base delle disposizioni riportate nel:

DPCM 13 novembre 2014, per quanto attiene ai documenti informatici presenti nell'archivio corrente dell'Ente.

DPCM 3 dicembre 2013 per i documenti inviati in conservazione.

3.4.1. Servizio archivistico

Il responsabile del sistema archivistico dell'intera amministrazione, ha individuato nei locali del primo piano del Museo Civico "S. Francesco fuori le mura", del piano terra del Palazzo Municipale e negli armadi ubicati nei diversi Servizi e/o Uffici delle sedi istituzionali dell'amministrazione medesima, la sede del relativo archivio storico, di deposito e corrente dell'amministrazione.

Il responsabile del servizio in argomento ha effettuato la scelta alla luce dei vincoli logistici imposti dagli edifici e della valutazione dei fattori di rischio che incombono sui documenti. Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha, in corso di perfezionamento, un piano specifico individuando, i soggetti incaricati di ciascuna fase.

Al riguardo, sono state regolamentate le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.

Il responsabile dell'archivio è a conoscenza, in ogni momento, della collocazione del materiale archivistico, avendo, a tal fine, predisposto degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.

Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità, nel tempo, di tutti i documenti trasmessi o ricevuti, adottando i formati previsti dalle regole tecniche vigenti.

3.4.2. Conservazione del registro giornaliero di protocollo

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Al riguardo di seguito si descrivono le modalità di produzione di invio in conservazione delle registrazioni di protocollo informatico con l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire l'immodificabilità della registrazione medesima. Tali modalità sono riportate nel manuale di conservazione del Comune di Chioggia.

Il SdP provvede all'esecuzione automatica della stampa su file in formato PDF del Registro giornaliero di protocollo. Il documento così creato riporta su un unico file con estensione PDF il riepilogo di tutte le registrazioni di protocollo eseguite nell'ambito della medesima giornata e, a seguire, gli eventuali annullamenti (parziali o totali) occorsi ai protocolli acquisiti nel corso dei giorni precedenti.

Per quanto attiene ai meta dati da inviare in conservazione unitamente alla copia del registro di cui sopra, sono stati suddivisi in tre sottogruppi:

Metadati di identificazione. Contengono le informazioni relative all'ente che sta inviando il documento (*File.PDF*) al conservatore e quelle del protocollo che identificano univocamente il documento. Sono memorizzati tra le proprietà del sistema (Ente, struttura, ecc.) e sulla registrazione del documento.

Metadati di profilo generali. Contengono le informazioni generali sul documento, come oggetto e data. Sono memorizzati sulla registrazione di protocollo.

Metadati di profilo specifici. Contengono le informazioni specifiche del tipo di documento, come numero di protocolli effettuati nella giornata, numero iniziale e numero finale. Sono memorizzati sulla registrazione di protocollo e tra le proprietà dell' Area Organizzativa Omogenea.

La produzione del documento avviene dopo la chiusura del Registro di protocollo e prima della riapertura al giorno successivo in modo che nessun altro documento possa essere protocollato nel registro della giornata precedente né in modalità manuale né in modalità automatica.

All'avvio del processo di creazione del pacchetto di versamento vengono elaborati i dati presenti nel registro di protocollo al fine di:

1. Ottenere i meta dati di profilo specifici da inviare al sistema di conservazione (Numero iniziale, Numero Finale, Data inizio registrazione, Numero di documenti registrati, Numero di documenti annullati).
2. Effettuare la registrazione del file PDF nel registro/repertorio stabilito e memorizzare tra gli attributi estesi del documento quelli calcolati precedentemente.
3. Predisporre il documento all'invio in conservazione indicando lo stato "da conservare".
4. In caso di anomalia durante il flusso inviare una notifica al responsabile della conservazione.

Il trasferimento del Pacchetto di versamento al sistema di conservazione avviene tramite canale *Web* che viene inviato manualmente al sistema di conservazione e registra lo stato del versamento stesso.

Il processo provvede a:

1. Estrarre dal registro giornaliero il documento da inviare in conservazione. *In generale è presente un solo documento da inviare ma nel caso sia avvenuto un problema nei giorni precedenti si effettua l'invio di tutti i documenti in attesa.*
2. Predisporre il pacchetto di versamento estraendo le informazioni necessarie dal documento e dal sistema.
3. In caso di esito positivo indicare nel documento lo stato "conservato".
4. In caso di esito negativo indicare nel documento lo stato "errore".

Nelle more di avvio del servizio di invio in conservazione sopra descritto il file PDF del registro giornaliero è registrato nel registro di protocollo interno del Comune di Chioggia a tutela della immodificabilità del medesimo ai sensi dell'art.3, comma 4, lettera d), del DPCM 13 novembre 2014.

4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'AOO.

Prima di entrare nel merito, occorre caratterizzare l'oggetto di scambio: il documento amministrativo.

Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è così classificabile:

- ricevuto;
- inviato;
- interno formale;
- interno informale.

Il documento amministrativo come oggetto di scambio, in termini tecnologici è così classificabile:

- informatico;
- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71" e "2. Fermo

restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità".

Pertanto, soprattutto nella fase transitoria di migrazione verso l'adozione integrale delle tecnologie digitali da parte dell'amministrazione, il documento amministrativo può essere disponibile anche nella forma analogica.

4.1. Documento ricevuto

La corrispondenza in ingresso può essere acquisita dalla AOO con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente. Un documento informatico può essere recapitato:

1. a mezzo posta elettronica convenzionale o certificata;
2. su supporto rimovibile quale, ad esempio, *cd rom, dvd, disk, pen drive*, consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per telegramma;
4. con consegna diretta da parte dell'interessato tramite una persona dallo stesso delegata alle UOP e/o agli UOR aperti al pubblico.

A fronte delle tipologie descritte ne esiste una terza denominata "Ibrida" composta da un documento analogico (lettera di accompagnamento) e da un documento digitale che comportano diversi metodi di acquisizione.

4.2. Documento inviato

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma, per mezzo della sola posta elettronica certificata se la dimensione del documento e/o di eventuali allegati, non supera la dimensione massima prevista, dal sistema di posta utilizzato dall'AOO, che è di 37 *Megabytes*, e con un limite di 50 destinatari.

In caso contrario, il documento informatico viene copiato, su supporto digitale rimovibile non modificabile e trasmesso al destinatario con altri mezzi di trasporto.

4.3. Documento interno formale

I documenti interni sono formati con tecnologie informatiche e, solo nella fase transitoria, lo scambio tra UOR/UU della AOO di documenti informatici di rilevanza amministrativa giuridico-probatoria, dopo averli trasformati in analogici, avviene per mezzo della posta interna cartacea.

In questo caso il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa sia sull'originale che sulla minuta e successivamente protocollato.

L'attività obbligatoria per la spedizione di un documento interno formale è la seguente:

- allegare sempre il documento principale firmato (su carta o digitalmente) al momento della protocollazione della corrispondenza in uscita;
- inserire inoltre, sempre, gli eventuali allegati al documento principale al momento della protocollazione della corrispondenza in uscita;
- procedere all'assegnazione (pulsante ASSEGNA) all'ufficio/servizio, prima di aver protocollato la corrispondenza in uscita. La modalità di selezione dell'ufficio di destinazione si attua mediante l'utilizzo della selezione "Organigramma Uffici" e/o "Organigramma Utenti".

Le attività utili ai fini dell'attività di ricerca nella fase di protocollazione della corrispondenza in uscita sono le seguenti:

- Inserire la classificazione utilizzando il menù a tendina che consente di individuarla direttamente dal "titolarlo"; tale dato risulta particolarmente utile in chiave di ricerca e di archiviazione del documento;
- compilare i campi relativi ad: ufficio competente, data del documento, data di invio/spedizione;
- effettuare un collegamento fra protocolli antecedenti e susseguenti creando una "catena documentale" fra documenti inerenti la stessa pratica, utilizzando il pulsante "Collegati".

4.4. Documento interno informale

Per questa tipologia di corrispondenza vale quanto illustrato nel paragrafo precedente ad eccezione della obbligatorietà dell'operazione di sottoscrizione e di protocollazione. Di conseguenza, per la formazione, la gestione e la sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascun UOR o UU della AOO adotta, nei limiti della propria autonomia organizzativa, le regole sopra illustrate ad eccezione della obbligatorietà dell'operazione di sottoscrizione e di protocollazione.

4.5. Il documento analogico - cartaceo

Per documento analogico si intende un documento amministrativo formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale. Di seguito si farà riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o *text editor*) e poi stampata.

In quest'ultimo caso si definisce "originale" il documento cartaceo, nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali in possesso di tutti i requisiti di garanzia e d'informazione del mittente e del destinatario, stampato su carta intestata e munito di firma autografa.

Un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione sostitutiva, descritte nel seguito del manuale.

4.6. Formazione dei documenti - Aspetti operativi

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa.

Ogni documento formato per essere inoltrato formalmente all'esterno o all'interno:

- deve trattare un unico argomento, indicato in maniera sintetica ma esaustiva dall'autore nello spazio riservato all'oggetto;

- deve essere identificato univocamente da un solo numero di protocollo;
- può fare riferimento a più fascicoli.

Le firme (*e le sigle se si tratta di documento analogico*) necessarie alla redazione e perfezione sotto il profilo giuridico del documento in partenza devono essere apposte prima della sua protocollazione.

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dal responsabile dei singoli UOR.

Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della AOO e dell'UOR che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione (via, numero civico, CAP, città, provincia);
- il numero di telefono della UOR;
- il codice fiscale dell'amministrazione.

Il documento deve inoltre recare almeno le seguenti informazioni:

- il luogo di redazione;
- la data (giorno, mese, anno);
- il numero di protocollo;
- il numero degli allegati, se presenti;
- l'oggetto;
- firma elettronica avanzata da parte dell'istruttore del documento e sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale; se trattasi di documento digitale,
- sigla autografa dell'istruttore e sottoscrizione autografa del responsabile del procedimento amministrativo (RPA) e/o del responsabile del provvedimento finale, se trattasi di documento cartaceo

4.7. Sottoscrizione di documenti informatici

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.

I documenti informatici prodotti dall'AOO, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità.

4.8. Requisiti degli strumenti informatici di scambio

Scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi è garantire sia l'interoperabilità, sia i requisiti minimi di sicurezza di seguito richiamati:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno della AOO;
- l'interconnessione tra AOO, ovvero l'interconnessione tra le UOP/UOR e UU, nel caso di documenti interni formali;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

4.9. Firma digitale

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 4.8 è la firma digitale utilizzata per inviare e ricevere documenti per l'AOO per sottoscrivere documenti, o qualsiasi altro *file* digitale con valenza giuridico-probatoria.

I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità. Tale processo si realizza con modalità conformi a quanto prescritto dalla normativa vigente in materia.

4.10. Verifica delle firme nel SdP per i formati .p7m

Nel SdP sono previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare. La sequenza delle operazioni previste è la seguente.

- apertura della busta "virtuale" contenente il documento firmato;
- verifica della validità del certificato; questa attività è realizzata verificando *on-line* le *Certificate Revocation List* (CRL)
- verifica dell'utilizzo, nell'apposizione della firma, di un certificato emesso da una *Certification Authority* (CA) presente nell'elenco pubblico dei certificatori accreditati e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle CA accreditate presso l'AgID con cadenza periodica;
- trasformazione del documento in uno dei formati standard previsto dalla normativa vigente in materia (PDF o XML o TIFF) e attribuzione della segnatura di protocollo;
- inserimento nel sistema documentale del SdP sia del documento originale firmato, sia del documento in chiaro;
- archiviazione delle componenti verificate e dei dati dei firmatari rilevati dal certificato in una tabella del database del SdP per accelerare successive attività di verifica di altri documenti ricevuti.

4.11. Uso della posta elettronica certificata

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.

Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo (cfr. par. 3.5 Trasmissione e interscambio dei documenti informatici). Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo è necessario eseguire le seguenti operazioni:

- Redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno: denominazione, indirizzo, casella di posta elettronica); firmare il documento (ed eventualmente associare il riferimento temporale al documento firmato);
- assegnare il numero di protocollo in uscita al documento firmato digitalmente o firmato e scansionato;

- ❑ inviare il documento firmato e protocollato in uscita alla casella di posta elettronica certificata del destinatario (procedura che effettua ogni stazione di protocollo in uscita presente all'interno di ogni UOP).

L'utilizzo della posta elettronica certificata (PEC) consente di:

firmare elettronicamente il messaggio;

conoscere in modo inequivocabile la data e l'ora di trasmissione;

garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario; interoperare e cooperare dal punto di vista applicativo con altre AOO.

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema di protocollazione della AOO ricevente. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato.

I messaggi di ritorno, che sono classificati in:

conferma di ricezione: (ricevuta di consegna e ricevuta di accettazione);

notifica di eccezione;

aggiornamento di conferma;

annullamento di protocollazione;

sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME.

Il servizio di posta elettronica certificata è strettamente correlato all'indice della pubblica amministrazione (IPA), dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico redatto in conformità alla normativa vigente e alle relative regole tecniche sono opponibili ai terzi. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notifica per mezzo della posta nei casi consentiti dalla legge.

5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, e le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione. L'UOP non effettua fotocopie della corrispondenza trattata, sia in ingresso che in uscita.

5.1. Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flusso riportati nelle pagine seguenti.

Tali flussi sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico probatoria. Essi si riferiscono ai documenti:

ricevuti dalla AOO, dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno alla AOO;

inviati dalla AOO, all'esterno o anche all'interno della AOO in modo formale.

I flussi gestiti all'interno del sistema archivistico dell'amministrazione/AOO dalla sezione di deposito e storica dell'archivio sono sviluppati, per omogeneità e completezza di trattazione, nel successivo capitolo 10. Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni è ricevuto e trasmesso per posta elettronica interna e non interessa il sistema di protocollo.

5.2. Flusso dei documenti in ingresso alla AOO

5.2.1. Provenienza esterna dei documenti

Oltre quelli richiamati nel capitolo precedente, i documenti trasmessi da soggetti esterni all'AOO possono essere tra gli altri eventuali supporti digitali rimovibili allegati a documenti cartacei. Questi documenti sono recapitati al Servizio di Protocollo Generale. La UOP protocolla i documenti, li scansiona e li assegna alle

UOR in indirizzo. L'assegnazione avviene con l'invio dei documenti scansionati utilizzando la procedura di protocollazione "Folium", oltre a ciò lo stesso documento cartaceo viene inviato alla UOR di riferimento. I documenti che transitano attraverso il servizio postale (pubblico o privato), indirizzati a tutta l'amministrazione, sono consegnati quotidianamente al Servizio di Protocollo, che si fa carico di selezionare, protocollare, con le modalità sopra descritte, e smistare la corrispondenza alle UOR indirizzate.

5.2.2. Provenienza di documenti interni formali

Per sorgente interna dei documenti si intende qualunque UOR/UU che invia formalmente la propria corrispondenza ad altra UOR della AOO. Ogni UOR trasmette la propria corrispondenza interna ad altra UOR della AOO protocollando il documento trasmesso e i suoi, eventuali, allegati. Provvede nella fase di protocollazione ad assegnare il documento protocollato alla UOR in indirizzo con l'utilizzo della procedura di protocollazione "Folium".

Il documento è, di norma, di tipo analogico secondo i formati standard illustrati nel precedente capitolo. In questo caso, il mezzo di recapito della corrispondenza considerato è la posta interna.

5.2.3. Ricezione di documenti informatici sulla casella di posta istituzionale

Di norma, la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile solo alla UOP dell'AOO.

Quando i documenti informatici pervengono alla UOP-Servizio di Protocollo, la stessa unità, previa verifica della leggibilità del documento, procede alla registrazione di protocollo ed alla assegnazione agli UOR/UU di competenza.

Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente illustrate.

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti, recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.

Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.

Qualora i messaggi di posta elettronica non siano conformi agli standard indicati dalla normativa vigente, ovvero non siano dotati di firma elettronica e si renda necessario attribuire agli stessi efficacia probatoria, il messaggio è inserito nel sistema di gestione documentale con il formato di origine apponendo la dicitura "documento ricevuto via posta elettronica" e successivamente protocollato, smistato, assegnato e gestito. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quello di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA).

Il personale della UOP controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale e verifica se sono da protocollare.

5.2.4. Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale

Nel caso in cui il messaggio venga ricevuto su una casella di posta elettronica non istituzionale o comunque non destinata al servizio di protocollazione, il messaggio stesso viene inoltrato alla casella di posta della UOR perché decida se richiedere la protocollazione alla UOP - Servizio di Protocollo istituzionale. I controlli effettuati sul messaggio sono quelli sopra richiamati.

5.2.5. Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica.

Nei casi in cui con un documento cartaceo sono trasmessi gli allegati su supporto rimovibile, considerata l'assenza di standard tecnologici e formali in materia di registrazione di *file* digitali, la AOO si riserva la facoltà di acquisire e trattare tutti quei documenti informatici così ricevuti che riesce a decodificare e interpretare con le tecnologie a sua disposizione.

In ogni caso sarà protocollato il documento cartaceo ed inviato con le modalità sopra descritte alla UOR in indirizzo, unitamente al documento informatico.

5.2.6. Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti pervenuti a mezzo posta sono consegnati alla UOP.

Le buste, o contenitori, sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario apposti sugli stessi.

La corrispondenza relativa a bandi di gara non viene aperta, ma, viene protocollata con l'indicazione dell'ora di arrivo, viene poi avvisata la UOR a cui è indirizzata che provvede nella stessa giornata al ritiro presso il Servizio di Protocollo.

La corrispondenza personale non viene aperta, né protocollata, ma viene consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, provvederà a inoltrarla all'Ufficio protocollo per la registrazione.

La corrispondenza ricevuta via telegramma, per ciò che concerne la registrazione di protocollo, è trattata come un documento cartaceo con le modalità descritte nel successivo capitolo 11.

Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione. La corrispondenza in ingresso viene timbrata all'arrivo alla UOP sull'involucro, viene, di norma, aperta il giorno lavorativo in cui è pervenuta, e contestualmente assegnata con indicazione manuale del destinatario sul documento medesimo e protocollata. La busta, per la posta raccomandata, viene allegata al documento per la parte recante i timbri postali.

5.2.7. Errata ricezione di documenti digitali

Nel caso in cui pervengano sulla casella di posta istituzionale dell'AOO, in una casella non istituzionale, messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore rispedisce il messaggio al mittente con la motivazione per cui il messaggio è tornato al mittente.

5.2.8. Errata ricezione di documenti cartacei

Se la busta è indirizzata ad altra amministrazione ed è ancora chiusa, viene restituita al servizio postale che provvede ad inoltrarla all'indirizzo corretto.

5.2.9. Attività di protocollazione dei documenti

Superati tutti i controlli precedentemente descritti i documenti, digitali o analogici, sono protocollati e gestiti secondo gli standard e le modalità indicate nel dettaglio nel capitolo 11.

5.2.10. Rilascio di ricevute attestanti la ricezione di documenti informatici

La ricezione di documenti comporta l'invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, l'altra al servizio di protocollazione informatica.

Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'AOO con gli standard specifici.

Il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvede alla formazione e all'invio al mittente di uno dei seguenti messaggi:

messaggio di conferma di protocollazione: un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto. Si differenzia da altre forme di ricevute di recapito generate dal servizio di posta elettronica dell'AOO in quanto segnala l'avvenuta protocollazione del documento, e quindi l'effettiva presa in carico;

messaggio di notifica di eccezione: un messaggio che notifica la rilevazione di una anomalia in un messaggio ricevuto.

5.2.11. Rilascio di ricevute attestanti la ricezione di documenti cartacei

Gli addetti alle UOP non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione.

La semplice apposizione del timbro datario della UOP per la tenuta del protocollo sulla copia, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale della UOP in merito alla ricezione ed all'assegnazione del documento.

Quando il documento cartaceo è consegnato direttamente dal mittente, o da altra persona incaricata alla UOP, ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, la UOP che lo riceve è autorizzata a:

rilasciare una ricevuta prodotta, all'atto della protocollazione, dal sistema di protocollo informatico con l'indicazione del Servizio del Comune di Chioggia a cui viene assegnato il documento protocollato con il riferimento al responsabile del Servizio.

5.2.12. Conservazione dei documenti informatici

I documenti informatici ricevuti dal Comune di Chioggia sono archiviati sui supporti di memorizzazione dei Servizi Informatici, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.

Tali documenti sono resi disponibili agli UOR/UU, attraverso la rete interna dell'amministrazione subito dopo l'operazione di assegnazione.

5.2.13. Conservazione delle copie per immagine di documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine (*copia per immagine di documento analogico*) attraverso un processo di scansione che avviene secondo le fasi di seguito indicate:

acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico *file*;

verifica della leggibilità e della qualità delle immagini acquisite;

collegamento del file delle immagini alle rispettive registrazioni di protocollo, in modo non modificabile;

memorizzazione del file delle immagini su supporto informatico, in modo non modificabile.

Le copie per immagine dei documenti cartacei sono archiviate sui sistemi dei Servizi Informatici, secondo le regole vigenti, in modo non modificabile al termine del processo di scansione.

I documenti cartacei dopo l'operazione di riproduzione in formato immagine vengono trattati diversamente in base alla loro tipologia.

Gli originali dei documenti cartacei ricevuti, di norma vengono inviati alle UOR.

In ogni caso non vengono riprodotti in formato immagine i documenti che contengono dati sensibili secondo la normativa vigente (d.lgs. 196/2003).

5.2.14. Assegnazione, presa in carico dei documenti e classificazione.

Gli addetti alla UOP provvedono:

1) a classificare il documento sulla base del Titolario di Classificazione in essere presso l'AOO;

2) ad inviare il documento all'UOR che identifica l'UU di destinazione;

l'UOR:

esegue una verifica di congruità in base alle proprie competenze;

in caso di errore restituisce il documento alla UOP mittente;

in caso di verifica positiva, esegue l'operazione di presa in carico riassegnandola al proprio interno ad un UU o direttamente al RPA;

5.2.15. Conservazione dei documenti nell'archivio corrente

Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le seguenti attività:

classificazione di livello superiore sulla base del titolario di classificazione adottato dall'AOO;

fascicolazione del documento secondo le procedure previste dall'AOO;

inserimento del fascicolo nel repertorio dei fascicoli nel caso di apertura di un nuovo fascicolo.

5.2.16. Conservazione dei documenti e dei fascicoli nella fase corrente

All'interno di ciascun Ufficio Utente (UU) di ciascun UOR della AOO sono stati individuati gli addetti alla organizzazione e alla tenuta dei fascicoli "attivi" (e chiusi in attesa di riversamento nell'archivio di deposito) e alla archiviazione dei documenti al loro interno.

5.3. Flusso dei documenti in uscita dalla AOO

5.3.1. Sorgente interna dei documenti

Per "sorgente interna (all'AOO) dei documenti" si intende l'unità organizzativa mittente interna all'AOO che invia, tramite il RPA, la corrispondenza ai destinatari siano esterni all'AOO o interni all'AOO.

Operativamente ogni UOR invia i documenti protocollati in uscita, utilizzando la procedura "Folium" ed assegna i documenti protocollati, con le modalità e nelle forme più opportune, di seguito specificate.

Per "documenti in uscita" s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra amministrazione, ovvero ad altro ufficio (UU o UOR) della stessa AOO, o a soggetti terzi esterni all'AOO.

Il documento è in formato digitale formato secondo gli standard illustrati nei precedenti capitoli.

5.3.2. Registrazione di protocollo e segnatura

Le operazioni di registrazione e di apposizione della segnatura del documento in uscita sono effettuate presso ogni UOR. In ogni UOR sono abilitate le postazioni di protocollo che corrispondono ad ogni postazione di lavoro di ogni dipendente, il quale può protocollare, con l'utilizzo della procedura "Folium", i documenti sia in formato digitale che in formato analogico.

In nessun caso gli operatori di protocollo sono autorizzati a riservare numeri di protocollo per documenti non ancora resi disponibili. La compilazione di moduli, se prevista, come, ad esempio, nel caso di spedizioni per raccomandata con ricevuta di ritorno, posta celere, corriere, è a cura di ogni singola UOR e sarà controllata dalla UOP istituzionale.

5.3.3. Trasmissione di documenti informatici

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla normativa vigente.

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno alla AOO).

Per la spedizione dei documenti informatici, l'AOO si avvale del servizio di "posta elettronica certificata", conforme a quanto previsto dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio delle ricevute di ritorno elettroniche.

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.

5.3.4. Trasmissione di documenti cartacei a mezzo posta

La UOP provvede direttamente a tutte le operazioni di spedizione della corrispondenza provvedendo:

- alla consegna all'ufficio postale della corrispondenza;
- alla consegna all'incaricato al ritiro della corrispondenza;
- alla verifica delle ricevute di invio e di ritorno per le raccomandate, predisposte dalle singole UOR, unitamente alla distinta delle medesime da rilasciare all'ufficio postale e/o all'incaricato del ritiro della corrispondenza.

5.3.5. Affrancatura dei documenti in partenza

Tutte le attività di affrancatura della corrispondenza inviata per posta vengono svolte dal servizio postale. Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla UOP almeno la giornata precedente a quella di lavorazione e di spedizione della corrispondenza.

5.3.6. Documenti in partenza per posta convenzionale con più destinatari

Qualora i destinatari siano più di uno vengono inviate solo le copie dell'unico originale prodotto dall'UOR/UU.

5.3.7. Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito, ovvero le ricevute delle raccomandate, ovvero le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo fascicolo.

Gli UOR/UU curano anche l'archiviazione delle ricevute di ritorno delle raccomandate. Queste ultime, sulle quali, precauzionalmente, è stato trascritto sia il numero di protocollo attribuito al documento a cui esse si riferiscono, sia l'UOR/UU mittente, sono inizialmente raccolte dalla UOP e successivamente consegnate alle UOR/UU medesime previo rilascio di ricevuta di consegna.

6. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

Il presente capitolo contiene le regole di assegnazione dei documenti in ingresso adottate dalla UOP.

6.1. Regole disponibili con il SdP

L'assegnazione dei documenti protocollati e segnati avviene sfruttando le funzionalità di seguito descritte.

Il SdP, per abbreviare il processo di assegnazione del materiale documentario oggetto di lavorazione, utilizza l'organigramma dell'AOO.

All'assegnazione segue la presa in carico del documento da parte del RPA e/o suo delegato, che provvede a inoltrarlo, se del caso, all'addetto istruttore della pratica.

6.2. Attività di assegnazione

Di seguito viene descritta con maggiore dettaglio l'operazione di assegnazione dei documenti ricevuti illustrata nel flusso di lavorazione del precedente paragrafo 5.2

L'attività di assegnazione consiste nell'operazione di inviare direttamente dalla UOP il documento protocollato e segnato all'UOR competente e la contestuale trasmissione del materiale documentario oggetto di trattazione.

Con l'assegnazione si provvede ad attribuire la responsabilità del procedimento amministrativo ad un soggetto fisico che si identifica nel RPA designato.

Preso atto dell'assegnazione, il RPA verifica la competenza e, se esatta, provvede alla presa in carico del documento che gli è stato assegnato.

Contestualmente alla protocollazione il mittente iniziale (UOP) provvede ad inviare, con le tecnologie adeguate, il documento in questione compilato nella parte segnatura (o timbro di segnatura) al UOR/UU/RPA di competenza.

L'assegnazione può essere effettuata: per smistamento, conoscenza o per competenza.

L'UOR competente è incaricata della gestione del procedimento a cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento amministrativo che prende avvio dal documento decorrono comunque dalla data di protocollazione.

Il SdP memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia è risultante anche ai fini di individuare i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

Per le attività relative al SUAP al SdP arriva la notifica di inoltro rilasciata dal portale utilizzato da tutti i soggetti autorizzati.

6.3. Corrispondenza di particolare rilevanza

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto utilizzato, viene inviato in busta chiusa direttamente al Gabinetto del Sindaco e/o Segretario Generale o in caso di impossibilità dei predetti interessati al Dirigente di riferimento;

6.4. Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'UOR competente attraverso i canali telematici dell'AOO al termine delle operazioni di registrazione, segnatura di protocollo, memorizzazione su supporti informatici in modo non modificabile interni al centro servizio.

Il responsabile dell'UOR è in grado di visualizzare i documenti, attraverso le funzionalità del SdP e, in base alle abilitazioni possedute, potrà:

visualizzare gli estremi del documento;
visualizzare il contenuto del documento;
individuare come assegnatario il RPA competente per la materia a cui si riferisce il documento ed assegnare il documento in questione.

La "presa in carico" dei documenti informatici viene registrata dal SdP in modo automatico e la data di ingresso dei documenti negli UOR competenti coincide con la data di assegnazione degli stessi. I destinatari del documento per "smistamento" per "competenza" e/o "per conoscenza" lo ricevono esclusivamente in formato digitale, con eventuale successiva consegna del documento in formato cartaceo per i documenti presentati al Front-Office del SdP.

6.5. Assegnazione dei documenti ricevuti in formato cartaceo

Al termine delle operazioni di registrazione, segnatura dei documenti ricevuti dall'AOO in formato cartaceo, i documenti medesimi sono assegnati al RPA di competenza per via informatica attraverso la rete interna dell'amministrazione. L'originale cartaceo riceve il seguente trattamento:

viene acquisito in formato immagine con l'ausilio di *scanner*;
può essere successivamente trasmesso/ritirato al/dal RPA, oppure essere conservato dalla UOP.

I documenti cartacei gestiti dalla UOP sono di norma assegnati entro il giorno successivo a quello di ricezione, salvo che vi figurino, entro detto lasso di tempo, uno o più giorni non lavorativi, nel qual caso l'operazione di smistamento viene assicurata entro le 24 ore dall'inizio del primo giorno lavorativo successivo.

Attraverso le funzioni del SdP e in base alle abilitazioni previste il responsabile dell'UOR potrà:

visualizzare gli estremi del documento;
visualizzare il contenuto del documento
individuare come assegnatario il RPA competente sulla materia oggetto del documento.

La "presa in carico" dei documenti informatici viene registrata dal sistema in modo automatico e la data di ingresso dei documenti nelle UOR di competenza coincide con la data di assegnazione degli stessi.

6.6. Modifica delle assegnazioni

Nel caso di assegnazione errata, l'UOR/UU che riceve il documento comunica l'errore e lo restituisce alla UOP, che procederà ad una nuova assegnazione.

Nel caso in cui un documento assegnato erroneamente ad un UU afferisca a competenze attribuite ad altro UU dello stesso UOR, l'abilitazione al relativo cambio di assegnazione è attribuita al dirigente della UOR medesima, o a persona da questi incaricata.

Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

7. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI INVIATI

Il presente capitolo riporta le regole di gestione dei documenti in uscita adottate da ogni singola UOR. L'UOR dopo aver protocollato in uscita il documento lo assegna all'ufficio destinatario, ad altra AOO, ad altra Amministrazione e a soggetti terzi esterni. Tale assegnazione è generata utilizzando la procedura di protocollazione "Folium" e garantita dal SdP.

8. UO RESPONSABILE DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, ORGANIZZAZIONE E TENUTA DEI DOCUMENTI

Il presente capitolo individua l'unità organizzativa responsabile delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno della AOO.

In base al modello organizzativo adottato dall'amministrazione, è stato istituito il SdP per la protocollazione in ingresso dei documenti arrivati all'AOO nelle diverse forme, formati e contenuti. Al servizio di Protocollo Informatico è preposto lo stesso RSP.

Relativamente alla organizzazione e alla tenuta dei documenti della AOO in cui è articolata l'amministrazione, all'interno della AOO in parola, è stato istituito il servizio archivistico.

I servizi in argomento sono stati identificati e formalizzati prima di rendere operativo il servizio di gestione informatica del protocollo, dei documenti e degli archivi.

8.1. Servizio archivistico

Il servizio archivistico è competente a gestire l'intera documentazione archivistica, ovunque trattata, distribuita o conservata, ai fini della sua corretta collocazione, classificazione, e conservazione. Al servizio archivistico è preposto il responsabile degli Archivi.

9. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

9.1. Documenti esclusi

Sono, esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53, comma 5, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. I documenti esclusi sono indicati negli allegati:

- Elenco tipologie documentarie soggette a registrazione di Repertorio;
- Elenco tipologie documentarie soggette ad altra forma di registrazione;
- Elenco tipologie documentarie non soggette a registrazione.

9.2. Documenti soggetti a registrazione particolare

Non vi sono documenti esclusi dalla registrazione di protocollo se non quelli elencati negli allegati sopra indicati, e non vi sono documenti soggetti a registrazione particolare.

10. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

10.1. Protezione e conservazione degli archivi pubblici

10.1.1. Caratteristiche generali

Il presente capitolo contiene il sistema di classificazione dei documenti, di formazione del fascicolo e di conservazione dell'archivio, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto della documentazione, anche con riferimento all'uso di supporti sostitutivi e di consultazione e movimentazione dei fascicoli.

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (titolario), cioè di quello che si suole definire "sistema preconstituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti".

Il titolare e il piano di conservazione sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di protocollazione informatica e di archiviazione, considerato che si tratta degli strumenti che consentono la corretta formazione, gestione e archiviazione della documentazione dell'amministrazione.

Il titolare, allegato al Manuale, e il piano di conservazione sono adottati dall'amministrazione con atti formali.

10.1.2. Misure di protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti dello Stato, delle regioni e degli enti pubblici sono beni culturali inalienabili.

I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'AOO, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

L'archivio non può essere smembrato, e deve essere conservato nella sua organicità. L'eventuale trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della direzione generale per gli archivi.

L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della suddetta direzione generale per gli archivi.

Lo scarto dei documenti dell'archivio in parola è subordinato all'autorizzazione della direzione generale per gli archivi, su proposta delle commissioni di sorveglianza istituite presso ciascun ufficio con competenza a livello provinciale o delle commissioni di scarto istituite presso ogni ufficio con competenza "subprovinciale".

Per l'archiviazione e la custodia nella sezione di deposito, o storica, dei documenti contenenti dati personali, si applicano le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che di supporti convenzionali.

10.2. Titolario o piano di classificazione

10.2.1. Titolario

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.

Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello.

Il titolo individua per lo più funzioni primarie e di organizzazione dell'ente (macro funzioni); le successive partizioni, classi e sottoclassi, corrispondono a specifiche competenze che rientrano concettualmente nella macro funzione descritta dal titolo, articolandosi gerarchicamente tra loro, secondo lo schema riportato nell'allegato Titolario di classificazione.

Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolare di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del vertice dell'amministrazione.

Il titolare è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali. L'aggiornamento del titolare compete esclusivamente al vertice dell'amministrazione, su proposta del RSP. La revisione, anche parziale, del titolare viene proposta dal RSP quando necessario ed opportuno.

Dopo ogni modifica del titolare, il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Il titolare non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Il sistema di protocollazione garantisce la storicizzazione delle variazioni di titolare e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolare vigente al momento della produzione degli stessi.

Di norma le variazioni vengono introdotte a partire dal 1 gennaio dell'anno successivo a quello di approvazione del nuovo titolare e hanno durata almeno per l'intero anno.

Rimane possibile, se il sistema lo consente, di registrare documenti in fascicoli già aperti fino alla conclusione e alla chiusura degli stessi.

Il titolare è stato elaborato da un gruppo di lavoro appositamente costituito all'interno dell'AOO nelle linee guida dei competenti organi dell'amministrazione archivistica statale.

10.2.2. Classificazione dei documenti

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.

Essa è eseguita a partire dal titolare di classificazione facente parte del piano di conservazione dell'archivio.

Tutti i documenti ricevuti e prodotti dagli UOR dell'AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolare.

10.3. Fascicoli e dossier

10.3.1. Fascicolazione dei documenti

Tutti i documenti registrati nel sistema di protocollo informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, possono essere riuniti in fascicoli, secondo le disposizioni impartite da ogni singola UOR al loro interno.

Ogni documento, dopo la classificazione, viene inserito nel fascicolo di riferimento.

I documenti sono archiviati all'interno di ciascun fascicolo, o, all'occorrenza, sottofascicolo o inserto, secondo l'ordine cronologico di registrazione.

10.3.2. Apertura del fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'AOO, il RPA provvede all'apertura di un nuovo fascicolo. La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

- indice di classificazione(cioè titolo, classe, sottoclasse, età);
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'AOO;
- data di apertura del fascicolo;
- AOO e UOR;
- collocazione fisica, di eventuali documenti cartacei;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Il fascicolo, di norma viene aperto all'ultimo livello della struttura gerarchica del titolare.

10.3.3. Chiusura del fascicolo

Il fascicolo viene chiuso al termine del procedimento amministrativo o con l'esaurimento dell'affare.

La data di chiusura si riferisce alla data dell'ultimo documento prodotto.

Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura. Gli elementi che individuano un fascicolo sono gestiti dal soggetto di cui al paragrafo precedente, primo capoverso, il quale è tenuto pertanto all'aggiornamento del repertorio dei fascicoli.

10.3.4. Processo di assegnazione dei fascicoli

Quando un nuovo documento viene recapitato all'AOO, l'UOR abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso debba essere ricollegato ad un affare o procedimento in corso e pertanto debba essere inserito in un fascicolo già esistente oppure se il documento si riferisce a un nuovo affare, o procedimento, per cui è necessario aprire un nuovo fascicolo. A seconda delle ipotesi, si procede come segue:

- se il documento si ricollega ad un *affare o procedimento in corso*, l'addetto:
 - seleziona il relativo fascicolo;
 - collega la registrazione di protocollo del documento al fascicolo selezionato;
 - invia il documento all'UU cui è assegnata la pratica;
- se il documento dà avvio ad un *nuovo fascicolo*, il soggetto preposto:
 - esegue l'operazione di apertura del fascicolo;
 - collega la registrazione di protocollo del documento al nuovo fascicolo aperto;
 - assegna il documento ad un istruttore;su indicazione del RPA;
 - invia il documento con il relativo fascicolo, al dipendente, che dovrà istruire la pratica per competenza.

10.3.5. Repertorio dei fascicoli

Il repertorio dei fascicoli, ripartito per ciascun titolo del titolare, è lo strumento di gestione e di reperimento dei fascicoli.

La struttura del repertorio rispecchia quella del titolare di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo.

Mentre il titolare rappresenta in astratto le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività.

10.4. Consultazione e movimentazione dell'archivio corrente, di deposito e storico

10.4.1. Principi generali

La richiesta di consultazione, e di conseguenza di movimentazione dei fascicoli, può pervenire dall'interno dell'amministrazione, oppure da utenti esterni all'amministrazione, per scopi giuridico-amministrativi o per scopi storici.

10.4.2. Consultazione ai fini giuridico-amministrativi

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15, che qui di seguito si riporta: "Esclusione dal diritto di accesso.

1. Il diritto di accesso è escluso:

- a. per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
- b. nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
- c. nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
- d. nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.

2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.

3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.

4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.

5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.

6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi:

- a. quando, al di fuori delle ipotesi disciplinate dall'articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione;
- b. quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
- c. quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;
- d. quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono;
- e. quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

7. Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale "

10.4.3. Consultazione da parte di personale esterno all'amministrazione

La domanda di accesso ai documenti viene presentata/inviata alla UOP, che provvede a smistarla alla UOR di riferimento che a sua volta provvede ad inoltrarla al servizio archivistico.

Presso la UOP, a cui fa riferimento il servizio archivistico, sono disponibili appositi moduli per la richiesta di accesso ai documenti.

Le richieste di accesso ai documenti della sezione storica dell'archivio possono essere inoltrate anche alla Soprintendenza per i Beni Archivistici territorialmente competente, con apposito modulo da questa predisposto.

Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale.

In tal caso il responsabile del servizio archivistico provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

L'ingresso all'archivio di deposito, e storico, è consentito solo agli addetti del servizio archivistico.

La consultazione dei documenti è possibile esclusivamente sotto la diretta sorveglianza del personale addetto.

Il rilascio di copie dei documenti dell'archivio, quando richiesto, avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'amministrazione.

In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione.

10.4.4. Consultazione da parte di personale interno all'amministrazione

Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito, o storica, compilando appositi moduli.

L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito, o storico, ad un ufficio del medesimo UOR/UU, od altro UOR/UU, avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.

Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa, redatta in duplice copia su un apposito modello contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, il suo UOR/UU e la sua firma.

Un esemplare della richiesta di consultazione viene conservata all'interno del fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio.

Tale movimentazione viene registrata a cura del responsabile del servizio archivistico in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna e quella di restituzione, nonché eventuali note sullo stato della documentazione, in modo da riceverla nello stesso stato in cui è stata consegnata.

Il responsabile del servizio archivistico verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.

L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, degli stessi rispettandone la sedimentazione archivistica e il vincolo.

Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'AOO.

In ogni caso, deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

11. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

11.1. Unicità del protocollo informatico

Nell'ambito della AOO il registro generale di protocollo è unico al pari della numerazione progressiva delle registrazioni di protocollo.

La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.

Il numero di protocollo è costituito da almeno sette cifre numeriche.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.

Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione che non è stata registrata presso una UOP viene considerata giuridicamente inesistente presso l'amministrazione.

Non è consentita la protocollazione di un documento già protocollato.

Il registro di protocollo è un atto pubblico originario, che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici.

11.2. Registro giornaliero di protocollo

Il RSP provvede alla 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.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato, al termine della giornata lavorativa, su supporti di memorizzazione non riscrivibili, i quali sono conservati in luogo sicuro a cura di un soggetto diverso, ai sensi dell'art.7. comma 5, del DPCM 31 ottobre 2000, (*responsabile della conservazione delle copie*) dal RSP ed appositamente nominato dall'AOO. Tale operazione viene espletata all'interno della UOP.

11.3. Registrazione di protocollo

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo, valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).

Su ogni documento ricevuto, o spedito, dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.

Tale registrazione è eseguita in un'unica operazione, senza possibilità, per l'operatore, di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;

- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;

- il mittente che ha prodotto il documento;

- il destinatario del documento;

- l'oggetto del documento;

Le variazioni su "oggetto", "mittente" e "destinatario" vengono mantenute con un criterio di storicizzazione dal SdP, evidenziando data, ora e utente che ha effettuato la modifica.

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili. Tali dati facoltativi sono descritti nei paragrafi seguenti.

11.3.1. Documenti informatici

I documenti informatici sono ricevuti, e trasmessi, in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'AOO.

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, che si può riferire sia al corpo del messaggio che ad uno dei *file* ad esso allegati che può assumere la veste di documento principale.

Tali documenti sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

Le UOR ricevono i documenti informatici interni di tipo formale protocollati al proprio indirizzo, sia ufficio che utente, presente nel flusso di assegnazione della procedura “Folium”, preposto a questa funzione.

11.3.2. Documenti analogici (cartacei e supporti rimovibili)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza.

La registrazione di protocollo di un documento cartaceo ricevuto, così come illustrato nel seguito, viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.

Nel caso di corrispondenza in uscita o interna formale, l'UOR esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

11.4. Elementi facoltativi delle registrazioni di protocollo

Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, il RSP, con proprio provvedimento, può modificare e integrare gli elementi facoltativi del protocollo.

La registrazione degli elementi facoltativi del protocollo, può essere modificata, integrata e cancellata in base alle effettive esigenze della UOP o degli UOR.

In caso di necessità, i dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

Per quanto concerne i campi integrativi, facoltativi presenti nel SdP sono previste specifiche funzionalità che consentono di gestire:

- ulteriori informazioni sul mittente/destinatario, soprattutto se persona giuridica;

- l'indirizzo completo del mittente/destinatario (via, numero civico, CAP, città, provincia, stato civile, sesso);

- il numero di matricola (se dipendente interno dell'amministrazione);

- il codice fiscale;

- il numero della partita IVA;

- il recapito telefonico;

- gli indirizzi di posta elettronica;

11.5. Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.

La segnatura di protocollo è l'apposizione, o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.

Essa consente di individuare ciascun documento in modo inequivocabile.

11.5.1. Documenti informatici

I dati della segnatura di protocollo di un documento informatico sono attribuiti, un'unica volta nell'ambito dello stesso messaggio, in *un file* conforme alle specifiche dell'*Extensible Markup Language (XML)* e compatibile con il *Document Type Definition (DTD)* reso disponibile dagli organi competenti. Le informazioni minime incluse nella segnatura sono le seguenti:

- codice identificativo dell'amministrazione;

- codice identificativo dell'area organizzativa omogenea;

- codice identificativo del registro

- data e numero di protocollo del messaggio ricevuto o inviato (art.18 c1)

- l'oggetto

- il mittente

- il destinatario o i destinatari

E' facoltativo riportare le seguenti informazioni:

- denominazione dell'amministrazione;

- codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;

numero di fascicolo.

Per i documenti informatici in partenza possono essere specificate, in via facoltativa, anche le seguenti informazioni:

- persona, ufficio destinatario;
- indice di classificazione
- individuazione degli allegati;
- informazioni sul procedimento e sul trattamento.

La struttura ed i contenuti del *file* di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.

Quando il documento è indirizzato ad altre AOO la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.

L'AOO che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.

Qualora l'AOO decida di scambiare con altre AOO informazioni non previste tra quelle definite come facoltative, può estendere il *file* di cui sopra, nel rispetto delle regole tecniche dettate dall'AgID, includendo le informazioni specifiche stabilite di comune accordo con l'AOO con cui interagisce.

11.5.2. Documenti cartacei

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione di una etichetta sulla quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- codice identificativo dell'amministrazione;
- codice identificativo dell'AOO;
- data e numero di protocollo del documento.

L'operazione di segnatura dei documenti in partenza viene integralmente eseguita dalla UOP, ovvero viene effettuata dall'UOR/UU/RPA competente che redige il documento se è abilitata, come UOP, alla protocollazione dei documenti in uscita.

L'operazione di acquisizione dell'immagine dei documenti cartacei viene effettuata solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.

Se è prevista l'acquisizione del documento cartaceo in formato immagine, il "segno" della segnatura di protocollo viene apposto sulla prima pagina dell'originale.

11.6. Annullamento delle registrazioni di protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrate in forma non modificabile - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare parzialmente la registrazione di protocollo.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RSP.

In tale ipotesi la procedura riporta la dicitura "annullato" o "annullato parzialmente" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.

Solo il RSP è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RSP.

Analoga procedura di annullamento va eseguita quando, stante le funzioni primarie di certificazione riconosciute dalle norme alla UOP, emerge che ad uno stesso documento in ingresso, ricevuto con mezzi di trasmissione diversi quali, ad esempio originale cartaceo, e_mail, siano stati attribuiti più numeri di protocollo.

11.7. Livello di riservatezza

IL SdP applica automaticamente il livello di riservatezza "base" a tutti i documenti protocollati. Se previsto per documenti contenenti informazioni con tutela della privacy è previsto l'applicazione del grado di riservatezza "classificato", primo grado di riservatezza che comprende anche i gradi:

Non Classificato

Classificato

Ristretto

Segreto

Top Secret

Il trattamento di documenti che richiedono/prevedono livelli maggiori di sicurezza esula dal presente manuale.

In modo analogo, il RPA che effettua l'operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza.

Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti invece che hanno un livello di riservatezza superiore lo mantengono.

11.8. Casi particolari di registrazioni di protocollo

Tutta la corrispondenza diversa da quella di seguito descritta viene regolarmente aperta, protocollata e assegnata con le modalità e le funzionalità proprie del SdP.

11.8.1. Circolari e disposizioni generali

Gli ordini di servizio, di norma, non vengono protocollati.

Le circolari ricevute vengono protocollate nel registro ufficiale di protocollo.

11.8.2. Documenti cartacei in uscita con più destinatari

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica e viene riportata su ogni documento originale.

11.8.3. Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio

La corrispondenza ricevuta con consegna diretta dall'interessato, o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.

Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta.

11.8.4. Fatture, assegni e altri valori di debito o credito

Le fatture (in caso di presentazione di fatture non elettroniche), gli assegni o altri valori di debito o credito sono protocollate sul registro ufficiale di protocollo e inviate quotidianamente, in originale, alla UOR competente.

11.8.5. Protocollazione di documenti inerenti gare di appalto confezionate su supporti cartacei

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo", o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non viene aperta dalla UOP, ma viene timbrata dalla medesima che provvede a protocollare la busta o il plico chiuso e a riportare sul medesimo la data, l'ora di arrivo ad inoltrarla alla UOR/UU competente.

Il plico così protocollato viene consegnato alla UOR/UU che provvede alla custodia, con mezzi idonei, sino all'espletamento della gara.

Dopo l'apertura delle buste, l'UOR che gestisce la gara riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.

Per motivi organizzativi tutti gli UOR sono tenuti ad informare con congruo anticipo il RSP dell'AOO in merito alle scadenze di concorsi, gare, bandi di ogni genere, con apposita e.mail.

11.8.6. Protocolli urgenti

La richiesta di protocollare urgentemente un documento è collegata ad una necessità indifferibile e di tipo straordinario.

Solo in questo caso il RSP si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale, o cartaceo, da spedire. Tale procedura viene osservata sia per i documenti in ingresso che per quelli in uscita.

11.8.7. Documenti non firmati

L'operatore di protocollo, conformandosi alle regole stabilite dal RSP attesta la data, la forma e la provenienza per ogni documento.

Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "mittente sconosciuto o anonimo" o "documento non sottoscritto".

Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.

È poi compito dell'UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

11.8.8. Protocollazione dei messaggi di posta elettronica convenzionale

Considerato che l'attuale sistema di posta elettronica convenzionale non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata come segue:

caso di invio, come allegato, di un documento scansionato munito di firma autografa: fermo restando che il RdP deve verificare la provenienza certa dal documento, in caso di mittente non verificabile, il RdP valuta, caso per caso, l'opportunità di trattare il documento inviato via *e-mail*;

caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale: il documento e/o il messaggio sono considerati come un documento elettronico inviato con qualunque mezzo di posta.

11.8.9. Protocollazione di documenti digitali pervenuti erroneamente

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all'AOO non competente, l'addetto al protocollo, previa autorizzazione del RSP, provvede ad annullare il protocollo stesso indicando nell'oggetto "protocollato per errore" comunicando al mittente l'errato invio.

11.8.10. Ricezione di documenti cartacei pervenuti erroneamente

Nel caso in cui sia protocollato un documento cartaceo erroneamente inviato all'AOO, l'addetto al protocollo, previa autorizzazione del RSP, provvede o ad annullare il protocollo stesso indicando nell'oggetto "protocollato per errore"; il documento oggetto della rettifica viene restituito al mittente con la dicitura "protocollato per errore".

11.8.11. Copie per "conoscenza"

Nel caso di copie per conoscenza si deve utilizzare la seguente procedura: chi effettua la registrazione e lo smistamento dell'originale e delle copie, registra sul registro di protocollo a chi sono state inviate le copie "per conoscenza".

11.8.12. Differimento delle registrazioni

Le registrazioni di protocollo dei documenti pervenuti presso l'AOO destinataria sono, di norma, effettuate nella giornata di arrivo e comunque non oltre le 48 ore dal ricevimento di detti documenti.

Qualora nei tempi sopra indicati non possa essere effettuata la registrazione di protocollo si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del RSP, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.

Il protocollo differito consiste nel rinvio dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento sopra citato.

11.8.13. Corrispondenza personale o riservata

La corrispondenza personale non viene aperta, ma viene consegnata al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati perché riguardano problematiche istituzionali, provvede a trasmetterli alla UOP per la protocollazione.

11.8.14. Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed gli eventuali allegati.

Tale verifica spetta al responsabile del procedimento amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel relativo fascicolo.

11.9. Gestione delle registrazioni di protocollo con il SdP

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono effettuate attraverso il SdP.

Il sistema di sicurezza dei Servizi Informatici garantisce la protezione di tali informazioni sulla base delle relativa architettura tecnologica, sui controlli d'accesso e i livelli di autorizzazione realizzati.

11.10. Registrazioni di protocollo

11.10.1. Attribuzione del protocollo

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il SdP appone al documento protocollato un riferimento temporale, come previsto dalla normativa vigente.

Il SdP assicura l'esattezza del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete. Come previsto dalla vigente normativa in materia di protezione dei dati personali le AOO aderenti al SdP sono informate della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo.

11.10.2. Registro informatico di protocollo

L'uso combinato dei meccanismi permette di conferire validità e integrità ai contenuti del *file* del registro di protocollo.

E' inoltre disponibile per le UOP del SdP una funzione applicativa di "Stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.

11.10.3. Tenuta delle copie del registro di protocollo

Presso i Servizi Informatici si provvede con periodicità giornaliera, alla memorizzazione su supporto ottico, in duplice copia tabelle dei registri di protocollo della AOO;

Le copie dei supporti sono conservate dal responsabile della sicurezza negli armadi ignifughi dell'area sicurezza dei Servizi Informatici, nel rispetto delle norme vigenti.

Le modalità di archiviazione sono regolamentate dal responsabile del Servizio Protocollo.

12. DESCRIZIONE DELLE FUNZIONI E DELLE MODALITÀ' OPERATIVE DEL SISTEMA DI PROTOCOLLO INFORMATICO

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'AOO, con particolare riferimento alle modalità di utilizzo dello stesso.

12.1. Descrizione funzionale ed operativa

La descrizione completa delle funzionalità dell'applicativo di protocollo Folium è disponibile e consultabile insieme ai manuali operativi negli allegati.

13. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Il presente capitolo illustra le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente, prevista dal SdP, e consultabile nell'allegato Protocollo di Emergenza.

13.1. Il registro di emergenza

Qualora non fosse possibile fruire del SdP per una interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza.

Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.

Qualora nel corso di un anno il registro di emergenza non venga utilizzato, il RSP annota sullo stesso il mancato uso.

Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite sul registro di protocollo generale.

Il registro di emergenza si configura come un repertorio del protocollo generale.

Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione sono associati anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale.

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo. In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

Il SdP realizza il registro di emergenza con un applicativo specifico, installato sulle postazioni di lavoro della AOO in modalità *stand alone*, fuori linea.

13.2. Modalità di apertura del registro di emergenza

Il RSP assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica *realtime*, le operazioni di protocollo siano svolte sul registro di emergenza informatico su postazioni di lavoro operanti fuori linea.

Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il RSP imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare.

Sul registro di emergenza sono riportate: la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.

Per semplificare e normalizzare la procedura di apertura del registro di emergenza il RSP ha predisposto il modulo riportato di seguito.

L'abilitazione alla registrazione dei documenti sui registri di emergenza è riservato solamente alla UOP istituzionale della AOO.

Servizio di gestione informatica del protocollo, dei documenti e degli archivi

Scheda di apertura/chiusura del registro di emergenza

AgID- Agenzia per l'Italia Digitale -

Area Organizzativa Omogenea Comune di Chioggia

Unità Organizzativa di registrazione di Protocollo

Causa dell'interruzione:

Data: gg / mm / aaaa di inizio/ fine interruzione
(depenare la voce incongruente con l'evento annotato)

Ora dell'evento hh /mm Annotazioni:

Numero protocollo xxxxxxx iniziale/finale
(depenare la voce incongruente con l'evento annotato)

Pagina n. _____

Firma del responsabile del servizio di protocollo

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il responsabile della tenuta del protocollo autorizza l'uso del registro di emergenza per periodi successivi di durata non superiore ad una settimana.

13.3. Modalità di utilizzo del registro di emergenza

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro, il numero totale di operazioni registrate manualmente.

La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.

Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono gli stessi previsti dal protocollo generale.

13.4. Modalità di chiusura e di recupero del registro di emergenza

E' compito del RSP verificare la chiusura del registro di emergenza.

E' compito del RSP, o di un suo delegato, riportare dal registro di emergenza al registro di protocollo generale del SdP le protocollazioni relative ai documenti protocollati in emergenza attraverso le postazioni di lavoro abilitate, con la maggior tempestività possibile, dal ripristino delle funzionalità del SdP.

Al fine di ridurre la probabilità di commettere errori in fase di trascrizione dei dati riportati dal registro di emergenza a quello del protocollo generale e di evitare la duplicazione di attività di inserimento, le informazioni relative ai documenti protocollati in emergenza, su una o più postazioni di lavoro dedicate della AOO, sono inserite nel sistema informatico di protocollo generale utilizzando un'apposita funzione di recupero dei dati.

Una volta ripristinata la piena funzionalità del SdP, il RSP provvede alla chiusura del registro di emergenza, annotando, sullo stesso il numero delle registrazioni effettuate e la data e l'ora di chiusura.

Per semplificare la procedura di chiusura del registro di emergenza il RSP utilizza il modulo utilizzato nella fase di apertura del registro di emergenza.

14. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI

14.1. Modalità di approvazione e aggiornamento del manuale

L'amministrazione adotta il presente "Manuale di gestione" su proposta del responsabile del servizio di protocollo informatico.

Il presente manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- modifiche apportate negli allegati dal RSP.

14.2. Regolamenti abrogati

Con l'entrata in vigore del presente manuale sono annullati tutti i regolamenti interni all'AOO nelle parti contrastanti con lo stesso.

14.3. Pubblicità del presente Manuale

Il presente manuale è disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento. Inoltre copia del presente manuale è:

- fornita a tutto il personale dell'AOO e se possibile, viene resa disponibile mediante la rete intranet;
- pubblicato all'Albo Pretorio online dell'Ente;
- pubblicato sul sito istituzionale dell'amministrazione.

14.4. Operatività del presente manuale

Il presente manuale è operativo il 15° giorno successivo alla sua pubblicazione all'Albo Pretorio dell'Ente.



Manuale di gestione del Protocollo Informatico, dei documenti e degli Archivi della Città di Chioggia

ALLEGATO 1

Definizione di Area Organizzativa Omogenea

Il DPR 28 dicembre 2000, n.445 (Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa) all'art. 50 stabilisce che all'interno di ciascuna amministrazione la creazione di grandi Aree Organizzative Omogenee, che assicurino criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna delle stesse. L'art.61, altresì, stabilisce che si costituisca un Servizio per ciascuna AOO, responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Al detto Servizio deve essere preposto un dirigente/responsabile, in possesso di idonei requisiti professionali.

Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse.

In base alle succitate disposizioni normative, il Comune di Chioggia ha disposto che nel Comune di Chioggia sia costituita un'unica Area Organizzativa Omogenea.



Manuale di gestione del Protocollo Informatico, dei documenti e degli Archivi della Città di Chioggia

ALLEGATO 2

Elenco delle tipologie documentarie soggette a registrazione di repertorio all'interno del sistema di protocollo informatico

Si riportano qui di seguito le tipologie di documento per le quali è prevista la registrazione a repertorio di cui all'art.9 del Manuale:

- decreti/ordinanze del Sindaco
- deliberazioni del Consiglio Comunale
- deliberazioni della Giunta Comunale
- determinazioni dei dirigenti
- ordinanze dei Dirigenti
- notifiche
- registro atti privati
- registro dell'albo pretorio
- regolamenti



Manuale di gestione del Protocollo Informatico, dei documenti e degli Archivi della Città di Chioggia

ALLEGATO 3

Elenco delle tipologie documentarie soggette ad altre forme di registrazione

- Atti di polizia giudiziaria
- Atti di stato civile
- Atti privati
- Atti rogati o autenticati dal Segretario Generale
- Carta d'identità
- Certificazioni anagrafiche rilasciate direttamente al richiedente
- Certificazioni stato civile rilasciate direttamente al richiedente
- Mandati di pagamento
- Ordinanze trattamento sanitario obbligatorio
- Ordinanze
- Regolamenti
- Reversali
- Tessere elettorali
- Verbale delle commissioni consiliari
- Verbali di violazione del codice della strada e extra cds



Manuale di gestione del Protocollo Informatico, dei documenti e degli Archivi della Città di Chioggia

ALLEGATO 4

Elenco delle tipologie documentarie non soggette a registrazione

- richieste di ferie
- richieste di permessi
- richieste di rimborso spese e missioni
- convocazioni ad incontri, riunioni, corsi di formazione interni
- comunicazione d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti, ecc.)
- comunicazioni interne tra uffici, prive di rilevanza giuridica
- gli inviti a manifestazioni che non attivano procedimenti amministrativi
- estratti di conto corrente bancario e postale
- avvisi di pagamento, comunicazioni di bonifici bancari
- comunicazioni per la regolarizzazione delle entrate
- offerte/preventivi/listini di prezzi non richiesti
- pubblicità conoscitiva di convegni
- pubblicità in generale
- curricula non richiesti
- atti di liquidazione
- mail considerate SPAM o virus in arrivo nelle PEC
- pec in arrivo che non contengano elementi essenziali per la protocollazione
- mail in ingresso e/o in uscita ricevute e/o inviate dall'organo politico (nel caso le mail abbiano, a valutazione dell'organo politico, rilevanza istituzionale, queste dovranno essere inviate al destinatario utilizzando il sistema di protocollazione "procedura Folium").



Manuale di gestione del Protocollo Informatico, dei documenti e degli Archivi della Città di Chioggia

ALLEGATO 5

Applicativo di gestione informatica dei documenti Applicativo di protocollazione "Folium"

Descrizione della procedura

L'applicativo per la gestione informatica dei documenti adottato dal Comune di Chioggia è "Folium" prodotto dalla ditta Deda Group.

Il prodotto attualmente in uso è la versione 4.12.0

La descrizione funzionale dell'applicativo è costituita dal Manuale fornito dalla ditta produttrice ed è disponibile in linea all'interno dell'applicativo stesso.

Privilegi di accesso

Si specificano qui di seguito i privilegi di accesso al sistema documentale informatico e, per ciascuna di esse, le autorizzazioni relative.

Amministratori: gli utenti di questo gruppo sono abilitati alla definizione dell'ambiente applicativo e alla supervisione della gestione sistema, mediante funzioni disponibili all'interno dell'applicativo stesso. Gli amministratori inseriscono e modificano le parametrizzazioni indispensabili per l'utilizzazione della procedura, sulla base delle norme del Manuale e delle indicazioni del Responsabile del Servizio (es: definiscono l'organigramma, il piano di classificazione e il piano di conservazione). Sono autorizzati ad effettuare operazioni che impattano con il sistema documentale (es: modifica dei campi identificativi del protocollo) e gli annullamenti delle registrazioni, su autorizzazione del Responsabile del Servizio. Creano e gestiscono account utente, definiscono i privilegi di accesso, come da richiesta del dirigente/responsabile.

Operatori di protocollo: i membri di questo gruppo sono abilitati alle operazioni di protocollazione in ingresso e consultazione di tutta la corrispondenza protocollata, secondo quanto sotto riportato:

- Protocollo Generale – operatori:

Doria Maurizio Responsabile di Protocollo, Ravagnan Franco, Penzo Sara, Marangon Fabio, Varagnolo Cosimo, Nordio Fabio;

Segreteria Generale – operatori:

Dott.ssa Targa Michela Segretario Generale e Dirigente Settore AA.GG. e II.;

- Edilizia Privata – Urbanistica – operatori:

Penzo Molly Roberta, Varagnolo Valeria, Penzo Barbara;

- Gabinetto del Sindaco:

Boscolo Gilberto – Segretario particolare del Sindaco, Zinato Marianna, De Bei Giusi;

- Polizia Locale – operatori:

Dott. Tiozzo Michele Comandante Polizia Locale e Dirigente Settore Polizia Locale e AA.Legali.

Livelli di sicurezza

- I livelli di sicurezza dei documenti sono gestiti automaticamente dal programma, che attribuisce anche una serie di ACL (Access Control List) implicite, in rapporto sia al livello di autorizzazione attribuito al Settore del Comune al quale un utente appartiene (il ruolo coincide generalmente con un'area della struttura organizzativa comunale). Un utente quindi accede ad un documento se:
- il documento è stato inserito da un utente che appartiene allo stesso ruolo;
- l'utente appartiene all'ufficio mittente/destinatario del documento;
- l'utente appartiene all'ufficio da cui in un qualsiasi momento è transitato il documento;
- l'utente appartiene ad un ufficio dal quale in un qualsiasi momento è transitata una copia del documento, sia per competenza sia per conoscenza;
- al ruolo è stata autorizzata visibilità sul livello di sicurezza del documento stesso.

L'allegato 5 è costituito anche dall'allegato documento fornito dalla ditta Dedagroup attestante la descrizione e funzionalità della procedura "Folium".

AT WORK

IDEE PER RENDERTI UNICO



Folium

protocollo informatico
gestione documentale

Dott.ssa Serena Bellagotti
8 novembre 2015

Argomenti

- Premesse e Normativa
- Struttura di Folium
- Protocollo
- Gestione PEC
- Fascicolazione (*focus on fascicolo informatico*)
- Classificazione
- Assegnazioni
- Firma digitale
- Gestione rubriche
- Ricerche
- (Conservazione)



Adempimenti normativi



- Istituzione **Area organizzativa omogenea** e iscrizione/aggiornamento dati su sito IPA;
- Nominare il **Responsabile della gestione documentale** e **Suo Vicario (per ogni AOO)**;
- Nominare il **Responsabile della conservazione** e il **Responsabile per il trattamento dati personali**;
- Redigere il **Manuale di gestione documentale (protocollo)**;
- Redigere il **Manuale di conservazione**;
- **Attivare i processi necessari alla corretta conservazione dei doc. digitali.**

Come organizzarsi



- **Rivedere i processi organizzativi e le modalità di produzione e gestione dei documenti.**
- **Verificare la rispondenza del SW per il protocollo e la gestione documentale ai requisiti definiti dalla norma.**
- **Dotare i funzionari con potere di firma dei dispositivi di firma digitale**
- **Attivare i processi necessari alla corretta conservazione dei doc. digitali**
- **Pianificare corsi di formazione a tutti i livelli, per tutto il personale coinvolto in processi che prevedano il trattamento dei documenti.**

Strumenti per la dematerializzazione



- Documento informatico
- Formati
- Firma digitale
- Validazione temporale
- PEC
- Conservazione sostitutiva

Obiettivi



- Apprendere i principali riferimenti normativi in materia di **dematerializzazione** della documentazione amministrativa e degli archivi per **promuovere il cambiamento culturale e organizzativo**.
- Conoscere principi e strumenti per una **efficace gestione dei documenti informatici e dei flussi documentali**.

Normativa



- **DPR 445/2000** Testo unico sulla documentazione amministrativa
- **D.lgs 42/2004** Codice dei beni culturali e del paesaggio
- **D.lgs 82/2005** Codice amministrazione digitale
- **D.lgs 235/2010** Nuovo Codice dell'amministrazione digitale
- **D.lgs 196/2003** Codice in materia di privacy

Regole Tecniche

- Regole tecniche inerenti la Firma digitale DPCM 22 feb. 2013
- Regole tecniche per il Protocollo informatico DPCM 3 dic. 2013
- Regole tecniche in materia di Conservazione DPCM 3 dic. 2013
- Regole tecniche in materia di Formazione e gestione dei documenti informatici DPCM 13 novembre 2014
- Circolare AGID 60/2013 formato e tipologia delle informazioni minime e accessorie associate ai messaggi scambiati tra PA
- Circolare AGID n. 65/2014 definisce le modalità per l'accreditamento e la vigilanza sui soggetti che svolgono attività di conservazione dei documenti informatici.

Manuale di gestione documentale



- È il più importante documento organizzativo della pubblica amministrazione digitale.
- *Il manuale di gestione (art. 5) descrive il sistema di gestione dei documenti informatici e fornisce le istruzioni per la puntuale **formazione del documento**, per il corretto funzionamento del servizio per la tenuta del **protocollo informatico**, della gestione dei **flussi documentali** e degli **archivi**.*

Manuale di gestione documentale



In particolare, il manuale deve descrivere:

- Le modalità di utilizzo di strumenti informatici per **la formazione dei documenti informatici**, ai sensi dell'art. 40, comma 1, del Codice e quindi in modo conforme a quanto previsto dal DPCM 13 novembre 2014
- I **formati** utilizzati per la formazione del documento informatico
- L'insieme minimo dei **metadati** associati ai documenti soggetti a registrazione e gli eventuali ulteriori metadati rilevanti ai fini amm.vi
- La descrizione del **flusso di lavorazione dei documenti ricevuti, spediti o interni**, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione;
- L'elenco dei documenti **esclusi** dalla registrazione di protocollo e l'elenco dei doc. soggetti a **registrazione particolare**.

Manuale di gestione documentale



In particolare, il manuale deve descrivere:

- L'indicazione delle **regole di smistamento e assegnazione** dei documenti;
- I criteri e le modalità per il rilascio delle **abilitazioni di accesso** interno ed esterno alle informazioni documentali;
- Le modalità di **formazione, implementazione e gestione dei fascicoli informatici** con l'insieme minimo dei metadati ad essi associati;
- La descrizione funzionale ed operativa del componente «sistema di protocollo informatico»;
- Le modalità di utilizzo del **registro di protocollo d'emergenza**;
- Le modalità di produzione e di conservazione delle registrazioni di protocollo informatico.

DPR 445/2000

- Riunisce in un unico testo le norme sulla documentazione amministrativa e sul doc. informatico.
- **Afferma la validità a tutti gli effetti di legge del doc. informatico.**
- Decreta l'eliminazione della frammentazione dei sistemi di protocollo.
- Collega il sistema di protocollo alla gestione dei flussi documentali.
- Stabilisce i principi di gestione degli archivi.

D.Lgs 42/2004

Parallelamente alla normativa in materia di gestione informatica dei doc. della PA, il legislatore ha introdotto, attraverso il **codice dei beni culturali e del paesaggio**, importanti cambiamenti in materia di tutela e conservazione degli archivi.

- Gli archivi e i singoli documenti degli Enti pubblici sono inalienabili e sono oggetto di particolare tutela in quanto considerati dalla legge beni culturali fin dall'origine.
- L'Ente pubblico ha l'obbligo di ordinare il proprio archivio.

CAD – D.Lgs 82/2005 e succ. modifiche

Ha lo scopo di assicurare e regolare la disponibilità, gestione, accesso, trasmissione, conservazione e la fruibilità dell'informazione in modalità digitale.

- **Validità dei doc. informatici** (da art. 22 a art. 23 ter)
- **Formazione dei doc. informatici** (art. 40)
- **Conservazione digitale dei documenti** (art.li 43 e 44 bis)
- **PEC** (art.li 6 e 65)
- **Firme** (art. 1 comma 1 lett. Q-bis e art. 28 comma 3 bis)

Applicazione e scadenze



Perché l'art. 40 del CAD fosse applicabile si è dovuto aspettare il 12 gennaio 2015, giorno in cui sono state pubblicate sulla Gazzetta le **Regole tecniche del documento informatico** di cui all'art. 71 del CAD.

Le regole tecniche stabiliscono le modalità di formazione e copia dei doc. informatici e fissano il termine ultimo per l'adeguamento dei sistemi di gestione informatica documentale al 12 agosto 2016.

! Dal 12 Agosto 2016 tutti i documenti della PA dovranno essere digitali.

Come si lavorerà?

Tutti i documenti dovranno essere formati con strumenti informatici.



I documenti dovranno essere:

- **firmati digitalmente e correttamente protocollati:** gli atti amm.vi con rilevanza interna potranno essere sottoscritti con firma elettronica avanzata (art. 23-ter del CAD)
- essere **raccolti nel fascicolo informatico** relativo al procedimento specifico (art. 42 del CAD)

Cosa è Folium

Folium è un software di **protocollo informatico e gestione documentale** che consente l'automazione dell'intero ciclo di vita della corrispondenza sia **in entrata** che **in uscita**, a partire dalla registrazione delle informazioni identificative **minime** di un documento con:

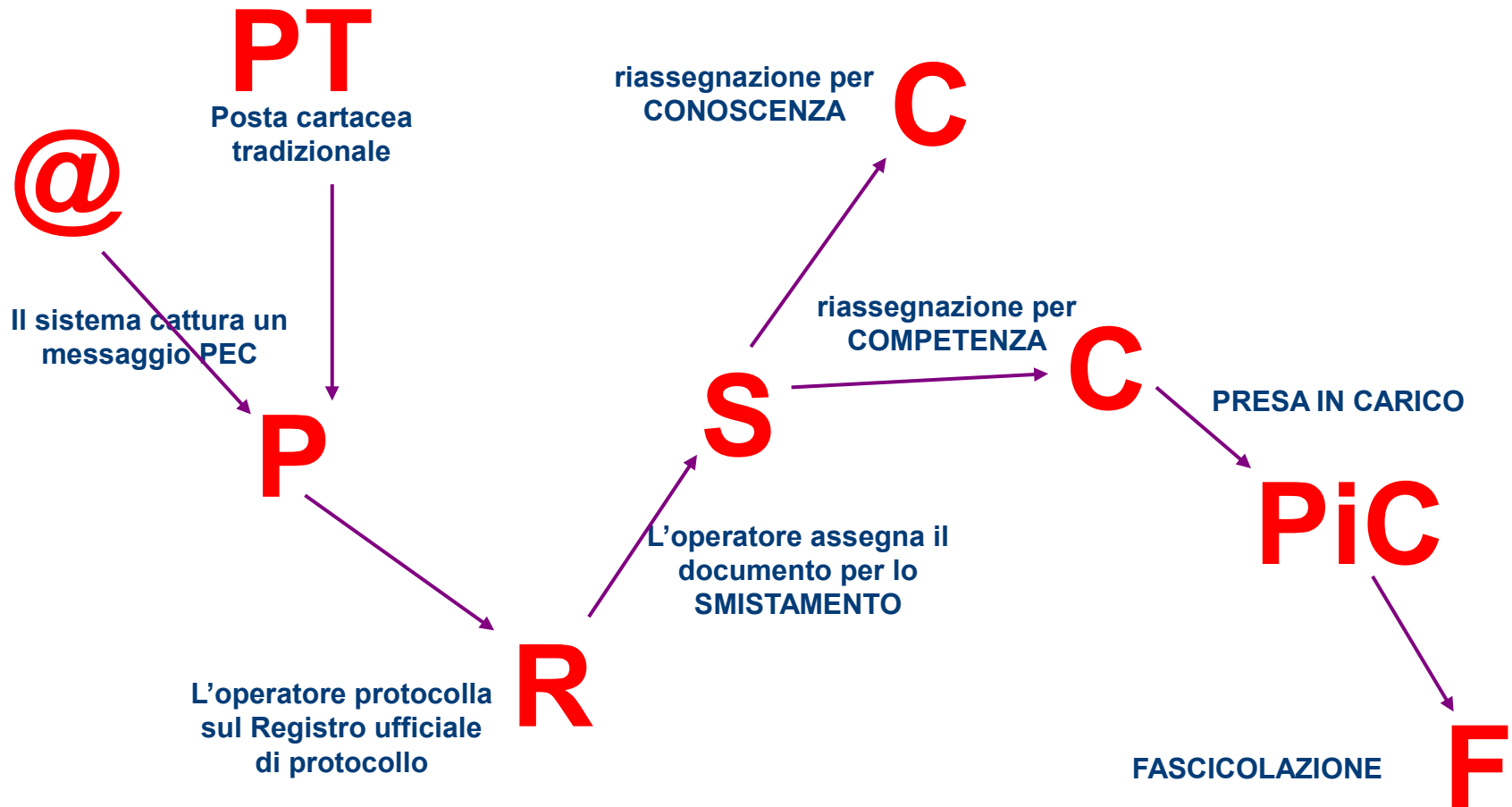
- *Assegnazione automatica del numero e data di protocollo*
- *Classificazione (secondo titolare)*
- *Assegnazione alle unità operative, soggetti responsabili e/o soggetti terzi (enti pubblici o privati)*
- *Fascicolazione*

Vantaggi con Folium

- **Dematerializzazione** (secondo il **D.Lgs 235/2010** gli enti dovranno utilizzare le comunicazioni cartacee solo quando sia impossibile utilizzare quelle telematiche)
- **Processi standard** per tutto l'Ente
- Posta elettronica certificata **PEC integrata nel Pdp**
Ricerche più rapide e sicure
- **Sicurezza** nella privacy
- **Risparmio** di tempo e risorse

Il protocollo informatico è garanzia di validità della data dell'evento di registrazione al pari della marca temporale.

Flusso di lavoro in ingresso

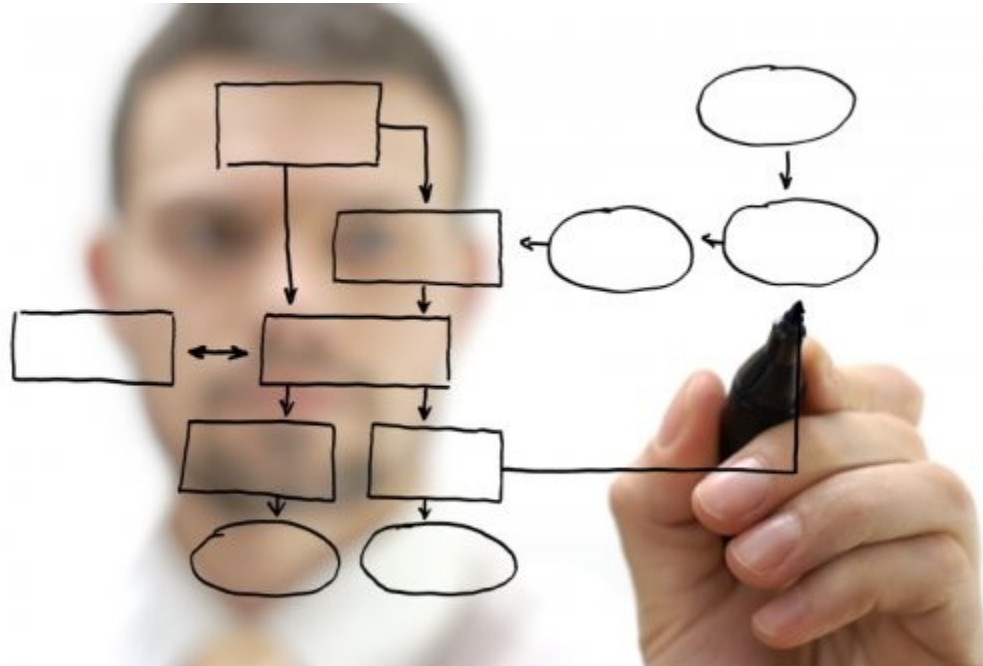


Premessa su Area organizzativa omogenea

L'Area organizzativa omogenea (AOO) è l'insieme di unità organizzative dell'amministrazione che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi di gestione dei flussi documentali in quanto presentano analoghe esigenze di gestione della documentazione.

In particolare, all'interno di una AOO esiste un solo servizio di protocollazione informatica dei documenti in entrata ed in uscita che adotta un **unico registro generale di protocollo**.

Struttura di Folium *alcune premesse...*



Folium - Come è strutturato

Prima di eseguire lo **Start up** del SW di protocollo andranno caricati e configurati i seguenti dati/parametri:

- 1)Area organizzativa omogenea
- 2)Ruoli (con i vari permessi applicativi)
- 3)Uffici
- 4)Utenti (abbinare utenti a ruoli ed uffici)
- 5)ACL (Liste di competenza)
- 6)Titolario (abbinare titolario alle ACL)
- 7)Casella/e di Posta elettronica certificata
- 8)Eventuali rubriche, Fascicoli, etc
- 9)Parametri di configurazione e demoni (sistemista)

Folium - Come è strutturato



Utente: **Serena Bellagotti**
Ufficio: (+)
Ruolo: **amministratore (+)**

Area organizzativa: **AOOPGRO** (p_gr)
Registro:

Versione: **4.12.0**
[Aiuto](#) [Home](#) [Uscita](#)

Organizzazione Applicazione Pratiche Estese Reports Eventi

Menù principale

Lista Aree Organizzative

Codice - Nome	Email Responsabile	Lettura Posta	Stato	Comandi
AOOPGRO - Provincia di Grosseto		Attivo		

Verifica Configurazione

Folium la soluzione globale per il protocollo, la gestione documentale ed i procedimenti.
© Dedagroup SPA 2001-2015

Ruoli : Folium dispone di vari ruoli applicativi che possono essere associati ad uno stesso utente. Tra i principali troviamo:

- *Amministratore*
- *Amministratore di AOO*
- *Sistemista*
- *Operatore standard*
- *Utente standard*
- *Operatore protocollo centrale (avrà per es. la gestione della PEC in entrata)*

Folium - Come è strutturato



Utente: Serena Bellagotti
Ufficio: (+)
Ruolo: amministratore

Area organizzativa: (scegli) (p_gr)
Registro:

Organizzazione	Applicazione	Pratiche Estese	Reports	Eventi
Arete organizzative	rganizzativa omogeneea			
Uffici				
Ruoli				
Utenti	ione			
AA00GRU	Provincia di Grosseto			

Inserimento, modifica cancelazione utenti

Modifica ufficio Storico modifiche

Inserisci nuovo ufficio

Disabilita ufficio

Elimina ufficio

ACL ufficio

Filtra per Aoo

Uffici -

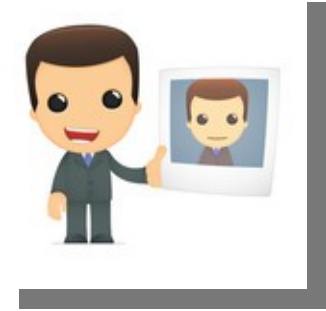
- AA001_DIREZIONE CENTRALE (DEDA_AOO)
- AA002_DIREZIONE TECNICA (DEDA_AOO)
- AA003_AFFARI GENERALI (DEDA_AOO)
- AA004_PROTOCOLLO (DEDA_AOO)
- AA005_DA STORICIZZARE PIPPO (DEDA_AOO)

Utenti ufficio



UserID	Cognome	Nome	Email	Resp.	Assegnatario per l'uff.
DEDAGROUP	DEDAGROUP	MASSIMO	massimo.gambino@alice.it	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
gambino	GAMBINO	MASSIMO	massimo.gambino@alice.it	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Modifica abilitazione assegnatari per questo ufficio

Impostazioni profilo utenti



Ogni **utente** registrato in **Folium** ha una **scheda profilo** modificabile (accessibile solo con il ruolo di *Amministratore*) che si caratterizza per:

-  **Dati identificativi** (*userid, password, nome, cognome, e-mail, C.F.*)
- **Uffici** a cui è abilitato l'utente
-  **Ruoli** a cui è abilitato (es. operatore standard, utente standard, etc)

Impostazioni profilo utenti



Utente: **Serena Bellagotti**
Ufficio: **(+)**
Ruolo: **amministratore (+)**

Area organizzativa: **A00PGRO** (p_gr)
Registro: **REGISTRO UFFICIALE**

[Aiut](#)

Organizzazione	Applicazione	Pratiche Estese	Reports	Eventi
----------------	--------------	-----------------	---------	--------

Modifica utente

UserId:

Password:

Conferma Password:

Cognome:

Nome:

Email:

Codice Fiscale:

Matricola:

Livello riservatezza: **NON CLASSIFICATO**

Abilitato Disabilitato

Invio e-mail notifica assegnazione:

Gestore emergenza:

Operatore emergenza:

I campi con questo colore sono obbligatori.

Uffici

Codice Ufficio:

Descrizione Ufficio:

Disponibili

A	PRESIDENTE
A10	PRESIDENTE DEL CONSIGLIO
A11	GIUNTA
A2	ASSESSORATO GOVERNO DEL TERRITORIO ED ENERGIE RINNOVABILI
A3	ASSESSORATO R.U. E BILANCIO
A4	ASSESSORATO SVILUPPO ECONOMICO E TURISMO

Selezionati

B02 - SERVIZIO COMUNICAZIONE E ICT
B021 - INFORMATIZZAZIONE ICT E INNOVAZIONE
B03 - AVVOCATURA
B04 - CONTENZIOSO
B06 - GAC - POLI
C - DIPARTIMENTO DI SVILUPPO SOSTENIBILE
C01 - UP DI STAFF INTERAREA E SEGRETERIA
C02 - SERVIZIO PROGRAMMI DI SVILUPPO SOSTENIBILE
C3 - AREA SVILUPPO RURALE E TURISMO

Ruoli utente

Ruoli	Ufficio	Aoo
Amministratore		
Amministratore di AOO		A00PGRC
WebService User		A00PGRC
operatore_standard		A00PGRC
protocollatore_ingresso		A00PGRC
protocollo_centrale		A00PGRC

Impostazioni Ruoli

E' possibile creare (oltre ai ruoli standard) dei ruoli *ad hoc*



Utente: **Serena Bellagotti**

Ufficio: [\(+\)](#)

Ruolo: **amministratore**

Are.

Reg

Organizzazione

Applicazione

Pratiche Estese

Reports

Ruoli applicativi

Nuovo

Cancela

Selezione	Nome	Descrizione
	<u>Amministratore</u>	Amministratore del sistema
	<u>Operatore</u>	Operatore di protocollo
	<u>Utente</u>	Utente del documentale
	<u>Amministratore di AOO</u>	Amministratore di AOO
<input type="checkbox"/>	<u>WebService User</u>	WebService User
<input type="checkbox"/>	<u>operatore standard</u>	Operatore generico
<input type="checkbox"/>	<u>protocollatore ingresso</u>	Protocolla in ingresso
<input type="checkbox"/>	<u>protocollo centrale</u>	Operatore di protocollo
<input type="checkbox"/>	<u>utenti responsabili</u>	Responsabili con potere di firma
<input type="checkbox"/>	<u>utente standard</u>	Utente documentale
<input type="checkbox"/>	<u>protocollatore ingresso pec</u>	Protocollatore in Ingresso, con accesso PEC
<input type="checkbox"/>	<u>utente pec</u>	utente pec

Impostazioni Ruoli

L'Amministratore definisce (attraverso una spunta) i **permessi** a cui sarà abilitato ogni singolo **ruolo**.

Organizzazione	Applicazione	Pratiche Estese	Reports
Modifica il ruolo n. 61			
Nome:	operatore_standard 50		
Descrizione:	Operatore generico 200		
Menu:	protocollazione		
Permessi:	<input type="checkbox"/> Abilitazione operazioni progressivo fascicolo <input type="checkbox"/> Accesso alle assegnazioni dell'ufficio <input type="checkbox"/> Amministrazione <input type="checkbox"/> Amministrazione di AOO <input type="checkbox"/> Annullamento parziale protocollazione <input type="checkbox"/> Annullamento protocollazione <input type="checkbox"/> Apertura registri <input checked="" type="checkbox"/> Assegnazione per competenza/conoscenza <input type="checkbox"/> Assegnazione per smistamento <input type="checkbox"/> Autorizzazione dati sensibili <input type="checkbox"/> Chiusura annuale registri <input type="checkbox"/> Chiusura registri <input checked="" type="checkbox"/> Classificazione <input type="checkbox"/> Conservazione Sostitutiva <input type="checkbox"/> Consultazione dei report (sola lettura) <input type="checkbox"/> Creazione e modifica dei report <input type="checkbox"/> Creazione/Modifica pratiche <input type="checkbox"/> Esecuzione reports <input type="checkbox"/> Firma Documenti <input type="checkbox"/> Gestione Formati Documenti <input type="checkbox"/> Impostazione lista di competenza <input type="checkbox"/> Invia documenti pratica <input type="checkbox"/> Lettura posta <input type="checkbox"/> Lettura registri <input type="checkbox"/> Limita cancellazione da fascicolo <input type="checkbox"/> Modifica registri <input checked="" type="checkbox"/> Modifica rubrica <input type="checkbox"/> Modifica titolare <input type="checkbox"/> Protocollazione in ingresso		

Focus su ruolo Operatore

Si eseguono protocollazioni:

- Interne
- Uscita
- Ingresso (facoltativo)



Utente: **Serena Bellagotti**

Ufficio: **Ufficio 1 (+)**

Ruolo: **operatore (+)**

Area organizzativa: **AOO1 (TEST)**

Registro:

Protocollazione	Ricerca	Assegnazioni	Registri	Rubriche	Fascicoli	Utente	Reports
Nuovo							
Da precedente							
Da precedente con allegati						Ultimi 30 giorni	
Rapida						0	
Comunicazioni							
test ...						30/06/2015	
Comunicazione di oggi ...						04/05/2015	

Folium la soluzione globale per il protocollo, la gestione documentale ed i procedimenti.

© Dedagroup SPA 2001-2015

Focus su ruolo Utente

Si vedono e si gestiscono:

- **Assegnazioni** (competenza, conoscenza, smistamento)
- **Documenti presi in carico**
- **Fascicoli**

folium Utente: **Serena Bellagotti** Area organizzativa: **c_f376 (TEST)**
Ufficio: **Organi Istituzionali (+)** Registro:
Ruolo: **uteresp (+)**

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
Quadro riassuntivo	Assegnazioni competenza					
Assegnazioni	Assegnazioni conoscenza			Ultimi 30 giorni		
Competenza				3		
Conoscenza	Assegnazioni per smistamento			0		
Smistamento				1		
Restituite	Assegnazioni effettuate in attesa			0		
Comunicazioni	Assegnazioni restituite					
Nessuna comunicazione	Tutte le assegnazioni					

Folium la soluzione globale per il protocollo, la gestione documentale ed i procedimenti.
© Dedagroup SPA 2001-2015

Focus su ruolo di Protocollore Centrale

E' un menù simile a quello dell'operatore, in più però di solito ha:

- **Gestione della PEC in ingresso**
- Gestione esclusiva delle rubriche (facoltativa)
- **Visualizzazione stampe registro e lettura del registro**
- **Annullamento di protocolli**

folium Utente: **Serena Bellagotti** Area organizzativa: **c_f376 (TEST)**
Ufficio: **Organi Istituzionali (+)** Registro:
Ruolo: **protoresp (+)**

Protocollo	Ricerca	Assegnazioni	Registri	Rubriche	Posta	Fascicoli	Utente	Reports
Quadro riassuntivo					Posta in arrivo			
Assegnazioni					Ricevute			
Restituite					Posta protocollata in ingresso			
					Posta in uscita			
Posta Elettronica					Posta inviata			
Messaggi in arrivo					Ricevi adesso			
Messaggi non inviati					Invia adesso			
					Cestino			
Comunicazioni					Inoltri - Risposte			
Nessuna comunicazione								

Folium la soluzione globale per il protocollo, la gestione documentale ed i procedimenti.
© Dedagroup SPA 2001-2015

La Protocollazione



Pagina di login di Folium

The logo for Folium, featuring the word "folium" in a bold, lowercase, sans-serif font. The letters are dark blue, with a lighter blue shadow effect behind them, giving it a 3D appearance.

Userid:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="Login"/>

Eseguire un protocollo

Ruolo: *operatore standard*



Utente: [Serena Bellagotti](#)
 Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
 Ruolo: [operatore standard \(+\)](#)

Area organizzativa: [AOPGRO \(p_gr\)](#)
 Registro:

Protocollazione	Ricerca	Assegnazioni	Registri	Rubriche	Fascicoli	Utente	Reports
Nuovo	Effettua una registrazione di protocollo						
Da precedente							
Da precedente con allegati				Ultimi 60 giorni			
				3			
Rapida							
Comunicazioni							
Nessuna comunicazione							

Folium la soluzione globale per il protocollo, la gestione documentale ed i procedimenti.
 © Dedagroup SPA 2001-2015

... si sceglie la modalità con cui si vuole effettuare il protocollo



Utente: [Serena Bellagotti](#)
 Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
 Ruolo: [operatore standard \(+\)](#)

Area organizzativa: [AOPGRO \(p_gr\)](#)
 Registro:

Protocollazione	Ricerca	Assegnazioni	Registri	Rubriche	Fascicoli	Utente	Reports
-----------------	---------	--------------	----------	----------	-----------	--------	---------

Selezione registro e modalità di protocollazione

Registro di CORRISPONDENZA	Descrizione	Data ultima reg.	Ingresso	Interna	Uscita
REGISTRO UFFICIALE	Registro Ufficiale Provincia di Grosseto	25/08/2015	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Maschera di protocollo in uscita (sfondo verde)



Utente: Serena Bellagotti
Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [protocollo centrale \(+\)](#)

Area organizzativa: [A00PGRD \(p_or\)](#)
Registro: [REGISTRO UFFICIALE](#)
Stato: **Uscita** - 27/08/2015

Versione: 4.12.0
[Aiuto](#) [Home](#) [Uscita](#)

Protocollo	Ricerca	Assegnazioni	Registri	Rubriche	Posta	Fascicoli	Utente	Reports
InterFKU								
Protocollo	Classificazione	Collegati	Info	Documento	Allegati			

Codice Oggetto:

Oggetto:

[Non inserire dati sensibili nell'Oggetto]

Destinatari (E' necessario inserire almeno un destinatario)

Invio E-mail singola Protocollo in modalità circolare

Descrizione: Mezzo sped.:

Denominazione	Indirizzo	Mezzo sped.	P.t.	Comandi

Ufficio Mittente Competente: **SEGRETARIO/ DIRETTORE GENERALE**

Data documento: (gg/mm/aaaa) Data spedizione: (gg/mm/aaaa) Data scadenza: (gg/mm/aaaa)

Firmatario: 50

Riservato: Conserva Dati: Richiesta conferma: Dati Sensibili:

Livello riservatezza: **NON CLASSIFICATO**

I campi con questo colore sono obbligatori. Per muoversi fra i pannelli si può anche usare il tasto F12.

Maschera di protocollo in ingresso (sfondo blu)



Utente: Serena Bellagotti
Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [protocollo centrale \(+\)](#)

Area organizzativa: [A00PGRO \(p_g\)](#)
Registro: [REGISTRO UFFICIALE](#)
Stato: **Ingresso** - 27/08/2015

Versione: 4.12
[Aiuto](#) [Home](#) [Uscì](#)

Protocollo	Ricerca	Assegnazioni	Registri	Rubriche	Posta	Fascicoli	Utente	Reports
InterPRO								
Protocollo	Classificazione	Collegati	Info	Documento	Allegati			

Codice Oggetto:

Oggetto:

[Non inserire dati sensibili nell'Oggetto]

Mittenti (E' necessario inserire almeno un mittente)

Descrizione Mezzo spec.:

Denominazione	Indirizzo	Mezzo sped.	P.C.	Comandi

Uffici Destinatari Competenti:

B - SEGRETARIO/ DIRETTORE GENERALE

Data documento: (gg/mm/aaaa) Data ricezione: (gg/mm/aaaa) Data scadenza: (gg/mm/aaaa)

Protocollo mittente: Firmatario:

Ricevuto: Conoscenza Data:

I campi con questo colore sono obbligatori. Per muoversi fra i pannelli si può anche usare il tasto F11

Cambia in Interna Cambia in Uscita Assegna

Maschera di protocollo interna



Utente: Serena Bellagotti
Ufficio: [SEGRETARIO / DIRETTORE GENERALE \(+\)](#)
Ruolo: [protocollo centrale \(+\)](#)

Area organizzativa: [A00PGRO \(p_gr\)](#)
Registro: [REGISTRO UFFICIALE](#)
Stato: **Interna** - 27/08/2015

Versione:
[Aiuto](#) [Home](#)

Protocollo	Ricerca	Assegnazioni	Registri	Rubriche	Posta	Fascicoli	Utente	Reports
InterPRO								

Protocollo	Classificazione	Collegati	Info	Documento	Allegati
------------	-----------------	-----------	------	-----------	----------

Codice Oggetto:

Oggetto:

[Non inserire dati sensibili nell'Oggetto]

Ufficio Mittente
Competente:

Uffid Destinatari
Competenti:



Data documento :

 (gg/mm/aaaa)

Data spedizione:

 (gg/mm/aaaa)

Data scadenza:

 (gg/mm/aaaa)

Firmatario:

50

Riservato:

Conserva Dati:

Dati Sensibili:

Livello riservatezza:

I campi con questo colore sono obbligatori. Per muoversi fra i pannelli si può anche usare il tast



[Cambia in Ingresso](#) [Cambia in Uscita](#) [Assegna](#) [Protoc](#)

Focus tecnico su Assegnazione obbligatoria

Con il ruolo di Amministratore, menu Configurazione si può impostare l'obbligo di assegnazione prima di eseguire protocollazione.

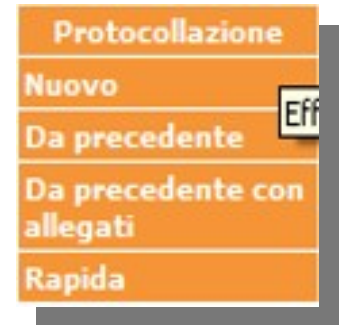
Nome amministrazione	Il nome dell'amministrazione	Dedagroup
Notifica assegnazione al responsabile	Invio della notifica di assegnazione anche al responsabile dell'ufficio	1
Numero data e aoo protocollazione in oggetto mail	Valori ammessi : 0,1. Se 1 l'oggetto della e-mail contiene i dati di protocollo	1
Numero massimo di destinatari in una mail	Viene usato nella fase di protocollazione con mezzo sped Email	50
Numero massimo di record per iteratore	Numero massimo di risultati restituiti dalle interrogazioni al DB. Non può essere maggiore di 1000.	10000
Numero righe paginazione	Numero righe paginazione	15
numero.tentativi.invio.mail	Numero massimo di tentativi per l'invio di email	10
Obbligo Assegnazione Documenti	Valori possibili: 0 = Nessun obbligo; 1 = obbligo in protocollazione; 2 = obbligo in protocollazione in ingresso; 3 = obbligo in protocollazione in uscita	1
Obbligo Classificazione	Valori possibili: 0 = Nessun obbligo; 1 = obbligo in protocollazione; 2 = obbligo in assegnazione; 3 = obbligo in fascicolazione	0

! Allo stesso modo si può configurare anche l'obbligo di Classificare.

Eseguire un protocollo

Menù **Protocollazione** → **Nuovo** → es. **Ingresso**

-
- I pannelli del protocollo:
 - > **Protocollazione**
 - Nuovo
 - Da precedente
 - **Da precedente con allegati (novità)**
 - Rapida
 - > **Classificazione**
 - > **Collegati**
 - > **Info**
 - > **Documento**
 - > **Allegati** (peso massimo 32 MB complessivi del doc.principale)



Protocollo in uscita

I 6 pannelli del protocollo



Utente: **Serena Bellagotti**
Ufficio: **Direzione Generale Affari Generali (+)**
Ruolo: **operatore (+)**

Area organizzativa: **AO01 (TEST)**
Registro: **REGISTRO UFFICIALE**
Stato: **Uscita - 23/10/2015**

Versione: 4.13.0
[Aiuto](#) [Home](#) [Uscita](#)

Protocollo in uscita navigation bar:

- Protocollo
- Classificazione
- Collegati
- Info
- Documento
- Allegati
- Conservazione

Nome Documento Esteso:

Codice Oggetto:

Oggetto:

[Non inserire dati sensibili nell'Oggetto]

Destinatari (E' necessario inserire almeno un destinatario)

Invio E-mail singole Protocollo in modalità circolare

Descrizione: Mezzo sped.:

Denominazione	Indirizzo	Mezzo sped.	P.C.	Comandi

Indice IPA

Ufficio Mittente Competente:

Data documento: (gg/mm/aaaa) Data spedizione: (gg/mm/aaaa) Data scadenza: (gg/mm/aaaa)

Firmatario:

Riservato: Conserva Dati: Richiesta conferma: Dati Sensibili:

Oggettario

È data la possibilità di **registrare** alcuni “**oggetti**” **ripetitivi** che sarà possibile riutilizzare da tutti i protocollatori per agevolare – ove possibile il lavoro dell'immissione.

L'immagine riporta l'inserimento di un nuovo oggetto che, potrà poi essere richiamato sia con codice mnemonico che tramite finestra popup.

The screenshot displays the 'Folium - Oggettario' web application interface. The main window shows a 'Nuovo Oggetto' (New Object) form with the following fields and elements:

- Codice:** A text input field containing the value '20'.
- Descrizione:** A large text area for entering the object's description.
- Condividi con altre AOO:** A checkbox that is currently unchecked.
- Buttons:** 'Salva' (Save) and 'Annulla' (Cancel) buttons.
- Note:** A message states 'I campi con questo colore sono obbligatori.' (Fields with this color are mandatory).

The interface also features a navigation bar with tabs for 'Protocollo', 'Classificazione', 'Collegati', 'Info', and 'Docum'. The bottom status bar indicates 'Intranet locale' and '100%' zoom.

Maschera di protocollo – uffici competenti

- Sia per la protocollazione **in ingresso** che per quella **in uscita** l'operatore ha facoltà di utilizzare il campo multivalore “Uffici Competenti”.



The screenshot shows a form titled "Uffici Competenti". It features two input fields at the top, with a grid icon, a checkmark icon, and an 'X' icon to their right. Below these is a larger, empty text area with an 'X' icon at its bottom right corner.

Il significato di queste informazioni aggiuntive è lasciato agli operatori.
Di norma:

- Per i **protocolli in uscita**, l'ufficio competente è l'ufficio che ha prodotto il documento (e che potrebbe differire dall'ufficio che lo sta protocollando).

Per i **protocolli in ingresso**, alcuni operatori indicano gli eventuali assegnatari del documento. Si tenga conto però che l'operazione di assegnazione viene svolta in modo diverso.

- La valenza di questa indicazione sarà quindi legata unicamente alla facilitazione nella ricerca.

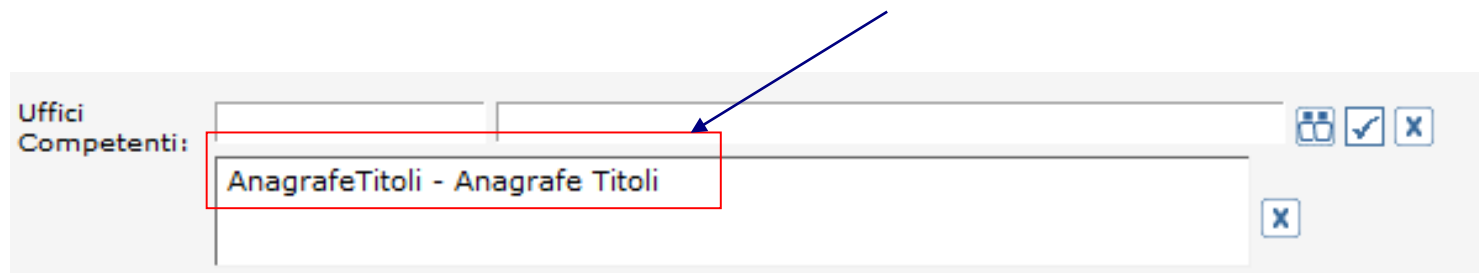
Maschera di protocollo – uffici competenti



Uffici Competenti:

The screenshot shows a form with two input fields at the top and a larger list area below. On the right side of the top row, there are three icons: a grid icon (circled in red), a checkmark icon, and an 'X' icon. Below the list area, there is another 'X' icon.

- L'operatore aziona il pulsante indicato con cerchio rosso. Si apre una finestra dove compare l'organigramma dell'ente con le sue gerarchie.
- Si seleziona una delle unità organizzative che, a valle della selezione, vanno ad occupare la posizione indicante l'avvenuta selezione





Uffici Competenti:

The screenshot shows the same form as above, but now the text 'AnagrafeTitoli - Anagrafe Titoli' is selected in the list area and enclosed in a red box. A blue arrow points from the top right towards the selected text. The icons on the right are now active, with the checkmark icon highlighted.

NB: Per le registrazioni di protocollo in uscita è possibile impostare il sistema in modo che popoli automaticamente il campo “ufficio competente” con la descrizione dell'ufficio del protocollatore per ogni nuova registrazione.

Maschera di protocollo – dati aggiuntivi

Data documento : (gg/mm/aaaa) Data ricezione: (gg/mm/aaaa) Data scadenza: (gg/mm/aaaa)

Protocollo mittente: 40   Firmatario: 50

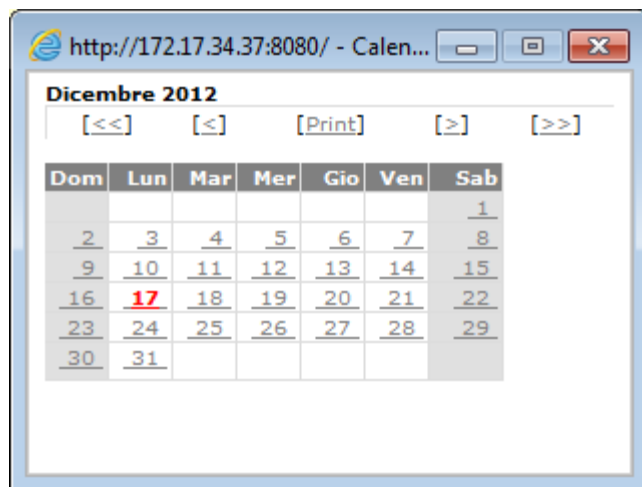
Riservato: Conserva Dati: Dati sensibili:

Livello riservatezza: **NON CLASSIFICATO** ▼

I pulsanti riportati sulla destra del campo “Protocollo Mittente” permettono di individuare eventuali doppioni già registrati in precedenza.

L’indicazione del firmatario, valida sia per l’ingresso che per l’uscita, ha rilevanza per le ricerche di tipo avanzato.

Il sistema registra anche il protocollo mittente rilevato sulla posta in ingresso.



Tutte le date indicate possono essere inserite a mano nella forma 10/09/2015. In alternativa l’utente può utilizzare il calendario che viene attivato dall’icona che compare a destra di ogni campo data.

Maschera di protocollo – dati aggiuntivi

Data documento : (gg/mm/aaaa) Data ricezione: (gg/mm/aaaa) Data scadenza: (gg/mm/aaaa)

Protocollo mittente: 40 Firmatario: 50

Riservato: Conserva Dati: Dati sensibili:

Livello riservatezza: **NON CLASSIFICATO** ▼

Riservato: il flag “riservato” può essere apposto unicamente da operatori selezionati. Il protocollo che sia stato definito “riservato” sarà visibile unicamente agli altri operatori di protocollo abilitati alla riservatezza ed agli utenti che risultino “assegnatari”.

Dati sensibili: anche questo flag viene abilitato solo da operatori qualificati. Ove un protocollo sia definito contenente “Dati sensibili” potrà essere visualizzato soltanto da utenti che, avendone fatta richiesta, ricevono una specifica autorizzazione dal “Responsabile per il trattamento dei dati”.

Livello riservatezza: si tratta di un ulteriore strumento di gestione della riservatezza che richiede la contemporanea definizione del livello di riservatezza degli utenti (es. non classificato, top secret, ristretto, segreto, classificato)

Maschera "Collegati"



Utente: Serena Bellagotti
Ufficio: SECRETARIO/ DIRETTORE GENERALE (+)
Ruolo: operatore standard (+)

Area organizzativa: AOOPGRO
Registro: REGISTRO UFFICIALE
Stato: Uscita - 25/08/2015

Protocollazione Ricerca Assegnazioni Registri Rubriche Fascicoli Utente

Protocollo Classificazione Collegati Info

Selezione documenti
(è possibile utilizzare chiavi parziali di ricerca utilizzando il carattere speciale *)

Dati protocollo	
Registro: <input type="text" value="REGISTRO UFFICIALE"/>	Modalità: <input type="radio"/> interna <input type="radio"/> ingresso <input type="radio"/> uscita <input checked="" type="radio"/> tutti <input type="radio"/> registrazioni
Anno Registro: <input type="text" value="2015"/> Oggetto*: <input type="text"/>	Mezzo di spedizione: <input type="text"/> <input type="checkbox"/> voci storicizzate
Tipo documento: <input type="text"/>	
Mittente Destinatario	
Codice: <input type="text"/> Cognome Nome*: <input type="text"/>	E-mail: <input type="text"/>
Indirizzo: <input type="text"/>	Provincia: <input type="text"/> Comune: <input type="text"/>
Altri dati	
Solo documenti dell'ufficio corrente <input type="checkbox"/>	Non spediti: <input type="checkbox"/>
Data da: <input type="text"/> (gg/mm/aaaa)	a: <input type="text"/> (gg/mm/aaaa)
Data Documento da: <input type="text"/> (gg/mm/aaaa)	a: <input type="text"/> (gg/mm/aaaa)
Data Ricezione/Spedizione da: <input type="text"/> (gg/mm/aaaa)	a: <input type="text"/> (gg/mm/aaaa)
Data Scadenza da: <input type="text"/> (gg/mm/aaaa)	a: <input type="text"/> (gg/mm/aaaa)
N Progressivo dal: <input type="text"/>	al: <input type="text"/>
Numero prot esterno: <input type="text"/>	Note: <input type="text"/>
Codice Titolare: <input type="text"/>	Collocazione: <input type="text"/>

Maschera “Documento”

- Contiene il **documento principale di protocollo**, firmato digitalmente o non firmato, proveniente da PEC o acquisito da file system o, ancora da scanner.
- Le descrizioni che seguono sono sostanzialmente identiche sia che si tratti di protocollo in entrata o in uscita.

Area organizzativa: **AOOPGRO** (p_gr) Versione: 4.12.0
Registro: [REGISTRO UFFICIALE](#) [Aiuto](#) [Home](#) [Uscita](#)
Stato: **Uscita** - 26/08/2015

Fascicoli	Utente	Reports	
Info	Documento	Allegati	

Info Documento Allegati

Info Utente Report Allegati

Maschera "Documento"

Imposta parametri scanner: permette di impostare i parametri di scansione prima di avviare l'acquisizione.

Area organizzativa: AOO PGRO (p_gr)
Registro: REGISTRO UFFICIALE
Stato: **Uscita** - 26/08/2015

Versione: 4.12.0
[Aiuto](#) [Home](#) [Uscita](#)

The screenshot shows a web interface for document management. At the top, there are navigation tabs: 'Fascicoli', 'Utente', 'Reports', 'Info', 'Documento', and 'Allegati'. Below the 'Documento' tab, there is a toolbar with several icons: a plus sign, a document with a checkmark, a document with a magnifying glass, a document with a printer icon, a document with a trash can icon, a document with a list icon, and a close button (X).

Elimina il documento acquisito: operazione possibile solo prima della protocollazione.

Acquisisci

Acquisisce anche file di tipo PDF, anche quelli che portano firma digitale ed eventuale marca temporale.

Acquisisci da scanner

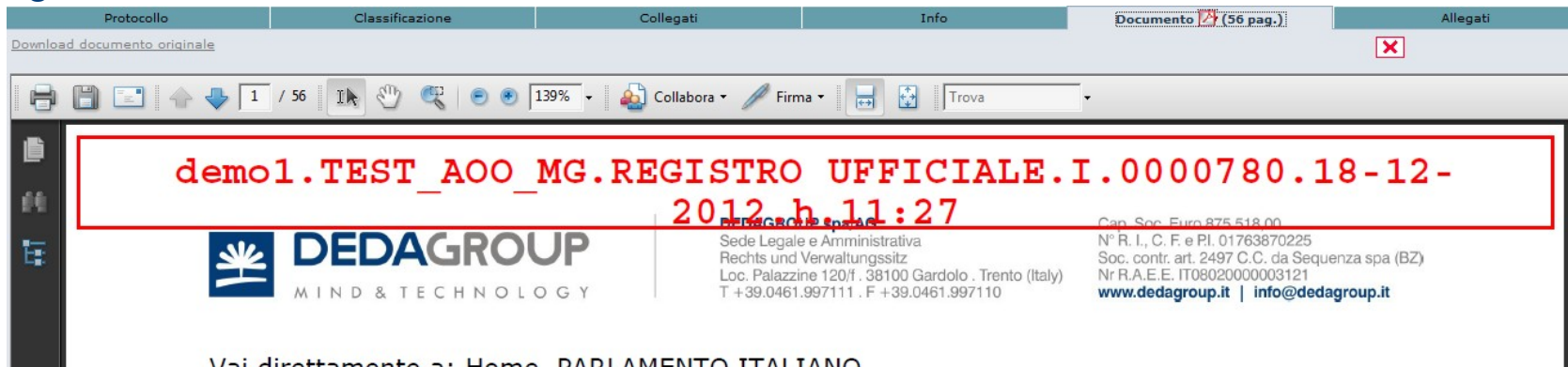
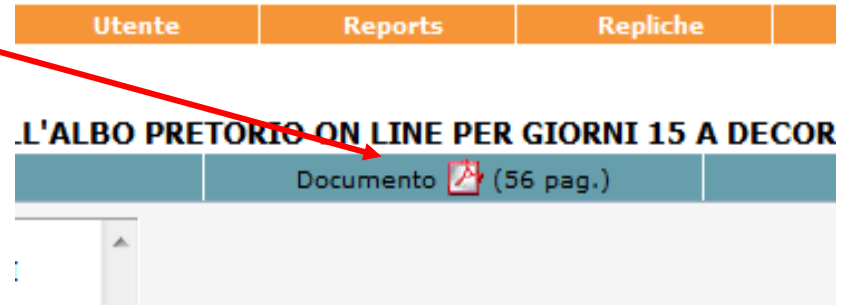
Acquisisci da file

Acquisisci da fascicolo

Acquisisci da file con conversione PDF preliminare: permette di acquisire qualsiasi file di tipo "Office" (doc, docx, xls, ppt, rtf, odt) e permette la conversione preliminare PDF senza conservare anche l'originale.

Documento

- Al documento acquisito, nel pannello documento compare l'icona tipica del prodotto Adobe e viene anche riportato il numero di pagine di cui il documento è costituito.
- Cliccando sull'icona appare il contenuto documentale, a tutta pagina dove è visibile anche il timbro (personalizzabile) di segnature.



! Vale la pena notare che, nel caso in cui il documento sia stato acquisito da "office" e convertito in PDF, sarà sempre disponibile all'operatore anche il download del documento originale.

Documento


Nel caso in cui il doc. acquisito come primario sia associato ad una firma digitale, tutti i dati di firma vengono mostrati nella collocazione evidenziata dove l'operatore può valutare la validità intrinseca della firma.
Il documento PDF viene estratto e mostrato con il visualizzatore nel browser.

Acquisisci una immagine digitale per questo documento

Firmatario	Valido dal	Sino al	Validità	Legale	CA	Località	E-mail	Org.Unit	Revocato	Info
FABIO LOMBARDI	03/03/2008	03/03/2014	Si	Si	LISIT Servizio di certificazione per la Firma Digitale			non presente	No	

1 / 2 139% Collabora Firma Trova

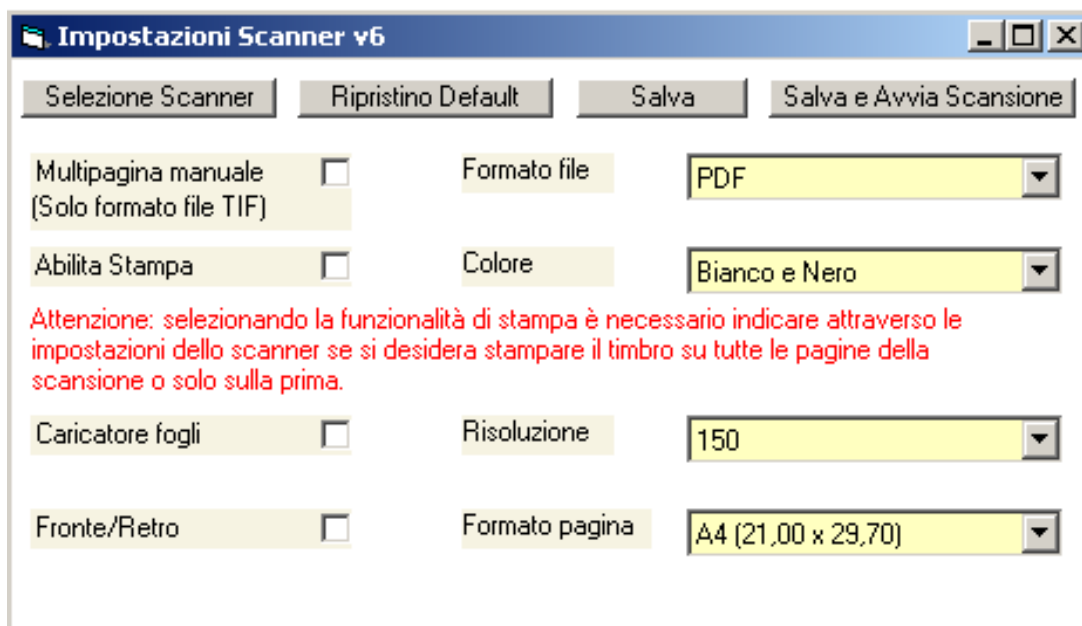
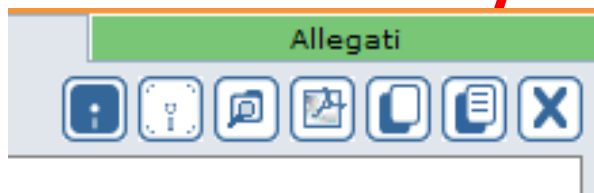
In caso di firma digitale Adobe, il visualizzatore Adobe Reader ci mette a disposizione strumenti di controllo supplementare: il [tool di verifica della firma](#)



Regional Lombardia

Documento – parametri scanner

Il dispositivo di scansione (TWAIN Compliant) dovrà essere stato preliminarmente installato con i suoi drivers.



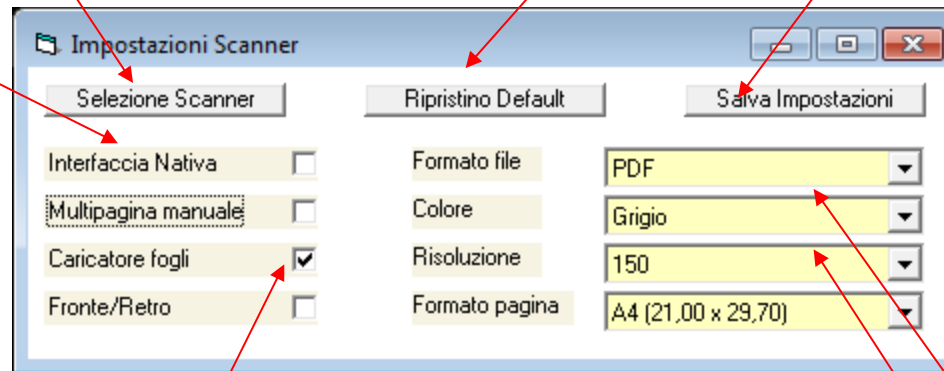
Documento – parametri scanner

Permette di selezionare il driver corretto dello scanner nel caso in cui siano installate più periferiche di acquisizione delle immagini (fotocamere, videocamere, scanner di diversa natura).

Permette di salvare le impostazioni testé definite e salvarle per le successive scansioni.

Effettua il ripristino delle condizioni di default

Se le altre impostazioni non dovessero funzionare a dovere il dispositivo può utilizzare la sua interfaccia Windows nativa!

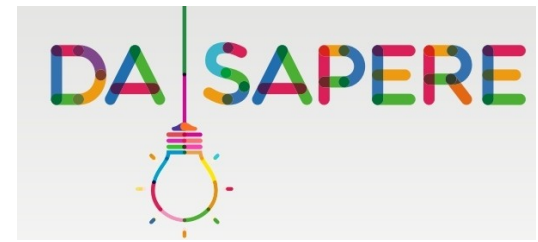


Permettono di attivare o disabilitare le modalità standard di acquisizione dei documenti:

- Caricatore di fogli o in alternativa la superficie piana;
 - Opzione Fronte Retro (quando disponibile)
- Multipagina manuale (consente di acquisire più pagine del documento quando non sia disponibile il modulo "caricatore di fogli").

Consentono di variare i parametri fondamentali dell'acquisizione, segnatamente il colore (le tre ipotesi sono colore, grigio, b/n) e la risoluzione (da 150 a 600 dpi)

Menù Utente - Profilo



Ufficio: [Direzione Generale Affari Generali \(+\)](#)

Ruolo: [operatore \(+\)](#)

Registro:

[Aiuto](#) [H](#)

Protocollo	Ricerca	Assegnazioni	Registri	Rubriche	Fascicoli	Utente	Reports
------------	---------	--------------	----------	----------	-----------	--------	---------



Profilo utente

UserId: bellagotti
Cognome: Bellagotti
Nome: Serena
Email: serena@cc.it
Codice Fiscale:
Matricola:
Uffici: 1oi - Organi Istituzionali AO - Aoo B1 - Sindaco C1 - Segretario Generale C10 - Affari Generali C11 - ATTIVITA FINANZIARIE E PATRIMONIO C12 - TECNICA LAVORI PUBBLICI E MANUTENZIONE C13 - TECNICA URBANISTICA PRIVATA URBANISTICA E AMBIENTE C14 - PUBBLICA ISTRUZIONE SPORT E SERVIZI SOCIALI C15 - POLIZIA LOCALE C16 - SVILUPPO LOCALE DG_AAGG - Direzione Generale Affari Generali SEG-GEN - SEGRETARIO GENERALE UFF1 - Ufficio 1
Abilitato: si



Notifica assegnazione

Invio e-mail notifica assegnazione:

Salva

Cambio password

Vecchia password: 100

Nuova password: 100

Conferma nuova password: 100


Salva

Allegati

Aggiungi un allegato

L'operatore può semplicemente descrivere l'allegato senza acquisirlo elettronicamente oppure acquisire il documento da:

- posta elettronica
- file system
- scanner

Protocollo	Classificazione	Collegati	Ir
Descrizione: <input type="text"/>			
Collocazione: <input type="text"/>			
Acquisisci una immagine digitale per questo allegato			
			

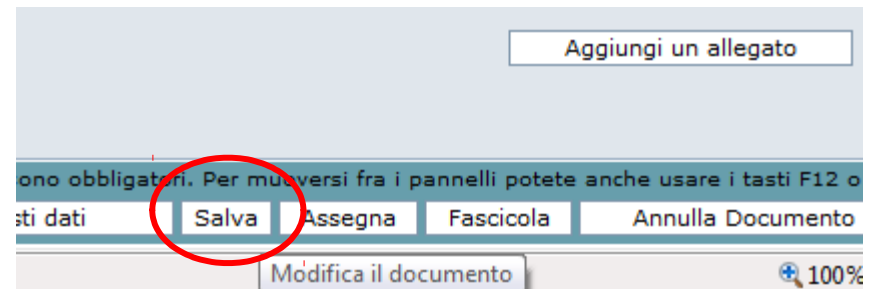
Allegati - Salvataggio

Dopo l'acquisizione del file allegato l'operatore preme il tasto OK per ciascun allegato.

L'operazione viene ripetuta se necessario per ciascun allegato.



Al termine delle operazioni di inserimento degli allegati l'operatore **non dimentichi mai** di effettuare il "Salva"



Allegati

Se un allegato contiene una **firma digitale**, il sistema è in grado di effettuare una verifica preliminare di validità giuridica.

REGISTRO UFFICIALE: PROTOCOLLO in Ingresso, N.72, data: 18/12/2012 - oggetto: TESTO DI UN OGGETTO RIPETITIVO DA RIUTILIZZARE

Protocollo	Classificazione	Collegati	Info
------------	-----------------	-----------	------

Descrizione:

Collocazione:

Acquisisci una immagine digitale per questo allegato

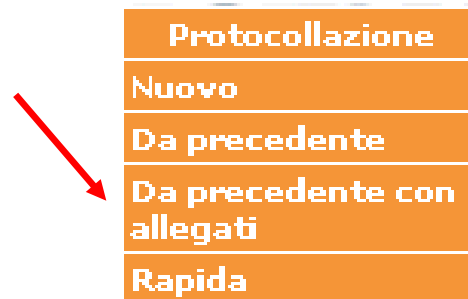
Firmatario	Valido dal	Sino al	Validità	Legale	CA	Località	E-mail	Org.Unit	Revocato	Info
Massimo Gambino	20/12/2011	20/12/2014	Si	Si	InfoCert Firma Qualificata			NON PRESENTE	No	

1 / 1 136% Collabora Firma Trova

Amministrazione demo

Novità!

Da precedente con allegati



La funzione di riproposizione di un protocollo è stata arricchita con la possibilità di riproposizione, oltre che dei dati anche degli allegati.

Protocollo con dati e allegati

Nella scheda profilo del protocollo

The screenshot displays the FOLium web interface for managing protocols. At the top, the user is identified as Daniele Rosa, working in the 'Ufficio 1 (+)' of the 'Area organizzativa: AG01 (TEST)'. The current document is 'REGISTRO UFFICIALE' with the state 'Ingresso' dated 07/08/2015. The interface includes a navigation menu with options like 'Protocollo', 'Ricerca', 'Assegnazioni', 'Registri', 'Rubriche', 'Posta', 'Fascicoli', and 'Utenti'. The main content area shows the details of a protocol with the title 'REGISTRO UFFICIALE: PROTOCOLLO in Ingresso, N.1652, data: 07/08/2015 - oggetto: Invio moduli'. The document name is 'Documento Generico' and the subject is 'Invio moduli'. Below this, there is a table for 'Mittenti' with columns for 'Nominalista', 'Indirizzo', 'Mezzo sped.', 'P.C.', and 'Spedizione'. The 'Uffici Destinatari Competenti' section is empty. At the bottom, there are fields for 'Data documento', 'Data ricezione', and 'Data scadenza', all set to 07/08/2015. The 'Protocollo mittente' and 'Firmatario' fields are also present. A red box highlights the button 'Nuovo con questi dati e allegati' in the bottom navigation bar.

foium

Utente: Daniele Rosa
Ufficio: Ufficio 1 (+)
Ruolo: operatore (+)

Area organizzativa: AG01 (TEST)
Registro: REGISTRO UFFICIALE
Stato: Ingresso - 07/08/2015

Versione: 4.12.0
Aiuto Home Uscita

Protocollo Ricerca Assegnazioni Registri Rubriche Posta Fascicoli Utenti

Precedente Successivo

REGISTRO UFFICIALE: PROTOCOLLO in Ingresso, N.1652, data: 07/08/2015 - oggetto: Invio moduli

Protocollo Classificazione Collegati Info Documento (1 pag.) Allegati (2) Conservazione

Nome Documento Esito: Documento Generico

Oggetto: Invio moduli

Mittenti

Nominalista	Indirizzo	Mezzo sped.	P.C.	Spedizione
Rosa,Matteo	-		No	

Uffici Destinatari Competenti:

Data documento: 07/08/2015 Data ricezione: 07/08/2015 Data scadenza: 07/08/2015

Protocollo mittente: Firmatario:

Nuovo protocollo Nuovo con questi dati Nuovo con questi dati e allegati Salva Assegna Fascicola Annulla Documento Rispondi

Selezione massiva assegnazioni

Novità!

E' stata introdotta la possibilità per l'utente di selezionare massivamente tutte le assegnazioni. La selezione ha effetto solo sulle assegnazioni presenti nella pagina visualizzata.

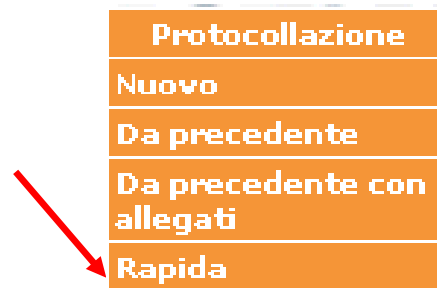
1 | 2

1 - 50 | totale: 82

Successivi

<input checked="" type="checkbox"/>	Registro	Nam.	Mod.	Oggetto	Mitt/Dest	Assegnante	Assegnatario	Data assegnazione	Tipo	Note	Pri.	Operazioni
<input checked="" type="checkbox"/>	REGISTRO UFFICIALE	1626	I	Telecom Italia S.p.A. - Fattura n. 8300172240 di data 05/05/2015	Telecom Italia S.p.A.	Elettronica Fatturazione - Ufficio 1	Ufficio 1	04/08/2015	Competenza		!	
<input checked="" type="checkbox"/>	REGISTRO UFFICIALE	1625	I	Telecom Italia S.p.A. - Fattura n. 8300171232 di data 05/05/2015	Telecom Italia S.p.A.	Elettronica Fatturazione - Ufficio 1	Ufficio 1	03/08/2015	Competenza		!	
<input checked="" type="checkbox"/>	REGISTRO UFFICIALE	1624	I	Benetton Spa - Fattura n. 123 di data 18/12/2014	Benetton Spa	Elettronica Fatturazione - Ufficio 1	Ufficio 1	03/08/2015	Competenza		!	
<input checked="" type="checkbox"/>	REGISTRO UFFICIALE	1623	I	Foo - Fattura n. 241123 di data 24/07/2015	Foo	Elettronica Fatturazione - Ufficio 1	Ufficio 1	02/08/2015	Competenza		!	
<input checked="" type="checkbox"/>	REGISTRO UFFICIALE	1622	I	Foo - Fattura n. 241115 di data 18/12/2014	Foo	Elettronica Fatturazione - Ufficio 1	Ufficio 1	03/08/2015	Competenza		!	
<input checked="" type="checkbox"/>	REGISTRO UFFICIALE	1621	I	Fabrizi Spa - Fattura n. 123 di data 18/12/2014	Fabrizi Spa	Elettronica Fatturazione - Ufficio 1	Ufficio 1	03/08/2015	Competenza		!	

Protocollazione rapida



Pei protocollatori in ingresso può essere utile usufruire di questa modalità che consente di eseguire una protocollazione in modo veloce e con i dati essenziali.

Maschera di Protocollazione rapida



Utente: Serena Bellaqotti
Ufficio: [SEGRETARIO / DIRETTORE GENERALE \(+\)](#)
Ruolo: [controllo centrale \(+\)](#)

Area organizzativa: [A00PGRO \(c qri\)](#)
Registro: [REGISTRO UFFICIALE](#)
Stato: [Ingresso - 27/08/2015](#)





Versione: 4.
[Aiuto](#) [Home](#) [...](#)

Protocollazione InterPRO







Cerca Assegnazioni Registri Rubriche Posta Fascicoli Utente Reports

Codice Oggetto:

Oggetto:

Acquisisci una immagine digitale per questo documento    

Mittenti (E' necessario inserire almeno un mittente)

Descrizione: Mezzo sped.:

Denominazione	Indirizzo	Mezzo sped.
<input type="text"/>		

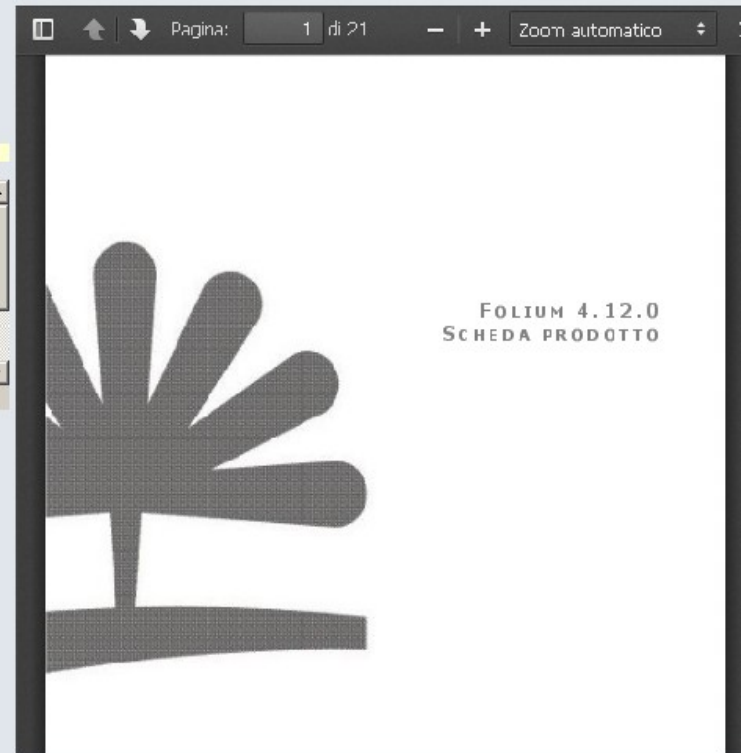
Classificazione:

Voci del titolare trovate:
01 Atti fondamentali e Organi
02 Organizzazione generale e
03 R. sorse informative
04 Personale

Classificazione del documento:

Data Documento: (gg/mm/aaaa) Protocollo mittente:

: campi con questo colore sono obbligatori.



Protocollo in ingresso da PEC

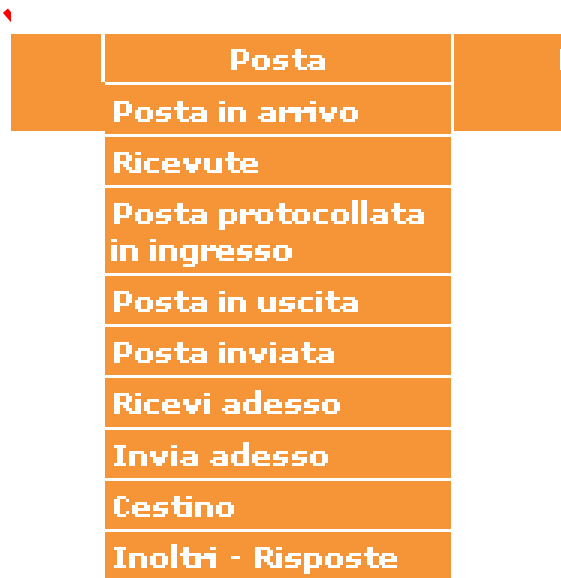


In caso di Multi-pec


! Qualora sia necessario configurare in Folium più di una casella di posta elettronica certificata, accertarsi che sia stato installato il modulo MULTIPPEC all'interno del proprio ambiente. In caso di dubbi contattare il Vs referente Dedagroup.

Protocollo ingresso PEC

Gli utenti abilitati alla protocollazione da PEC hanno visibilità sul menù “Posta” da cui possono analizzare l’elenco dei messaggi di posta elettronica in arrivo.



Si precisa che le caselle di posta che l’operatore potrà tenere sotto controllo potranno essere:

-  La casella PEC istituzionale dell’ente
-  Una o più delle altre caselle di PEC che l’ente può gestire

Protocollo ingresso PEC

Cliccando sul sottomenù *Posta*, *Posta in arrivo*, l'operatore di protocollo potrà scegliere la casella di posta da cui poi ottenere l'elenco dei messaggi ricevuti.



Protocollazione InterPRO	Ricerca	Assegnazioni	Registri	Rubriche	Posta
-----------------------------	---------	--------------	----------	----------	-------

Posta in arrivo
Selezionare dalla lista una casella di posta elettronica (Ingresso o Uscita), quindi cliccare sul tasto 'Cerca'. Verrà mostrato un elenco delle e-mail da protocollare.

<input checked="" type="radio"/> Caselle:	provincia.grosseto@postacert.toscana.it (messaggi da protocollare in ingresso)	Cerca
<input type="radio"/> Cartelle:	provincia.grosseto@postacert.toscana.it (messaggi da protocollare in ingresso)	
	protocollo@provincia.grosseto.it (messaggi da protocollare in uscita)	
	sviluppo.provinciagr@postacert.toscana.it (messaggi da protocollare in ingresso)	

Protocollo ingresso PEC

Ecco un esempio di elenco delle e-mail ricevute.
Ogni riga dell'elenco corrisponde ad una e-mail ricevuta.

Queste e-mail provengono da PEC.

Queste e-mail contengono almeno una firma digitale.

Protocollo Visualizza Verifica firma Seleziona Tutti Deseleziona Tutti Cestina Allega

vai alla pagina di 2 Vai

Successivi 3

	Mittente	Destinatario	Oggetto	Data	Firma	Tipo	Errore interoperabile
<input type="checkbox"/>	Per conto di: apaci@postacert.toscana.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Portale Ap@ci - Comunicazione modifica Mail	30/11/2012 18:15			
<input type="checkbox"/>	Per conto di: marco.serafino@dedagroup.it	alessandro.festuccia@pec-mail.it;	ANOMALIA MESSAGGIO: test allegato con accenti	29/11/2012 18:03			
<input type="checkbox"/>	Per conto di: alessandro.festuccia@ingpec.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Conferma Ricezione	28/11/2012 12:41			
<input type="checkbox"/>	Per conto di: apaci@postacert.toscana.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Portale Ap@ci - Comunicazione conferma Registrazione	27/11/2012 16:58			
<input type="checkbox"/>	Per conto di: alessandro.festuccia@pec-mail.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Ricevuta protocollo	26/11/2012 12:07			
<input type="checkbox"/>	Per conto di: a.derenzo@agora.it	alessandro.festuccia@pec-mail.it;	ANOMALIA MESSAGGIO: Fwd: I: files allegato protocollazione in errore	26/11/2012 10:41			
<input type="checkbox"/>	Per conto di: a.derenzo@agora.it	alessandro.festuccia@pec-mail.it;	ANOMALIA MESSAGGIO: Fwd: I: files allegato protocollazione in errore	26/11/2012 10:41			
<input type="checkbox"/>	Per conto di: alessandro.festuccia@ingpec.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Protocollo nr: 113 - del 26/10/2012 - AOO8 - otta senza segnatura	26/10/2012 12:05			
<input type="checkbox"/>	Per conto di: marco@pec.serafino.name	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: 10	16/10/2012 15:59	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	Per conto di: marco@pec.serafino.name	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: 9	16/10/2012 15:59	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	Per conto di: marco@pec.serafino.name	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: 8	16/10/2012 15:58	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	Per conto di: marco@pec.serafino.name	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: 7	16/10/2012 15:58	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	Per conto di: marco@pec.serafino.name	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: 6	16/10/2012 15:58	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	Per conto di: marco@pec.serafino.name	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: I: dalla mail pec de serafino 5	16/10/2012 15:57	<input checked="" type="checkbox"/>		

Protocollo ingresso PEC

Visualizzare il contenuto dell'e-mail ricevuta: si seleziona l'e-mail desiderata e si preme il pulsante "Visualizza".

Caselle: massimo.gambino@cert.legalmail.it (messaggi da protocollare in ingresso) ▼
 Cartelle: casella1 ▼

Cerca

Protocolla **Visualizza** Verifica firma Seleziona Tutti Deseleziona Tutti Elimina Allega

vai alla pagina _____ di 2 Vai

		Mittente	Destinatario	Oggetto
<input type="checkbox"/>		Per conto di: apaci@postacert.toscana.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Portale di Registrazione
<input type="checkbox"/>		Per conto di: a.derenzo@agora.it	alessandro.festuccia@pec-mail.it;	ANOMALIA MESSAGGIO: Fwd: I errore
<input type="checkbox"/>		Per conto di: alejandro.festuccia@pec-mail.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Ricevuta
<input type="checkbox"/>		Per conto di: alejandro.festuccia@pec-mail.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Ricevuta
<input type="checkbox"/>		Per conto di: alejandro.festuccia@pec-mail.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Protocollo TEST_AOO_MG - TEST AREA OI
<input type="checkbox"/>		Per conto di: alejandro.festuccia@pec-mail.it	alessandro.festuccia@pec-mail.it;	POSTA CERTIFICATA: Ricevuta
<input type="checkbox"/>		Per conto di: mailer-daemon@vlefpecsmtp004.dmz.infocert.it	alessandro.festuccia@pec-mail.it;	ANOMALIA MESSAGGIO: Return details
<input checked="" type="checkbox"/>		Per conto di: comunedilodi@legalmail.it	provincia.lodi@pec.regione.lombardia.it;	POSTA CERTIFICATA: (Rif: 06- PUBBLICAZIONE ALL'ALBO PRE DECORRERE DAL 08/06/2012 (DELLA CONCESSIONE LO 0142: DAMIANO IN

Protocollo ingresso PEC

Visualizzare il contenuto dell'e-mail ricevuta: il sistema mostra il contenuto della e-mail:



Utente: MASSIMO GAMBINO
Ufficio: [UFFICIO 50_01](#)
Ruolo: [operatore](#)

[Protocollo](#) [Ricerca](#) [Assegnazioni](#) [Registri](#)

[Torna all'elenco](#)

Data: 27/06/2012 09:13
Mittente: Per conto di: comunedilodi@legalmail.it
Destinatario: provincia.lodi@pec.regione.lombardia.it
Oggetto: POSTA CERTIFICATA: (Rif: 06-2012/0022592) RELATA PUBBLIC RICHIEDENTE LUCCHINI DAMIANO IN

RELATA PUBBLICAZIONE ALL'ALBO PRETORIO ON LINE PER GIORNI 15 A DECORRERE DAL 08/06/2012 DELLA DOMANDA DI RINNOVO DELLA CONCESSIONE LO 014251995 RICHIEDENTE LUCCHINI DAMIANO IN

N. Allegati

- | | |
|---|---|
| 1 | Corpo Messaggio.txt |
| 2 | messaggio-originale.eml |
| 3 | Segnatura.xml |
| 4 | relata concessione lo 014251995.pdf.p7m |

Sono visibili:

la data di ricezione, il mittente, il destinatario e l'oggetto; segue il contenuto del messaggio e, ancora sotto, tutti gli allegati.

Si osserva la presenza del file "**segnatura.xml**" che ci indica la **presenza di un protocollo interoperabile**: il file segnatura.xml è stato trasmesso a cura del protocollo mittente e, secondo quanto previsto dalla circolare AIPA 28/2001, agevolerà il lavoro del protocollatore in quanto tutti i **metadati del protocollo mittente** sono stati trasmessi al protocollo ricevente.

Di norma tutti gli allegati possono essere consultati in questa fase.

Non il file .p7m che verrà reso visibile solo nella successiva fase di protocollazione.

Focus su Segnatura .xml



Utente: MASSIMO GAMBINO

Ufficio: UFFICIO 50_01

Ruolo: operatore

Protocollo

Ricerca

Assegnazioni

Registri

Torna all'elenco

Data: 27/06/2012 09:13
Mittente: Per conto di: comunedilodi@legalmail.it
Destinatario: provincia.lodi@pec.regione.lombardia.it
Oggetto: POSTA CERTIFICATA: (Rif: 06-2012/0022592) RELATA PUBBLIC RICHIEDENTE LUCCHINI DAMIANO IN

RELATA PUBBLICAZIONE ALL'ALBO PRETORIO ON LINE PER GIORNI 15 A DECORRERE DAL 08/06/2012 DELLA DOMANDA DI RINNOVO DELLA CONCESSIONE LO 014251995 RICHIEDENTE LUCCHINI DAMIANO IN

N.	Allegati
1	Corpo Messaggio txt
2	messaggio-originale.eml
3	Segnatura.xml
4	relata concessione lo 014251995.pdf.p7m

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <Segnatura versione="2001-05-07" xml:lang="it">
- <Intestazione>
- <Identificatore>
  <CodiceAmministrazione>c_e648</CodiceAmministrazione>
  <CodiceAOO>c_lo</CodiceAOO>
  <NumeroRegistrazione>0022592</NumeroRegistrazione>
  <DataRegistrazione>2012-06-27</DataRegistrazione>
</Identificatore>
- <Origine>
  <IndirizzoTelematico tipo="smtp">comunedilodi@legalmail.it</IndirizzoTelematico>
- <Mittente>
- <Amministrazione>
  <Denominazione>COMUNE DI LODI</Denominazione>
  <CodiceAmministrazione>c_e648</CodiceAmministrazione>
- <IndirizzoPostale>
  <Denominazione>Piazza Broletto 1 26900 LODI (LO)</Denominazione>
  </IndirizzoPostale>
  <IndirizzoTelematico tipo="smtp">n.a.</IndirizzoTelematico>
  <Telefono>03714091</Telefono>
  <Fax>0371409448</Fax>
  </Amministrazione>
- <AOO>
```

Segnatura.xml è di norma visibile nel browser e contiene i dati del prot mittente!

Verifica firma digitale

Verificare la presenza della firma digitale (se presente)

Posta in arrivo

Selezionare dalla lista una casella di posta elettronica (Ingresso o Uscita), quindi cliccare sul tasto 'Cerca'. Verrà mostrato un elenco delle e-mail da protocollare.

Caselle: provincia.grosseto@postacert.toscana.it (messaggi da protocollare in ingresso) Cartelle: PEC ENTE

Protocolla

Visualizza

Verifica firma



Allega

Inoltra

Rispondi A

Seleziona Tutti

Deseleziona Tutti

		Mittente	Destinatario	Oggetto	Data	Firma
<input checked="" type="checkbox"/>		Per conto di: arpat.protocollo@postacert.toscana.it	provincia.grosseto@postacert.toscana.it;	POSTA CERTIFICATA: #FD#ARPAT\2015\58744 \27-08-2015107776	27/08/2015 11:00	

Verifica firma digitale

Verificare la presenza della firma digitale (se presente)



Utente: [Serena Bellagotti](#)
Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [protocollo centrale \(+\)](#)

Area organizzativa: [A00PGRO \(p_gr\)](#)
Registro:

Protocollo InterPRO	Ricerca	Assegnazioni	Registri	Rubriche	Posta	Fascicoli	Utente
------------------------	---------	--------------	----------	----------	-------	-----------	--------

Messaggio da: Per conto di: arpat.protocollo@postacert.toscana.it
Oggetto: POSTA CERTIFICATA: #FD#ARPAT\2015\58744\27-08-2015107776

Informazioni sulla firma del file: pagamento s pomata 2015.pdf.p7m

Firmatario	Valido dal	Sino al	Validità	Legale	CA	Località	E-mail	Org.Unit	Revocato	Info
ANEDDA FABIO	04/01/2013	05/01/2019	Si	Si	ArubaPEC S.p.A. NG CA 3	IT		ARPAT/04686190481	No	

Informazioni sulla firma del file: par fav rinnovo s.pomata 2015.pdf.p7m

Firmatario	Valido dal	Sino al	Validità	Legale	CA	Località	E-mail	Org.Unit	Revocato	Info
ANEDDA FABIO	04/01/2013	05/01/2019	Si	Si	ArubaPEC S.p.A. NG CA 3	IT		ARPAT/04686190481	No	

[Torna all'elenco](#)

➤ Al termine dell'operazione di verifica, click su "Torna all'elenco"

Protocollo ingresso PEC 1

Click su protocolla

Protocolla

Il sistema potrà richiedere di selezionare un Registro ed il verso di protocollazione.



Utente: **Serena Bellagotti**
Ufficio: **SECRETARIO / DIRETTORE GENERALE (+)**
Ruolo: **protocollo centrale (+)**

Area organizzativa: **A00PGRO (p_gr)**
Registro:

Protocollazione InterPRO	Ricerca	Assegnazioni	Registri	Rubriche	Posta	Fascicoli	Utente
-----------------------------	---------	--------------	----------	----------	-------	-----------	--------

Selezione registro e modalità di protocollazione

Registro di CORRISPONDENZA	Descrizione	Data ultima reg.	Ingresso
REGISTRO UFFICIALE	Registro Ufficiale Provincia di Grosseto	27/08/2015	<input type="checkbox"/>

Protocollo ingresso PEC 2

Selezionare il file da acquisire come documento principale per il protocollo; tutti gli altri saranno portati fra allegati.

La presenza di una firma digitale aiuta la selezione!

folium Utente: [Serena Bellagotti](#)
Ufficio: [SEGRETARIO / DIRETTORE GENERALE \(+\)](#)
Ruolo: [protocollo centrale \(+\)](#)

Protocollazione **InterPRO** Ricerca Assegnazioni Registri Rubriche

Protocollazione della posta
Selezionare la parte del messaggio che formerà il contenuto PDF del messaggio protocollato.
Le altre parti saranno inserite come allegati del documento protocollato.
Le parti con formati non convertibili in pdf non sono selezionabili.

Data: 27/08/2015 11:00
Mittente: Per conto di: arpat.protocollo@postacert.toscana.it
Destinatario: provincia.grosseto@postacert.toscana.it
Oggetto: POSTA CERTIFICATA: #FD#ARPAT\2015\58744\27-08-2015107776

Parti del messaggio	
<input type="radio"/>	Corpo Messaggio txt
<input type="radio"/>	Corpo Messaggio html
<input checked="" type="radio"/>	paqamento s pomata 2015.pdf.p7m
<input type="radio"/>	par fav rinnovo s.pomata 2015.pdf.p7m
<input type="radio"/>	segnatura.xml
<input type="radio"/>	Nessun contenuto

Protocolla Torna indietro

**Una volta selezionato, Click su
protocolla**

Protocollo ingresso PEC 3

Protocollo InterPRO

Protocollo Classificazione Collegati Info Documenti Allegati (4)

Codice Oggetto:

Oggetto:

[Non inserire dati sensibili nell'Oggetto]

Mittenti (E' necessario inserire almeno un mittente)

Descrizione: Mezzo sped.:

Denominazione	Indirizzo	Mezzo sped.	P.C.	Comandi
AGENZIA REGIONALE PER LA PROTEZIONE AMBIENTALE DELLA TOSCANA	-	P.C.C.	<input type="checkbox"/>	<input type="button" value="X"/> <input type="button" value="Print"/> <input type="button" value="Menu"/>

Uffici Destinatari Competenti:

Data documento: Data ricezione: Data scadenza:

Protocollo mittente: Firmatario:

I campi con questo colore sono obbligatori. Per muoversi fra i pannelli si può anche usare il tasto FINE

Tutte le informazioni presenti in segnatura entrano automaticamente nell'attuale protocollo.

Osservazione

Articolo 53 DPR 445/2000

1. La Registrazione di Protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni:

- a) **numero di protocollo** del documento (generato automaticamente dal sistema e registrato in forma non modificabile);
- b) **data di registrazione** di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c) **mittente** per i documenti ricevuti o, in alternativa, il **destinatario o i destinatari** per i documenti spediti, registrati in forma non modificabile;
- d) **oggetto del documento**, registrato in forma non modificabile;
- e) data e protocollo del documento ricevuto, se disponibili;
- f) 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.

Osservazione

- Cliccando sul pulsante “**Protocolla**” otteniamo numero e data di prot.
- Classificazione, eventuale scansione e/o caricamento del documento e degli allegati potranno anche essere effettuati in un secondo momento, ma non è prassi consigliata!

E' buona norma effettuare queste operazioni prima della protocollazione.
E' cmq obbligo allegare il documento e gli allegati entro la mezzanotte del giorno di registrazione del protocollo.



! Nel caso di invio mezzo PEC, cliccando sul pulsante “protocolla” viene contestualmente inviata la posta con il relativo documento e allegati.

Osservazione

Una volta cliccato sul pulsante **Protocolla**, Numero e data, forniti dal sistema senza alcuna interferenza da parte dell'utente, compaiono in una stringa di testo nella parte superiore della pagina:

The screenshot shows the FOLIUM system interface. At the top left is the 'folium' logo. To its right, user information is displayed: 'Utente: Massimo Gambino', 'Ufficio: ufficio per test (Aoo-Test)', and 'Ruolo: operatore (+)'. Further right, organizational details are shown: 'Area organizzativa: Aoo-Test (TEST)', 'Registro: REGISTRO UFFICIALE', and 'Stato: Ingresso - 17/12/2012'. Below this is a navigation bar with buttons for 'Protocollo', 'Ricerca', 'Assegnazioni', 'Registri', 'Rubriche', 'Posta', 'Fascicoli', 'Utente', and 'Re'. A link for 'Precedente' is visible. The main content area displays the document title: 'REGISTRO UFFICIALE: PROTOCOLLO in Ingresso, N.69, data: 17/12/2012 - oggetto: TESTO DI UN OGGETTO RIPETITIVO DA RIUTILIZZARI'. Below the title is a table with columns: 'Protocollo', 'Classificazione', 'Collegati', and 'Info'. The 'Classificazione' column contains the text 'Documento Generico'. Below the table, the 'Nome Documento Esteso:' field is filled with 'Documento Generico'. The 'Oggetto:' field contains the text 'TESTO DI UN OGGETTO RIPETITIVO DA RIUTILIZZARE A CURA DEI PROTOCOLLATORI'. At the bottom, the 'Mittenti' section contains a table with columns: 'Nominativo', 'Indirizzo', 'Mezzo sped.', 'P.C.', and a small icon column. The data row shows: 'Provincia di Grosseto', 'Piazza Dante Alighieri, 35 Grosseto _', 'Raccomandata A/R', 'No', and a small icon.

Protocollo	Classificazione	Collegati	Info
	Documento Generico		

Nominativo	Indirizzo	Mezzo sped.	P.C.	
Provincia di Grosseto	Piazza Dante Alighieri, 35 Grosseto _	Raccomandata A/R	No	

Oggetto e mittente compaiono, in modalità immodificabile, negli spazi previsti.

Registro giornaliero di protocollo



Utente: **Utente Amministratore**
Ufficio: **SUAP**
Ruolo: **amministratore di aoo (+)**

Area organizzat
Registro:

Organizzazione **Registri** **Titolario** **Documentale** **Rubriche** **Reports**

Modifica il registro: **registro ufficiale**

Codice:	REGISTRO UFFICIALE
Descrizione:	Registro Ufficiale AOO AOO_DG 512
Apertura/chiusura automatica:	SI ▼
Stampa giornaliera registro:	Orizzontale ▼
Tipo:	Ufficiale
Email invio registro	mario.rossi@comune.genova.it
Ultimo Progressivo:	21

Salva Annulla

Utenti dell'area organizzativa: AOO_DG

Abilitazione / disabilitazione alla protocollazione su questo registro

Abilitato	Cognome	Nome	UserID	Responsabile registro	Email
<input checked="" type="checkbox"/>	Abbadelli	Antonio	utente5a	<input checked="" type="checkbox"/>	nomail@nomail.com



Poteva e può essere inviato ad un indirizzo email (solitamente quello del RSP)

La stampa giornaliera del registro, inviata solo alla mail di cui sopra, viene ora salvata in Folium.

Registro giornaliero di protocollo

Le stampe giornaliere sono visibili solo al ruolo **Amministratore di AOO** abilitato nella nuova sezione **Registri → Stampe giornaliere**, filtrate per registro e per data (per default viene proposto l'ultimo mese)

Elenco stampe registri

Stampe dal  (gg/mm/aaaa) al  (gg/mm/aaaa)

Registro:

- REGISTRO UFFICIALE
- REG2
- A001INT

Registro giornaliero di protocollo

Modifica il registro: registro ufficiale

Codice:	REGISTRO UFFICIALE
Descrizione:	Registro Ufficiale AOO1 512
Apertura/chiusura automatica:	SI
Stampa giornaliera registro:	Verticale
Tipo:	Ufficiale
Email invio registro	responsabileregistro@ente.it
Ultimo Progressivo:	1790

Salva Annulla

Utenti dell'area organizzativa: AOO1

Abilitazione/disabilitazione alla protocollazione su questo registro

Abilitato	Cognome	Nome	UserID	Responsabile registro	Visualizza stampa	Email	CodiceFiscale	Matricola
<input type="checkbox"/>	Bianchi	Luca	utentegd	<input type="checkbox"/>		nomail@nomail.com		
<input type="checkbox"/>	Canali	Roberto	utente22c	<input type="checkbox"/>		nomail@nomail.com		
<input checked="" type="checkbox"/>	Carlini	Fabio	utente2b	<input type="checkbox"/>		nomail@nomail.com		
<input type="checkbox"/>	Dandini	Vittorio	utente2d	<input type="checkbox"/>		nomail@nomail.com		
	Della Seta	Giorgio	utente22b		<input checked="" type="checkbox"/>	nomail@nomail.com		
<input checked="" type="checkbox"/>	Elettronica	Fatturazione	ESB	<input type="checkbox"/>		nomail@nomail.com		
<input type="checkbox"/>	Felicetti	Mauro	utente11c	<input type="checkbox"/>		nomail@nomail.com		
<input checked="" type="checkbox"/>	Galanti	Fabrizio	utente1d	<input type="checkbox"/>		nomail@nomail.com		
<input checked="" type="checkbox"/>	Gambino	Massimo	gambino	<input checked="" type="checkbox"/>	<input type="checkbox"/>	nomail@nomail.com		
<input checked="" type="checkbox"/>	Giambanco	Francesco	ufo	<input type="checkbox"/>		nomail@nomail.com		
<input type="checkbox"/>	Gigli	Anna	utente11d	<input type="checkbox"/>		nomail@nomail.com		
<input type="checkbox"/>	Giuliani	Esposito	utesesc	<input type="checkbox"/>		nomail@nomail.com		
<input checked="" type="checkbox"/>	Lamberti	Ester	utente11b	<input type="checkbox"/>		nomail@nomail.com		
<input checked="" type="checkbox"/>	Marillo	Francesca	utentegdgc	<input type="checkbox"/>		nomail@nomail.com		
<input checked="" type="checkbox"/>	Ragusi	Sonia	utente11a	<input type="checkbox"/>		nomail@nomail.com		
<input checked="" type="checkbox"/>	Rosa	Daniele	utente1a	<input type="checkbox"/>	<input checked="" type="checkbox"/>	nomail@nomail.com		
<input checked="" type="checkbox"/>	Simoncelli	Ugo	utente2a	<input type="checkbox"/>		nomail@nomail.com		
	Stella	Elena	utente2c		<input type="checkbox"/>	nomail@nomail.com		



Registro giornaliero di protocollo

Ai fini normativi non occorre firmare il Rgp, ma se qualche amministrazione decidesse di farlo, si deve attivare una configurazione specifica in Folium che aprirà la funzione di firma nel Pannello Registri → Stampe giornaliere










folium Utente: Daniele Rosa Area organizzativa: A001 (TEST) Versione: 4.13.0
Ufficio: Direzione Generale Affari Generali (+) Registro: REGISTRO UFFICIALE Aiuto Home Uscita
Ruolo: amministratore di aoo (+) Stato:

Organizzazione Registri Titolare Documentale Rubriche Eventi Applicazione Comunicazioni Conservazione

Elenco stampe registri

Stampe dal 16/09/2015 al 23/09/2015
Registro: REGISTRO UFFICIALE
Cerca

1 - 4 | totale: 4

Data Stampa	Nome Documento	Nome Documento Firmato	Data Firma	Stato conservazione	Data richiesta	Data invio	Data archiviazione	Data conservazione	Responsabile conservazione	ID Documento	Pacchetto di archiviazione	Note	Operazioni
22/09/2015	AOO1_REGISTRO UFFICIALE-20150922-20150923103714.pdf			Esportato Correttamente	23/09/2015	23/09/2015							  
21/09/2015	AOO1_REGISTRO UFFICIALE-20150921-20150922162421.pdf	1441915011675AOO1_REGISTRO UFFICIALE-20150916-20150919013016.pdf.p7m	22/09/2015	Conservato Correttamente	22/09/2015	22/09/2015	22/09/2015	22/09/2015	enerj	3	3		 
17/09/2015	AOO1_REGISTRO UFFICIALE-20150917-20150918143436.pdf	1441841416293AOO1_REGISTRO UFFICIALE-20150909-20150918013016.pdf	18/09/2015	Conservato Correttamente	18/09/2015	18/09/2015	18/09/2015	18/09/2015	enerj	2	2		 
16/09/2015	AOO1_REGISTRO UFFICIALE-20150916-20150917115037.pdf	1441755016871AOO1_REGISTRO UFFICIALE-20150916-20150917013016.pdf.p7m	17/09/2015	Conservato Correttamente	17/09/2015	17/09/2015	17/09/2015	17/09/2015	enerj	1	1		 

Le funzioni disponibili per ciascuna stampa sono le seguenti:



Download documento: consente di scaricare la stampa corrispondente

Firma P7M: consente di apporre la firma p7m

Firma PDF: consente di apporre la firma pdf

Download documento firmato: consente di scaricare la corrispondente stampa firmata

Fascicolazione





Elettronica

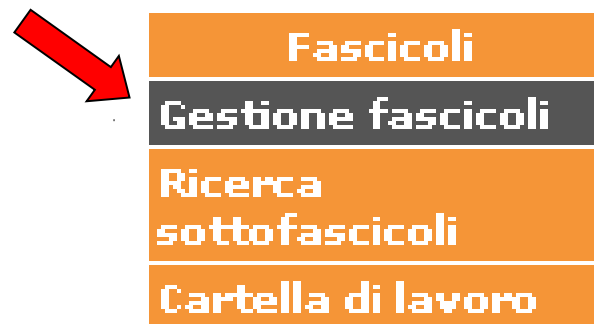


Cartacea



Fascicolazione

La gestione dei fascicoli (consultazione, creazione, etc) si esegue con il ruolo di **Utente** il quale consente di accedere al menù “Fascicoli”



Cosa è il fascicolo

- È l'insieme dei documenti che possono afferire al medesimo **procedimento amministrativo**, o che riguardano uno **stesso affare**, o che appartengono a una **medesima tipologia**.
- Costituisce l'unità di base, fondamentale per la gestione e la conservazione della documentazione relativa a ciascun procedimento o affare.
- Ciascun **fascicolo** è individuato almeno da:
 - *anno di istruzione*
 - *oggetto*
 - *codice di classificazione*

Perché fascicolare?

- Per *fascicolazione* si intende l'attività di riconduzione logica e fisica di un documento all'interno dell'unità dell'archivio che ne raccoglie i precedenti.
- Il fascicolo permette di relazionare tutta la documentazione relativa ad un affare, identificarne i tempi ed i responsabili.
- Il fascicolo permette di **tracciare l'azione amministrativa** durante la trattazione dell'affare e dopo la conclusione di esso.

Normativa di riferimento



CAD - Art. 41 (aggiornato dal D.L. 235/2010)

1. Le PA gestiscono i procedimenti amm.vi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente.

1-bis. La gestione dei procedimenti amm.vi è attuata in modo da consentire, mediante strumenti automatici, il rispetto di quanto previsto all' articolo 54 , commi 2-ter e 2-quater.

2. La **Pubblica amministrazione** titolare del procedimento **raccoglie in un "fascicolo informatico" gli atti, i documenti e i dati del procedimento** medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della L.7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata L.7 agosto 1990, n. 241.

Normativa di riferimento



2-bis. Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento.

Le regole per la costituzione, l'identificazione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico ed il sistema pubblico di connettività, e comunque **rispettano i criteri dell'interoperabilità e della cooperazione applicativa**; regole tecniche specifiche possono essere dettate ai sensi dell' articolo 71, di concerto con il Ministro della funzione pubblica.

Normativa di riferimento



2-ter. Il fascicolo informatico reca l'indicazione:

- a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- b) delle altre amministrazioni partecipanti;
- c) del responsabile del procedimento;
- d) dell'oggetto del procedimento;
- e) dell'elenco dei doc. contenuti, salvo quanto disposto dal comma 2-quater;
- e-bis) dell'identificativo del fascicolo medesimo.

2-quater. Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata L. 241/1990.

Normativa di riferimento

DPR 445/2000 - Art. 67 (doc. cartacei)



Trasferimento dei documenti all'archivio di deposito

1. Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a **trasferire fascicoli** e serie documentarie relativi a procedimenti conclusi **in un apposito archivio di deposito** costituito presso ciascuna amministrazione.
2. Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.
3. Il responsabile del servizio per la gestione dei flussi documentali e degli archivi deve formare e conservare un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito.

Normativa di riferimento



Art. 5 (al punto h) DPCM 3 del 3 dicembre 2013

Stabilisce che il *Manuale di gestione del protocollo* deve contenere le modalità di formazione, implementazione e gestione dei fascicoli informatici relativi ai procedimenti e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;

Titolario e classificazione dei documenti



Titolario e classificazione dei doc. in una USL

Il **Titolario** è uno schema ad albero diviso per "**categorie**" o "**titoli**" numerati, che corrispondono ciascuno alle varie **funzioni svolte dall'ente**.

A loro volta i "**titoli**" sono suddivisi ciascuno in "**classi**" o "**sezioni**", che corrispondono alle varie **tipologie di documenti per ciascuna funzione**.

Il titolo/categoria
08.00.00
corrisponde alla
funzione Risorse
umane.

08	08	00	Valutazione	1
08	08	01	Dirigenti	1
08	08	02	Personale del comparto	1
08	09	00	Procedimenti disciplinari	1
08	10	00	Adempimenti contributivi, assicurativi e fiscali	1
08	11	00	Quiescenza e cessazioni	1
08	12	00	Inabilità al lavoro, invalidità, infermità, equo indennizzo	1
08	13	00	Tutela della salute e sorveglianza sanitaria	1
08	14	00	Formazione e aggiornamento del personale	1
08	15	00	Deontologia professionale ed etica del lavoro	1
08	16	00	Libera professione intra moenia	1
08	16	01	Libera professione individuale	1
08	16	02	Libera professione d'équipe	1
08	16	03	Libera professione d'azienda	1
08	16	04	Libera professione allargata	1
08	16	05	Libera professione in convenzione	1
08	16	06	Vendita di prestazioni, consulti e consulenze	1
08	16	07	Acquisizione di prestazioni, consulti e consulenze	1

Categoria/Titolo

Classi/Sezioni

Titolario e classificazione dei documenti

- E' uno strumento dell'archivio corrente, che serve per dividere e catalogare la documentazione (prodotta o ricevuta da un soggetto) in settori e categorie, schematizzando in maniera logica le sue competenze e funzioni.
- E' uno strumento indice ad n. livelli che **describe** complessivamente tutte **le funzioni dell'ente**.
Non deve essere confuso con l'organigramma che describe invece la struttura organizzativa e le gerarchie.
- Ogni procedimento, ogni pratica, ogni fascicolo e quindi **ogni documento amministrativo dell'ente dovrebbe essere sempre classificato e cioè associato ad una delle "foglie" del titolario**.

Dove si trova il Titolare in Folium

Ruolo: Amministratore di AOO

Menù: Titolare



Utente: **Serena Bellagotti**
Ufficio: [Aoo \(+\)](#)
Ruolo: [amministratore di aoo \(+\)](#)

Area organizzativa: **AOO_serena** (TEST)

Registro:

Organizzazione	Registri	Titolario	Documentale	Rubriche	Eventi	Applicazione	Comunicazioni
Titolario		Modifica					
		Caricamento da Excel					

[Inserisci](#) [Modifica](#) [Elimina](#) [Stampa](#) [Stampa Repertori](#) [Export](#)

I nodi titolari contrassegnati dal simbolo * non hanno una Lista di Competenza associata

Visualizza voci storicizzate:

 [Titolario](#)

Classificazione di un documento in Folium

- Il documento è classificato se nel riquadro “*Classificazione del documento*” compare **almeno una voce descrittiva**.



folium Utente: Serena Bellagotti Are
Ufficio: SEGRETARIO/ DIRETTORE GENERALE (+) Re
Ruolo: operatore_standard (+) Sta

Protocollazione Ricerca Assegnazioni Registri Rubriche Fa

Protocollo **Classificazione** Collegati

Ricerca le voci del titolare per: _____

Codice: Descrizione:

Voci del titolare trovate:

- 01.01 Legislazione, circolari
- 01.02 Affari generali
- 01.03 Stemma, gonfalone, sigilli, logo
- 01.04 Statuto
- 01.05 Regolamenti

Classificazione del documento:

- 01.01 Legislazione, circolari

Tipo documento:

Classificazione documento in Folium

Protocollazione Ricerca Assegnazioni Registri Rubriche

Protocollo **Classificazione** Collegati

Ricerca le voci del titolare per:

Codice: 04. Descrizione:

Voci del titolare trovate:

- 04.01 Entrate
- 04.02 Uscite
- 04.03 Partecipazioni finanziarie
- 04.04 Bilancio preventivo, variazioni di bilancio verifiche contabili
- 04.05 Piano esecutivo di gestione (PEG)

Dal pulsante **“Seleziona titolare”** si apre la finestra popup che può essere sfogliata nodo per nodo. Individuato quello voluto basta cliccarci sopra per ottenere la classificazione del documento.

Classificazione d

folium

Protocollazione

Pr

Ricerca le voci

Codice: 04.

Voci del titolare

- 04.01 Entrate
- 04.02 Uscite
- 04.03 Partec
- 04.04 Bilanci
- 04.05 Piano e

Classificazione

04.05 Piano e

http://172.17.34.37:8080/?id=394&cmd=expand&storicizzate=false&banner=false&selTitolario=true#3 - Windo...

Titolario

I nodi titolari contrassegnati dal simbolo * non hanno una Lista di Competenza associata

Visualizza voci storicizzate:

- Titolario
 - 01 Amministrazione generale
 - 02 Organi di governo, gestione, controllo, consulenza e garanzia *
 - 03 Risorse umane *
 - 04 Risorse finanziarie e patrimoniali *
 - 01 Entrate *
 - 02 Uscite *
 - 03 Partecipazioni finanziarie *
 - 04 Bilancio preventivo, variazioni di bilancio verifiche contabili *
 - 05 Piano esecutivo di gestione (PEG) *
 - 06 Rendiconto della gestione *
 - 07 Adempimenti fiscali *
 - 08 Inventari e rapporti dei beni *

Classificazione documento in Folium

Protocollo Classificazione

Ricerca le voci del titolare per:

Codice: Descrizione:

Voci del titolare trovate:

- 02.18 Organi esecutivi circoscrizionali
- 04.05 Piano esecutivo di gestione (PEG)

Classificazione del documento:

Nel campo “**Descrizione**” è possibile inserire la parola (o parte di parola) che si desidera ricercare nell’intero titolare di classificazione.

Facendo precedere la descrizione da un * (asterisco), il sistema è in grado di effettuare ricerche anche su parole “interne” alla descrizione.

Classificazione documento in Folium

Ove l'operatore conosca preliminarmente la voce di classificazione da utilizzare potrà semplicemente digitarla all'interno del campo codice e premere poi il pulsante "Inserisci titolare da codice".

Protocollo Classificazione

Ricerca le voci del titolare per:

Codice: Descrizione:

Voci del titolare trovate:

04.01	Entrate
04.02	Uscite
04.03	Partecipazioni finanziarie
04.04	Bilancio preventivo, variazioni di bilancio verifiche contabili
04.05	Piano esecutivo di gestione (PEG)

Classificazione del documento:

Classificazione documento in Folium

Per rimuovere una voce di classificazione erroneamente inserita sarà sufficiente selezionarla dal riquadro di “Classificazione del documento” e premere poi il pulsante “Deseleziona”

The screenshot displays the 'Classificazione' tab in the Folium software. At the top, there is a navigation bar with tabs for 'Protocollo' and 'Classificazione'. Below this, a search section titled 'Ricerca le voci del titolare per:' contains a 'Codice:' field with the value '04.05' and a checked checkbox, and a 'Descrizione:' field. A list of 'Voci del titolare trovate:' is shown below, with the following items: '04.01 Entrate', '04.02 Uscite', '04.03 Partecipazioni finanziarie', '04.04 Bilancio preventivo, variazioni di bilancio verifiche contabili', and '04.05 Piano esecutivo di gestione (PEG)'. Below the list are two buttons: a downward arrow and an upward arrow. The 'Classificazione del documento:' section at the bottom shows a table with one row: '04.05 Piano esecutivo di gestione (PEG)'. To the right of this row is a button labeled 'Deseleziona'. A red arrow points from the text 'Deseleziona' in the text above to this button.

ACL – Liste di competenza

Cenni alle liste di competenza

Le Liste di competenza sono **elenchi di Utenti e/o Uffici** a cui sono associati i **permessi** utili per accedere alle Pratiche e ai documenti in esse contenuti.



Utente: **Serena Bellagotti**
Ufficio: **SECRETARIO / DIRETTORE GENERALE (+)**
Ruolo: **amministratore di aoo (+)**

Organizzazione	Registri	Titolario	Documentale	R	
Arete organizzative					
Utenti					
Uffici	tive				
Liste di competenza					
Gestione caselle di posta	a di Grosseto	Email Responsabile	Letture Posta	Stato	Comandi
Gestione cartelle di ricezione			Attivo	<input checked="" type="checkbox"/>	

Folium la soluzione globale per il protocollo, la gestione documentale ed i procedimenti.
© Dedagroup SPA 2001-2015

Le Liste di competenza sono gestite dall'**Amministratore di AOO**.

Liste di competenza - ACL

Le ACL possono essere associate alle voci del Titolario soprattutto per determinare i diritti di accesso alle Pratiche, in base alla classificazione ad esse applicata.

Inoltre l'assegnazione di un documento protocollato può essere guidata (oltre che dall'organigramma) dalla Lista di competenza.

folium Utente: Serena Bellagotti Area organizzat
Ufficio: [SEGRETARIO / DIRETTORE GENERALE \(+\)](#) Registro:
Ruolo: [amministratore di aoo \(+\)](#)

Organizzazione Registri Titolario Documentale Rubriche Repo
Comunicazioni

Liste di competenza (permessi di accesso ai documenti).

Nome: 128
Utente:  
Ufficio:  
Cerca Pulisci

Aggiungi Elimina

Successivi 12

Selezione	Nome	Comandi
<input type="checkbox"/>	ACL_Albo Pretorio	 
<input type="checkbox"/>	ACL_Archivio e Spese postali	 
<input type="checkbox"/>	ACL_Area Ambiente	 
<input type="checkbox"/>	ACL_Area Servizi ai comuni e imprese	 
<input type="checkbox"/>	ACL_Aree protette_forestazione_antincendio	 
<input type="checkbox"/>	ACL_Assessorato Ambiente	 
<input type="checkbox"/>	ACL_Assessorato Governo del territorio ed energie rinnovabili	 
<input type="checkbox"/>	ACL_Assessorato Infrastrutture e Trasporti	 
<input type="checkbox"/>	ACL_Assessorato Politiche Giovanili, PO, Cooperazione Internazionale	 
<input type="checkbox"/>	ACL_Assessorato Politiche del Lavoro, Sociali	 
<input type="checkbox"/>	ACL_Assessorato R.U. e Bilancio	 

Liste di competenza - come è strutturata



Utente: Serena Bellagotti
Ufficio: SEGRETARIO/ DIRETTORE GENERALE (+)
Ruolo: amministratore di aoo (+)

Area organizzativa: AOOPGRO (p_gr)
Registro:



Modifica della lista di competenza: ACL_Consiglio

Nome:

I campi con questo colore sono obbligatori.

Elenco permessi per la lista di competenza:

Attenzione: nel caso in cui venga specificato un ufficio verranno aggiunti anche gli uffici gerarchicamente sovraordinati con il permesso di sola lettura.

Selezione	Nome	Tipo	Permesso	Posizione
<input type="checkbox"/>	PRESIDENTE DEL CONSIGLIO	UFFICIO	Lettura/Scrittura	▼
<input type="checkbox"/>	UP UFFICIO DEL CONSIGLIO PROVINCIALE	UFFICIO	Lettura/Scrittura	▲ ▼
<input type="checkbox"/>	SEGRETARIO/ DIRETTORE GENERALE	UFFICIO	Lettura	▲ ▼
<input type="checkbox"/>	PRESIDENTE	UFFICIO	Lettura	▲ ▼
<input type="checkbox"/>	INTERAREA AFFARI GENERALI E SEGRETERIA GENERALE	UFFICIO	Lettura/Scrittura	▲

Aggiungi un permesso (ACE)

Permesso :

Ufficio o utente :

ole
are

- **Lettura**
- **Scrittura**
- **Cancellazione**

Creazione di un fascicolo

Creazione del Fascicolo

La gestione dei fascicoli (consultazione, creazione, etc) si esegue con il ruolo di **Utente** il quale consente di accedere al menù “Fascicoli”.



Utente: **Serena Bellagotti**

Ufficio: **Direzione Generale Affari Generali (+)**

Ruolo: **utente (+)**

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli
---------	--------------	-----------	-----------	---------	-----------

Quadro riassuntivo

Assegnazioni	Ultimi 30 giorni
<u>Competenza</u>	354
<u>Conoscenza</u>	149
<u>Smistamento</u>	144
<u>Restituite</u>	0

Gestione fascicoli

Ricerca
sottofascicoli

Cartella di lavoro

Da qui è possibile vedere le **assegnazioni in carico**.

Una volta aperto il menù «Fascicoli», cliccare su «Gestione fascicoli»

Creazione Fascicolo



Utente: Serena Bellagotti
Ufficio: SEGRETARIO/ DIRETTORE GENERALE (+)
Ruolo: utente_standard (+)

Area organizzativa: AOOPGRO (p_gr)
Registro: REGISTRO UFFICIALE
Stato: **Ingresso** - 27/08/2015

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
---------	--------------	-----------	-----------	---------	-----------	--------

Ricerca fascicoli

Fascicoli generici

Nome:	<input type="text"/>	258	Descrizione:	<input type="text"/>	512
Responsabile:	<input type="text"/>	128	Stato:	<input type="text"/>	
Data Apertura dal:	<input type="text"/>	(gg/mm/aaaa)	Data Apertura al:	<input type="text"/>	(gg/mm/aaaa)
Data Chiusura dal:	<input type="text"/>	(gg/mm/aaaa)	Data Chiusura al:	<input type="text"/>	(gg/mm/aaaa)
Data Scadenza dal:	<input type="text"/>	(gg/mm/aaaa)	Data Scadenza al:	<input type="text"/>	(gg/mm/aaaa)
Codice titolare:	<input type="text"/>	20			
Anno:	<input type="text"/>	N° repertorio da:	<input type="text"/>	a:	<input type="text"/>
PIVA/Codice fiscale:	<input type="text"/>	512	<input type="checkbox"/>	Ricerca nel sottoalbero	
N° fascicolo :	<input type="text"/>	12	<input type="checkbox"/>	solo fascicoli di questo ufficio	
Collocazione:	<input type="text"/>	128	Liste di Competenza:	<input type="text"/>	

Stampa:

Cerca Nuovo fascicolo Caricamento da Excel



Da questa maschera si possono **eseguire ricerche** (all'interno dei fascicoli) oppure **creare nuovi fascicoli**.

Creare nuovo fascicolo

Menù Fascicoli, Gestione fascicoli, Nuovo fascicolo

Selezionare la voce di titolare desiderata (la lista di competenza se configurata compare automaticamente) e cliccare su **Continua ...**

Classifica

Scegli la classificazione

Ricerca per

Codice: 01.01 Descrizione:

Voci del titolare trovate:

- 01.01 Legislazione, circolari
- 01.02 Affari generali
- 01.03 Stemma, gonfalone, sigilli, logo
- 01.04 Statuto
- 01.05 Regolamenti

Classificazione del fascicolo:

- 01.01 Legislazione, circolari

Lista di Competenza Classificazione:

- ACL_Ente

Annulla Continua

Principali caratteristiche del fascicolo in Folium

Un fascicolo si identifica per:

- **Numerazione** (ogni fascicolo ha un numero progressivo che lo identifica)
- **Nome** (campo obbligatorio)
- **Descrizione** (campo obbligatorio)
- Responsabile
- Voce di titolare associata
- **Data apertura** (campo obbligatorio)
- Data chiusura
- Responsabile (facoltativo)
- Richiedente (facoltativo)
- **Stato** (aperto, chiuso)
- etc

Creare fascicolo

Compilare la maschera (almeno con nome, descrizione, responsabile) e cliccare su **Continua...**

Modulo

Passo 2: Inserimento campi liberi

Nome:	<input type="text"/>	256
Descrizione:	<input type="text"/>	1024
Responsabile:	<input type="text"/>	128
Collocazione:	<input type="text"/>	128
Data Apertura:	<input type="text" value="27/08/2015"/> (gg/mm/aaaa)	
Data Scadenza:	<input type="text"/> (gg/mm/aaaa)	
Richiedente:	<input type="text"/>	50
PIVA/Codice fiscale:	<input type="text"/>	16
Data Chiusura:	<input type="text"/> (gg/mm/aaaa)	
Stato:	Aperta	
Livello Riservatezza:	NON CLASSIFICATO	
Livello di Complessità:	non definita	
Segnatura Archivistica:	<input type="text"/>	50

Livello di riservatezza

Focus

Oltre alla scelta della **lista di competenza** un ulteriore filtro che può determinare o meno la visibilità del fascicolo e del suo contenuto è determinato dal **Livello di Riservatezza** che, se impostato (l'impostazione di default è infatti **Non classificato**), si aggiunge al meccanismo delle Liste di competenza.

Impostando infatti un Livello di riservatezza sul fascicolo se ne consentirebbe l'accesso ai soli Utenti di pari livello o con un livello di riservatezza più elevato.

I Livelli di riservatezza disponibili sono:

- **Top secret**
- **Segreto**
- **Ristretto**
- **Classificato**
- **Non classificato**

Un Utente con livello “Segreto” potrà ad esempio accedere ai fascicoli con livello di riservatezza “Ristretto” ma non potrà accedere ai fascicoli con livello di riservatezza “Top Secret”.

Creare fascicolo

Il Fascicolo è stato creato!



Operazioni nei fascicoli





Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
---------	--------------	-----------	-----------	---------	-----------	--------

Nuova Ricerca Salva ricerca

1 - 1 | totale: 1

	N° fascicolo	Nome	Descrizione	Titolario	Repertorio	Responsabile	Apertura	Chiusura	Scadenza	Stato	Accl	Comandi
<input type="checkbox"/>	15237	pippo	pippo	01.01. Legislazione, circolari	2015/1		27/08/2015			Aperta	ACL_Ente	   

Il comando **Elimina*** consente di eliminare il fascicolo nel caso in cui non sia aperto e non contenga documenti.

1 - 1 totale: 1		
Stato	Accl	Comandi
Aperta	ACL_Ente	   

Visualizza contenuto

Modifica

Chiudi fascicolo

Elimina*

Operazioni nei fascicoli

Una volta creato il fascicolo possiamo richiamarlo ed **esplorarne il contenuto**, spostare dei documenti da un fascicolo ad un altro, fare l'upload di doc. per esempio dal ns desktop al fascicolo, creare sotto-fascicoli, etc

The screenshot displays the FOIUM web application interface. At the top left is the 'foium' logo. User information includes: Utente: Serena Bellagotti, Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#), Ruolo: [utente_standard \(+\)](#). Organizational details: Area organizzativa: **AOOPGRO** (p_gr), Registro: . Version: 4.12.0. Navigation links: [Aiuto](#), [Home](#), [Uscita](#). A top navigation bar contains: Ricerca, Assegnazioni, In carico, Documento, Dossier, Fascicoli, Utente. A red arrow points to the 'Fascicoli' tab. The main content area is titled 'Modifica fascicolo n. 15237' and has three tabs: Fascicolo, Fascicoli collegati, and **Contenuto (Documenti: 0)**. The 'Contenuto' tab is active, showing a table with columns: Nome, Descrizione, Data Cr., Data Prot., Stato, Note, Comandi. The table is currently empty. A left sidebar titled 'Operazioni' contains various icons. At the bottom, there are buttons for 'Salva', 'Stampa copertina', and 'Annulla'. A note at the bottom left states: 'I campi con questo colore sono obbligatori.'

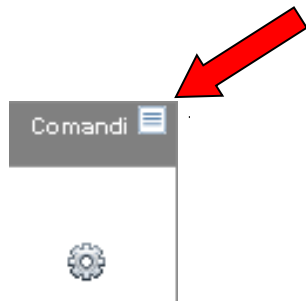
In questa sezione troveremo tutti i documenti contenuti nel fascicolo (vedi slide successiva).

Operazioni nei fascicoli

Ci sono documenti nel fascicolo!



Fascicoli collegati		Contenuto (Documenti: 5)			Procedimenti		
1							
	Nome	Descrizione	Data Cr.	Stato	Prog.	Note	Comandi
<input type="checkbox"/>	<u>8 La Beni Stabili.pdf</u>		21/07/2015 09:57:51		1		
<input type="checkbox"/>	<u>AGORA FOLIUM_.pdf</u>		21/07/2015 09:58:16		2		
<input type="checkbox"/>	<u>Delibera di G.C. n. 109 del 24.08.2010.pdf</u>	test 32	21/07/2015 09:58:39		3		
<input type="checkbox"/>	<u>TEST.AOO1.REGISTRO UFFICIALE.I.0001454.12-06-2015.h.23:43</u>	test / QUESTA E' UNA NOTA CHE SI VEDRA'	12/08/2015 23:43:07		4		
<input type="checkbox"/>	<u>TEST.AOO1.REGISTRO UFFICIALE.I.0001631.04-08-2015.h.15:26</u>	protocollo e metto una nota / metto una nota	04/08/2015 15:26:28		5		



Griglia

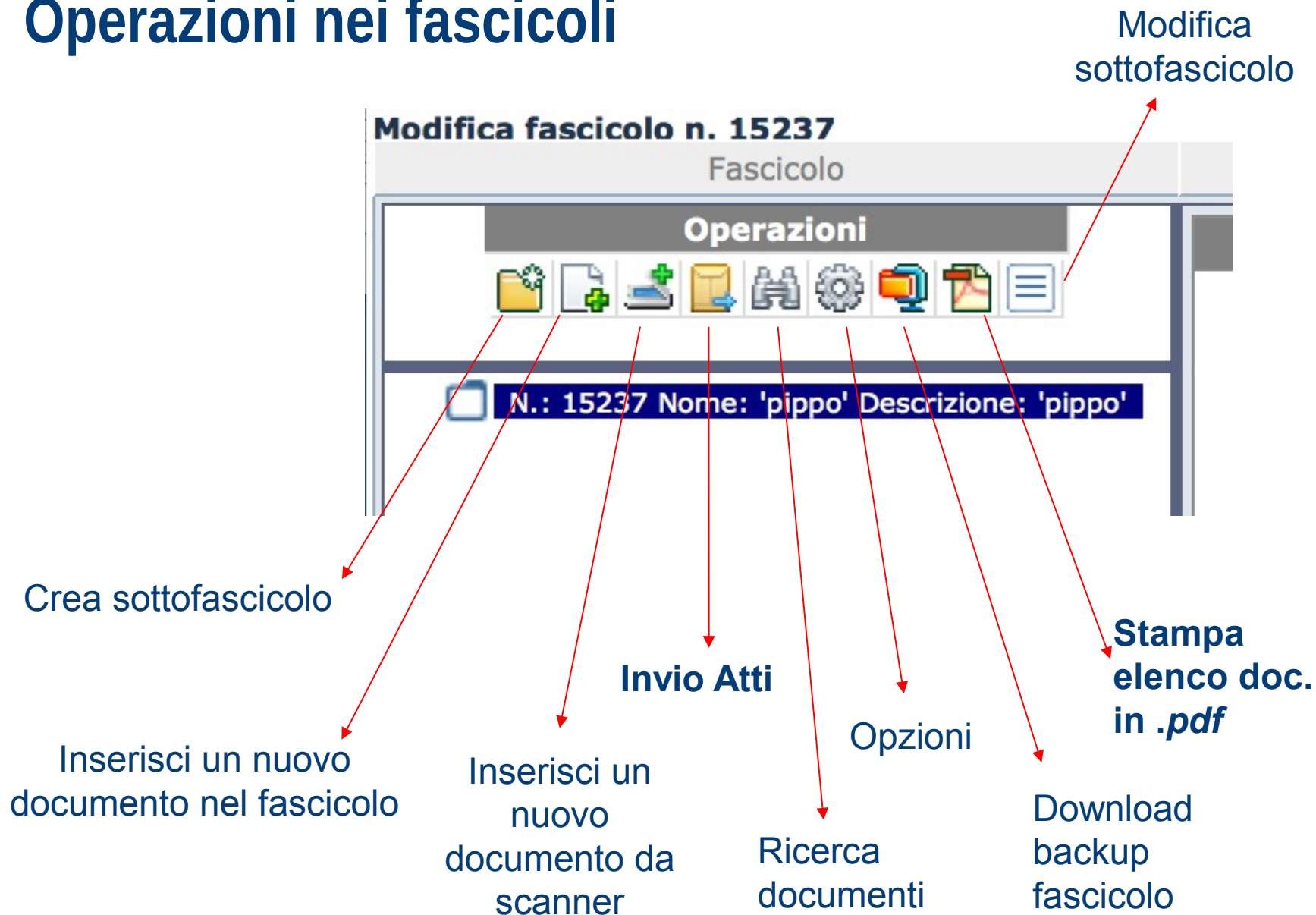
Selezionare le colonne da visualizzare

- Nome
- Descrizione
- Mitt/Dest
- Mod.
- Riservatezza
- Priorit
- Data Cr.
- Data Prot.
- Data Fasc.
- Stato
- Note
- Timbro

Annulla Salva

consente di vedere nella

Operazioni nei fascicoli



Stampa elenco doc. in .pdf

Focus



Questa funzione (prevista da normativa) può essere molto utile per gli operatori in quanto **permette di stampare in formato .pdf l'intero elenco dei documenti contenuti nel fascicolo.**



- Questa funzione consente di trasmettere agevolmente alla casella e-mail dell'ufficio di protocollo tutto il contenuto del fascicolo ai fini della protocollazione in uscita ed invio ad altra amministrazione o altra AOO.
- Questa funzione richiede che, **nel fascicolo**, sia presente un **documento principale firmato digitalmente**.
- Dopo aver cliccato l'apposito pulsante verrà richiesto di selezionare il documento firmato digitalmente; verrà così confezionata una e-mail con allegati i documenti contenuti nel fascicolo.

Operazioni nei fascicoli – Stampa copertina



Utente: **Serena Bellagotti**
Ufficio: **SEGRETARIO/ DIRETTORE GENERALE (+)**
Ruolo: **utente_standard (+)**

Area organizzativa: **AOOPGRO (p_gr)**
Registro:

Versione: **4.12.0**
[Aiuto](#) [Home](#) [Uscita](#)

Ricerca | **Assegnazioni** | **In carico** | **Documento** | **Dossier** | **Fascicoli** | **Utente**

Fascicolo		Fascicoli collegati		Contenuto (Documenti: 0)	
Nome:	<input type="text" value="pippo"/> 256			Ricerca le voci del titolare per:	
Descrizione:	<input type="text" value="pippo"/> 1024	Codice:	<input type="text"/>	Descrizione:	<input type="text"/>
Responsabile:	<input type="text"/> 128	Voci del titolare trovate:		<ul style="list-style-type: none">01 Atti fondamentali e Organi02 Organizzazione generale e rapporti istituzionali03 Risorse informative04 Personale05 Risorse finanziarie e bilancio	
Collocazione:	<input type="text"/> 128			Classificazione del fascicolo:	
Data Apertura:	<input type="text" value="27/08/2015"/> (gg/mm/aaaa)			<input type="text" value="01.01 Legislazione, circolari"/>	
Data Scadenza:	<input type="text"/> (gg/mm/aaaa)			Lista di Competenza Classificazione:	
Richiedente:	<input type="text"/> 50			<input type="text" value="ACL_Ente"/>	
PIVA/Codice fiscale:	<input type="text"/> 16			Ufficio proprietario del fascicolo: <input type="text" value="B"/>	
Data Chiusura:	<input type="text"/> (gg/mm/aaaa)				
Stato:	<input type="text" value="Aperta"/>				
Livello Riservatezza:	<input type="text" value="NON CLASSIFICATO"/>				
Livello di Complessità:	<input type="text" value="non definita"/>				

I campi con questo colore sono obbligatori.



Stampa copertina

Fascicolo: pippo Anno 2015

Amministrazione p_gr - Provincia di Grosseto

Aoo AOOPGRO

Data stampa: 04/09/2015

Informazioni Generali

Nome:	pippo
Descrizione:	pippo
Numero identificativo:	15237
Responsabile:	
Collocazione:	
Data apertura:	27/08/2015
Data scadenza:	
Richiedente:	
PIVA/Cod. Fiscale:	
Data chiusura:	
Stato Fascicolo:	Aperta
Livello riservatezza:	NON CLASSIFICATO
Segnatura archivio:	
Titolario:	Legislazione, circolari (01)
Repertorio:	2015/1
Acl:	ACL_Ente
Ufficio proprietario:	SEGRETARIO/ DIRETTORE GENERALE (B)

È possibile stampare la copertina con i dati caratteristici del fascicolo ed utilizzarla per apporla sui fascicoli cartacei.

Cartella di lavoro



Utente: **Serena Bellagotti**

Ufficio: **Direzione Generale Affari Generali (+)**

Ruolo: **utente (+)**

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli
Quadro riassuntivo					Gestione fascicoli
					Ricerca sottofascicoli
					Cartella di lavoro
Assegnazioni				Ultimi 30 giorni	
<u>Competenza</u>				354	
<u>Conoscenza</u>				149	
<u>Smistamento</u>				144	
<u>Restituite</u>				0	



Dalla voce di menù **Fascicoli>>>Cartella di lavoro** è possibile accedere direttamente alla propria cartella di lavoro.

Questa particolare cartella, del tutto simile ad un fascicolo è **visibile solo all'utente che vi accede** e può essere usata per inserire nel sistema dei documenti da lavorare.

Assegnazioni



Assegnazioni

Con il ruolo di **utente** si possono verificare le Assegnazioni ricevute. Le Assegnazioni sono di 3 tipi: *Competenza, Conoscenza, Smistamento*

Il menu **Assegnazioni** consente di accedere a:

- 1) Elenco degli eventuali protocolli ricevuti (per Competenza, per Conoscenza o per Smistamento)
- 2) Elenco delle Assegnazioni effettuate dall'Utente documentale e in attesa di essere prese in carico
- 3) Elenco delle Assegnazioni rifiutate/restituite dall'assegnatario

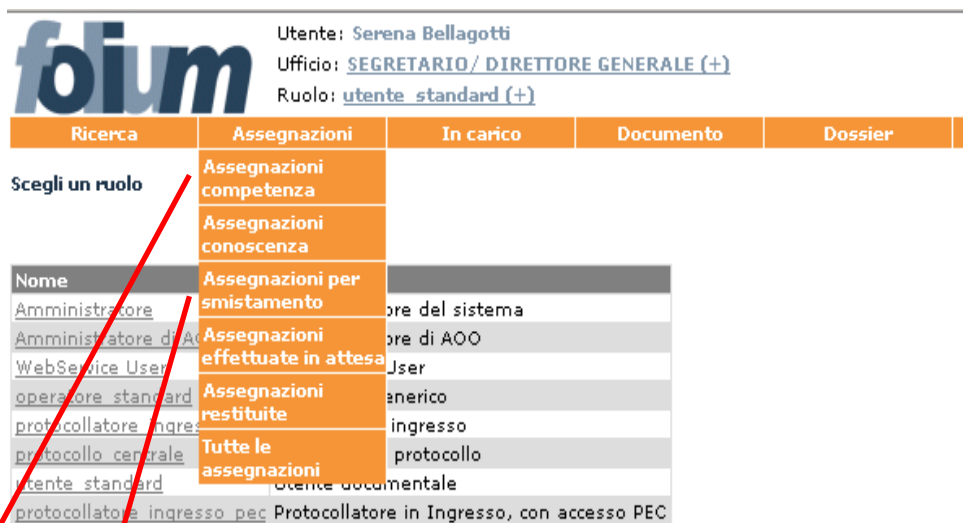


Utente: Serena Bellagotti
Ufficio: [SECRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [utente standard \(+\)](#)

Ricerca	Assegnazioni	In carico	Documento
Scegli un ruolo	Assegnazioni competenza		
	Assegnazioni conoscenza		
Nome	Assegnazioni per smistamento		
Amministratore		ore del sistema	
Amministratore di A	Assegnazioni effettuate in attesa	ore di AOO	
WebService User		User	
operatore standard	Assegnazioni restituite	enerico	
protocollatore ingre		ingresso	
protocollo centrale	Tutte le assegnazioni	protocollo	
utente standard		utente documentale	
protocollatore ingresso pec		Protocollatore in Ingresso, con accesso PEC	

Presenza in carico e/o restituzione

In generale le assegnazioni per poter essere lavorate devono essere “prese in carico”.



The screenshot shows the FOLium web interface. At the top left is the 'folium' logo. To the right, the user's profile is displayed: 'Utente: Serena Bellagotti', 'Ufficio: SEGRETARIO / DIRETTORE GENERALE (+)', and 'Ruolo: utente_standard (+)'. Below this is a navigation bar with tabs: 'Ricerca', 'Assegnazioni', 'In carico', 'Documento', and 'Dossier'. The 'Assegnazioni' tab is active, showing a dropdown menu with options: 'Assegnazioni competenza', 'Assegnazioni conoscenza', 'Assegnazioni per smistamento', 'Assegnazioni effettuate in attesa', 'Assegnazioni restituite', and 'Tutte le assegnazioni'. Below the menu is a table of assignments with columns for 'Nome' and 'Descrizione'. The table lists various roles like 'Amministratore', 'WebService User', 'operatore standard', 'protocollatore ingresso', 'utente_standard', and 'protocollatore ingresso_pec'. Two red arrows point from the 'Assegnazioni competenza' and 'Assegnazioni per smistamento' options in the dropdown menu to the text below.

Le assegnazioni ricevute per competenza e/o smistamento oltre ad essere **prese in carico** dall'operatore, quest'ultimo può **restituirle al mittente** con un apposito tasto denominato “Restituisci”.

Prendi in carico

Restituisci

Presenza in carico



Utente: Serena Bellagotti
Ufficio: [SECRETARIO / DIRETTORE GENERALE \(+\)](#)
Ruolo: [utente standard \(+\)](#)

Area organizzativa: [A00PGRO \(F_gr\)](#)
Registro: [REGISTRO UFFICIALE](#)
Stato: **Ingresso** - 27/08/2015

Versione: [Aiuto](#) [Hc](#)

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente	
---------	--------------	-----------	-----------	---------	-----------	--------	--

Elenco documenti in carico

1 - 1 | totale

	Registro	Mod.	Num.	Oggetto	Mitt/Dest	Assegnatario	Assegnazione	Presenza in carico	Note	Pri.	Operazioni
<input type="checkbox"/>	REGISTRO UFFICIALE	I	2415	POSTA CERTIFICATA: AVCP - Assolvimento degli obblighi di trasmissione e PUBBLICAZIONE - scadenza 31 Gennaio 2014.	certificata@pec.italsoft-mc.it ;	Bellagotti Serena	22/01/2014	22/01/2014		!	

Ricerca fascicoli

(è possibile utilizzare chiavi parziali di ricerca utilizzando il carattere speciale *)

Nome:	<input type="text" value=""/>	64	Descrizione:	<input type="text" value=""/>	512
Responsabile:	<input type="text" value=""/>	50	Stato:	<input type="text" value=""/>	
Data Apertura da:	<input type="text" value=""/>	(gg/mm/aaaa)	Data Apertura al:	<input type="text" value=""/>	(gg/mm/aaaa)
Data Chiusura dal:	<input type="text" value=""/>	(gg/mm/aaaa)	Data Chiusura al:	<input type="text" value=""/>	(gg/mm/aaaa)
Data Scadenza dal:	<input type="text" value=""/>	(gg/mm/aaaa)	Data Scadenza al:	<input type="text" value=""/>	(gg/mm/aaaa)
Codice titolare :	<input type="text" value=""/>	20			
Anno:	<input type="text" value=""/>	N° repertorio da:	<input type="text" value=""/>	a:	<input type="text" value=""/>
PIVA/Codice fiscale	<input type="text" value=""/>	512	<input type="checkbox"/>	R cerca nel sottalbero	
N° fascicolo	<input type="text" value=""/>	12	<input type="checkbox"/>	solo fascicoli di questo ufficio	
Collocazione	<input type="text" value=""/>	128			
Visualizzazione:	lista <input checked="" type="radio"/>	albero <input type="radio"/>			

Attenzione : la ricerca restituirà solo i fascicoli per i quali si possiede almeno il permesso di scrittura.

Fascicolare il documento



Utente: Serena Bellagotti
 Ufficio: [SEGRETARIO / DIRETTORE GENERALE \(+\)](#)
 Ruolo: [utente_standard \(+\)](#)

Area organizzativa: [A00PGRO \(F_gr\)](#)
 Registro: [REGISTRO UFFICIALE](#)
 Stato: **Ingresso** - 27/08/2015

Versio
[Aiuto](#) [Hc](#)

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
Elenco documenti in carico		Elenco in carico				
Concludi		Inserisci nel fascicolo	Elenco documenti conclusi			

1 - 1 | totale

	Registro	Mod.	Num.	Oggetto	Mitt/Dest	Assegnatario	Assegnazione	Preso in carico	Note	Pri.	Operazioni
<input type="checkbox"/>	REGISTRO UFFICIALE	I	2415	POSTA CERTIFICATA: AVCP - Assolvimento degli obblighi di trasmissione e PUBBLICAZIONE - scadenza 31 Gennaio 2014	certificata@pec.italsoft-mc.it ;	Bellagotti Serena	22/01/2014	22/01/2014		!	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Ricerca fascicoli

(è possibile utilizzare chiavi parziali di ricerca utilizzando il carattere speciale *)

Nome:	<input type="text"/>	64	Descrizione:	<input type="text"/>	512
Responsabile:	<input type="text"/>	50	Stato:	<input type="text"/>	
Data Apertura da:	<input type="text"/>	(gg/mm/aaaa)	Data Apertura al:	<input type="text"/>	(gg/mm/aaaa)
Data Chiusura dal:	<input type="text"/>	(gg/mm/aaaa)	Data Chiusura al:	<input type="text"/>	(gg/mm/aaaa)
Data Scadenza dal:	<input type="text"/>	(gg/mm/aaaa)	Data Scadenza al:	<input type="text"/>	(gg/mm/aaaa)
Codice titolario :	<input type="text"/>	20			
Anno:	<input type="text"/>	N° repertorio da:	<input type="text"/>	a:	<input type="text"/>
PIVA/Codice fiscale	<input type="text"/>	512	<input type="checkbox"/> R cerca nel sottalbero <input type="checkbox"/> solo fascicoli di questo ufficio		
N° fascicolo	<input type="text"/>	12			
Colocazione	<input type="text"/>	128			
Visualizzazione:	lista <input checked="" type="radio"/>	albero <input type="radio"/>			

Cerca

Attenzione : la ricerca restituirà solo i fascicoli per i quali si possiede almeno il permesso di scrittura.

Concludere il documento



Utente: Serena Bellagotti
Ufficio: [SEGRETARIO / DIRETTORE GENERALE \(+\)](#)
Ruolo: [utente_standard \(+\)](#)

Area organizzativa: [A00PGRO \(F_gr\)](#)
Registro: [REGISTRO UFFICIALE](#)
Stato: **Ingresso** - 27/08/2015

Versione: [Aiuto](#) [Hc](#)

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
Elenco documenti in carico		Elenco in carico				
Concludi		Inserisci nel fascicolo	Elenco documenti conclusi			

1 - 1 | totale

	Registro	Mod.	Num.	Oggetto	Mitt/Dest	Assegnatario	Assegnazione	Preso in carico	Note	Pri.	Operazioni
<input type="checkbox"/>	REGISTRO UFFICIALE	I	2415	POSTA CERTIFICATA: AVCP - Assolvimento degli obblighi di trasmissione e PUBBLICAZIONE - scadenza 31 Gennaio 2014	certificata@pec.italsoft-mc.it ;	Bellagotti Serena	22/01/2014	22/01/2014		!	

Ricerca fascicoli

(è possibile utilizzare chiavi parziali di ricerca utilizzando il carattere speciale *)

Nome:	<input type="text"/>	64	Descrizione:	<input type="text"/>	512
Responsabile:	<input type="text"/>	50	Stato:	<input type="text"/>	
Data Apertura da:	<input type="text"/>	(gg/mm/aaaa)	Data Apertura al:	<input type="text"/>	(gg/mm/aaaa)
Data Chiusura dal:	<input type="text"/>	(gg/mm/aaaa)	Data Chiusura al:	<input type="text"/>	(gg/mm/aaaa)
Data Scadenza dal:	<input type="text"/>	(gg/mm/aaaa)	Data Scadenza al:	<input type="text"/>	(gg/mm/aaaa)
Codice titolare :	<input type="text"/>	20			
Anno:	<input type="text"/>	N° repertorio da:	<input type="text"/>	a:	<input type="text"/>
PIVA/Codice fiscale	<input type="text"/>	512	<input type="checkbox"/>	R cerca nel sottalbero	
N° fascicolo	<input type="text"/>	12	<input type="checkbox"/>	solo fascicoli di questo ufficio	
Colocazione	<input type="text"/>	128			
Visualizzazione:	lista <input checked="" type="radio"/>	albero <input type="radio"/>			

Cerca

Attenzione : la ricerca restituirà solo i fascicoli per i quali si possiede almeno il permesso di scrittura.

Assegnare / Riassegnare un documento



Utente: [Serena Bellagotti](#)
Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [utente standard \(+\)](#)

Area organizzativa: [AOOPGRO \(p_gr\)](#)
Registro:

Versi
[Aiuto](#) [Itc](#)

Ricerca

Assegnazioni

In carico

Documento

Dossier

Fascicoli

Utente

Elenco documenti in carico

Concludi

Inserisci nel fascicolo

Assegna

1 - 1 | totale:

	Registro	Mod.	Num.	Oggetto	Mitt/Dest	Assegnatario	Assegnazione	Presenza in carico	Note	Pri.	Operazioni
<input type="checkbox"/>	REGISTRO UFFICIALE	I	2415	POSTA CERTIFICATA: AVCP - Assolvimento degli obblighi di trasmissione e PUBBLICAZIONE - scadenza 31 Gennaio 2014	certificata@pec.italsoft-mc.it	Bellagotti Serena	22/01/2014	22/01/2014		!	

1. **Flaggare il documento** che si vuole assegnare
2. **Cliccare su Assegna**

Assegnare

... se click su Assegna



Utente: [Serena Bellagotti](#)
Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [utente standard \(+\)](#)

Area organizzativa: [AOOPGRO \(p_gr\)](#)
Registro:

[Aiuto](#)

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
---------	--------------	-----------	-----------	---------	-----------	--------

Riassegnazione Massiva

Tipo: Ricerca assegnatari per: Priorità: Data scadenza:

- Liste di competenza
- Organigramma

Descrizione

Operazioni

Riassegnare

... se click su Riassegna



Utente: [Serena Bellagotti](#)
Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [utente standard \(+\)](#)

Area organizzativa: [A00PGRO \(p_gr\)](#)
Registro:

[Ai](#)

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
---------	--------------	-----------	-----------	---------	-----------	--------

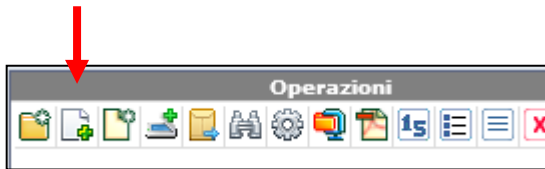
REGISTRO UFFICIALE: PROTOCOLLO in Ingresso, N.2415, data: 08/01/2014 - oggetto: POSTA CERTIFICATA: AVCP - Assolvimento degli obblighi di trasmissione e

[Inserisci Competenza](#) [Inserisci Conoscenza](#) [Inserisci Smistamento](#) [Modifica](#) [Elimina](#) [Storia assegnazioni](#)

	Assegnatario	Tipo	Assegnazione	Assegnante	Priorità	Note	Data Scadenza	Data inizio
<input type="checkbox"/>	Bellagotti Serena	utente	Competenza	Bellagotti Serena	media			22/01/2014 12:15:00
<input type="checkbox"/>	SEGRETARIO/ DIRETTORE GENERALE	ufficio	Smistamento	Cappelli Tamara	media			08/01/2014 09:30:35
	UP SUPPORTO AGLI ORGANI ISTITUZIONALI	ufficio	Smistamento	Cappelli Tamara	media			08/01/2014 09:30:43
	Bellagotti Serena	utente	In carico	Bellagotti Serena	media			22/01/2014 12:15:13

[Torna](#)

Fascicolazione dei documenti non protocollati



Nel fascicolo si possono caricare documenti non protocollati (funzione di upload)



The screenshot shows the FOIUM software interface. At the top, the user is identified as 'Serena Bellagotti' in the 'Direzione Generale Affari Generali (+)' office. The organizational area is 'AOO1 (TEST)'. The interface includes a navigation menu with options like 'Ricerca', 'Assegnazioni', 'In carico', 'Documento', 'Dossier', 'Fascicoli', and 'Utente'. The main area is titled 'Modifica fascicolo n. 1072' and shows a list of documents under the 'Contenuto (Documenti: 2)' tab. The table below lists two documents:

Nome	Descrizione	Data Cr.	Stato	Note	Comandi
TEST.AOO1.REGISTRO.UFFICIALE.1.0001470.23-06-2015.h.17:36	ANOMALIA MESSAGGIO: Il test doc con notifica	23/06/2015 17:36:52			
mod71_TARI.pdf		29/09/2015 17:05:04			

A context menu is open over the second document, listing various actions: Link, Sposta, Checkout, Protocolla, Firma PDF, Firma P7M, Blocca, Cancella, Profilo, Note, Versioni, Ad, Download, and Cambia priorit.

Firma digitale da fascicolo



La Firma digitale



- è l'equivalente elettronico di una tradizionale firma autografa apposta su carta.
- Deve essere contestualizzata nel tempo: è indispensabile stabilire se la firma è stata creata prima della scadenza o revoca del certificato... associando al documento un riferimento temporale opponibile a terzi.
- è associata stabilmente al documento elettronico sulla quale è apposta e lo arricchisce di informazioni che ne attestano con certezza l'integrità, l'autenticità, la non ripudiabilità, consentendo così al documento sottoscritto di assumere la piena **efficacia probatoria**.

Lettura Firma digitale in Folium

Firma digitale



Pades: è un acronimo che sta per *PDF Advanced Electronic Signature*. In buona sostanza si tratta di una firma elettronica basata sul formato PDF.

Cades è uno dei più diffusi poiché il file d'estensione .p7m della cosiddetta busta informatica, da esso prodotta, è riconosciuto dalla normativa vigente come valido per garantire l'interoperabilità tra i sistemi di firma digitale.

Xades: Folium gestisce questo tipo di firma inclusa nei file .xml (ad esempio in alcune fatture elettroniche).

La Firma digitale

E' un particolare tipo di firma elettronica avanzata basata su un sistema di **due chiavi crittografiche**, una **pubblica** (necessaria a verificare che il doc. provenga effettivamente dal titolare) e l'altra **privata** (necessaria ad apporre la firma) e su un certificato qualificato.



Lettura Firma digitale in Folium

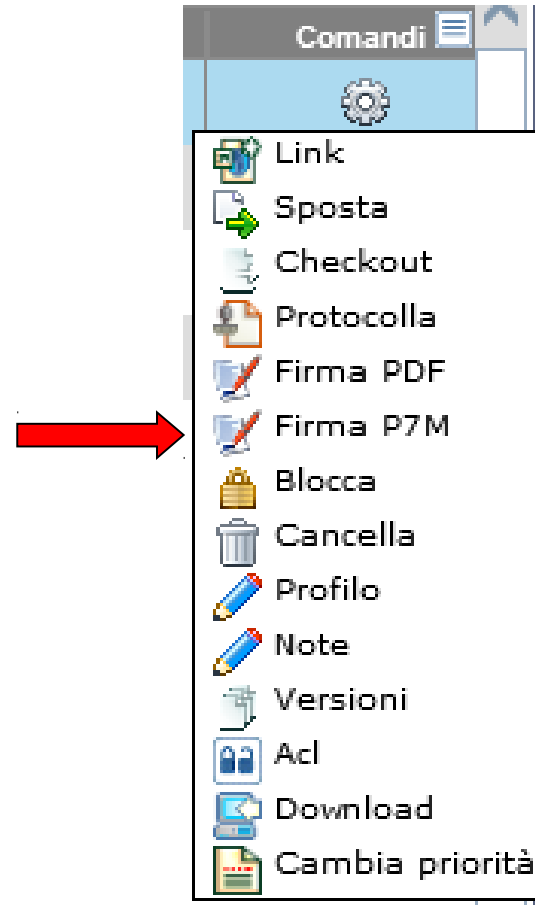


- Secondo il CAD e secondo la Deliberazione dell'allora CNIPA n° 45 del 21/05/2009, il formato di firma PAdES, così come la firma CAdES e XAdES sono i tre formati consentiti per le firme elettroniche qualificate e digitali.
- **Il Pdp Folium è in grado di riconoscerli tutti e tre** e di riportare a video un pannello con indicate le specifiche della firma (firmatario, data della firma, validità, etc)
- I file firmati con il formato di firma PAdES, al contrario di quanto accade con il formato del CAdES, mantengono l'estensione .pdf.

Firma digitale nel fascicolo

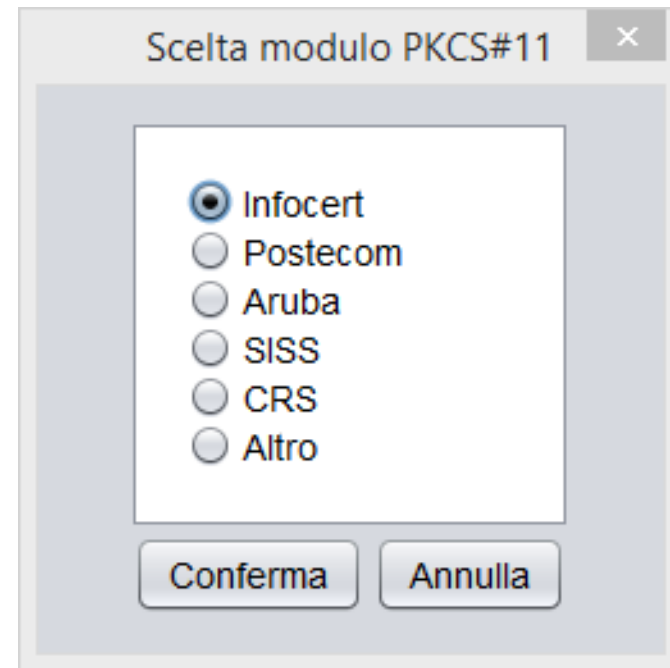
Si fa un flag sul file .pdf da firmare digitalmente e si clicca su Firma (pdf o p7m)

! Il dispositivo di firma (chiavetta token o smart card) deve essere già connesso al pc!



Firma digitale nel fascicolo

La **prima volta** che si utilizza la firma digitale, il sistema ci chiederà di specificare il tipo di gestore.



Firma digitale nel fascicolo

ISTRUZIONI ACCESSO RAS FORNITORI

Collegamento al RAS e Autenticazione

Buongiorno, come richiesto dalla Dott.ssa Garini le invio i parametri per il collegamento in teleassistenza all'applicativo FOLIUM installato presso la nostra sede di Sondrio – Via N. sauro 38.

Per accedere al nostro RAS server bisogna configurare una connessione remota con i seguenti parametri :

Telefono(ISDN**)	: 0342 520082
Userid	: radminagora
Password	: agoraradmin
IP address	: 172.19.1.140

** collegamento è possibile sia in modalità analogica che ISDN.

Firma

Chiudi



Cliccare sul tasto Firma

Firma digitale nel fascicolo

Una volta digitato il PIN nell'apposito campo e se la firma sarà andata a buon fine, si vedrà nella parte destra dello schermo le specifiche della firma:



...Successivamente il sistema ci chiederà se vogliamo apporre una **ulteriore firma** digitale oppure una **firma di convalida**:

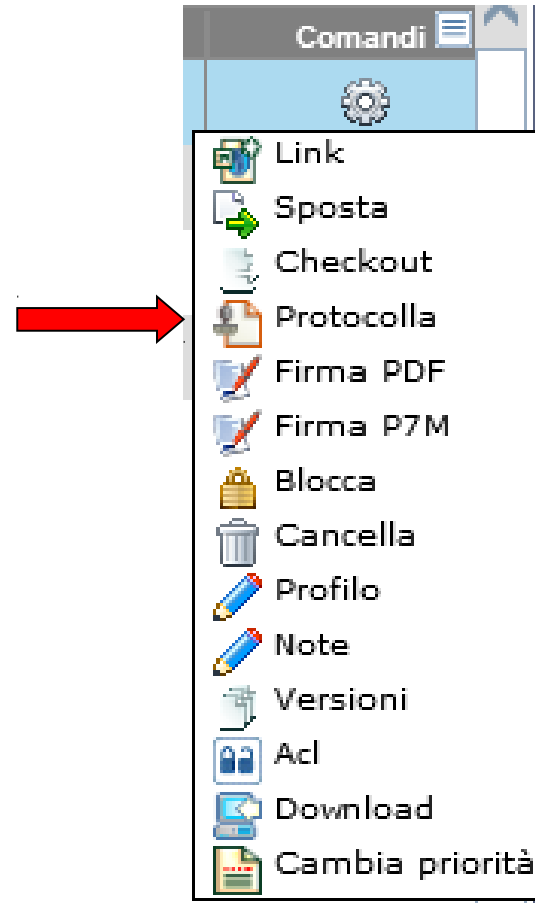
Aggiungi firma

Firma di convalida

Chiudi

Protocollo da fascicolo

Si fa un flag sul file .pdf da protocollare e si clicca su Protocolla



Protocollo da fascicolo

...Una volta cliccato su Protocolla, il sistema ci fa scegliere su quale registro vogliamo protocollare (Interna o Uscita)



Utente: **Serena Bellagotti**
Ufficio: **Direzione Generale Affari Generali (+)**
Ruolo: **utente (+)**

Area organizzativa: **AOO1 (TEST)**
Registro:

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
---------	--------------	-----------	-----------	---------	-----------	--------

Selezione registro e modalità di protocollazione

Registro di CORRISPONDENZA	Descrizione	Data ultima reg.	Interna	Uscita
REGISTRO UFFICIALE	Registro Ufficiale AOO AOO1	30/09/2015	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Torna alla lista documenti](#)

Protocollo da fascicolo

...a questo punto si aprirà la maschera di protocollo (in questo caso di uscita)

foium Utente: [Serena Bellagotti](#) Area organizzativa: **A001 (TEST)** [Ve](#)
Ufficio: [Direzione Generale Affari Generali \(+\)](#) Registro: [REGISTRO UFFICIALE](#) [Aiuto](#)
Ruolo: [utente \(+\)](#) Stato: **Uscita - 30/09/2015**

Ricerca Assegnazioni In carico Documento Dossier Fascicoli Utente

Protocollo Classificazione **C** Collegati Info Documento Allegati

Nome Documento Esteso:

Codice Oggetto:

Oggetto:

[Non inserire dati sensibili nell'Oggetto]

Destinatari (E' necessario inserire almeno un destinatario)

Invio E-mail singole Protocollazione in modalità circolare

Descrizione: Mezzo sped.:

Denominazione	Indirizzo	Mezzo sped.	P.C.	Comandi
---------------	-----------	-------------	------	---------

Ufficio Mittente:

Competente:

Data documento: (gg/mm/aaaa) Data spedizione: (gg/mm/aaaa) Data scadenza: (gg/mm/aaaa)

Paginazione nel fascicolo

News



Utente: Daniele Rosa
Ufficio: Ufficio 1 (+)
Ruolo: utente (+)

Area organizzativa: A001 (TEST)
Registro: [REGISTRO UFFICIALE](#)
Stato: **Ingresso** - 23/09/2015

Versione: 4.13.0
[Aiuto](#) [Home](#) [Uscita](#)

Ricerca Assegnazioni In carico Documento Dossier Fascicoli Utente

Modifica fascicolo n. 1058

Fascicolo Fascicoli collegati **Contenuto (Documenti: 471)** Procedimenti

Operazioni

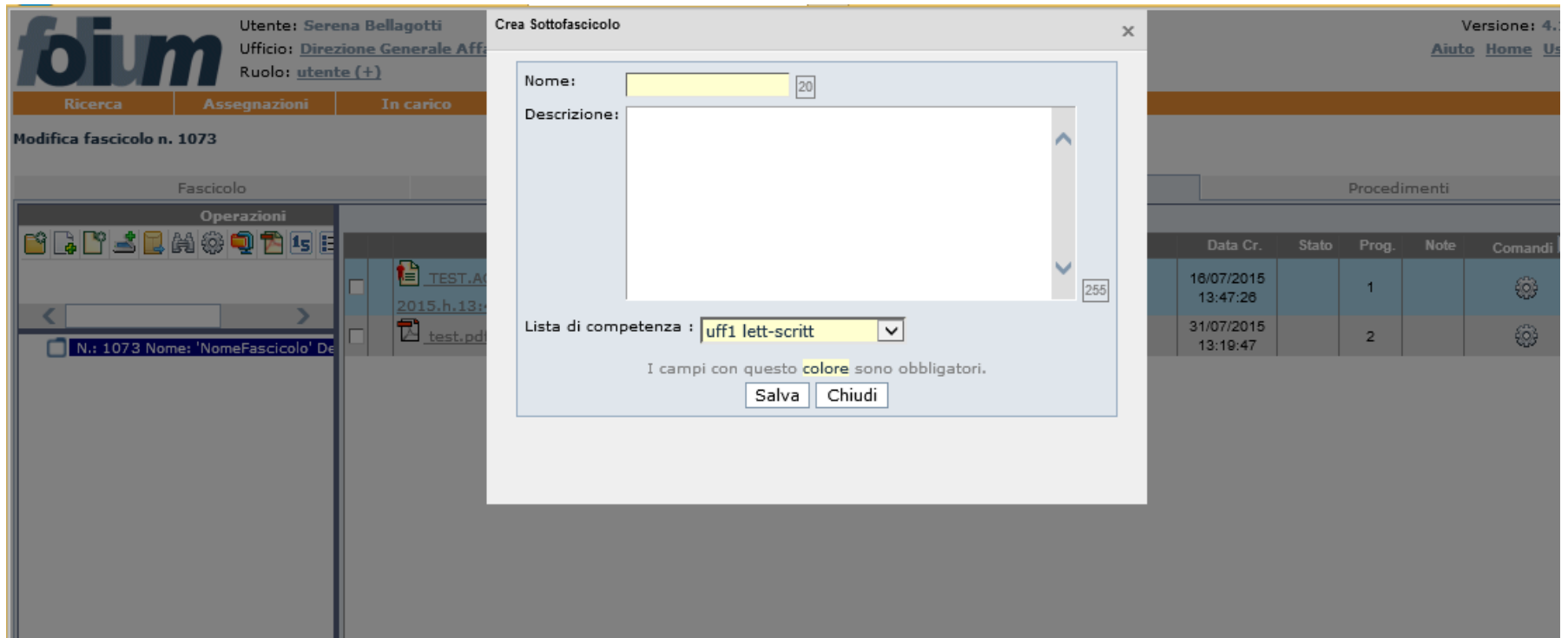
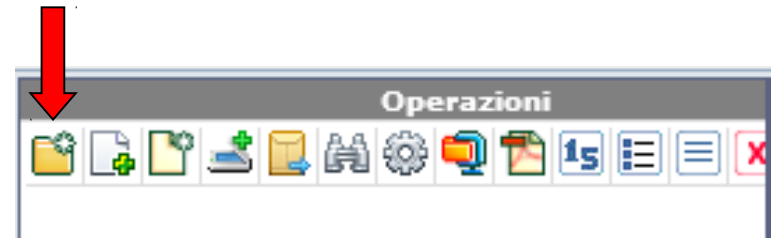
N.: 1058 Nome: 'Fatture 2015' Descrizione: 'Fatture 2015'

	Nome	Descrizione	Mitt/Dest	Data Cr.	Stato	Note	Comandi
<input type="checkbox"/>	TEST.A001.REGISTRO UFFICIALE.I.0000866.27-03-2015.h.15:45	Fattura n. 58 U.detto 2014 12-18 - Copia a Ric...	Clienti/Car	27/03/2015 15:45:14			
<input type="checkbox"/>	TEST.A001.REGISTRO UFFICIALE.I.0000868.30-03-2015.h.15:09	Fattura (Spese Dottore n. 133 di data 18/03/2014)	Clienti/Spese	30/03/2015 15:09:16			
<input type="checkbox"/>	TEST.A001.REGISTRO UFFICIALE.I.0000869.30-03-2015.h.15:12	Fattura n. 58 U.detto 2014 12-18 - Copia a Ric...	Fattori/Spa	30/03/2015 15:12:05			
<input type="checkbox"/>	TEST.A001.REGISTRO UFFICIALE.I.0000870.30-03-2015.h.15:23	Fattura (Spese Dottore n. 133 di data 18/03/2014)	Clienti/Spese	30/03/2015 15:23:04			
<input type="checkbox"/>	TEST.A001.REGISTRO UFFICIALE.I.0000871.30-03-2015.h.15:25	Fattura n. 58 U.detto 2014 12-18 - Copia a Ric...	Fattori/Spa	30/03/2015 15:25:53			
<input type="checkbox"/>	TEST.A001.REGISTRO UFFICIALE.I.0000872.30-03-2015.h.15:33	Fattura (Spese Dottore n. 133 di data 18/03/2014)	Clienti/Spese	30/03/2015 15:33:09			
<input type="checkbox"/>	TEST.A001.REGISTRO UFFICIALE.I.0000873.30-03-2015.h.15:37	Fattura n. 58 U.detto 2014 12-18 - Copia a Ric...	Clienti/Spa	30/03/2015 15:37:04			
<input type="checkbox"/>	TEST.A001.REGISTRO UFFICIALE.I.0000874.30-03-	Fattura (Spese Dottore n. 133 di data 18/03/2014)	Clienti/Spese	30/03/2015			

La funzione riduce i tempi di apertura del fascicolo o accesso a sottofascicoli.

Creazione sottofascicolo

Posizionarsi sul fascicolo all'interno del quale si vuole creare un sottofascicolo e cliccare il pulsante "Crea sottofascicolo":



The screenshot shows the 'foium' application interface. The user is logged in as 'Serena Bellagotti' from the 'Direzione Generale Affari'. The main window displays 'Modifica fascicolo n. 1073'. A dialog box titled 'Crea Sottofascicolo' is open, allowing the user to create a new sub-folder. The dialog contains the following fields and options:

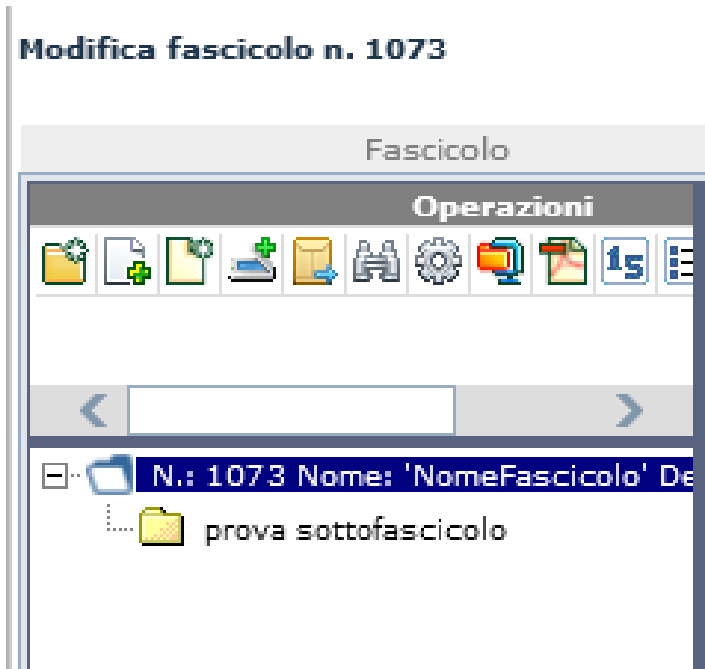
- Nome:** A text input field with a character count of 20.
- Descrizione:** A large text area with a character count of 255.
- Lista di competenza:** A dropdown menu currently set to 'uff1 lett-scritt'.

Below the fields, a note states: "I campi con questo colore sono obbligatori." (Fields with this color are mandatory). At the bottom of the dialog are 'Salva' and 'Chiudi' buttons.

In the background, a table of 'Procedimenti' (Procedures) is visible:

Data Cr.	Stato	Prog.	Note	Comandi
18/07/2015 13:47:26		1		
31/07/2015 13:19:47		2		

Creazione sottofascicolo



Consigli:

! Attenzione a non creare una sotto-alberatura troppo articolata.

Il Fascicolo deve essere più snello possibile e deve essere chiuso una volta terminato il procedimento o l'anno solare (a seconda dei criteri).

Si consiglia di utilizzare lo stesso criterio di scrittura (Maiuscolo o Minuscolo) e di nominare il fascicolo in modo più chiaro possibile per consentire ai colleghi di trovare documenti in caso di VS assenza.

Approfondimento sulla Gestione delle Rubriche



Inserimento manuale

Attenzione! Non tutti gli utenti hanno la possibilità di aggiornare le rubriche dei corrispondenti. Avranno cmq la facoltà di inserire comunque i nominativi necessari alla protocollazione anche se tali nominativi non andranno ad arricchire le rubriche.

Inserimento libero



Mezzo spedizione:

Fisica

Giuridica

Codice:	<input type="text"/>	10	Cognome:	<input type="text"/>	40
Nome:	<input type="text"/>	40	Toponimo:	<input type="text"/>	30
Dug:	<input type="text"/>	-	Comune:	<input type="text"/>	50
Civico:	<input type="text"/>	10	Email:	<input type="text"/>	128
Provincia:	<input type="text"/>				
Cap:	<input type="text"/>	8			

Ok

Annulla

Visualizzazione Estesa

Inserimento manuale

Inserimento libero

Mezzo spedizione:

Fisica Giuridica

Codice: 10

Nome: 40

Cognome: 40

Dug: -

Toponimo: 30

Civico: 10

Provincia:

Comune: 50

Cap: 8

Email: 128

Codice fiscale: 16

Note: 500

Consenso alle regole di privacy per quanto riguarda l'utilizzo dell'e-mail: SI NO

Telefono: 16

Fax: 16

Note indirizzo: 200

Ok Annulla Salva in rubrica

Approfondimento su “Indice PA”

All'indirizzo <http://indicepa.gov.it/documentale/index.php> è possibile accedere all'indice delle pubbliche amministrazioni dove sono presenti le caselle di posta elettronica istituzionali.

La rubrica viene aggiornata da ciascuna pubblica amministrazione ed ha un'efficacia notevole quando dobbiamo inviare documenti ad altre Pubbliche Amministrazioni.

The screenshot shows the homepage of the 'Indice PA' website. At the top, there is a navigation bar with the logo 'indicepa.gov.it' and the tagline 'IPA Indice delle Pubbliche Amministrazioni'. To the right of the logo is a search bar with a 'Cerca' button and a magnifying glass icon. Further right are links for 'Area Riservata', 'Cos'è', 'Per gli Enti', 'Consulta i dati', and 'Documenti'. Below the navigation bar, the main heading reads 'La comunicazione con le PA inizia da qui.' followed by a search input field. On the right side, there is a 'Numeri Verdi' section with the number '800 129 986' and three service icons: 'Apri un ticket', 'Controlla un ticket aperto', and 'Verifica browser'. Below the search bar, there are two featured articles. The first is titled 'Fatturazione elettronica' and includes a date '10-04-15' and a brief description about the obligation of electronic invoicing starting from March 31, 2015. The second is titled 'In primo piano' and includes a date '27-04-15' and a description of the new IPA website's user interface. On the far right, there is a section titled 'Amministrazioni più cliccate' with a numbered list of six government entities.

indicepa.gov.it
IPA Indice delle Pubbliche Amministrazioni

Area Riservata

Cos'è Per gli Enti Consulta i dati Documenti

La comunicazione con le PA inizia da qui.

Cerca

Numeri Verdi
800 129 986

Apri un ticket

Controlla un ticket aperto

Verifica browser

Fatturazione elettronica

In primo piano

Amministrazioni più cliccate

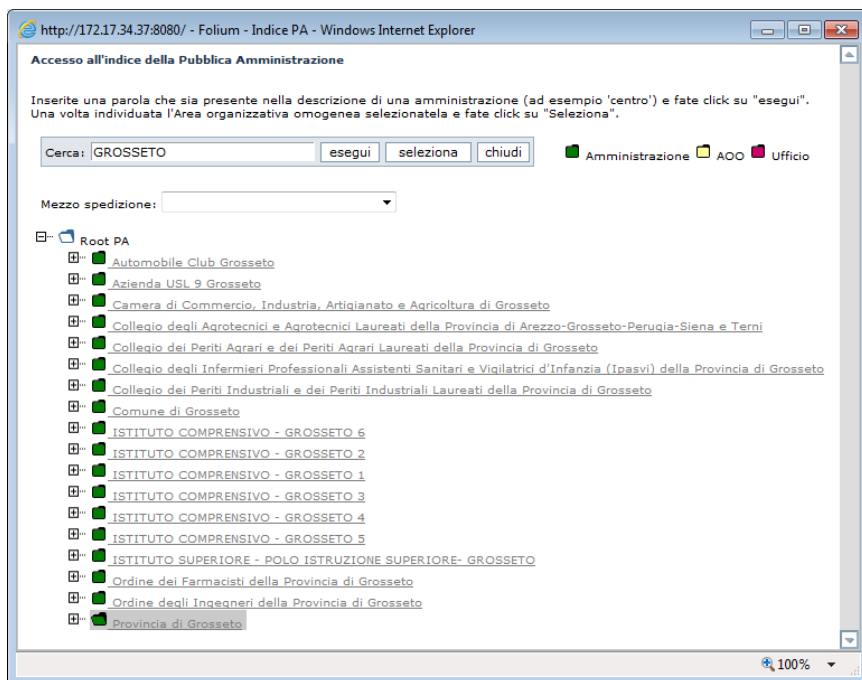
- 1 Agenzia delle Entrate
- 2 Regione Lombardia
- 3 Ministero del Lavoro e delle Politiche Sociali
- 4 Ministero dell'Istruzione, dell'Università e della Ricerca
- 5 Ministero della Salute
- 6 Ministero dell'Interno

10-04-15
Dal 31 Marzo 2015 la fatturazione elettronica è un obbligo verso tutta la pubblica amministrazione. Se non sai ancora entrare a far parte

27-04-15
Online da oggi il nuovo sito IPA. Ha una nuova linea grafica e un'organizzazione di contenuti più vicina ai non addetti ai lavori. La parola chiave è **semplicità**: una struttura

Approfondimento su "Indice PA"

Folium permette un accesso diretto a tale rubrica a partire dalla propria interfaccia utente, senza bisogno di accedere ad iPA attraverso l'interfaccia http.



Mittenti (E' necessario inserire almeno un mittente)



NB: nel caso il sistema non restituisse i dati attesi è probabile che si debba configurare il sistema introducendo le necessarie credenziali.


UTILIZZO: si inserisce la parola da ricercare e di clicca su "esegui"; dall'elenco dei risultati si **seleziona** la voce di interesse; si indica l'eventuale **mezzo di spedizione**; si aziona il pulsante "**selezione**". Il nominativo, l'indirizzo e la e-mail verranno inseriti automaticamente fra i mittenti o destinatari in Folium

Mittenti (E' necessario inserire almeno un mittente)

Denominazione	Indirizzo	Mezzo sped.	P.C.	Comandi
Provincia di Grosseto	Piazza Dante Alighieri, 35 Grosseto -	Posta Prioritaria	<input type="checkbox"/>	<input type="button" value="X"/> <input type="button" value="Print"/> <input type="button" value="Menu"/>

Rubrica persone fisiche

Rubrica Persone Fisiche



Cognome

Nome

Codice

Nessun nominativo trovato.

Se dal risultato della ricerca l'operatore individua il corrispondente desiderato, potrà selezionarlo, indicare il mezzo di spedizione (es. PEC) ed infine utilizzarlo.

Rubrica Persone Fisiche

Cognome

Nome

Codice

Mezzo spedizione

Nominativi trovati : 5

Selezione	Copia dati	Codice	Mittente	Email
<input type="checkbox"/>	<input type="checkbox"/>	GMBLSE	GAMBINO ELISA	MASSIMO.GAMBINO@CERT.LEGALMAIL.IT
<input checked="" type="checkbox"/>	<input type="checkbox"/>		GAMBINO IN ALICE MASSIMO	massimo.gambino@alice.it
<input type="checkbox"/>	<input type="checkbox"/>		GAMBINO IN DEDA massimo	massimo.gambino@dedagroup.it
<input type="checkbox"/>	<input type="checkbox"/>		GAMBINO MASSIMO	
<input type="checkbox"/>	<input type="checkbox"/>		GAMBINO MASSIMO IRO GABRIELE	massimo.gambino@cert.legalmail.it

Se, a seguito di ricerca, non si trova alcuna corrispondenza o se il corrispondente ricercato non è stato individuato, l'operatore (solo se abilitato a tale funzione) potrà effettuare l'inserimento di un nuovo nominativo attraverso il tasto "Nuovo".

Rubrica persone fisiche – aggiungi nominativo



Utente: Serena Bellagotti
Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [protocollatore ingresso \(+\)](#)

Area organizzativa: [AOPGRO \(p_gr\)](#)
Registro: [REGISTRO UFFICIALE](#)
Stato: **Uscita** - 25/08/2015

Protocollazione	Ricerca	Assegnazioni	Registri	Rubriche	Fascicoli	Utente
-----------------	---------	--------------	----------	----------	-----------	--------

Rubrica Persone

Inserire un criterio di ricerca

Criteri di ricerca

Nome:	<input type="text"/>	Cognome:	<input type="text"/>	Codice:	<input type="text"/>
Comune:	<input type="text"/>	Provincia:	<input type="text"/>		
Telefono:	<input type="text"/>	Email:	<input type="text"/>		
I primi	<input type="text" value="100"/>	Stampa in PDF:	<input type="checkbox"/>		



Utente: Serena Bellagotti
Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [protocollatore ingresso \(+\)](#)

Area organizzativa: [AOPGRO \(p_gr\)](#)
Registro: [REGISTRO UFFICIALE](#)
Stato: **Uscita** - 25/08/2015

Ver:
[Aiuto !](#)

Protocollazione	Ricerca	Assegnazioni	Registri	Rubriche	Fascicoli	Utente	Reports
-----------------	---------	--------------	----------	----------	-----------	--------	---------

Aggiungi nuovo nominativo nella rubrica delle persone

Codice:	<input type="text" value="20"/>
Nome:	<input type="text" value="40"/>
Cognome:	<input type="text" value="40"/>
Telefono:	<input type="text" value="16"/>
Fax:	<input type="text" value="16"/>
Codice fiscale:	<input type="text" value="16"/>
Note:	<input type="text" value="500"/>
Mezzo di spedizione default:	<input type="text"/>
Consenso alle regole di privacy per quanto riguarda l'utilizzo dell'e-mail: SI <input type="radio"/> NO <input type="radio"/>	

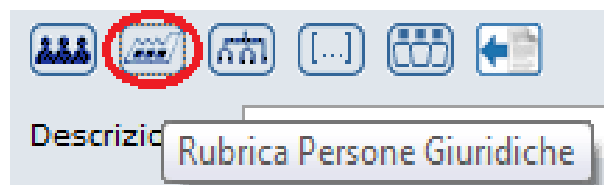
I campi con questo colore sono obbligatori.

Aggiungi nuovo indirizzo

Dug:	<input type="text" value="-"/>	Toponimo:	<input type="text"/>
Civico:	<input type="text" value="10"/>	Cap:	<input type="text" value="8"/>
Provincia:	<input type="text"/>	Comune:	<input type="text"/>
Telefono:	<input type="text" value="16"/>	Fax:	<input type="text" value="16"/>
Note indirizzo:	<input type="text" value="200"/>		

I campi con questo colore sono obbligatori.

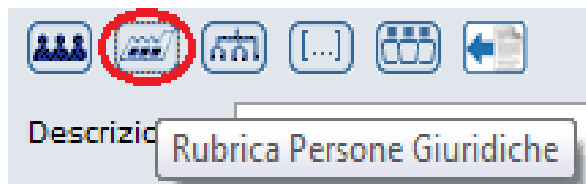
Rubrica persone giuridiche



Il comportamento è identico a quello della rubrica delle persone fisiche. Al nome ed al cognome si sostituisce la denominazione.

- Nella gestione delle Persone Giuridiche può essere attivata l'obbligatorietà di un codice specifico che, se necessario, potrà coincidere con la partita IVA della Persona Giuridica.
- Il sistema prevede:
 - Una maschera di ricerca da cui iniziare sempre le attività
 - Un modulo di inserimento del nominativo a cui può far seguito un ulteriore modulo per l'inserimento di indirizzi plurimi per lo stesso nominativo.

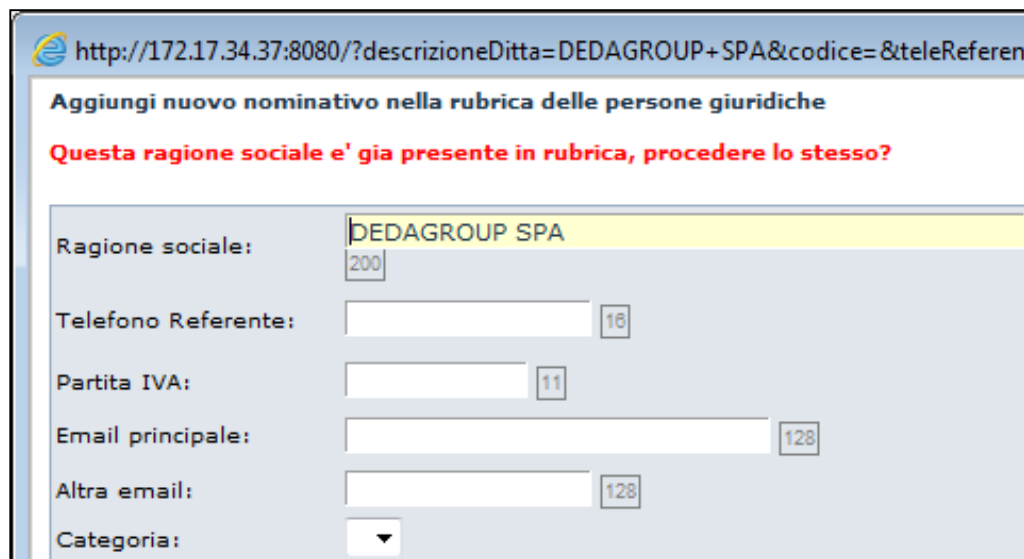
Rubrica persone giuridiche



- All'atto dell'inserimento di un nuovo nominativo nella rubrica il sistema è in grado di rilevare eventuali doppioni e, in questo caso, invia un messaggio di allerta!

Il controllo viene eseguito sono nel caso di identità fra nominativo presente

- e nominativo inserito.

A screenshot of a web browser window. The address bar shows a URL: http://172.17.34.37:8080/?descrizioneDitta=DEDAGROUP+SPA&codice=&teleReferen. The page content includes a heading "Aggiungi nuovo nominativo nella rubrica delle persone giuridiche" and a red warning message: "Questa ragione sociale e' gia presente in rubrica, procedere lo stesso?". Below the warning is a form with the following fields: "Ragione sociale:" with a dropdown menu showing "DEDAGROUP SPA" and a small box with "200"; "Telefono Referente:" with a text input field and a small box with "16"; "Partita IVA:" with a text input field and a small box with "11"; "Email principale:" with a text input field and a small box with "128"; "Altra email:" with a text input field and a small box with "128"; and "Categoria:" with a dropdown menu.

Rubriche con nominativi multipli



Utente: [Serena Bellagotti](#)
Ufficio: [SEGRETARIO/ DIRETTORE GENERALE \(+\)](#)
Ruolo: [protocollatore ingresso \(+\)](#)

Area organizzativa: [AOPGRO \(p_gr\)](#)
Registro: [REGISTRO UFFICIALE](#)
Stato: [Uscita - 25/08/2015](#)

Versi
[Aiuto](#) [H](#)

[Protocollo](#) [Ricerca](#) [Assegnazioni](#) [Registri](#) [Rubriche](#) [Fascicoli](#) [Utente](#) [Reports](#)

Rubrica Persone Giuridiche

Criteri di ricerca

Ragione sociale:	<input type="text" value="comunc di latina"/>	Codice:	<input type="text"/>	Categoria:	<input type="text"/>
Comune:	<input type="text"/>	Provincia:	<input type="text"/>		
Telefono:	<input type="text"/>	Email:	<input type="text"/>		
I Primi:	<input type="text" value="100"/>	Stampa in PDF:	<input type="checkbox"/>		

[Cerca](#) [Aggiungi](#) [Modifica](#) [Elimina](#)

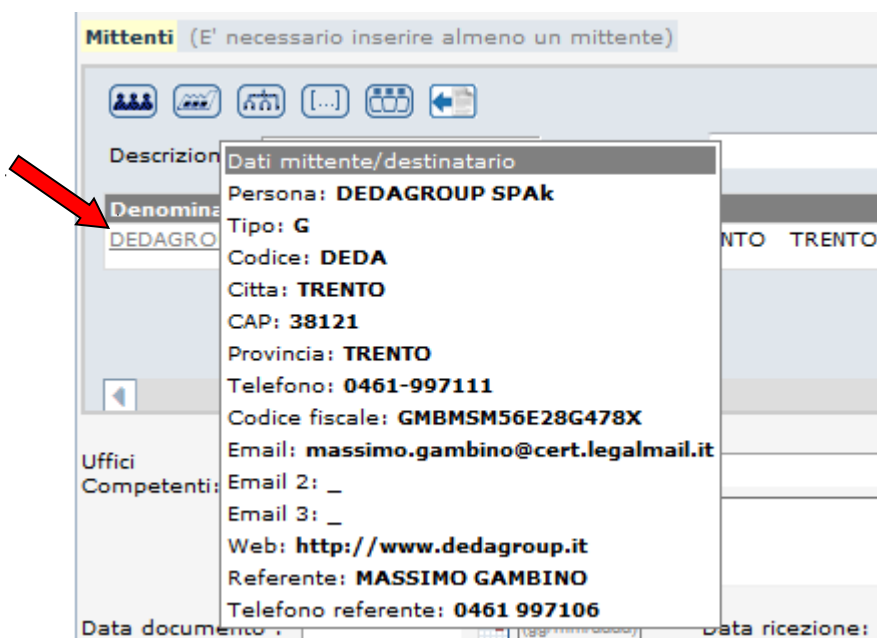
	<u>Codice</u>	<u>Ragione sociale</u>	<u>Referente</u>	<u>Partita IVA</u>	<u>Settore</u>	<u>Mezzo di spedizione</u>	<u>Email</u>	<u>Indirizzi</u>
<input type="checkbox"/>		COMUNE DI LATINA					URP@PEC.COMUNE.LATINA.IT	
<input checked="" type="checkbox"/>		COMUNE DI LATINA				POSTA PRIORITARIA		*LATINA

In caso di anagrafiche “sporche”, si possono selezionare dei nominativi con un flag e cliccare su Elimina.

Si consiglia di inserire e mantenere i nominativi con almeno la PEC di riferimento.

Inserimento dei nominativi da rubrica

Quando inseriamo nella maschera di protocollo un nominativo da una delle Rubriche, i dati presenti possono superare le capacità di visualizzazione della pagina. Per questo motivo è stata predisposta una funzionalità per cui, **sfiorando con il mouse** il mittente (o il destinatario) il sistema mostra tutti i metadati di dettaglio:



Approfondimento sulla Ricerca dei Documenti



Ricerche con ruolo operatore

Con il ruolo di **Operatore standard** si possono eseguire delle ricerche:



Utente: **Serena Bellagotti**
Ufficio: **SEGRETARIO/ DIRETTORE GENERALE (+)**
Ruolo: **operatore_standard (+)**

Area organizzativa: **AOOPGRO (p_gr)**
Registro:

Protocollazione	Ricerca	Assegnazioni	Registri	Rubriche	Fascicoli	Utente	Reports
	Numero/Data						
Quadro riassuntivo	Ultimi protocolli						
	In lavorazione						
Assegnazioni	Avanzata		Ultimi 60 giorni				
Restituite	Codice a barre		3				
	Ricerche salvate						
	Storico						
Comunicazioni	Ricevute PEC						
Nessuna comunicazi	Ricerca riversati						



Utente: **Serena Bellagotti**
Ufficio: **SEGRETARIO/ DIRETTORE GENERALE (+)**
Ruolo: **operatore_standard (+)**

Protocollazione	Ricerca	Assegnazioni	Registri
-----------------	---------	--------------	----------

Selezione documenti protocollati/registrati

La ricerca trova, per il registro selezionato, la protocollazione con lo specifico numero di protocollo nell'anno attuale se non diversamente specificato, altrimenti si può ricercare per data di protocollazione. E' importante specificare che se viene selezionata una data il campo 'Anno Registro' non viene considerato

Numero progressivo:

Anno Registro: oppure

Data: [gg/mm/aaaa]

Nome Registro:

Stampa in PDF:

Ordine decrescente:

Cerca

Ricerca per numero/data di protocollo



Ricerca avanzata – ruolo operatore



Utente: **Serena Bellagotti**
Ufficio: **SEGRETARIO/ DIRETTORE GENERALE (+)**
Ruolo: **operatore_standard (+)**

Area organizzativa: **AOOPGRO (p_gr)**
Registro:

Protocollo | Ricerca | Assegnazioni | Registri | Rubriche | Fascicoli | Utente


Selezione documenti

Dati protocollo	
Registro: REGISTRO UFFICIALE	Modalità: <input type="radio"/> interna <input type="radio"/> ingresso <input type="radio"/> uscita <input checked="" type="radio"/> tutti <input type="radio"/> registrazioni
Anno Registro: 2015 Oggetto*: <input type="text"/>	Mezzo di spedizione: <input type="text"/> <input type="checkbox"/> voci storicizzate
Tipo documento: <input type="text"/>	
Mittente Destinatario	
Codice: <input type="text"/> Cognome Nome*: <input type="text"/>	E-mail: <input type="text"/>
Indirizzo: <input type="text"/> Provincia: <input type="text"/>	Comune: <input type="text"/>
Altri dati	
Solo documenti dell'ufficio corrente <input type="checkbox"/>	Non spediti: <input type="checkbox"/>
Data da: <input type="text"/> (gg/mm/aaaa)	a: <input type="text"/> (gg/mm/aaaa)
Data Documento da: <input type="text"/> (gg/mm/aaaa)	a: <input type="text"/> (gg/mm/aaaa)
Data Ricezione/Spedizione da: <input type="text"/> (gg/mm/aaaa)	a: <input type="text"/> (gg/mm/aaaa)
Data Scadenza da: <input type="text"/> (gg/mm/aaaa)	a: <input type="text"/> (gg/mm/aaaa)
N Progressivo dal: <input type="text"/>	al: <input type="text"/>
Numero prot esterno: <input type="text"/>	Note: <input type="text"/>
Codice Titolare: <input type="text"/>	Collocazione: <input type="text"/>
01 Atti fondamentali e Organi 02 Organizzazione generale e rapporti istituzionali	<input type="checkbox"/> Visualizza voci storicizzate

Per chi è
attribuito su
più di un
ufficio,
assicurarsi
sempre di
essere
sull'ufficio
competente
rispetto alla
ricerca che si
vuole eseguire.

Ricerche con ruolo *utente*

Con il ruolo di **Utente standard** si possono eseguire delle ricerche:



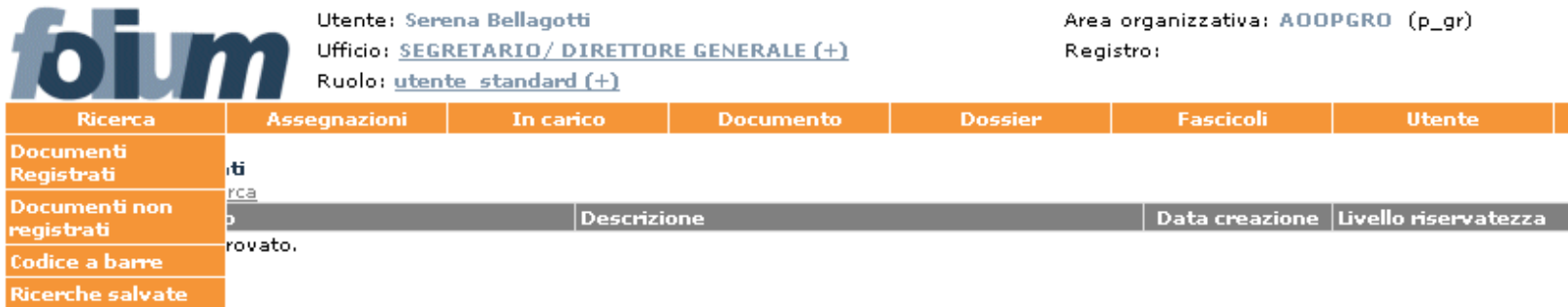
The screenshot shows the FOLium interface. At the top left is the 'folium' logo. To its right, user information is displayed: 'Utente: Serena Bellagotti', 'Ufficio: SEGRETARIO/ DIRETTORE GENERALE (+)', and 'Ruolo: utente standard (+)'. On the right side, organizational details are shown: 'Area organizzativa: A00PGRO (p_gr)' and 'Registro:'. Below this is a navigation menu with seven items: 'Ricerca', 'Assegnazioni', 'In carico', 'Documento', 'Dossier', 'Fascicoli', and 'Utente'. A red arrow points to the 'Ricerca' menu item, which has opened a dropdown list containing: 'Documenti Registrati', 'Documenti non registrati', 'Codice a barre', and 'Ricerche salvate'. Below the menu is a table header with columns: 'Descrizione', 'Data creazione', and 'Livello riservatezza'.

Tramite la voce di menu Ricerca >>> **Documenti Registrati** (protocollati) è possibile accedere alla funzione di ricerca di documenti registrati dall'Operatore di protocollo nelle diverse tipologie di Registri dell'AOO.

Documenti registrati: ricerca di documenti protocollati nelle diverse tipologie di Registro (corrispondenza/interno) e già fascicolati in un fascicolo su cui l'Utente documentale possiede i diritti di visibilità.

Ricerche con ruolo *utente*

Con il ruolo di **Utente standard** si possono eseguire delle ricerche:



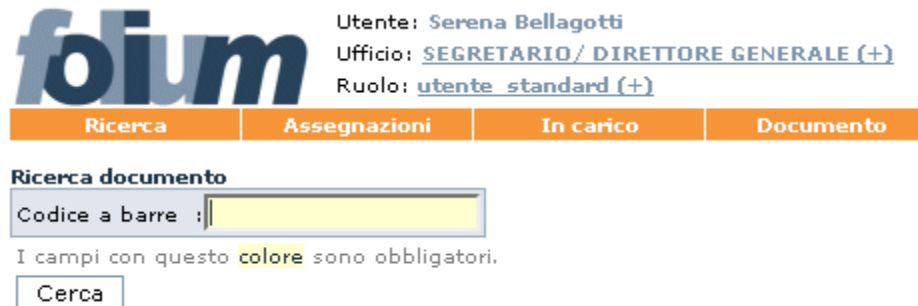
The screenshot shows the FOIUM system interface. At the top left is the 'foium' logo. To the right, user information is displayed: 'Utente: Serena Bellagotti', 'Area organizzativa: A00PGRO (p_gr)', 'Ufficio: SECRETARIO/ DIRETTORE GENERALE (+)', and 'Registro:'. Below this is a navigation menu with orange tabs: 'Ricerca', 'Assegnazioni', 'In carico', 'Documento', 'Dossier', 'Fascicoli', and 'Utente'. The 'Ricerca' tab is active, and a red arrow points to a sub-menu on the left containing: 'Documenti Registrati', 'Documenti non registrati', 'Codice a barre', and 'Ricerche salvate'. The 'Documenti non registrati' option is highlighted. Below the menu, a table header is visible with columns: 'Descrizione', 'Data creazione', and 'Livello riservatezza'.

Tramite la voce di menu Ricerca >>> **Documenti non registrati** è possibile accedere alla funzione di ricerca di documenti (non protocollati) inseriti in un fascicolo dall'Utente documentale tramite la funzione di Upload.

I documenti possono essere ricercati in base al *nome del file*, alla sua *descrizione* o al suo *contenuto*.

Ricerche per codice a barre

Consente di effettuare la ricerca di un protocollo in Registro, tramite l'inserimento nell'apposito campo del suo codice a barre generato automaticamente dal sistema.



folium Utente: [Serena Bellagotti](#)
Ufficio: [SEGRETARIO / DIRETTORE GENERALE \(+\)](#)
Ruolo: [utente_standard \(+\)](#)

Ricerca	Assegnazioni	In carico	Documento
---------	--------------	-----------	-----------

Ricerca documento

Codice a barre :

I campi con questo colore sono obbligatori.

Ricerca documenti in carico

Menù In carico, Elenco in carico



Utente: Serena Bellagotti
Ufficio: SEGRETARIO/ DIRETTORE GENERALE (+)
Ruolo: utente_standard (+)

Area organizzativa: /
Registro:

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli
---------	--------------	-----------	-----------	---------	-----------

Cerca documenti in carico

Data assegnazione dal : (gg/mm/aaaa) Al (gg/mm/aaaa)

Data presa in carico dal : (gg/mm/aaaa) Al (gg/mm/aaaa)

Numero protocollo: Oggetto:

Codice Titolare:

- 01 Atti fondamentali e Organi
- 02 Organizzazione generale e rapporti istituzionali
- 03 Risorse informative
- 04 Personale
- 05 Risorse finanziarie e bilancio
- 06 Patrimonio, Economato e risorse strumentali
- 07 Programmazione e pianificazione territoriale
- 08 Attività produttive
- 09 Ambiente e Conservazione della natura
- 10 Attività Lavori e Servizi pubblici
- 11 Istruzione, cultura, politiche sociali, PO e sport
- 12 Formazione professionale

**Maschera
di ricerca**

Ricerca documenti in carico



Utente: **Serena Bellagotti**
Ufficio: **SEGRETARIO / DIRETTORE GENERALE (+)**
Ruolo: **utente_standard (+)**

Area organizzativa: **AOPGRO (p_gr)**
Registro:

[Aiù!](#)

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente	
---------	--------------	-----------	-----------	---------	-----------	--------	--

Elenco documenti in carico

1 - 1 | [tc](#)

	Registro	Mod.	Num.	Oggetto	Mitt/Dest	Assegnatario	Assegnazione	Preso in carico	Note	Pri.	Operazioni
<input type="checkbox"/>	REGISTRO UFFICIALE	I	2415	POSTA CERTIFICATA: AVCP - Assolvimento degli obblighi di trasmissione e PUBBLICAZIONE - scadenza 31 Gennaio 2014.	certificata@pec.italsoft-mc.it ;	Bellagotti Serena	22/01/2014	22/01/2014		!	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Ricerca fascicoli

(è possibile utilizzare chiavi parziali di ricerca utilizzando il carattere speciale *)

Nome:	<input type="text"/>	64	Descrizione:	<input type="text"/>	512
Responsabile:	<input type="text"/>	50	Stato:	<input type="text"/>	
Data Apertura dal:	<input type="text"/>	(gg/mm/aaaa)	Data Apertura al:	<input type="text"/>	(gg/mm/aaaa)
Data Chiusura dal:	<input type="text"/>	(gg/mm/aaaa)	Data Chiusura al:	<input type="text"/>	(gg/mm/aaaa)
Data Scadenza dal:	<input type="text"/>	(gg/mm/aaaa)	Data Scadenza al:	<input type="text"/>	(gg/mm/aaaa)
Codice titolare :	<input type="text"/>	20			
Anno:	<input type="text"/>	N° repertorio da:	<input type="text"/>	a:	<input type="text"/>
PIVA/Codice fiscale	<input type="text"/>	512	<input type="checkbox"/>	Ricerca nel sottoalbero	
N° fascicolo	<input type="text"/>	12	<input type="checkbox"/>	solo fascicoli di questo ufficio	
Collocazione	<input type="text"/>	128			
Visualizzazione:	lista	<input checked="" type="radio"/>	albero	<input type="radio"/>	

Attenzione : la ricerca restituirà solo i fascicoli per i quali si possiede almeno il permesso di scrittura.

Ricerca documenti conclusi

Con il ruolo di **Utente standard** si possono eseguire delle ricerche anche per quanto concerne i documenti conclusi:



Utente: **Serena Bellagotti**
Ufficio: **SECRETARIO / DIRETTORE GENERALE (+)**
Ruolo: **utente standard (+)**

Area organizzativa: **ADOPGRO (p_gr)**
Registro:

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
Documenti selezionati Torna ai criteri di ricerca		Elenco in carico				
Percorso documento		Elenco documenti conclusi				
Nessun documento trovato.						

Ricerca documenti conclusi



Utente: **Serena Bellagotti**
Ufficio: **SECRETARIO / DIRETTORE GENERALE (+)**
Ruolo: **utente standard (+)**

Area organizzativa: **AOOPGRO (p_gr)**
Registro:

Ricerca	Assegnazioni	In carico	Documento	Dossier	Fascicoli	Utente
---------	--------------	-----------	-----------	---------	-----------	--------

Elenco documenti conclusi

Data dal : (gg/mm/aaaa) Al (gg/mm/aaaa)
Numero protocollo: Oggetto:
Codice Titolare:
Collocazione:

- 01 Atti fondamentali e Organi
- 02 Organizzazione generale e rapporti istituzionali
- 03 Risorse informative
- 04 Personale
- 05 Risorse finanziarie e bilancio
- 06 Patrimonio, Economato e risorse strumentali
- 07 Programmazione e pianificazione territoriale
- 08 Attività produttive
- 09 Ambiente e Conservazione della natura
- 10 Attività Lavori e Servizi pubblici
- 11 Istruzione, cultura, politiche sociali, PO e sport
- 12 Formazione professionale

	Registro	Num.	Oggetto	Mitt/Dest	Assegnatario	Preso in carico	Data conclusione
<input type="checkbox"/>	REGISTRO UFFICIALE	168074	<u>(DOCUMENTO ANNULLATO)</u>		Bellagotti Serena	01/10/2013	22/05/2014

Conservazione digitale



Conservazione digitale

Con il **DPCM 3 dicembre 2013** sul sistema di conservazione si assiste all'introduzione del:

- **“Sistema di conservazione” logicamente distinto dal “Sistema di gestione documentale”**
- **Responsabile della conservazione - Rdc**
- **Manuale della conservazione - Mdc**

Normativa

Art. 43 e 44
CAD

**Conservazione
obbligatoria dei
doc. e requisiti
per la
conservazione**

DPCM 3
dicembre
2013

**Regole tecniche
sulla
conservazione
dei doc.
informatici**

La
conservazione
digitale è un
obbligo?

Cosa prevede
la normativa?

DPCM 13
novembre
2014

**Regole tecniche
sulla formazione e
gestione dei doc.
informatici**

Regolamento
2014/910/UE
(eIDAS)

**Doc. elettronico è
qualsiasi contenuto
conservato in forma
elettronica**

art. 44 CAD

- ✓ Individua gli obiettivi del sistema di conservazione
- ✓ Obbliga l'ente a nominare un proprio Responsabile della conservazione

DPCM 3
dicembre 2013

- ✓ Descrive il Sdc, definendo:
 - le fasi del processo
 - i soggetti coinvolti
 - i modelli organizzativi
 - i compiti del Rdc
- ✓ Impone alle PA, anche in caso di affidamento all'esterno, di designare come proprio Rdc un dirigente o un funzionario

DPCM 13
novembre 2014

- ✓ Indica le tipologie di oggetti da inviare in conservazione (documenti, fascicoli, aggregazioni documentali, registri, repertori informatici)

Quali sono le principali indicazioni dei riferimenti normativi?

Conservazione



Cartaceo

Archivio

Digitale



Cosa è la conservazione sostitutiva

E' una **procedura** (legale e informatica) regolamentata dalla normativa, **in grado di garantire nel tempo la validità legale di un documento informatico**, inteso come una *rappresentazione di atti o fatti e dati su un supporto sia esso cartaceo o informatico* (Delibera CNIPA 11/2004).

-
- Essa consente di **risparmiare sui costi di stampa, stoccaggio e archiviazione.**

Conservare digitalmente significa sostituire i doc. cartacei con l'equivalente doc. in formato digitale che viene “bloccato” (nella forma, contenuto e tempo) attraverso la **firma digitale** e la **marca temporale**.



Ecosistema della gestione doc. informatici



Cosa è la conservazione sostitutiva

Proteggere nel tempo gli archivi digitali prodotti dalle PA, *impedendone il danneggiamento, la perdita o la distruzione.*



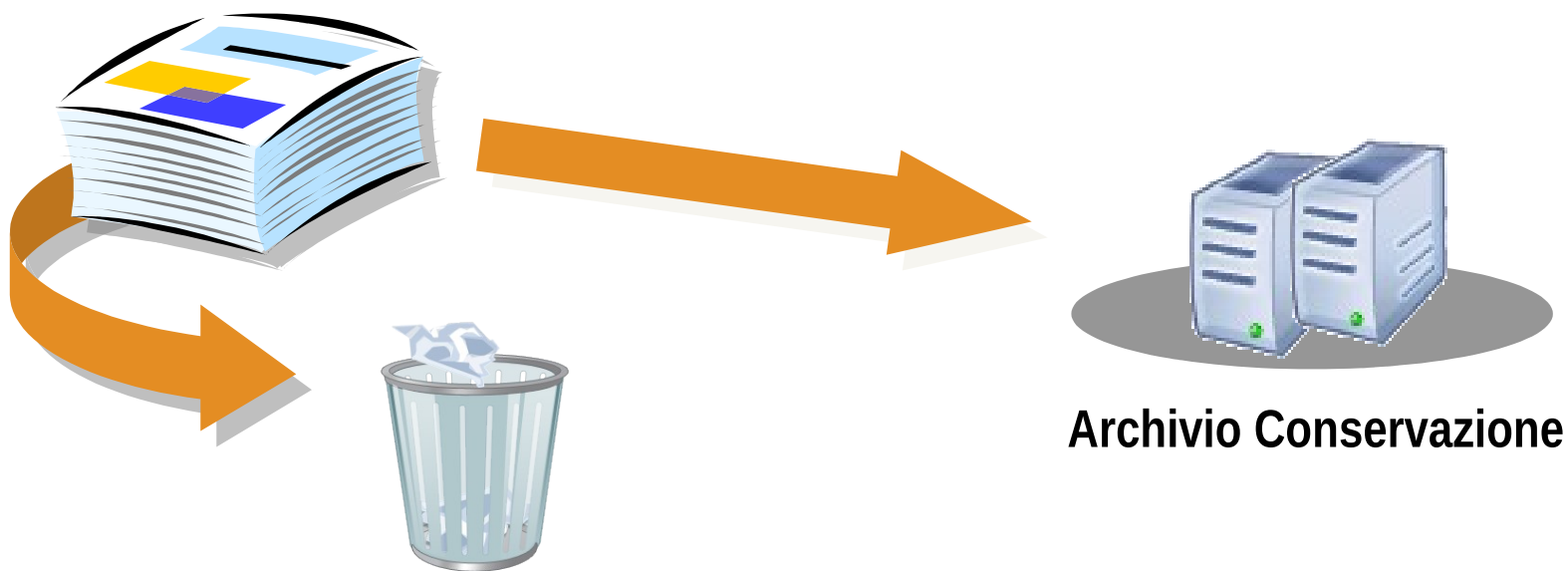
Consentire l'accesso *controllato* a dati, doc. e informazioni e la diffusione degli stessi per fini amm.vi e di ricerca; **tutelare e valorizzare la memoria storica.**

Garantire **autenticità, integrità, leggibilità, reperibilità**

Predisporre idonee misure per la qualità e la sicurezza fisica, logica e tecnologica dei sistemi.

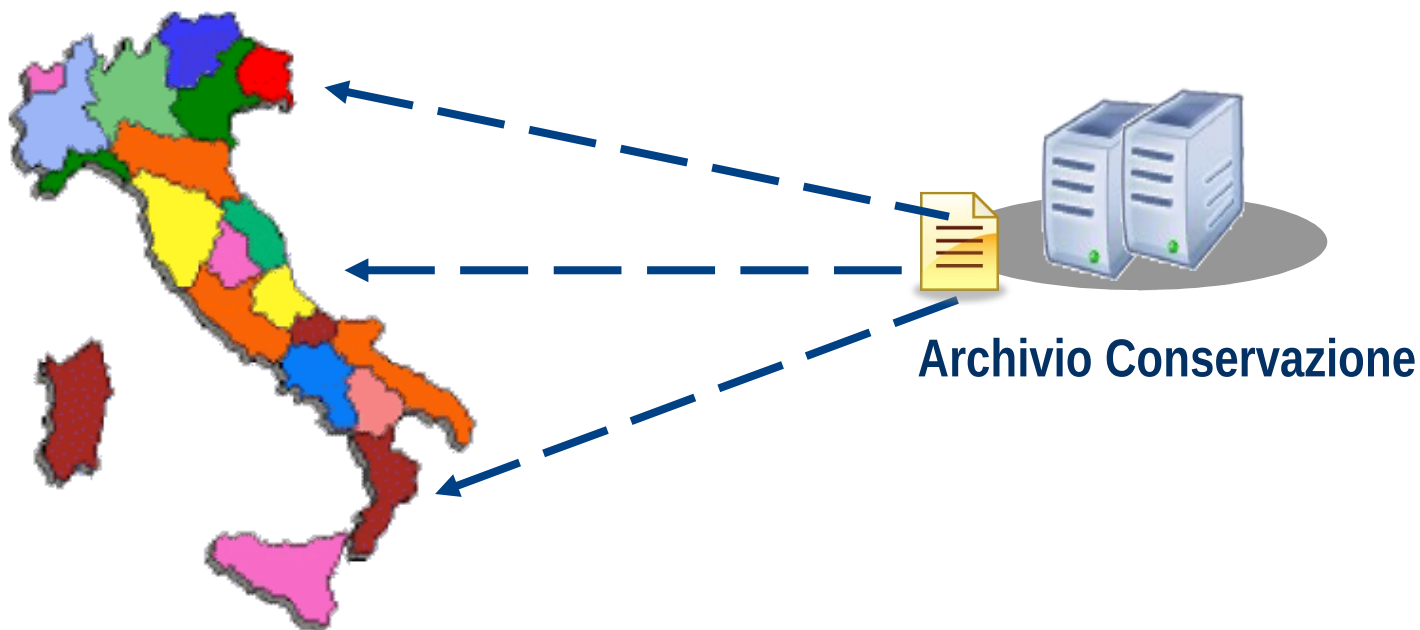
dei

Eliminazione spazi di archivio



Archivio Conservazione

Accesso distribuito ai dati



La consultazione documentale è svincolata da luogo e dal tempo

Dalla conservazione cartacea a quella digitale

- **Riduzione degli spazi** di conservazione dei doc.
- Notevole **risparmio cartaceo**
- **Abbattimento dei costi "nascosti" di gestione**
- **Accessibilità e Velocità di ricerca** dei documenti a distanza
- **Integrità** dei documenti
- **Sicurezza**
- **Leggibilità** dei doc. anche a distanza di tempo

Sistema di conservazione (Sdc)

Art. 44 del Codice amministrazione digitale - CAD

Requisiti per la conservazione dei documenti informatici:

1. Il sistema di conservazione dei documenti informatici assicura :
 - a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'AOO di riferimento di cui all'articolo 50, comma 4, del DPR 445/2000
 - b) l'integrità del documento
 - c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari
 - d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del D.lgs 196/2003 e dal suo disciplinare tecnico pubblicato in All. B

Sistema di conservazione (Sdc)

1-bis. Il Sistema di conservazione è gestito da un **Responsabile** che opera d'intesa con il **Resp. del trattamento dei dati personali** di cui all'art 29 del D.lgs n. 196/2003 , e, ove previsto, con il **Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi** di cui all'articolo 61 del DPR 445/2000, nella definizione e gestione delle attività di rispettiva competenza.

1-ter. Il Rdc **può chiedere la conservazione dei doc. informatici** o la certificazione della conformità del relativo processo di conservazione **ad altri soggetti (pubblici o privati)** che offrono idonee garanzie organizzative e tecnologiche. (vedi art. 44 bis Conservatori accreditati).

Quali sono i modelli possibili per le PA?

In house

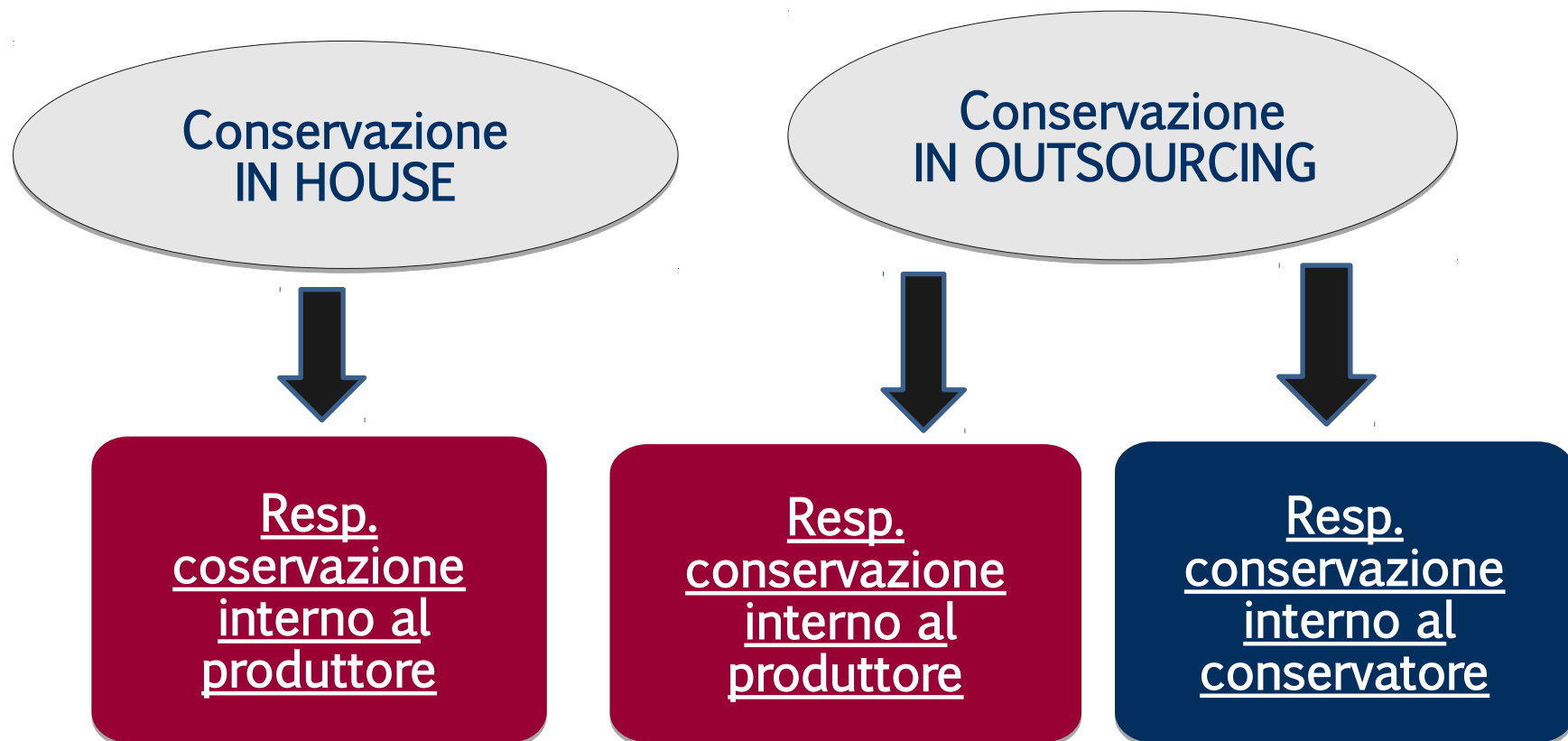
La conservazione è svolta all'interno della struttura organizzativa

Outsourcing

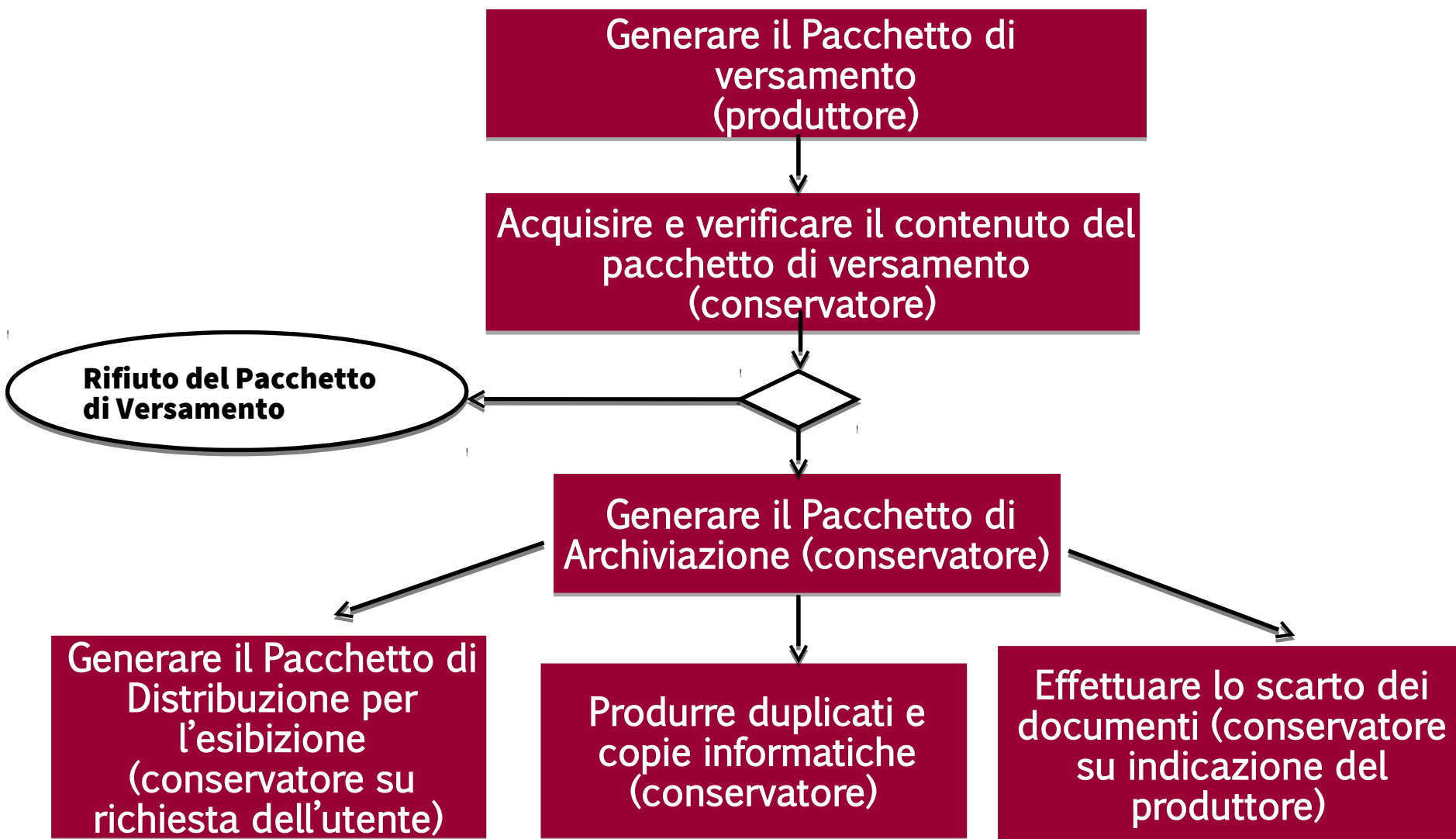
La conservazione è affidata ai conservatori accreditati inseriti nell'elenco AGID

In house o in outsourcing, il sistema di conservazione deve rispettare le Regole tecniche del DPCM 3 dicembre 2013

Quali sono le figure professionali previste?



Il conservatore come si rapporta con il soggetto produttore e l'utente finale?



Soggetti coinvolti nel processo di conservazione

Art. 6 DPCM 3 dicembre 2013

Regole tecniche in materia di sistema di conservazione



Soggetti coinvolti nel processo di conservazione

- **Produttore:** persona fisica o giuridica che trasmette i documenti da conservare mediante pacchetti di versamento. (Nelle PA solitamente si identifica con il Responsabile della gestione documentale).
- **Responsabile della Conservazione:** definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato.
- **Utente:** persona fisica o giuridica che richiede l'accesso ai documenti presenti nel sistema di conservazione al fine di acquisire dati, documenti e informazioni.

Quali sono le attività di competenze del **Produttore**?

- Concordare con il conservatore gli elementi contenuti nel manuale di conservazione (**tipologie documentali, tempi di versamento e conservazione**, formati e metadati descrittivi)
- Definire le **modalità di colloquio con il conservatore** e di generazione del Pacchetto di versamento
- **Produrre il Pacchetto di versamento** contenente i documenti e i relativi metadati descrittivi
- **Inviare il Pacchetto di versamento al conservatore e verificare l'esito della procedura di trasferimento** (accettazione o rifiuto)

Responsabile della Conservazione



**Responsabile
Conservazione**



Responsabile della Conservazione

Art. 7 DPCM 3 dicembre 2013

Regole tecniche in materia di sistema di conservazione

Comma 1. Il Responsabile della conservazione (Rdc) opera d'intesa con il Resp. del trattamento dei dati personali, con il Resp. della sicurezza e con il Resp. dei sistemi informativi che, nel caso delle pubbliche amm.ni centrali, coincide con il Resp. dell'ufficio di cui all'art. 17 del Codice, oltre che con il Resp. della gestione documentale, per quanto attiene alle pubbliche amministrazioni.

In particolare il Rdc:

- a) definisce le caratteristiche e i requisiti del Sistema di conservazione (Sdc) in funzione della tipologia dei doc. da conservare;
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformita' alla normativa vigente;

Responsabile della Conservazione

- c) genera il rapporto di versamento, secondo le modalita' previste dal Mdc;
- d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e) effettua il monitoraggio della corretta funzionalita' del Sdc;
- f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrita' degli archivi e della leggibilita' degli stessi;
- g) al fine di garantire la conservazione e l'accesso ai documenti, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalita'; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale

Responsabile della Conservazione

- i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;
- j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- m) predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Responsabile della Conservazione

Comma 2. Ai sensi dell'art. 44, comma 1-ter, del Codice, il Rdc e le PA possono chiedere di certificare la conformita' del processo di conservazione a soggetti, pubblici o privati che offrano idonee garanzie organizzative e tecnologiche, ovvero a soggetti a cui e' stato riconosciuto il possesso dei requisiti di cui all'art. 44-bis, comma 1, del Codice, distinti dai conservatori o dai conservatori accreditati.

Comma 3. Nelle pubbliche amministrazioni, il ruolo del Rdc e' svolto da un dirigente o da un funzionario formalmente designato.

Comma 4. Nelle pubbliche amministrazioni, il ruolo di Rdc puo' essere svolto dal responsabile della gestione documentale ovvero dal coordinatore della gestione documentale, ove nominato.

Formati indicati per la Conservazione

La scelta dei formati idonei alla conservazione oltre al soddisfacimento delle caratteristiche di:

- *apertura*
- *sicurezza*
- *portabilità*
- *funzionalità*
- *supporto allo sviluppo*
- *diffusione*

deve essere strumentale a che il documento assuma le caratteristiche di *immodificabilità* e di *staticità* previste dalle regole tecniche.

<http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione>

Formati indicati per la Conservazione

- *PDF - PDF/A*
- *TIFF*
- *JPG*
- *Office Open XML (OOXML)*
- *Open Document Format*
- *XML*
- *TXT*
- *Formati Messaggi di posta elettronica*



La nuova funzione di **gestione dei formati ammessi** viene resa disponibile per consentire agli enti di poter vincolare la propria gestione documentale esclusivamente ai formati desiderati.

- (E' utilizzabile solo dall'**Amministratore** e quanto impostato ricade pertanto sull'intero ente).
- Per attivarla è necessario **valorizzare a 1 la proprietà "Gestione formati"**, impostabile nella sezione Applicazione > Configurazione, e **attivare il permesso applicativo "Gestione formati"** per il ruolo Amministratore.
- La nuova funzione consente di specificare quali formati di documento sono ammessi in Folium e quali anche per l'invio in conservazione e per la firma digitale.
- Per accedere alla nuova sezione è necessario selezionare il **menu**

Gestione formati

consente di rendere immediatamente attive le modifiche apportate

RUIMI Ruolo: [amministratore \(+\)](#)

Organizzazione | Applicazione | Pratiche Estese | Documenti Estesi | **Formati** | Eventi

Gestione formati

1 - 36 | totale: 36

	Descrizione	Formato	Ammesso in Folium	Ammesso Conservazione	Ammesso alla firma
<input type="checkbox"/>	bmp	BMP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	MS Word	DOC	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	MS Word	DOCX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Email	EML	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	gif	GIF	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	htm	HTM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	tsd	TSD	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	tsr	TSR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	txt	TXT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	wfm	WFM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	xls	XLS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	xlsx	XLSX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	xml	XML	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Manuale di conservazione

Documento informatico obbligatorio, **art. 8 del DPCM 3 dicembre 2013.**



Manuale di conservazione

1. Il **Manuale di conservazione** illustra l'**organizzazione**, i **soggetti coinvolti** e i **ruoli svolti** dagli stessi, il modello di funzionamento, la **descrizione del processo**, la descrizione delle architetture e delle infrastrutture utilizzate, le **misure di sicurezza adottate**.

2. Il **Manuale di conservazione** e' un **doc. informatico** che riporta, almeno:
- a) i dati dei soggetti che nel tempo hanno assunto la Responsabilita' del Sdc, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
 - b) la struttura organizzativa comprensiva delle funzioni, delle responsabilita' e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
 - c) la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;

Manuale di conservazione

- d) la descrizione delle modalita' di presa in carico di uno o piu' pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- f) la modalita' di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- g) la descrizione del Sistema di conservazione, comprensivo di tutte le componenti tecnologiche e delle procedure di gestione e di evoluzione delle medesime;

Manuale di conservazione

- h) la descrizione delle procedure di monitoraggio della funzionalità del Sdc e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- i) la descrizione delle procedure per la produzione di duplicati o copie;
- j) i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione;
- k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi dove è previsto il suo intervento;
- l) le normative in vigore nei luoghi dove sono conservati i documenti.

Conservazione Digitale con Folium - Enerj

folium

Userid:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="Login"/>

Conservazione Digitale Folium – Enerj

E' necessario attivare il modulo di conservazione (attività sistemistica)

Menù Conservazione



Utente: **Serena Bellagotti**
Ufficio: **Aoo (+)**
Ruolo: **amministratore di aoo (+)**

Area organizzativa: **AOO_serena** (TEST)
Registro:

Gestione documenti da conservare

Organizzazione Registri Titolare Documentale Rubriche Eventi Applicazione Comunicazioni Conservazione

Da inviare
Gestione feedback
Pacchetti generati

Lista Aree Organizzative

Codice - Nome	Email Responsabile	Letture Posta	Stato	Comandi
AOO_serena - AOO_Serena		Disattiva	■	

Folium la soluzione globale per il protocollo, la gestione documentale ed i procedimenti.
© Dedagroup SPA 2001-2015

L'amministratore di AOO e, se abilitato, l'**Operatore** potranno visualizzare ed operare su un nuovo menù, quello della **Conservazione**.

Conservazione – da inviare



Permette di accedere al modulo di selezione massiva.



Utente: **Serena Bellagotti**
Ufficio: **Aoo (+)**
Ruolo: **amministratore di aoo (+)**

Area organizzativa: **AOO_serena (TEST)**
Registro:



Ricerca documenti da conservare

Data protocollo * da (gg/mm/aaaa) a (gg/mm/aaaa)

Registro *

Formato Solo firmati Solo email

Modalità interna ingresso uscita tutti registrazioni

Protocollatore

Mezzo di spedizione voci storicizzate

Tutti i documenti Seleziona documenti completi

Significa tutti i protocolli e loro allegati anche senza firma digitale.

NB: Tale opzione rileva tutti i documenti associati ai protocolli o alle registrazioni individuati nelle date e nel registro specificati (documenti originali, documenti principali e allegati). La ricerca non prevede la verifica della presenza di firma sui documenti.

Conservazione – da inviare

Una volta che si è impostato i **parametri di ricerca** e si è cliccato su **Cerca**, il sistema ci restituisce i documenti. Questi ultimi possono essere o inviati massivamente tutti in conservazione oppure solo quelli selezionati.

ata protocollo * da a

registro *

formato Solo firmati Solo email

modalità interna ingresso uscita tutti registrazioni

protocollore

mezzo di spedizione voci storicizzate

filtri i documenti Seleziona documenti completi

**NB: Tale opzione rileva tutti i documenti associati ai protocolli o alle registrazioni individuati nelle date e nel registro specificati (documenti originali, documenti principali e allegati).
La ricerca non prevede la verifica della presenza di firma sui documenti.**

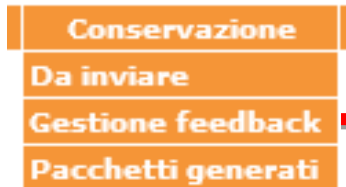
1 - 9 | totale: 9

<input type="checkbox"/>	N.	N. protocollo	Data protocollo	Modalità	Mittente/Destinatari	Oggetto	Tipo file	Nome	Descrizione	Firmato
<input type="checkbox"/>	1	1743	08/09/2015	USCITA	destinatario	oggetto	Allegato	email_31552.eml	RICEVUTA ACCETTAZIONE del messaggio inviato a: ilaria.cereser@dedagroup.it;	No
<input type="checkbox"/>	2	1777	17/09/2015	INGRESSO	pec2 dest - TRENTO	POSTA CERTIFICATA: test mail bergamo	Documento originale	3971_proto_email_09520-134-15-PIA_Sollecito AUA SIR. CO.pdf.p7m		Si
<input type="checkbox"/>	3	1777	17/09/2015	INGRESSO	pec2 dest - TRENTO	POSTA CERTIFICATA: test mail bergamo	Allegato	messaggio-originale.eml	Allegato del messaggio di posta	No
<input type="checkbox"/>	4	1797	25/09/2015	INGRESSO	Info.Promozione_noreply@libero.it	RC Auto a partire da 206 euro, scopri	Allegato	messaggio-originale.eml	Allegato del messaggio di posta	No

Per ricercare le fatture: ricercare protocollatore "ESB" oppure "fatturazione" (a seconda di quello che si è inserito in Folium).



Conservazione – Gestione feedback



Permette di verificare lo stato dei documenti da conservare. c



Utente: **Serena Bellagotti**
Ufficio: **Direzione Generale Affari Generali (+)**
Ruolo: **amministratore di aoo (+)**

Organizzazione Registri Titolare Documentale Rubr

Ricerca documenti non correttamente inviati alla conservazione - Gestione feedback

Tipo pacchetto:

Numero pacchetto:

Intervallo numeri di protocollo
Dal: Al:

Intervallo date di protocollo/stampa registro
Dal: (gg/mm/aaaa) Al: (gg/mm/aaaa)

Intervallo date di invio in conservazione
Dal: (gg/mm/aaaa) Al: (gg/mm/aaaa)

Utente richiesta esportazione:

Stato documento:

Codice errore:

Registro:

Ad oggi abbiamo due tipologie di pacchetto: **PROTO** e **RGP** (registro giornaliero di protocollo)

- Con errori (stati 2, 4, 6)
- Da Esportare (stato 0)
- Esportato Correttamente (stato 1)
- Non Esportato (stato 2)
- Archiviato Correttamente (stato 3)
- Non Archiviato (stato 4)
- Conservato Correttamente (stato 5)
- Non Conservato (stato 6)

Cerca

Conservazione – Gestione feedback

Ricerca documenti non correttamente inviati alla conservazione - Gestione feedback

Tipo pacchetto:

Numero pacchetto:

Intervallo numeri di protocollo

Dal: Al:

Intervallo date di protocollo/stampa registro

Dal: (gg/mm/aaaa) Al: (gg/mm/aaaa)

Intervallo date di invio in conservazione

Dal: (gg/mm/aaaa) Al: (gg/mm/aaaa)

Utente richiesta esportazione:

Stato documento:

Codice errore:

Registro:

Cerca

Re-invio

Seleziona Tutti

Deseleziona Tutti

Con questa ricerca si verificano eventuali documenti in stato di errore. A seconda dei casi si può operare il re-invio dei documenti alla conservazione.

1 - 25 | totale: 81

1 | 2 | 3 | 4

Successivi

	Numero protocollo	Tipo	Nome documento	Numero pacchetto	Stato documento	Data richiesta esportazione	Utente richiesta esportazione	Data esportazione	Data archiviazione	ID documento	Note
<input type="checkbox"/>	1452	Documento originale	3511_3-REG-1434099519169-test.pdf		Non Esportato	08/07/2015	Rosa Daniele				Documento non trovato.
<input type="checkbox"/>	1451	Allegato	IT01234567890_42359_EC_001.xml		Non Esportato	08/07/2015	Rosa Daniele				Documento non trovato.
<input type="checkbox"/>	1451	Allegato	IT01234567890_42359.xml		Non Esportato	08/07/2015	Rosa Daniele				Documento non trovato.

Conservazione – Pacchetti generati

Questo tasto permette di visualizzare il report sui pacchetti/volumi generati. E' un **cruscotto riepilogativo**.

- Conservazione
- Da inviare
- Gestione feedback
- Pacchetti generati

Elenco pacchetti di archiviazione generati

Tipo pacchetto: PROTO
RGP

Elenco pacchetti di archiviazione generati

Tipo pacchetto: PROTO



N. pacchetto	Tipo pacchetto	Data invio	N. documenti da esportare	N. documenti Esportati	N. documenti non esportati	N. documenti archiviati	N. documenti non archiviati	N. documenti conservati	N. documenti non conservati	Operazioni
	PROTO	11/12/2014	27	0	77	0	4	0	0	
43	PROTO	29/09/2015	0	1	0	0	0	0	0	
42	PROTO	29/09/2015	0	3	0	0	0	0	0	
41	PROTO	16/09/2015	0	7	0	0	0	0	0	
40	PROTO	29/07/2015	0	120	0	0	0	0	0	
37	PROTO	08/07/2015	0	7	0	0	0	0	0	
36	PROTO	08/07/2015	0	13	0	0	0	0	0	
35	PROTO	08/07/2015	0	9	0	0	0	0	0	
34	PROTO	08/07/2015	0	12	0	0	0	0	0	
33	PROTO	08/07/2015	0	1	0	0	0	0	0	
32	PROTO	01/07/2015	0	5	0	0	0	0	0	
31	PROTO	01/07/2015	0	10	0	0	0	0	0	
29	PROTO	19/05/2015	0	6	0	0	0	0	0	
28	PROTO	04/05/2015	0	8	0	0	0	0	0	

Ciclo della conservazione con Folium - Enerj

1) Marcatura dei documenti = apposizione ai documenti dello **Stato 0** (da esportare) da parte dell'amministratore di AOO o dagli Operatori. La marcatura può essere singola o massiva.

Demone gestione volumi: questo demone guarda IL DB, trova i doc. in stato 0 e gli assegna il numero di pacchetto/volume.

Demone invio documenti: questo demone cerca i doc. con stato 0 e con num. di volume assegnato e li mette sulla cartella FTP con il file xml.

2) Esportazione FTP

- Correttamente esportato : **1** (stato)
- Non Correttamente esportato : **2**

Demone recupero esiti

3) Archiviazione

- Correttamente archiviato : **3**
- Non Correttamente archiviato : **4**

Demone recupero esiti

4) Conservazione

- Correttamente Conservato : **5**
- Non Correttamente Conservato : **6**

Attività a carico dell'Ente produttore

Attività a carico dell'Ente produttore						
	1	2	3	4	5	6
Registrazioni di protocollo giornaliero	Formazione del Registro giornaliero di protocollo (ad es. pdf/A)	Associazione metadati	Produzione del Pacchetto di Versamento	Trasferimento al sistema di conservazione	Ricezione del rapporto di versamento prodotto e trasmesso all'Ente dal sistema di conservazione	Verifica del buon esito dell'operazione di versamento tramite il rapporto di versamento prodotto dal sistema di conservazione.
Giorno x	entro le ore 24:00 del primo giorno lavorativo successivo al giorno x					

Note tecniche (per sistemista)

Per la conservazione devono essere configurati i seguenti **Demoni** di Folium:

- **JDOC Gestione Stampe registri** invia in conservazione le stampe giornaliere dei registri (esecuzione ogni ora)
- **JDOC Gestione Volumi** (esecuzione una volta ogni 15/30 gg)
- **JDOC Invio Documenti** (una volta al giorno) Qui devono essere inseriti anche i dati FTP (li fornirà il conservatore).
- **JDOC Recupero esiti** (esecuzione una volta al giorno). Questo demone legge i feedback provenienti da Enerj inerenti sia i documenti che i pacchetti/volumi.

Menù "**Configurazione**"

- **Firma stampe registro:** Se impostato a 1, viene abilitata la funzione di firma delle stampe giornaliere del registro.
- **Selezione documenti completi conservazione:** Valori possibili 0,1. Se vale 1, in fase di ricerca documenti da inviare alla conservazione sostitutiva vengono attivati il campo per la selezione del tipo mezzo di spezione ed una checkbox per la ricerca di documenti completi.

La cartella FTP è composta di 3 sottocartelle: Immagini, Volumi, Feedback (qui vanno a finire i feedback provenienti da Enerj).



www.dedagroup.it | info@dedagroup.it





Manuale di gestione del Protocollo Informatico, dei documenti e degli Archivi della Città di Chioggia

ALLEGATO 6

Formazione, acquisizione, trattamento e conservazione dei documenti informatici

1. Formazione

Il comune di Chioggia forma i propri documenti secondo le disposizioni dell'art.40 del Codice dell'Amministrazione Digitale e le regole tecniche di cui all'art.71. Ogni documento informatico così formato deve permettere l'identificazione del Comune di Chioggia attraverso le seguenti informazioni:

- la denominazione e il logo dell'Amministrazione
- la denominazione del Settore e del Servizio mittente, corredata dell'indirizzo e dei recapiti telefonici e e-mail
- il codice fiscale dell'Amministrazione

Il documento, inoltre, dovrà contenere anche:

- il luogo e la data di redazione
- il numero e la data di registrazione nel sistema di protocollo informatico
- l'oggetto del documento, indicato in modo sintetico ma chiaro ed esaustivo.

I documenti informatici, per garantire l'accessibilità, sono redatti con dimensione carattere non inferiore a 11 e con i seguenti font:

- Arial
- Calibri
- Tahoma
- Time New Roman
- Verdana

I documenti informatici formali prodotti dal Comune di Chioggia, se vanno trasmessi all'estero, vengono di norma sottoscritti con un dispositivo di firma digitale e registrati nel sistema di protocollo informatico oppure per quello che riguarda i documenti interni all'Amministrazione, se hanno forma esclusivamente informatica e rilevanza giuridica procedimentale, devono essere protocollati e sottoscritti con un dispositivo di firma digitale.

2. Ricezione dei documenti informatici provenienti dall'estero.

La ricezione dei documenti informatici indirizzati al Comune di Chioggia è assicurata tramite una casella di posta elettronica certificata P.E.C. dichiarata istituzionale e pubblicata nell'indice nazionale della Pubblica Amministrazione. L'indirizzo della P.E.C. del comune di Chioggia è il seguente: chioggia@pec.chioggia.org.

3. Ricezione e scarico dei documenti informatici in ingresso alla P.E.C. istituzionale.

Lo scarico della casella di posta elettronica certificata e lo smistamento è di competenza del Servizio Protocollo Generale.

La protocollazione dei documenti in ingresso pervenuti alla P.E.C. istituzionale chioggia@pec.chioggia.org, è di competenza del Servizio Protocollo Generale.

I dipendenti autorizzati sono responsabili delle operazioni di ricezione di documenti informatici, e verificano la presenza degli elementi essenziali alla registrazione di protocollo.

Le ricevute e gli avvisi provenienti dai gestori del servizio di posta elettronica certificata, nonché quelli provenienti dai sistemi di gestione informatica dei documenti dei destinatari, devono essere riconosciuti dal sistema e collegati ai messaggi cui si riferiscono. La notifica al mittente dell'avvenuto recapito del messaggio è assicurata dagli specifici standard del servizio di posta elettronica certificata dell'AOO.

Se i documenti informatici spediti da caselle di posta elettronica certificata pervengono direttamente a caselle nominative di dipendenti del Comune, essi sono valutati dal ricevente e, se soggetti a registrazione di protocollo o ad altra forma di registrazione, devono rispondere al mittente chiedendo di inoltrare la mail all'indirizzo istituzionale del Comune per la registrazione.

I documenti informatici che pervengono alla casella di posta elettronica certificata dichiarata istituzionale vengono protocollati, laddove previsto, e/o inoltrati all'ufficio di destinazione con le modalità previste nel manuale.



*Manuale di gestione del Protocollo Informatico, dei documenti e
degli Archivi della Città di Chioggia*

ALLEGATO 7

Schema del piano di classificazione o TITOLARIO

Amministrazione: 027008 - Comune di Chioggia

Titolario - Area Organizzativa: COMUNE DI CHIOGGIA

Data: 16.05.2017

CODICE	DESCRIZIONE	ACL	INS DOC
01	Amministrazione generale		Nessuno
01.01	Legislazione e circolari esplicative		Documenti/ Pratiche
01.02	Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica		Documenti/ Pratiche
01.03	Statuto		Documenti/ Pratiche
01.04	Regolamenti		Documenti/ Pratiche
01.05	Stemma, gonfalone, sigillo		Documenti/ Pratiche
01.06	Archivio generale		Documenti/ Pratiche
01.07	Sistema informativo	prova	Documenti/ Pratiche
01.08	Informazioni e relazioni con il pubblico		Documenti/ Pratiche
01.09	Politica del personale; ordinamento degli uffici e dei servizi		Documenti/ Pratiche
01.10	Relazioni con le organizzazioni sindacali e di rappresentanza del personale		Documenti/ Pratiche
01.11	Controlli esterni		Documenti/ Pratiche
01.12	Editoria e attività informativo-promozionale interna ed esterna		Documenti/ Pratiche
01.13	Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti		Documenti/ Pratiche
01.14	Interventi di carattere politico e umanitario; rapporti istituzionali		Documenti/ Pratiche
01.15	Forme associative per esercizio di funzioni e servizi		Documenti/ Pratiche
01.16	Area e città metropolitana		Documenti/ Pratiche
01.17	Associazionismo e partecipazione		Documenti/ Pratiche
01.18	Protocollo Generale		Documenti/ Pratiche
02	Organi di governo, gestione, controllo, consulenza e garanzia		Nessuno
02.01	Sindaco		Documenti/ Pratiche

CODICE	DESCRIZIONE	ACL	INS DOC
02.02	Vice-sindaco		Documenti/ Pratiche
02.03	Consiglio		Documenti/ Pratiche
02.04	Presidente del Consiglio	prova	Documenti/ Pratiche
02.05	Conferenza dei capigruppo e Commissioni del Consiglio		Documenti/ Pratiche
02.06	Gruppi consiliari		Documenti/ Pratiche
02.07	Giunta		Documenti/ Pratiche
02.08	Commissario prefettizio e straordinario		Documenti/ Pratiche
02.09	Segretario e Vice-segretario		Documenti/ Pratiche
02.10	Direttore generale e dirigenza		Documenti/ Pratiche
02.11	Revisori dei conti		Documenti/ Pratiche
02.12	Difensore civico		Documenti/ Pratiche
02.13	Commissario ad acta ¹		Documenti/ Pratiche
02.14	Organi di controllo interni		Documenti/ Pratiche
02.15	Organi consultivi		Documenti/ Pratiche
02.16	Consigli circoscrizionali		Documenti/ Pratiche
02.17	Presidenti dei Consigli circoscrizionali		Documenti/ Pratiche
02.18	Organi esecutivi circoscrizionali		Documenti/ Pratiche
02.19	Commissioni dei Consigli circoscrizionali		Documenti/ Pratiche
02.20	Segretari delle circoscrizioni		Documenti/ Pratiche
02.21	Commissario ad acta delle circoscrizioni		Documenti/ Pratiche
02.22	Conferenza dei Presidenti di quartiere		Documenti/ Pratiche
03	Risorse umane		Nessuno
03.01	Concorsi, selezioni, colloqui		Documenti/ Pratiche
03.02	Assunzioni e cessazioni		Documenti/ Pratiche
03.03	Comandi e distacchi; mobilita		Documenti/ Pratiche

CODICE	DESCRIZIONE	ACL	INS DOC
03.04	Attribuzione di funzioni, ordini di servizio e missioni		Documenti/ Pratiche
03.05	Inquadramenti e applicazione contratti collettivi di lavoro		Documenti/ Pratiche
03.06	Retribuzioni e compensi		Documenti/ Pratiche
03.07	Adempimenti fiscali, contributivi e assicurativi		Documenti/ Pratiche
03.08	Tutela della salute e sicurezza sul luogo di lavoro		Documenti/ Pratiche
03.09	Dichiarazioni di infermita ed equo indennizzo		Documenti/ Pratiche
03.10	Indennita premio di servizio e trattamento di fine rapporto, quiescenza		Documenti/ Pratiche
03.11	Servizi al personale su richiesta		Documenti/ Pratiche
03.12	Orario di lavoro, presenze e assenze		Documenti/ Pratiche
03.13	Giudizi, responsabilita e provvedimenti disciplinari		Documenti/ Pratiche
03.14	Formazione e aggiornamento professionale		Documenti/ Pratiche
03.15	Collaboratori esterni		Documenti/ Pratiche
04	Risorse finanziarie e patrimoniali		Nessuno
04.01	Entrate		Documenti/ Pratiche
04.02	Uscite		Documenti/ Pratiche
04.03	Partecipazioni finanziarie		Documenti/ Pratiche
04.04	Bilancio preventivo, variazioni di bilancio verifiche contabili	prova	Documenti/ Pratiche
04.05	Piano esecutivo di gestione (PEG)		Documenti/ Pratiche
04.06	Rendiconto della gestione		Documenti/ Pratiche
04.07	Adempimenti fiscali		Documenti/ Pratiche
04.08	Inventari e consegnatari dei beni		Documenti/ Pratiche
04.09	Beni immobili		Documenti/ Pratiche
04.10	Beni mobili		Documenti/ Pratiche
04.11	Economato		Documenti/ Pratiche
04.12	Oggetti smarriti e recuperati		Documenti/ Pratiche

CODICE	DESCRIZIONE	ACL	INS DOC
04.13	Tesoreria		Documenti/ Pratiche
04.14	Concessionari ed altri incaricati della riscossione delle entrate		Documenti/ Pratiche
04.15	Pubblicita e pubbliche affissioni		Documenti/ Pratiche
05	Affari Legali		Nessuno
05.01	Contenzioso		Documenti/ Pratiche
05.02	Responsabilita civile e patrimoniale verso terzi; assicurazioni		Documenti/ Pratiche
05.03	Pareri e consulenze		Documenti/ Pratiche
06	Pianificazione e gestione del territorio		Nessuno
06.01	Urbanistica: piano regolatore generale e varianti		Documenti/ Pratiche
06.02	Urbanistica: strumenti di attuazione del Piano regolatore generale		Documenti/ Pratiche
06.03	Edilizia privata	EdiliziaPrivata	Documenti/ Pratiche
06.04	Edilizia pubblica		Documenti/ Pratiche
06.05	Opere pubbliche		Documenti/ Pratiche
06.06	Catasto		Documenti/ Pratiche
06.07	Viabilita		Documenti/ Pratiche
06.08	Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi		Documenti/ Pratiche
06.09	Ambiente: autorizzazioni, monitoraggio e controllo		Documenti/ Pratiche
06.10	Protezione civile ed emergenze		Documenti/ Pratiche
06.11	Patrimonio Demanio		Documenti/ Pratiche
07	Servizi alla persona		Nessuno
07.01	Diritto allo studio e servizi		Documenti/ Pratiche
07.02	Asili nido e scuola materna		Documenti/ Pratiche
07.03	Promozione e sostegno delle istituzioni di istruzione e della loro attivita		Documenti/ Pratiche

CODICE	DESCRIZIONE	ACL	INS DOC
07.04	Orientamento professionale; educazione degli adulti; mediazione culturale		Documenti/ Pratiche
07.05	Istituti culturali (Musei, biblioteche, teatri, Scuola comunale di musica, etc.)		Documenti/ Pratiche
07.06	Attività ed eventi culturali		Documenti/ Pratiche
07.07	Attività ed eventi sportivi		Documenti/ Pratiche
07.08	Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale		Documenti/ Pratiche
07.09	Prevenzione, recupero e reintegrazione dei soggetti a rischio		Documenti/ Pratiche
07.10	Informazione, consulenza ed educazione civica		Documenti/ Pratiche
07.11	Tutela e curatela di incapaci		Documenti/ Pratiche
07.12	Assistenza diretta e indiretta, benefici economici		Documenti/ Pratiche
07.13	Attività ricreativa e di socializzazione		Documenti/ Pratiche
07.14	Politiche per la casa		Documenti/ Pratiche
07.15	Pari opportunità		Documenti/ Pratiche
08	Attività economiche		Nessuno
08.01	Agricoltura e pesca		Documenti/ Pratiche
08.02	Artigianato		Documenti/ Pratiche
08.03	Industria		Documenti/ Pratiche
08.04	Commercio		Documenti/ Pratiche
08.05	Fiere e mercati		Documenti/ Pratiche
08.06	Esercizi turistici e strutture ricettive		Documenti/ Pratiche
08.07	Promozione e servizi		Documenti/ Pratiche
08.08	SUAP - Attività Produttive		Documenti/ Pratiche
08.09	Turismo		Documenti/ Pratiche
09	Polizia locale e sicurezza pubblica		Nessuno

CODICE	DESCRIZIONE	ACL	INS DOC
09.01	Prevenzione ed educazione stradale		Documenti/ Pratiche
09.02	Polizia stradale		Documenti/ Pratiche
09.03	Informative		Documenti/ Pratiche
09.04	Sicurezza e ordine pubblico		Documenti/ Pratiche
10	Tutela della salute		Nessuno
10.01	Salute e igiene pubblica		Documenti/ Pratiche
10.02	Trattamento Sanitario Obbligatorio		Documenti/ Pratiche
10.03	Farmacie		Documenti/ Pratiche
10.04	Zooprofilassi veterinaria		Documenti/ Pratiche
10.05	Randagismo animale e ricoveri		Documenti/ Pratiche
11	Servizi demografici		Nessuno
11.01	Stato civile		Documenti/ Pratiche
11.02	Anagrafe e certificazioni		Documenti/ Pratiche
11.03	Censimenti		Documenti/ Pratiche
11.04	Polizia mortuaria e cimiteri		Documenti/ Pratiche
11.05	Rilevazioni statistiche		Documenti/ Pratiche
12	Elezioni e iniziative popolari		Nessuno
12.01	Albi elettorali		Documenti/ Pratiche
12.02	Liste elettorali		Documenti/ Pratiche
12.03	Elezioni		Documenti/ Pratiche
12.04	Referendum		Documenti/ Pratiche
12.05	istanze, petizioni e iniziative popolari		Documenti/ Pratiche
13	Leva militare		Nessuno
13.01	Leva		Documenti/ Pratiche
13.02	Ruoli matricolari		Documenti/ Pratiche
13.03	Caserme, alloggi e servitu militari		Documenti/ Pratiche

CODICE	DESCRIZIONE	ACL	INS DOC
13.04	Requisizioni per utilita militari		Documenti/ Pratiche
14	Oggetti Diversi		Nessuno
14.01	Oggetti Diversi		Documenti/ Pratiche



*Manuale di gestione del Protocollo Informatico, dei documenti e
degli Archivi della Città di Chioggia*

ALLEGATO 8

Applicativo di protocollazione di Emergenza

Folium

**Guida per l'uso dell'applicativo di
Protocollazione di emergenza**

Versione 4.5

30 Settembre 2005

Copyright Agorà Telematica

Indice

INSTALLAZIONE CLIENT.....	3
AVVIO CLIENT.....	3
IMPOSTAZIONE PARAMETRI DI CONFIGURAZIONE.....	5
PROTOCOLLAZIONE DOCUMENTI	7
STAMPA REGISTRO	9
INVIO DATI.....	10

INSTALLAZIONE CLIENT

Eeguire il file **ProtocolloEmergenza.exe** e seguire le istruzioni della procedura di installazione. Al termine della procedura di installazione sarà creato sul desktop del proprio computer il file **Protocollo di Emergenza** per l'avvio dell'applicativo.

AVVIO CLIENT

Eeguire il file **Protocollo di Emergenza** presente su desktop o nell'elenco dei programmi e digitare nella maschera visualizzata i seguenti dati:

- un **Nome utente** valido ovvero la login di un utente che sia presente all'interno dell'Applicativo (lato server) e che sia associato ad un Ufficio dell'Organigramma;
- la **Data apertura Registro** di Emergenza ovvero la data di registrazione dei protocolli in stato di emergenza. La data dovrà essere digitata nel formato gg/mm/aaaa.
- il **Nome del Registro di emergenza** ovvero un nome univoco rispetto a quello utilizzato dalle altre postazioni client, tale da garantire, in associazione ai progressivi di protocollo generati su ogni singola postazione client, l'univocità dei protocolli acquisiti. Il campo accetta solo caratteri di tipo alfanumerico.



Dopo aver inserito correttamente i dati, sarà visualizzata la seguente finestra utile ad effettuare la protocollazione dei documenti:

Protocollazione di emergenza

Utente	operatore
Data Registro	12/10/2005
Nr prog	1
Codice AOO	A0001
Codice amm	demo1

Logout

Protocollazione
Documenti
Invia dati
Configurazione

Oggetto

Data documento

Data ricezione

Protocollo mittente

Modalità

Ingresso

Uscita

Note

Mittenti / Destinatari

Descrizione	Indirizzo	Cap e città	
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input type="radio"/> Giuridica <input checked="" type="radio"/> Fisica

Elimina
Aggiungi

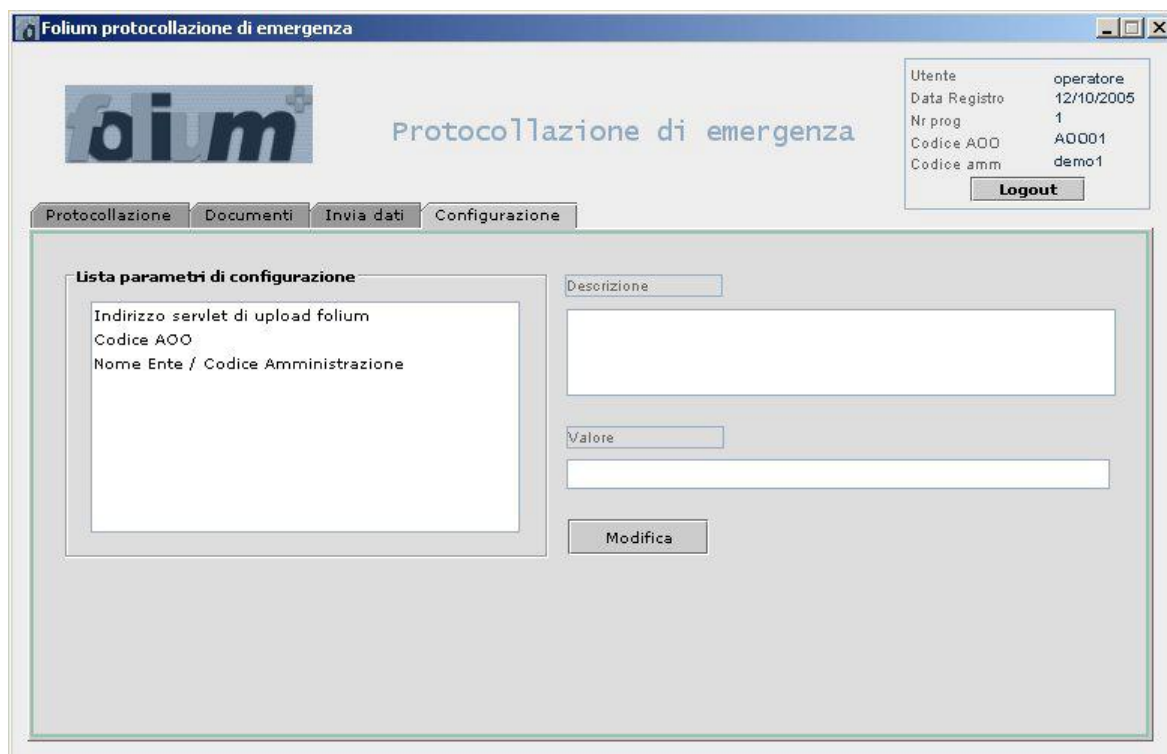
Attenzione tutti i campi di questo colore sono obbligatori

Protocolla

IMPOSTAZIONE PARAMETRI DI CONFIGURAZIONE

Prima di iniziare a protocollare i documenti, è necessario impostare i parametri di configurazione dell'applicazione client con i dati dell'AOO interessata alla protocollazione di emergenza. Cliccare quindi sul pannello **Configurazione**.

Nella maschera visualizzata è necessario impostare opportunamente i seguenti parametri di configurazione:



- **Indirizzo servlet di upload Folium**

Selezionando dalla Lista dei parametri di configurazione: **Indirizzo servlet di upload Folium**, sarà necessario impostare nel campo **Valore** la corretta URL di connessione all'applicativo web: di default compare l'indirizzo <http://localhost/folium>, nel caso ci fossero problemi nell'invio dei dati contattare il centro servizi.

Dopo aver inserito il valore corretto nell'apposito campo, è necessario cliccare sul pulsante **Modifica**.

- **Codice Aoo**

Selezionando dalla Lista dei parametri di configurazione: **Codice AOO**, sarà necessario impostare nel campo **Valore** il **Codice** esatto dell'**Area Organizzativa Omogenea** nella quale dovranno essere protocollati i documenti. In fase di importazione, i protocolli di emergenza verranno infatti inseriti nel Registro ufficiale dell'AOO specificata.

Dopo aver inserito il valore corretto nell'apposito campo, è necessario cliccare sul pulsante **Modifica**.

- **Nome Ente / Codice Amministrazione**

Selezionando dalla Lista dei parametri di configurazione: **Nome Ente/Codice Amministrazione**, sarà necessario impostare nel campo **Valore** il **Codice dell'ente (Amministrazione)** a cui appartiene l'AOO interessata alla protocollazione di emergenza.

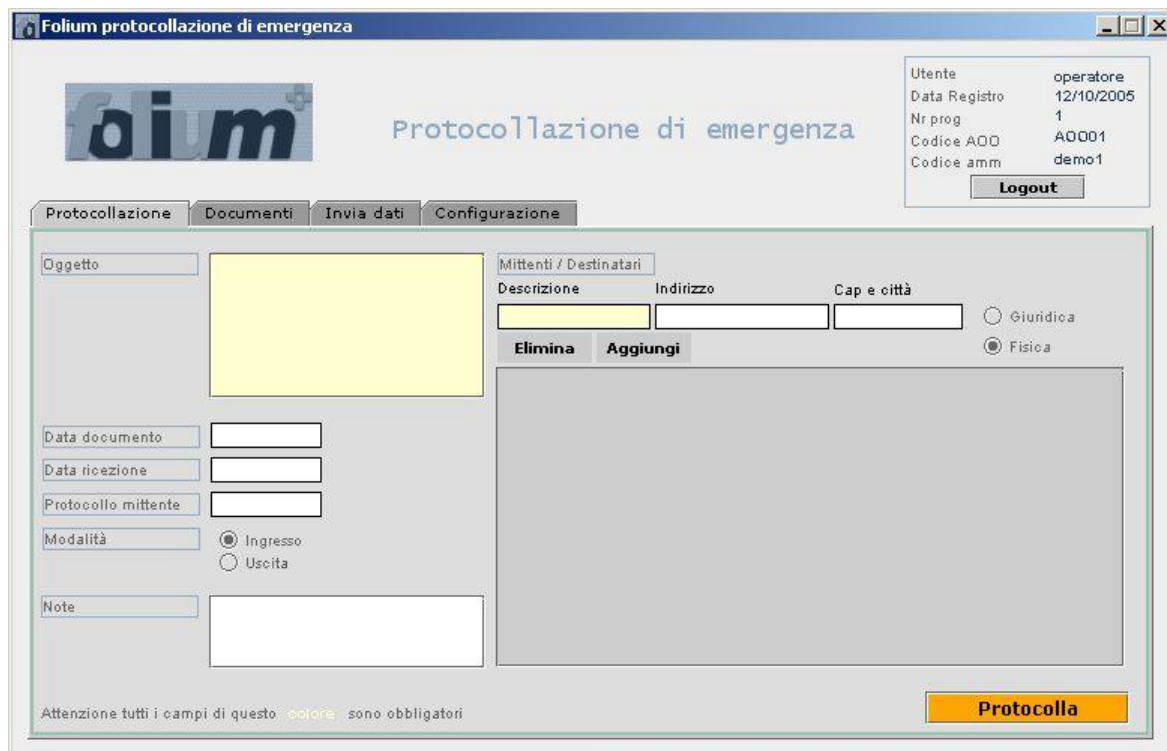
ATTENZIONE : E' necessario digitare il codice esatto, riportando anche le eventuali lettere maiuscole.

Dopo aver inserito il valore corretto nell'apposito campo, è necessario cliccare sul pulsante **Modifica**.

I parametri di configurazione potranno essere modificati in qualsiasi momento senza riavviare l'applicazione.

PROTOCOLLAZIONE DOCUMENTI

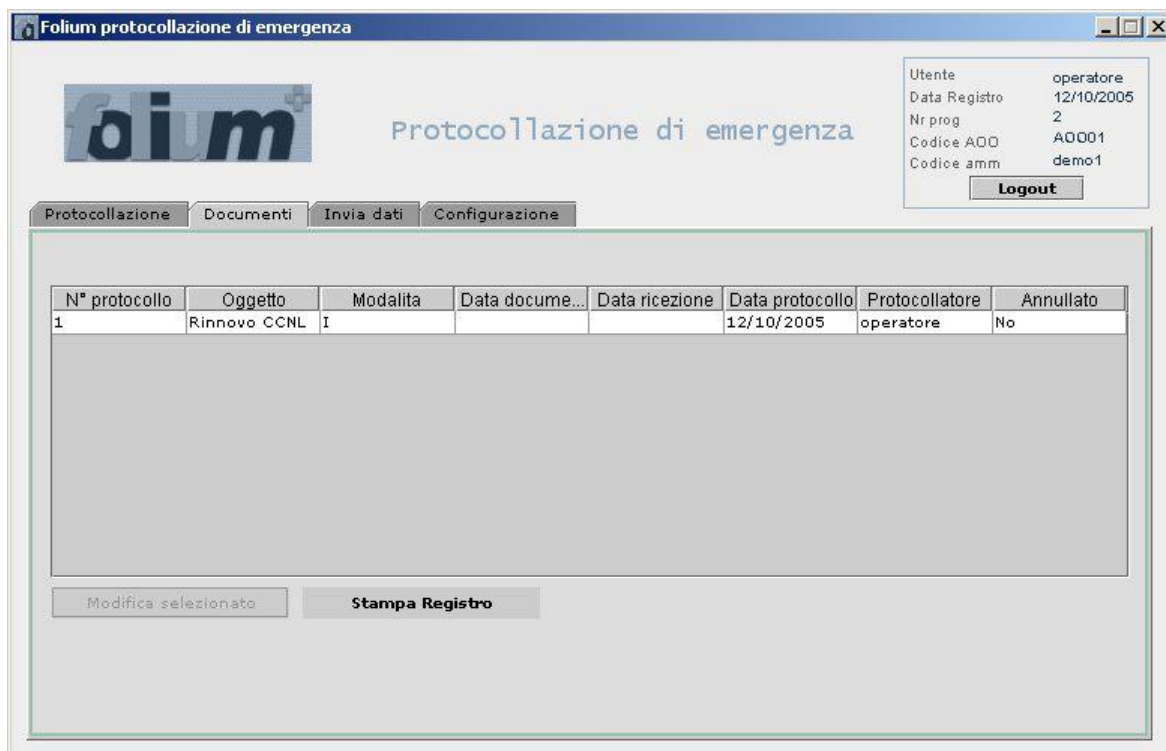
La protocollazione di emergenza potrà essere effettuata inserendo i dati di profilazione dei documenti nel pannello **Protocollazione**.



Selezionare quindi la modalità di protocollazione: **Ingresso/Uscita** e digitare i dati negli appositi campi. Rispetto ad essi, i campi di colore giallo (**Oggetto** e **Mittenti/Destinatari**) sono obbligatori. Nella registrazione del mittente o destinatario dovrà essere specificato se si tratta di **Persona Fisica** o **Giuridica** e dovrà essere inserito il **Cap** e la **Città** separati da uno spazio (Es. 00159 Roma).

Dopo aver inserito i dati del documento interessato alla protocollazione di emergenza, è possibile cliccare sul pulsante **Protocolla**.

Il documento protocollato verrà quindi riportato in elenco nella tabella visibile nel pannello **Documenti** e sarà quindi possibile procedere ad una nuova protocollazione.



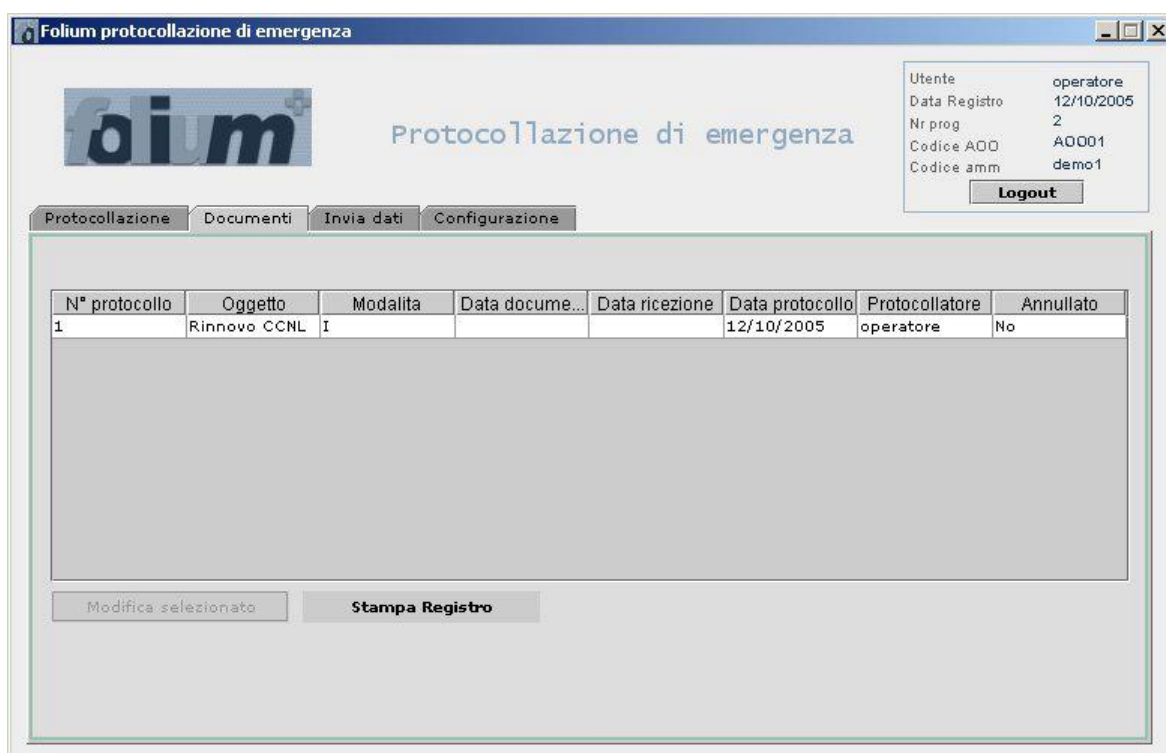
I dati di un protocollo già acquisito potranno essere modificati selezionando il documento dalla tabella e cliccando sul pulsante **Modifica selezionato**.

Attenzione: rispetto ai documenti già protocollati sarà possibile modificare unicamente le **Note** per i protocolli in ingresso e in uscita e la **Data ricezione** e il **Protocollo mittente** per i protocolli in ingresso.

STAMPA REGISTRO

Il pulsante **Stampa registro** presente nel pannello **Documenti** genera un file in formato .csv (utilizzabile con Excel) contenente la stampa dei protocolli di emergenza ordinati per numero protocollo e data.

I file .csv delle stampe vengono depositati nella sottocartella **report** contenuta nella cartella di installazione dell'applicativo (Es: C:\Programmi\protocollo-emergenza-folium\report).



La stampa dell'elenco dei protocolli di emergenza sarà comunque effettuata automaticamente al momento dell'invio dei dati sul server, con indicazione dell'avvenuta stampa tramite alert.

INVIO DATI

Al termine della procedura di emergenza è possibile accedere al pannello **Invia dati** per trasferire verso l'applicazione web tutti i protocolli acquisiti.

Affinché l'invio dei dati abbia esito positivo, è necessario che:

- Il sistema di protocollazione sia attivo e raggiungibile.
- L'indirizzo di upload sia esatto (vedi Cap. *Impostazione parametri di configurazione*);
- L'AOO specificata nel pannello di configurazione corrisponda all'AOO configurata all'interno dell'Applicativo server (vedi Cap. *Impostazione parametri di configurazione*);
- L'Ente o l'Amministrazione specificata nel pannello di configurazione corrisponda a quella configurata all'interno dell'Applicativo server (vedi Cap. *Impostazione parametri di configurazione*);
- L'utente (nome utente) con cui sono stati registrati i protocolli di emergenza esista all'interno dell'Applicativo server e sia associato ad un Ufficio dell'Ente;
- Non sia già stato effettuato dallo stesso utente (nome utente) un precedente invio di dati verso l'Applicativo server, e i relativi protocolli non siano ancora stati importati all'interno del Registro Ufficiale dall'Amministratore di sistema.

Per inviare i dati all'Applicativo server è necessario quindi cliccare sul pulsante **Invia dati** dell'omonimo pannello. Al termine del processo di invio, un apposito messaggio avviserà l'utente sull'esito dell'operazione.

In caso di esito positivo, i protocolli di emergenza saranno trasferiti dal client verso il server e pertanto non saranno più presenti nel pannello **Documenti**.

I protocolli trasmessi saranno infine recapitati sul server all'Amministratore di Ente, che provvederà ad allinearli sul Registro di Protocollo Ufficiale dell'AOO interessata alla protocollazione di emergenza, secondo le procedure definite nel manuale di gestione.



Manuale di gestione del Protocollo Informatico, dei documenti e degli Archivi della Città di Chioggia

ALLEGATO 9

Elenco Caselle P.E.C. iscritte all'I.P.A.

alessandro.ferro@pec.chioggia.org
ba.penzo@pec.chioggia.org
beniamino.boscolo@pec.chioggia.org
chioggia@pec.chioggia.org
claudia.convento@pec.chioggia.org
commercio@pec.chioggia.org
daniela.sassi@pec.chioggia.org
daniele.padoan@pec.chioggia.org
davidepenzo@pec.chioggia.org
domenico.zanni@pec.chioggia.org
elettorale@pec.chioggia.org
elisa.busetto@pec.chioggia.org
endri.bullo@pec.chioggia.org
fatturazione.elettronica@pec.chioggia.org
genny.mantoan@pec.chioggia.org
gianluca.naccari@pec.chioggia.org
giovanni.tiozzo@pec.chioggia.org
giudicedipace@pec.chioggia.org
giuseppe.casson@pec.chioggia.org
ilaria.lunardi@pec.chioggia.org
jonatan.montanariello@pec.chioggia.org
leonardo.ranieri@pec.chioggia.org
luciano.passarella@pec.chioggia.org
marcellina.segantin@pec.chioggia.org
marco.dolfin@pec.chioggia.org
marcomarangon@pec.chioggia.org
mariachiara.boccatto@pec.chioggia.org
mario.veronese@pec.chioggia.org
mfreguggia@pec.chioggia.org
michele.tiozzo@pec.chioggia.org

napettilucio@pec.chioggia.org
nicola.salvagno@pec.chioggia.org
paola.landri@pec.chioggia.org
paolo.bonfa@pec.chioggia.org
personale@pec.chioggia.org
politiche.educative@pec.chioggia.org
poliziale@pec.chioggia.org
romina.tiozzo@pec.chioggia.org
servizi.sociali@pec.chioggia.org
stefanopenzo@pec.chioggia.org
suap@pec.chioggia.org
vanessapenzo@pec.chioggia.org
vigili.urbani@pec.chioggia.org



Manuale di gestione del Protocollo Informatico, dei documenti e degli Archivi della Città di Chioggia

ALLEGATO 10

Elenco Assegnatari Firma Digitale

Cognome	Nome	Data di nascita
ALBANESE	SANDRA	13.08.1959
ARDIZZON	PAOLA	20.10.1960
ARDIZZON	PAOLO	09.10.1954
BALLARIN	DANIELA	27.04.1969
BALLARIN	GIANNA	15.08.1957
BELLEMO	IVANO	12.03.1973
BERGO	DANIELE	29.09.1956
BOSCOLO TODARO	MARIA GRAZIA	12.02.1954
BOSCOLO SALE	MARZIA	26.08.1975
BRUNI	RICCARDO	14.11.1972
BULLO	ENDRI	29.05.1953
D'ESTE	ANGELA	02.11.1977
DORIA	MAURIZIO	02.09.1955
DUO'	ROSINA	20.03.1965
FABRIS	FABRIZIO	14.09.1958
FERRO	ALESSANDRO	22.10.1974
FREGUGGIA	MARIALISA	18.09.1952
GIANNI	CARLO	15.04.1969
GRADARA	NAZZARENO	27.10.1957
GREGO	MASSIMO	01.09.1956
LAZZARIN	DANIELA	05.06.1972
MANFREDI	STEFANIA	10.10.1969
MARAFIN	GRAZIANO	01.12.1962
MARANGON	MARCO	01.09.1967
MONARO	SARA	11.04.1976
NAPETTI	LUCIO	10.04.1964
PAPA	CARMELO	06.10.1956
PASSARELLA	PAOLO	05.09.1960
PENZO	MARIO	26.07.1953
PENZO	TIZIANO	20.03.1975

PENZO	DAVIDE	27.09.1971
PENZO	DAVIDE	18.06.1993
PENZO	CRISTINA	18.11.1969
PENZO	VANESSA	24.01.1970
PERINI	MASSIMO	17.01.1962
PERINI	DEBORA	26.08.1969
PIEROBON	MASSIMO	21.10.1955
ROSTEGHIN	MAURO	17.11.1961
SALVAGNO	WALTER	25.08.1973
SAMBO	FERNANDO	28.12.1974
SPAGNA	PAOLO	18.07.1953
STECCO	DANIELE	16.12.1977
TELLOLI	FRANCESCA	03.06.1983
TIOZZO NETTI	MICHELE	16.06.1966
TIOZZO PEZZOLI	ARIANNA	02.03.1962
TOMMASIN	MASSIMO	19.02.1961
TRAPELLA	PATRIZIA	23.03.1967
VERONESE	ALBERTO	01.06.1972
VERONESE	MARCO	08.05.1971
VERONESE	MARIO	03.09.1953
VIANELLO	LUCIO	20.04.1952
ZAMBON	ENNIO	23.05.1959



*Manuale di gestione del Protocollo Informatico, dei documenti e
degli Archivi della Città di Chioggia*

ALLEGATO 11

Piano della sicurezza dei documenti informatici

A cura del CED – Servizi Informatici



Città di Chioggia

città d'arte

SETTORE URBANISTICA

Servizi Informatici

Tel. 041-5534867 fax 041-400058

PREMESSA

La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici.

In attuazione a tale direttiva l'Agenzia per l'Italia digitale AgID ha provveduto ad emanare l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni".

Con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», le Misure minime sono ora divenute di obbligatoria adozione per tutte le Amministrazioni.

Le Misure, che si articolano sull'attuazione di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di attuazione. Il livello minimo è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi e rappresentano inoltre obiettivi di miglioramento per le amministrazioni.

I Servizi Informatici del Comune di Chioggia, alla luce di quanto precedentemente riportato, hanno iniziato un processo di analisi ed adeguamento del piano di sicurezza informatica dell'Ente, entro la fine dell'anno 2017 sarà compilato il modulo di implementazione allegato alla circolare, come da previsione di legge.



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

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	Modalità di implementazione	Liv
1.1.1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Implementato un sistema di inventariazione automatico delle risorse collegate al network dell'Ente con un applicativo dedicato che cataloga i dispositivi hardware.	M
1.1.2	Implementare ABSC 1.1.1 attraverso uno strumento automatico		S
1.1.3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.		A
1.1.4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.		A
1.2.1	Implementare il "logging" delle operazioni del server DHCP.		S
1.2.2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.		S
1.3.1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Nella fase di collegamento di un nuovo dispositivo, il software dedicato all'inventariamento rileva il nuovo dispositivo e, previa autorizzazione dell'amministratore di sistema, aggiorna l'inventario e cataloga il nuovo dispositivo.	M
1.3.2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.		S
1.4.1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Il servizio dedicato all'inventariamento rileva autonomamente l'IP del dispositivo registrandolo all'interno dell'inventario.	M
1.4.2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.		S
1.4.3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.		A
1.5.1	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.		A
1.6.1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.		A



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

ABSC:2 CSC: 2 - INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

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	Modalità di implementazione	Liv
2.1.1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Implementato un sistema di rilevazione automatizzato del software presente per ciascun tipo di sistema. Stilato un elenco di software autorizzato e relative versioni. Stilato un elenco di software non autorizzato identificando le postazioni in cui deve essere disinstallato il software non autorizzato. Viene distribuita al personale la lista del software autorizzato e pianificate le attività propedeutiche atte a inibire l'installazione del software non autorizzato.	M
2.2.1	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.		S
2.2.2	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare) la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).		S
2.2.3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.		A
2.3.1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Implementato un sistema di rilevazione automatizzato del software presente per ciascun tipo di sistema finalizzato all'individuazione del software non autorizzato con l'indicazione del dispositivo dove procedere alla disinstallazione del software non autorizzato.	M
2.3.2	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.		S
2.3.3	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.		A
2.4.1	Utilizzare macchine virtuali e/o sistemi air-gapped1 per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.		A



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

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	Modalità di implementazione	Liv
3.1.1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	E' stato definito un documento interno con le configurazioni standard sicure decise dai servizi informatici. Il documento si trova presso i locali dei Servizi Informatici che sono accessibili esclusivamente dal personale assegnato al servizio.	M
3.1.2	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio) disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.		S
3.1.3	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.		A
3.2.1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	E' stata definita una configurazione standard per ogni tipologia di sistema presente all'interno dell'ente, come riportato alla misura 3.1.1.	M
3.2.2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Vengono ripristinati i sistemi secondo quanto previsto dalla misura 3.1.1.	M
3.2.3	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.		S
3.3.1	Le immagini d'installazione devono essere memorizzate offline.	Le immagini dei pc sono su dispositivi mobili collocate all'interno della cassaforte posta all'interno dei locali dei servizi informatici.	M
3.3.2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.		S
3.4.1	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).	L'accesso ai server dall'esterno avviene per mezzo di apposite policy implementati sui sistemi di protezione perimetrali, firewall.	M
3.5.1	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.		S
3.5.2	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.		A



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

ABSC_ID#	Descrizione	Modalità di implementazione	Liv
3.5.3	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.		A
3.5.4	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.		A
3.6.1	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.		A
3.7.1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.		A



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

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	Modalità di implementazione	Liv
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.	L'Ente ha adottato un sistema di controlli per mezzo di un software che fornisce lo stato dei pc collegati alla rete lan.	M
4.1.2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.		S
4.1.3	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).		A
4.2.1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.		S
4.2.2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità.		S
4.2.3	Verificare nei log da presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.		S
4.3.1	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.		S
4.3.2	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.		S
4.4.1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Il software utilizzato di cui alla misura 4.1.1 si aggiorna in autonomia.	M
4.4.2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione		S
4.5.1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Pianificato uno studio di fattibilità per l'implementazione regolare degli aggiornamenti dei sistemi operativi. Pianificazione degli aggiornamenti degli applicativi dove possibile verificandone l'ambito di sicurezza.	M
4.5.2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Pianificato uno studio di fattibilità per l'implementazione di procedure finalizzate all'aggiornamento continuo dei sistemi air-gapped. Pianificato la definizione di un regolamento per normare il loro utilizzo.	M



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

ABSC_ID#	Descrizione	Modalità di implementazione	Liv
4.6.1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.		S
4.7.1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Pianificato uno studio di fattibilità per l'applicazione di un sistema automatico che permetta la verifica dell'applicazione delle patch necessarie a contrastare le vulnerabilità evidenziate e formuli dei report che consentano l'accettazione di ragionevoli rischi.	M
4.7.2	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.		S
4.8.1	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.).	Pianificato uno studio di fattibilità per l'applicazione di un metodo di analisi che valuti le criticità dei sistemi, individuato i rischi connessi e definendo delle contromisure.	M
4.8.2	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	Pianificato uno studio di fattibilità per l'applicazione di un metodo di trattamento del rischio che permette la prioritizzazione delle criticità dei sistemi, individuato i rischi connessi e definendo delle contromisure.	M
4.9.1	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.		S
4.1.0	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.		S



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

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	Modalità di implementazione	Liv
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.	Gli Utenti con privilegi amministrativi sono gli addetti dei Servizi Informatici che possiedono competenze adeguate al ruolo che ricoprono.	M
5.1.2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Le utenze amministrative sono usate per le operazioni che ne richiedono i privilegi. Gli accessi sono registrati con un servizio di raccolta automatizzato che ne garantisce la protezione e l'integrità secondo le specifiche degli stessi come da provvedimento del Garante della Privacy sugli amministratori di sistema, recita che: "le aziende private e pubbliche devono registrare e conservare i dati relativi agli accessi degli Amministratori di sistema ai sistemi contenenti dati sensibili da loro gestiti, al fine di agevolare la verifica sulla loro attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici" GU n. 300, 24/12/2008.	M
5.1.3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.		S
5.1.4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.		A
5.2.1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Pianificato un piano per la redazione di un documento che riepiloghi tutte le utenze amministrative e la definizione di apposite nomine per gli amministratori di sistema.	M
5.2.2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.		A
5.3.1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	I nuovi dispositivi vengono configurati secondo criteri predefiniti per essere inseriti nella rete dell'ente, viene personalizzato con le credenziali dell'utente utilizzatore.	M
5.4.1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.		S
5.4.2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.		S
5.4.3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.		S
5.5.1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.		S
5.6.1	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.		A



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

ABSC_ID#	Descrizione	Modalità di implementazione	Liv
5.7.1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Pianificato un piano di sostituzione delle credenziali amministrative in base ai servizi amministrativi configurati all'interno delle Ente. Valutazione del rischio e dell'impatto operativo sull'erogazione dei servizi ai cittadini.	M
5.7.2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.		S
5.7.3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Pianificato uno studio di fattibilità un metodo operativo per la sostituzione delle credenziali amministrative per evitare l'invecchiamento delle password.	M
5.7.4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	E' stata implementata una policy di gruppo in active directory sul server di dominio, che gestisce la cronologia delle password utilizzate dagli utenti ed impedisce il riutilizzo di password recenti.	M
5.7.5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.		S
5.7.6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.		S
5.8.1	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.		S
5.9.1	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.		S
5.10.1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Sono state create credenziali specifiche per ogni applicativo e per ogni base dati che richiede l'accesso amministrativo. Ogni profilo non amministrativo possiede la propria utenza personale. Le varie utenze sono distinte.	M
5.10.2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Viene creato un utente con relativa password per ogni utenza con privilegi amministrativi sia interna che esterna.	M
5.10.3	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.	Le utenze di default dei sistemi e definite anonime, come "root", "administrator", "admin" vengono usate solo in caso di emergenza e per configurazioni particolari. Solo il personale incaricato all'uso conosce tali credenziali che sono contenuti nella documentazione che risiede all'interno dei locali dei servizi informatici.	M
5.10.4	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).		S



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

ABSC_ID#	Descrizione	Modalità di implementazione	Liv
5.11.1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali di amministrative sono consultabili dalla documentazione in possesso dei servizi informatici che si trova nei locali utilizzati dagli addetti, accessibili esclusivamente dal personale assegnato al servizio. I locali sono protetti da un sistema anti-intrusione.	M
5.11.2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizza autenticazione a più fattori per accedere con privilegi amministrativi.	M



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

ABSC:8 CSC: 8 - DIFESA 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	Modalità di implementazione	Liv
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.	L'Ente ha implementato un sistema antivirus su tutti i dispositivi dell'Ente, inoltre ogni dispositivo che appartiene alla rete è collegato al server che gestisce l'antivirus e si occupa di mantenerlo costantemente aggiornato.	M
8.1.2	Installare su tutti i dispositivi firewall ed IPS personali.	Tutti i dispositivi sono dotati di un sistema di protezione la cui gestione è centralizzata.	M
8.1.3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.		S
8.2.1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.		S
8.2.2	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi antimalware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.		S
8.2.3	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.		A
8.3.1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'utilizzo di dispositivi esterni a quelli necessari per le attività aziendali non è consentito. Qualora si tentasse di accedere alla rete con dispositivi propri, intervengono le policy di dominio che limitano l'accesso alle risorse.	M
8.3.2	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.		A
8.4.1	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP) Address SPACE Layout Randomization (ASLR) virtualizzazione, confinamento, etc. disponibili nel software di base.		S
8.4.2	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.		A
8.5.1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.		S
8.5.2	Installare sistemi di analisi avanzata del software sospetto.		A
8.6.1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.		S



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

ABSC_ID#	Descrizione	Modalità di implementazione	Liv
8.7.1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' stata implementata una policy di gruppo in active directory sul server di dominio, che inibisce l'esecuzione automatica dei contenuti per cd e unità removibili.	M
8.7.2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Pianificato una verifica del sistema che inibisce l'esecuzione automatica dei contenuti dinamici (per esempio macro) presenti nei file tramite policy di sistema. Molte postazioni sono state limitate attraverso i privilegi assegnati al profilo dell'utilizzatore.	M
8.7.3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Il Comune di Chioggia utilizza una web mail, non viene installato sui dispositivi nessun client di posta.	M
8.7.4	Disattivare l'anteprima automatica dei contenuti dei file.	E' stata implementata una policy di gruppo in active directory sul server di dominio, che impedisce l'anteprima automatica del contenuto dei file anche per le risorse di rete.	M
8.8.1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Nel momento in cui viene connesso un supporto removibile al pc, il sistema antivirus lo intercetta e ne verifica il contenuto.	M
8.9.1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	La posta elettronica è gestita da un operatore esterno e prevede anche il filtro antispam.	M
8.9.2	Filtrare il contenuto del traffico web.	Tutto il traffico web proveniente dalla rete del Comune di Chioggia viene filtrato da un sistema software che individua i tentativi di accesso a siti non sicuri o malevoli.	M
8.9.3	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).	Sono stati implementati sistemi che analizzano i messaggi di posta elettronica e il traffico web per bloccare file allegati alle mail o in fase di download da siti web, non necessari all'organizzazione o potenzialmente pericolosi.	M
8.10.1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.		S
8.11.1	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.		S



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

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	Modalità di implementazione	Liv
10.1.1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Implementato un sistema di copie di tutte le informazioni del sistema informatico dell'ente necessarie a ripristinare il sistema nella misura necessaria ad erogare i servizi minimi al cittadino.	M
10.1.2	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.		A
10.1.3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.		A
10.2.1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.		S
10.3.1	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.	Le copie di sicurezza delle informazioni necessarie a ripristinare il sistema per i servizi minimi al cittadino sono adeguatamente protette e inaccessibili. Le copie remote vengono eseguite su canale protetto e criptato.	M
10.4.1	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.	I supporti contenenti le copie delle informazioni necessarie a ripristinare il sistema per i servizi minimi al cittadino sono dislocate al di fuori del perimetro dell'organizzazione e sono inaccessibili all'infrastruttura dell'organizzazione.	M



Comune di Chioggia - Elenco Misure Minime

Elenco delle misure minime implementate dall'ente

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	Modalità di implementazione	Liv
13.1.1	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Pianificato una analisi dei dati finalizzata a individuare quelli con particolari requisiti di riservatezza. Pianificato uno studio di fattibilità' per l'applicazione di sistemi crittografici per le banche dati rilevanti.	M
13.2.1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti		S
13.3.1	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.		A
13.4.1	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.		A
13.5.1	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.		A
13.5.2	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.		A
13.6.1	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.		A
13.6.2	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.		A
13.7.1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.		A
13.8.1	Bloccare il traffico da e verso url presenti in una blacklist.	Tale attività viene eseguita per mezzo di un software che è stato configurato in modo da negare l'accesso a siti potenzialmente malevoli o non necessari all'organizzazione.	M
13.9.1	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.		A