CONSIGLIO REGIONALE DEL PIEMONTE - Deliberazione dell'Ufficio di Presidenza

Deliberazione 14 maggio 2025, n. 111

ADOZIONE DEL MANUALE DI GESTIONE E DI CONSERVAZIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DEL CONSIGLIO REGIONALE DEL PIEMONTE. (CG/LS/GM)

Documento allegato

CONSIGLIO REGIONALE DEL PIEMONTE

Ufficio di Presidenza

Delibera n. 111/2025 - Cl. 6.2.1

Oggetto ADOZIONE DEL MANUALE DI GESTIONE E DI CONSERVAZIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DEL CONSIGLIO REGIONALE DEL PIEMONTE. (CG/LS/GM)

Seduta n. 19

L'anno 2025, il giorno 14 maggio alle ore 13.37 - presso la sede di Palazzo Lascaris, via Alfieri n. 15, Torino - si è riunito l'Ufficio di Presidenza del Consiglio Regionale.

Sono presenti: il Presidente NICCO, il Vice Presidente GRAGLIA, il Vice Presidente RAVETTI, i Consiglieri Segretari CAROSSO, CASTELLO, CERA.

Non sono presenti:

A relazione del Presidente NICCO

ADOZIONE DEL MANUALE DI GESTIONE E DI CONSERVAZIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DEL CONSIGLIO REGIONALE DEL PIEMONTE. (CG/LS/GM)

VISTI

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

il Codice dell’Amministrazione Digitale (D.Lgs. n. 82/2005 e s.m. i.), che disciplina l’uso delle tecnologie dell’informazione e della comunicazione nell’azione amministrativa;

le Linee guida sulla formazione, gestione e conservazione dei documenti informatici adottate da AgID con determinazione n. 407/2020 e in vigore dal 1° gennaio 2022, che individuano i criteri e le regole per garantire la corretta gestione documentale e la conservazione a norma dei documenti digitali;

il Piano Triennale per l’Informatica nella Pubblica Amministrazione 2024-2026, che pone tra le priorità strategiche la dematerializzazione dei processi amministrativi e il rafforzamento della gestione e conservazione dei documenti digitali;

CONSIDERATO CHE

in attuazione delle Linee guida AgID e del Piano Triennale per l’ Informatica nella PA 2024-2026, l’Ente ha redatto un documento unico, denominato “Manuale di gestione e di conservazione del protocollo informatico, dei documenti e dell’archivio”, contenente le regole, le responsabilità e i processi per la formazione, gestione, conservazione e accesso ai documenti digitali dell’Ente;

il suddetto Manuale risponde ai requisiti normativi e agli standard tecnici richiesti, e costituisce uno strumento fondamentale per garantire trasparenza amministrativa, efficacia operativa e tutela del patrimonio documentale;

entro giugno 2025 le amministrazioni devono pubblicare, nella sezione “Amministrazione trasparente” del proprio sito istituzionale, il manuale di gestione documentale, la nomina del Responsabile della gestione documentale per ciascuna AOO e, se presenti più AOO, la nomina del Coordinatore della gestione documentale;

entro giugno 2026, devono essere pubblicati anche il manuale di conservazione e la nomina del Responsabile della conservazione;

RITENUTO

di dover procedere all’approvazione formale del Manuale di gestione e di conservazione del protocollo informatico, dei documenti e dell’archivio redatto dall’Ente;

di dover nominare formalmente le figure responsabili previste dalle Linee guida;

di dover garantire la pubblicazione del documento e delle nomine in “Amministrazione trasparente”;

L'Ufficio di Presidenza, ***unanime***,

D E L I B E R A

1. l'approvazione del “Manuale di gestione e di conservazione del protocollo informatico, dei documenti e dell’archivio”, **allegato** al presente atto, redatto conformemente alle Linee guida AgID e agli obiettivi del Piano Triennale per l’Informatica nella PA 2024-2026;

2. di abrogare con la presente la deliberazione dell'Ufficio di Presidenza n. 41 del 1 marzo 2018 e i suoi allegati;

3. di delegare il direttore responsabile della direzione Amministrazione, Personale, Sistemi informativi e Organismi di Garanzia alla nomina del responsabile della gestione documentale e della conservazione;

4. di delegare il direttore responsabile della direzione Amministrazione, Personale, Sistemi informativi e Organismi di Garanzia alla pubblicazione del Manuale e alle nomine nella sezione “Amministrazione trasparente” del sito istituzionale dell’ Ente, entro i termini fissati dal Piano Triennale.

CONSIGLIO REGIONALE DEL PIEMONTE

MANUALE DI GESTIONE E DI CONSERVAZIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO

REDAZIONE A CURA DI:
Graziella Miraudo – archivista del Consiglio regionale del Piemonte
Loredana Sparti – segreteria Direzione Amministrazione, Personale, Sistemi informativi e Organismi di Garanzia del Consiglio regionale del Piemonte

Torino, maggio 2025

SOMMARIO

PRINCIPI GENERALI

1.1 PREMESSA

Le Linee Guida AGID/2021 abrogano tutte le precedenti disposizioni
fatte salve le seguenti:
- art. 2 comma 1, Oggetto e ambito di applicazione;
- art. 6, Funzionalità;
- art. 9, Formato della segnatura di protocollo;
- art. 18 commi 1 e 5, Modalità di registrazione dei documenti informatici;
- art. 20, Segnatura di protocollo dei documenti trasmessi;
- art. 21, Informazioni da includere nella segnatura.

del DPCM 3 dicembre 2013 contenente "Regole tecniche per il protocollo informatico"

Il manuale di gestione 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).

Il presente "Manuale di gestione documentale del protocollo informatico, dei documenti e dell'archivio" sostituisce quello adottato con deliberazione n. 41 del 01/03/2018 ed ha tra i suoi allegati il Titolario con Piano di conservazione integrato (Allegato 1).

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 il personale addetto al servizio e per i soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

Il protocollo informatico costituisce l'infrastruttura di base tecnico-funzionale del processo di transizione al digitale e di trasparenza dell'attività dell'amministrazione.

Il manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni necessarie per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione, invio o ricezione e archiviazione dei documenti.

Il presente documento, pertanto, si rivolge non solo al personale addetto al protocollo, ma, in generale, a tutti i soggetti interni ed 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

II presente manuale di gestione del protocollo, dei documenti e degli archivi viene aggiornato in base alle linee guida AGID.
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 del Consiglio regionale del Piemonte.
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:

- ✓ "Ente", Consiglio regionale del Piemonte
- ✓ "Codice", il decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (CAD) e s.m.i.;
- ✓ "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" AGID maggio 2021
- ✓ DPR 445/2000 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" TUDA e s.m.i.
- ✓ "Regole tecniche protocollo", il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico fatte salve le modifiche apportate dalle Linee Guida AGID maggio 2021;
- ✓ INAD "Indice Nazionale dei Domicili digitali"

Di seguito si riportano gli acronimi utilizzati più frequentemente:

- ✓ **AOO** - Area Organizzativa Omogenea;
- ✓ **SA** – Servizio Archivistico;
- ✓ **SdP** – Sistema di Protocollo;
- ✓ **RPA** - Responsabile del Procedimento Amministrativo - il personale che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- ✓ **RTD** – Responsabile per la Transizione al Digitale - Coordina e garantisce la trasformazione digitale della PA
- ✓ **RGD** - Responsabile della gestione documentale – Gestisce il servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi
- ✓ **RPD (DPO)** – Responsabile protezione dati – gestisce il registro dei trattamenti, vigila sulla tenuta dello stesso e coordina l'attività di prevenzione degli incidenti sulla protezione dei dati
- ✓ **Struttura Nodo Responsabile** - rappresenta la struttura apicale (direzioni e settori);
- ✓ **Nodo Operativo** – rappresenta la struttura operativa.

1.4 AREE ORGANIZZATIVE OMOGENEE

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

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

All'interno della AOO il sistema di protocollazione è decentrato, e tutta la corrispondenza in ingresso è gestita dai Nodi Responsabili delle direzioni e del Protocollo generale, mentre in uscita è gestita da ciascuno dei Nodi Responsabili e del 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 e alle attività afferenti è preposto il/la Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito SA) di concerto con il/la dirigente responsabile.

In relazione alla modalità di fruizione del servizio di protocollo adottata dall'Ente, 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'Ente;
- ✓ verificare il rispetto dell'applicazione alle disposizioni normative delle 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, dei flussi documentali e le attività di gestione degli archivi;
- ✓ autorizzare le eventuali operazioni di annullamento della registrazione di protocollo;
- ✓ 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 DEL REGISTRO GIORNALIERO DI PROTOCOLLO

Nell'ambito del Servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, al termine della giornata lavorativa, il contenuto del registro informatico di protocollo, viene automaticamente prodotto e inviato in conservazione.

1.7 TUTELA DEI DATI PERSONALI

L'Ente, titolare dei dati di protocollo e dei dati particolari, contenuti nella documentazione amministrativa di propria competenza, ha ottemperato al dettato del decreto legislativo 30 giugno 2003, n. 196 e s.m.i e del Regolamento UE 679/2016 (GDPR)- con atti formali aventi rilevanza interna ed esterna, si rimanda quindi alla normativa in vigore.

1.8 CASELLE DI POSTA ELETTRONICA E ACCREDITAMENTO IPA

L'Ente si è dotato di diverse caselle di posta elettronica certificata istituzionale per la corrispondenza, sia in ingresso che in uscita che costituiscono l'indirizzo virtuale dell'Ente e di tutte le strutture che ad essa fanno riferimento.

L’Ente, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA), fornendo le informazioni che lo individuano.

L'IPA è accessibile, tramite il relativo sito internet, a tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni modifica delle proprie credenziali di riferimento nonché la data a partire dalla quale la modifica stessa sarà operativa: sarà così garantita l'affidabilità dell'indirizzo di posta elettronica indicato. Con la stessa tempestività, l'amministrazione comunica la soppressione, ovvero la creazione di una AOO.

1.9 SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI

Con l'inizio dell’attività operativa del protocollo informatico, è stato adottato un unico sistema di classificazione, di seguito denominato Titolario, per l'archivio unico dell'Ente.

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

Al fine di agevolare la classificazione archivistica e l’assegnazione per competenza della documentazione, il titolario è stato pubblicato sulla *Intranet* a disposizione di tutto il personale dell’Ente.

1.10 FORMAZIONE

Nell'ambito dei piani formativi richiesti a tutte le pubbliche amministrazioni sulla formazione e la valorizzazione del personale, l'Ente stabilisce periodicamente percorsi formativi, specifici e generali, che coinvolgono tutte le figure professionali sul tema della transizione al digitale e l’aggiornamento dei documenti relativi alla gestione del flusso documentale.

1.11 DEMATERIALIZZAZIONE DEI PROCEDIMENTI AMMINISTRATIVI DELL’ENTE

L’Ente ha procedure tali da consentire, in coerenza con le disposizioni normative e regolamentari in materia, che siano prodotti, gestiti, inviati e conservati solo documenti informatici.

È prevista la riproduzione su carta degli originali informatici firmati e protocollati solo nel caso in cui il/la destinatario/destinataria non sia nelle condizioni di ricevere e visualizzare i documenti informatici.

Gli eventuali documenti cartacei ricevuti, dopo registrazione e segnatura di protocollo, sono sottoposti al processo di scansione per la loro dematerializzazione, benché venga conservato l’originale cartaceo (cfr. paragrafo 5.2.12).

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 all'eliminazione dei registri di protocollo 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 dall'Ente sono registrati nel registro ufficiale di protocollo informatico. Pertanto, tutti gli eventuali registri di protocollo, interni all'Ente, diversi dal registro ufficiale di protocollo informatico, sono aboliti ed eliminati con l'entrata in vigore del manuale stesso.

Il SA esegue comunque, periodicamente, dei controlli a campione sui Nodi Responsabili per verificare la corretta esecuzione del piano e l'utilizzo regolare dell'unico registro ufficiale di protocollo e, attraverso controlli ed ispezioni mirate, la validità dei criteri di classificazione utilizzati.

PIANO DI SICUREZZA INFORMATICA RELATIVO ALLA FORMAZIONE, GESTIONE, TRASMISSIONE, INTERSCAMBIO, ACCESSO ALLA CONSERVAZIONE DEI DOCUMENTI

Al fine di assicurare la sicurezza dell'impianto tecnologico dell'Ente, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti, sono adottate le seguenti misure tecniche ed organizzative:

- utilizzo di apparati firewall (Web application firewall e sistemi di Intrusion prevention system) per la protezione contro specifiche tecniche di violazione e compromissione dei sistemi e dei servizi applicativi;
- protezione contro specifiche tipologie di minacce (Distribuited Denail of service) che hanno l'obiettivo di rendere momentaneamente indisponibili i sistemi;
- autenticazione e autorizzazione per l'accesso degli/delle utenti;
- separazione fisica degli ambienti di produzione dagli ambienti di sviluppo e test;
- assegnazione ad ogni utente di una credenziale di identificazione costituita da un certificato digitale e da un profilo di autorizzazione, conformi al D.lgs. 196/2003 e s.m.i. e al Regolamento UE 679/2016 (GDPR);
- criteri e procedure per il salvataggio ed il ripristino della disponibilità dei dati, in conformità e nel rispetto del D.lgs. 196/2003 e s.m.i. e al Regolamento UE 679/2016 (GDPR);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati particolari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli/le interessati/interessate solo in caso di necessità.
- nomina ufficiale per il personale preposto al trattamento dati.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli

accessi e delle operazioni, svolte con il sistema di protocollazione e gestione dei documenti utilizzati, saranno consultati solo in caso di necessità dal/dalla Responsabile del Servizio e dal/dalla titolare dei dati e, ove previsto, dalle forze dell'ordine.

3.1. FORMAZIONE DEI DOCUMENTI – ASPETTI DI SICUREZZA

Il sistema di gestione documentale rispetta la normativa e le regole tecniche in vigore.

3.2. GESTIONE DEI DOCUMENTI

Il sistema operativo del server è configurato in modo tale da consentire:

- l'accesso esclusivo al server del sistema di gestione documentale da parte di utenti autorizzati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso.

Il sistema di gestione documentale:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato (Titolario);

3.3. LA GESTIONE DELLA SICUREZZA DEGLI ACCESSI AL SISTEMA

La gestione delle utenze è funzionale a garantire il processo di gestione dei documenti all’interno del sistema di gestione documentale.

3.4. CREAZIONE DELL’UTENZA

Le regole per controllare l'assegnazione dei privilegi di accesso al sistema di gestione documentale sono definite come segue:

- sono utilizzati identificativi univoci (imputabili a singolo individuo) per le utenze, in modo tale che l’utente sia responsabile delle proprie azioni; l'utilizzo di utenze tecniche (non direttamente imputabili a singolo individuo) non è consentito; sono previste utenze applicative, nei casi di alimentazione massiva asincrona dell’archivio, accompagnata dall’identificazione della persona fisica responsabile del dato.
- gli ID utente assegnati in passato ad altri/altre utenti non sono ri-assegnati;
- è attribuito un profilo tale per cui il livello di accesso fornito è appropriato e coerente al ruolo;
- l'accesso al sistema è fornito solo a conclusione delle procedure di autorizzazione;
- i privilegi dell’utente che abbia cambiato ruolo, posto di lavoro o abbia lasciato l'organizzazione sono rimossi o bloccati;

- sono eseguiti controlli periodici al fine di rimuovere o bloccare gli account non in uso.

3.5. CICLO DI VITA UTENZE CON AMPI PRIVILEGI

Con particolare riferimento alle Utenze con ampi privilegi si applicano le seguenti regole:

- annualmente, con le policy descritte ai punti precedenti, sono rivalidati i profili con ampi privilegi all'utente già assegnatario, questo anche nel caso in cui non abbia cambiato ruolo, posto di lavoro o non abbia lasciato l'organizzazione;
- è compito dei/delle Responsabili di Struttura, sulla base degli elenchi aggiornati, forniti dai sistemi informativi aziendali, circa le utenze con ampi privilegi, verificare che quanto descritto al punto precedente sia applicato.

3.6. GESTIONE DELLA PASSWORD

Una password è una stringa di caratteri utilizzata per l'autenticazione e, insieme all'ID utente, permette di dimostrare l'identità dell'utente.
Per garantire la riservatezza della password, i processi di assegnazione e di verifica sono eseguiti secondo le regole seguenti:

- l'utente deve essere informato/informata dei comportamenti da seguire e delle proprie responsabilità nell'utilizzo dei sistemi informatici, ivi incluse le norme per la gestione delle proprie password;
- l'utente deve essere dotato di una password temporanea sicura per il primo accesso, che deve essere costretto/costretta a modificare immediatamente a seguito del primo log-in;
- l'identità dell'utente che richiede una nuova password (temporanea) deve essere verificata prima dell'assegnazione;
- la comunicazione di una nuova password all'utente richiedente deve essere eseguita adottando metodi adeguati che consentano di mantenere la riservatezza;
- le password di default, fornite normalmente dal fornitore hardware/software, devono essere modificate subito dopo l'installazione di sistemi o di software;
- la combinazione di ID utente e password è il metodo più comune per verificare l'identità dell'utente, ma esistono anche altre tecnologie atte ad identificare ed autorizzare gli utenti (quali ad esempio la biometria, i token hardware, ecc.). Procedure per la gestione di tali tecnologie alternative devono attenersi alle direttive di cui sopra.
- Nello specifico del sistema documentale l'utente dell'Ente accede tramite user name e password.

3.7. REVISIONE DEI PRIVILEGI DI ACCESSO

Al fine di mantenere un controllo efficiente ed efficace in materia di accesso alle informazioni ed ai sistemi, è obbligatorio effettuare periodiche revisioni dei privilegi di accesso degli utenti utilizzando un processo formale basato sui seguenti principi:

- i diritti di accesso ed i relativi privilegi devono essere ri-attribuiti dopo ogni cambiamento di ruolo o la cessazione del rapporto di lavoro;
- le modifiche alle utenze con abilitazioni privilegiate devono essere registrate per

permettere una revisione periodica delle stesse.

3.8. FORMATI DI DOCUMENTI UTILIZZATI – FIRMATI – NON FIRMATI

3.8.1 DOCUMENTI INFORMATICI

I documenti informatici devono essere formati utilizzando formati portabili statici non modificabili che non possano contenere macro istruzioni o codici eseguibili.
Nella scelta sono preferiti gli standard documentali ISO e gli standard che consentono il WYSIWYG (What You See Is What You Get), ovvero che forniscono sulla carta una disposizione grafica uguale a quella rappresentata sullo schermo del computer.
Sono accettate e protocollate le comunicazioni in cui i documenti allegati rispettano le seguenti condizioni:
- Si suggerisce l'utilizzo del formato PDF – PDF/A, perché di maggior diffusione e leggibilità.
- Sono comunque accettati i formati TIFF, JPG, XML, p7m, TXT, EML.

Allegati in formati diversi (per esempio .doc, .xls, .dvg,) verranno rifiutati.
Nel caso di file compressi (.zip, .rar…), dopo la loro decompressione si procederà alla verifica degli stessi ed alla successiva acquisizione solo nel caso di formati ammessi.

3.8.2 DOCUMENTI INFORMATICI FIRMATI

Sono accettate e protocollate le comunicazioni in cui i documenti allegati firmati o marcati digitalmente rispettano le seguenti condizioni:
- Le firme si appongono a documenti nei formati sopra indicati (il formato dei documenti deve essere convertito in uno dei formati ammessi prima della sottoscrizione con firma digitale),
- Le firme siano valide al momento della ricezione da parte dell'Ente.

3.9. LA GESTIONE DELLA SICUREZZA APPLICATIVA

La gestione della sicurezza è definita attraverso delle regole di accesso agli oggetti del sistema che determinano:

- le abilitazioni alle funzionalità di cui possono disporre gli utenti all'interno del sistema;
- le restrizioni agli accessi sugli oggetti condivisi gestiti (fascicoli, serie, ...), in maniera indipendente dalle abilitazioni alle funzionalità.

Gli aspetti che concorrono nella gestione della sicurezza sono:

- livelli di visibilità;
- profilazione;
- controllo degli accessi (*ACL – A*ccess *C*ontrol *L*ist).

3.9.1. LIVELLI DI VISIBILITÀ

Sono applicati alle informazioni in modo da renderle visibili ed accessibili all'utente opportunamente profilato/profilata. Sono abbinati ai seguenti dati:

- *dati personali*: visibili a qualunque tipo di utente;
- *dati particolari*: visibili solo ad opportuni utenti profilati/profilate;

La visibilità delle informazioni è gestita tramite assegnazione specifica a:

- *struttura aggregativa:* limita la visibilità di tutti i suoi contenuti, nonché la visibilità della struttura aggregativa stessa. Il limite di visibilità di una struttura aggregativa si applica anche ai suoi metadati;
- *documento:* limita la visibilità del singolo documento.

Per quanto riguarda i dati personali e particolari, la limitazione della visibilità è indipendente dalla classificazione: un documento con più classificazioni ha sempre la medesima riservatezza.

I livelli di visibilità sono applicati oltre che alla consultazione anche alla ricerca, per cui il risultato di una ricerca rispetta il grado di visibilità dell'utente che l'ha eseguita e quindi presenta le sole strutture aggregative e i soli documenti che rispettano tale grado di visibilità.

3.9.2. PROFILAZIONE

La profilazione è il processo di attribuzione delle funzionalità ad un *profilo*. Ad ogni utente sono associati uno o più profili in base alle attività che deve svolgere definendo le *identità* (associazione utente-profilo).

L'associazione tra utente (CHI), collocazione (DOVE) e profili (COSA) è detta *identità collocata* e rappresenta il ruolo che l'utente riveste nei suoi ambiti lavorativi.

Ogni identità è collocata in una struttura organizzativa dell'Ente (nodo organizzativo) definendo il ruolo che l'utente riveste nel suo ambito lavorativo.

Gli utenti possono essere contemporaneamente collocati in più nodi dell'albero organizzativo andando a definire più identità collocate. Le collocazioni, oltre a descrivere la struttura di appartenenza dell'utente, sono fortemente legate alla profilazione; l'utente può rivestire ruoli differenti nell'Ente a seconda di dove è collocato/collocata in organigramma (Es. Mario Rossi svolge le mansioni di protocollista nell'ufficio Sistemi Informativi e di archivista per il Settore Personale).

3.9.3. CONTROLLO DEGLI ACCESSI (ACL – ACCESS CONTROL LIST)

Il controllo degli accessi indica se l'utente può applicare una funzionalità ad un certo oggetto del sistema di gestione documentale. La gestione delle abilitazioni degli/delle utenti all'accesso ai contenuti avviene attraverso liste di accessi (*ACL*), associate ad ogni singola struttura aggregativa. Le *ACL* specificano quali operazioni fondamentali (lettura, modifica, ecc.) sono possibili e quale gruppo di utenti può compierle. Le *ACL* sono definite solo sulle strutture aggregative, secondo le regole di seguito descritte.

3.9.4. ABILITAZIONI PER L'ACCESSO AL TITOLARIO

Ad ogni voce di titolario sono associate la "AOO, la Struttura e il Nodo". L'operatività sulla voce è consentita solo ai gruppi di utenti che appartengono alle AOO, alle Strutture e ai Nodi associati alla voce. Nel nostro Ente tutte le voci sono a disposizione dell'utente

3.9.5. ABILITAZIONI PER L'ACCESSO AI FASCICOLI TEMPORANEI

I fascicoli temporanei sono strutture aggregative particolari, utilizzate per la "classificazione parziale" dei documenti e per lo smistamento del flusso documentale in ingresso. Il loro accesso è quindi legato solo allo smistamento dei documenti e non a delle specifiche *ACL*. La creazione e la visibilità sono di competenza del SA.

3.9.6. ABILITAZIONI PER L'ACCESSO ALLE STRUTTURE AGGREGATIVE

Le operazioni possibili sulle strutture aggregative, *serie*, *dossier* e *fascicoli*, collegate alle *ACL* sono:

- Read (accesso e lettura della struttura aggregativa);
- Insert (creazione della struttura aggregativa e sua alimentazione);
- Modify (modifica della struttura aggregativa e azioni di riclassificazione e invito).

Una serie è sempre associata ad una struttura/nodo e, di conseguenza, ad una AOO ed ha una propria ACL.

3.9.7. ABILITAZIONI PER L'ACCESSO AI DOCUMENTI

Non è gestito il controllo degli accessi tramite *ACL* a livello di singolo documento. Quindi la visibilità di un documento dipende dall'identità collocata associata all'utente e dalla ACL presente sulla struttura aggregativa che lo contiene.

3.9.8. ABILITAZIONI PER L'ACCESSO ALLE TIPOLOGIE DI SERIE:

Le abilitazioni dipendono dalla tipologia di serie:

- *Serie di fascicoli:* Ogni singolo fascicolo presente all'interno della serie ha una struttura responsabile che non è sempre la stessa del nodo appartenente alla struttura associata alla serie e ad una *ACL* popolata alla creazione del fascicolo.
- *Serie tipologiche di documenti:* La serie tipologica di documenti ha un nodo responsabile ed una *ACL* definita a livello di serie. Il nodo responsabile è uno dei nodi che compongono la struttura organizzativa associata alla serie. Non sono previsti diritti di accesso sui singoli documenti; per dare l'accesso ad un utente su un singolo documento contenuto in una serie tipologica di documenti è comunque possibile utilizzare le funzionalità di smistamento dei documenti.
- *Serie di dossier:* all'interno della serie di dossier ogni singolo dossier ha un'associazione ad un nodo responsabile non sempre appartenente alla struttura cui la serie è associata e una *ACL*, popolata alla creazione con le regole definite per il fascicolo.

3.9.9. INVITI

L'invito è una modalità per dare accesso a strutture aggregative sulle quali un nodo organizzativo non ha privilegi. L'invito è applicato a *serie*, *dossier* e *fascicoli*.

L’invito è fatto solo a cura del nodo responsabile della materia della struttura aggregativa. Il destinatario dell’invito è sempre un nodo; non è consentito invitare un singolo utente del sistema. Le modalità di invito sono:

- in *lettura* per strutture aggregative appartenenti oppure non appartenenti alla stessa AOO;
- in *lettura/alimentazione* per strutture aggregative solo appartenenti alla stessa AOO.

L’invito è revocabile da parte del nodo che lo ha attivato.

Le regole di propagazione degli inviti in lettura hanno le seguenti caratteristiche:

- l’attivazione di un invito su un intero dossier:
    - propaga l’invito in lettura anche sulla serie di dossier che lo contiene, così, nel corso della navigazione, è possibile raggiungere il dossier;
    - non è propagato alcun invito verso i fascicoli all’interno del dossier: questi per essere visibili dal nodo invitato dovranno essere ulteriormente oggetto di invito da parte del nodo responsabile. Sono comunque visibili e accessibili i documenti all’interno del dossier in quanto i singoli documenti non hanno *ACL* specifiche.
- l’attivazione di un invito su un fascicolo all’interno di una serie di fascicoli propaga l’invito in lettura anche sulla serie di fascicoli che lo contiene; in questo modo è reso disponibile l’accesso al fascicolo nel corso della navigazione.

MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LA FORMAZIONE E LO SCAMBIO DEI DOCUMENTI INFORMATICI

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

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;

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

- informatico;
- analogico.

4.1. DOCUMENTO RICEVUTO

La corrispondenza ricevuta viene acquisita dall'Ente con diverse modalità, in base alla tipologia di trasmissione utilizzata dal/dalla mittente.

Un documento può essere recapitato:

1. a mezzo posta elettronica ordinaria o certificata;
2. a mezzo posta ordinaria o corriere;
3. a mezzo posta raccomandata;
4. per telegramma;
5. con consegna diretta da parte dell'interessato, o tramite una persona delegata, alle Strutture responsabili o aperti al pubblico;
6. ibrida: un documento analogico (lettera di accompagnamento) e un documento digitale su supporto informatico;
7. tramite servizi on line.

Ciascuna tipologia comporta metodi diversi di acquisizione.

4.2. DOCUMENTO INVIATO

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma, per mezzo della sola posta elettronica certificata o, in casi eccezionali, in formato analogico per posta ordinaria, raccomandata a/r, fax qualora non coinvolgano PA.

4.3. DOCUMENTO INTERNO

I documenti interni sono formati con tecnologie informatiche e lo scambio tra Strutture dell'Ente avviene attraverso il sistema documentale che prevede la possibilità di smistamento per firma elettronica, firma digitale, conseguente smistamento per protocollazione interna e smistamento verso la Struttura competente.

4.4. DOCUMENTO ANALOGICO (CARTACEO)

Il documento analogico è un documento formato su supporto cartaceo prodotto con strumenti analogici (es. documento scritto a mano o a macchina da scrivere) o con strumenti informatici (es. documento prodotto con un sistema di videoscrittura e stampato).
È considerato originale analogico il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali e sostanziali, comprendente tutti gli elementi di garanzia e di informazione, del mittente e del destinatario e dotato di firma autografa.
Si definisce copia dell'originale del documento conservato agli atti dell'AOO mittente, cioè nel fascicolo relativo alla pratica

Si può utilizzare il formato analogico esclusivamente qualora non sia stato dichiarato il domicilio digitale da parte del cittadino.

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

4.5. 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:

- contenere, nello spazio riservato all'oggetto, l'argomento trattato, indicato dall'autore/autrice, in maniera sintetica ma esaustiva;
- essere identificato univocamente da un solo numero di protocollo;
- essere classificato e può far riferimento anche a più fascicoli.

Le firme necessarie alla redazione e perfezionamento, sotto il profilo giuridico, del documento in partenza devono essere apposte prima della sua protocollazione.

II documento deve consentire l'identificazione dell'Ente mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'Ente;
- l'indicazione completa della Struttura responsabile che ha prodotto il documento;
- l'indirizzo completo dell'Ente (via, numero civico, CAP, città, provincia);
- il numero di telefono;
- l'indirizzo e-mail/PEC della Struttura responsabile che ha prodotto il documento.

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 digitale da parte del/della Responsabile della Struttura;
- se il documento è analogico deve contenere sigla autografa dell'istruttore e sottoscrizione autografa del/della Responsabile della Struttura.

4.6 FORMAZIONE DEI DOCUMENTI INFORMATICI

Come indicato dalla normativa dalle Linee guida dell'AgID, il documento informatico è formato mediante una delle seguenti principali modalità:

a) redazione tramite l'utilizzo di appositi strumenti software;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

La fase di formazione interna da parte dell'AOO di un documento informatico è

generalmente gestita esternamente al sistema di gestione documentale, da opportune procedure gestionali (ad esempio: Atti amministrativi, Bilancio, Applicazioni di workflow, ecc) o direttamente da strumenti di word processing. Una volta conclusa la redazione del documento, il sistema di gestione documentale può gestire il giro di visto/i e firma/e, se non è già stato compiuto all'interno della procedura gestionale. Il processo parte dall'inserimento del documento all'interno dell'appropriata struttura aggregativa (ad es. serie, fascicolo) nella porzione di titolario che riguarda la materia trattata, su cui è definita una responsabilità specifica da Organigramma. Al termine del flusso di visto e firma, il documento risulta ben formato e atto ad assolvere le funzioni per cui è stato prodotto (perfetto ed efficace). Nel caso in cui la procedura gestionale fornisca un documento già perfezionato (completo di visti e firma), il sistema di gestione documentale può acquisirlo via servizi applicativi o tramite procedure massive.

Le risorse strumentali e le procedure utilizzate per la formazione, archiviazione e conservazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'AOO-Struttura-Nodo di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati e/o protocollati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

Per attribuire in modo certo la titolarità del documento e la sua integrità il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui alle "Regole tecniche sul documento informatico".

Quando il documento informatico viene inserito nel sistema di gestione documentale ad esso vengono associati i metadati. L'insieme minimo dei metadati è costituito da:

a) l'identificativo univoco e persistente;

b) il riferimento temporale;

c) l'oggetto;

d) il soggetto che ha formato il documento;

e) l'eventuale destinatario/destinataria;

f) l'impronta del documento informatico.

Eventuali ulteriori metadati sono definiti in funzione del contesto e delle necessità gestionali e conservative.

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, al fine di garantirne l'immodificabilità, sono convertiti in formato pdf secondo gli standard previsti dalla normativa vigente in materia di conservazione (vedi Allegato 2 alle "Regole tecniche sul documento informatico").

4.8. FIRMA DIGITALE

La firma digitale è utilizzata per dare ai documenti informatici la valenza giuridico-probatoria.

L'acquisizione del documento all'interno del sistema di gestione documentale prevede la verifica della firma digitale e la produzione di un rapporto di verifica che viene archiviato sotto forma di metadati del documento.

I passi di verifica previsti sono:

1. Verifica conformità e integrità della busta crittografica;
2. Verifica della consistenza della firma;
3. Verifica della validità del certificato di firma;
4. Verifica dell'Ente certificatore (CA - Certification Authority);
5. Verifica della lista di revoca del certificato (CRL – Certificate Revocation List aggiornata disponibile);
6. Verifica lista di revoca – certificato non presente nella CRL.

- I tipi di firma digitale in uso nell'Ente sono CADES, PADES e XADES. I soggetti del Consiglio cui viene assegnata una firma digitale per ragioni di servizio sono tenuti a provvedere tempestivamente al rinnovo dei certificati prossimi alla scadenza, con l'anticipo comunicato dal settore sistemi informativi,"

Il rapporto di verifica con esito positivo sui sei passi garantisce la presenza di una firma digitale e quindi il valore giuridico del documento informatico presente nel sistema di gestione documentale.

4.9. 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. 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;
- convertirlo in pdf che garantisca l'immodificabilità dei documenti e utilizzo della posta elettronica certificata deliberate dall'Ente;
- apporvi la firma digitale;
- inserirlo nel sistema di gestione documentale, all'interno della struttura aggregativa relativa al procedimento di cui tratta;
- smistarlo per protocollazione in partenza;
- inserire i dati del/della destinatario/destinataria: denominazione, indirizzo, casella di posta elettronica (ricavati dalla funzionalità AOO – Interscambio presente nella ricerca anagrafica del protocollo informatico)
- prima di ogni invio a soggetto esterno bisogna verificare su INAD la presenza di un domicilio digitale;
- assegnare il numero di protocollo in uscita al documento firmato digitalmente;
- invio del messaggio contenente il documento firmato e protocollato in uscita alla casella di posta del destinatario.

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

- garantire l'immodificabilità del 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 appartenenti ad altre amministrazioni.

Gli automatismi sopra descritti consentono 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.

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.

Prima di ogni invio a soggetti esterni è opportuno verificare la presenza su INAD del domicilio digitale.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al/alla destinatario/destinataria se trasmesso all'indirizzo elettronico da questi/questa 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 a terzi. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale, nei casi consentiti dalla legge, alla notifica per mezzo della posta.

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.

Le strutture nodo responsabile non effettuano fotocopie della corrispondenza trattata, sia in ingresso che in uscita.

5.1. GENERALITÀ

Per descrivere i flussi di lavorazione dei documenti all'interno dell'Ente 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:

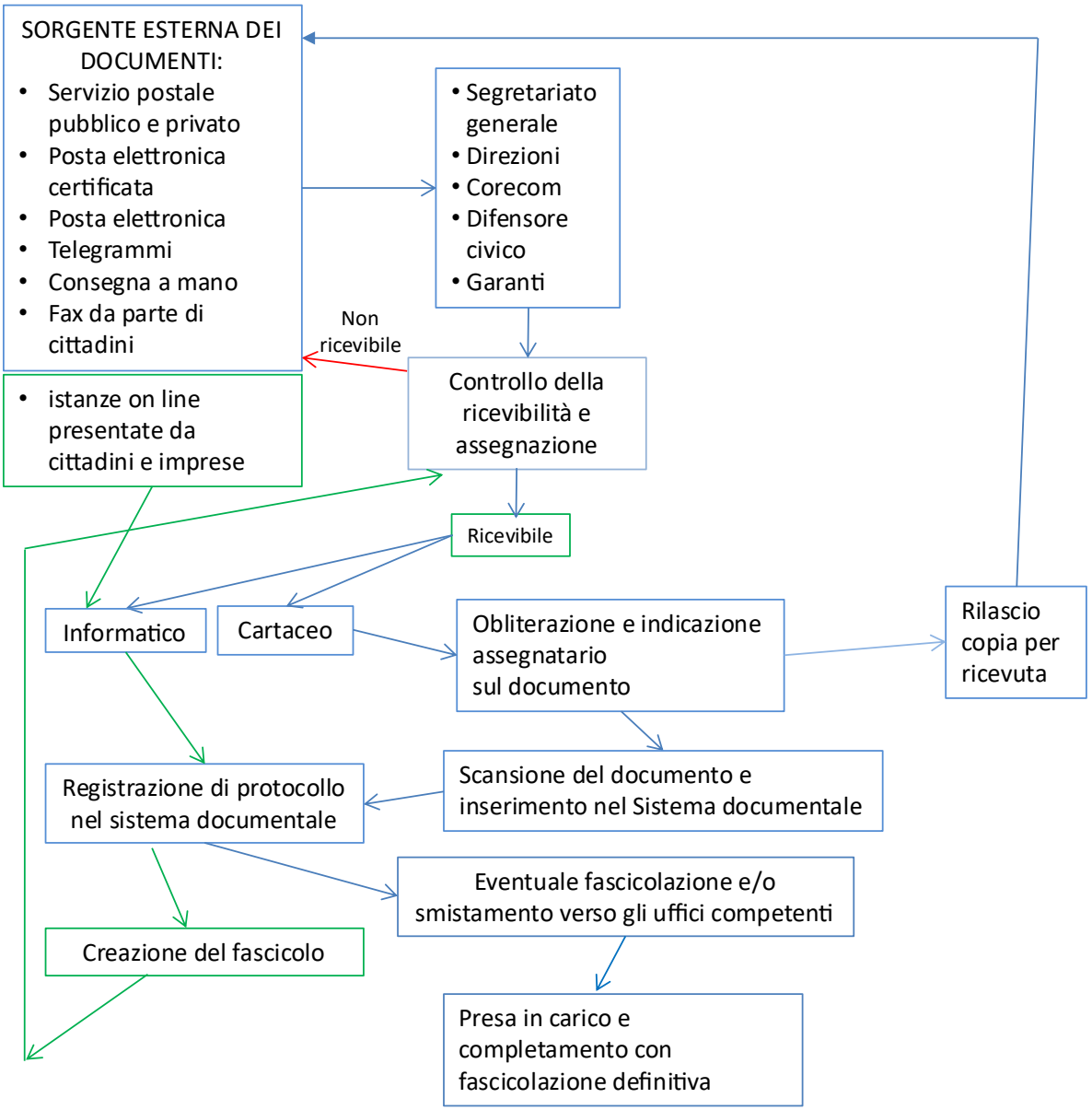
- ricevuti dalla AOO, dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno alla AOO;
- inviati dalla AOO all'esterno o anche all'interno della AOO in modo formale.

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 ma non esclude la possibilità di inserimento nel sistema documentale.

5.1.1. SORGENTE ESTERNA DEI DOCUMENTI:

- Servizio postale pubblico e privato;
- Posta elettronica certificata;
- Posta elettronica;
- Telegrammi;
- Consegna a mano;
- Fax da parte di cittadini/cittadine;
- Servizi on line;
- Istanze on line presentate da cittadini e imprese

5.2. DIAGRAMMA DI FLUSSO DEI DOCUMENTI IN ENTRATA ALLA AOO



5.2.1. RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ELETTRONICA CERTIFICATA ISTITUZIONALE (PEC)

Di norma, la ricezione dei documenti informatici avviene tramite la casella di posta elettronica certificata istituzionale che è accessibile solo al Segretariato generale, alle Direzioni o alle Strutture Nodo Responsabile dell'AOO che, previa verifica della validità della firma apposta, della leggibilità del documento nonché della autenticità, della provenienza e dell'integrità dei documenti stessi, procede alla registrazione di protocollo ed alla assegnazione ai Nodi Operativi di competenza.

Nel caso in cui pervengano sulla casella di posta elettronica certificata istituzionale dell'AOO messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore/operatrice, senza registrare nel protocollo, rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - Non di competenza di questo Ente". Nell'eventualità che sia già stata effettuata la registrazione di protocollo si risponderà con nota protocollata al mittente che non è di competenza dell'Ente.

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti, recanti standard del formato dei documenti (Allegato 2), modalità di trasmissione, definizione dei tipi di informazioni minime, associate ai documenti protocollati.

Qualora i documenti allegati ai messaggi di posta elettronica certificata non siano dotati di firma digitale e si renda necessario attribuire agli stessi efficacia probatoria, il messaggio è inserito nel sistema di gestione documentale apponendo la dicitura, come nota formale, "documento ricevuto via posta elettronica certificata con il formato di origine non idoneo su indicazione del/della responsabile del procedimento amministrativo (RPA)" 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/dalla RPA.

Il personale del Segretariato generale, delle Direzioni o delle Strutture Nodo Responsabile controlla più volte nella giornata lavorativa i messaggi pervenuti nella casella di posta istituzionale e verifica se sono da protocollare.

5.2.2. RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ELETTRONICA ORDINARIA ISTITUZIONALE

Nel caso in cui il messaggio sia ricevuto su una casella di posta elettronica ordinaria istituzionale, per poter procedere alla protocollazione, si dovrà trasformare la mail ricevuta in formato pdf. I controlli da effettuare sul messaggio sono quelli richiamati nel paragrafo precedente.

5.2.3. RICEZIONE DI ISTANZE ON LINE PRESENTATE DAI CITTADINI E IMPRESE ATTRAVERSO LA PROCEDURA MOON

Il cittadino o l'impresa può presentare la propria istanza accedendo al sito del Consiglio regionale e accreditandosi con SPID, CIE O CNS (Carta Nazionale dei Servizi), per esempio la presentazione della richiesta di patrocinio oneroso.

5.2.4. 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 allegati su supporto rimovibile il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e adempimenti del caso (es. verifica firma mittente, etc..).
L'acquisizione degli allegati digitali nel SdP può avvenire solo se la grandezza totale di ogni allegato non supera il limite di 20 Megabyte.
Attualmente il sistema documentale consente di archiviare documenti informatici sino ad una dimensione massima di 20 MB; il limite è imposto dal requisito di avere transazioni web on-line sincrone di scrittura sui file system documentali che, in un'unica transazione, effettuino i controlli formali sui documenti e sui metadati, scrivano sul DB i metadati e archivino nel file system il documento informatico.

Nell'eventualità che il documento superi le dimensioni supportate in fase di protocollazione si andrà a segnalare, nella nota formale, l'esistenza dell'allegato descrivendolo e motivandone la mancanza. Sarà cura del/della Responsabile del procedimento inserire un'ulteriore nota formale con l'indicazione di dove verrà archiviato il documento mancante.

5.2.5. RICEZIONE DI DOCUMENTI CARTACEI A MEZZO POSTA CONVENZIONALE

I documenti pervenuti a mezzo posta sono consegnati al Segretariato generale o alla Direzione.

Per la corrispondenza relativa alle gare d'appalto si fa riferimento alle modalità specificate nelle "Linee guida in materia di contratti pubblici", come riportato nel Piano Triennale di Prevenzione della Corruzione (PTPC).

Solo la corrispondenza che riporta sul contenitore la dicitura "riservata personale" non è aperta ed è consegnata direttamente al/alla destinatario/destinataria il/la quale dopo la verifica della ricevibilità provvederà alla consegna al protocollo.

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 9 "Modalità di produzione e di conservazione delle registrazioni di protocollo informatico".

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 è aperta lo stesso giorno lavorativo in cui è pervenuta e obliterata dalla Direzione competente. Prima della protocollazione essa è assegnata contestualmente all'apertura, con indicazione del destinatario e la sigla di chi assegna il documento. Nel caso di raccomandate, la busta è allegata al documento per la parte recante i timbri postali.

5.2.6. PROVENIENZA DI DOCUMENTI INTERNI FORMALI

Per documento interno formale si intende qualunque documento prodotto e inviato formalmente da una struttura ad un'altra dell'Ente.

Il documento interno deve essere solo in formato digitale, sottoscritto digitalmente,

protocollato in modalità "interna" e il mezzo di trasmissione deve essere lo smistamento interno alla gestione documentale.

La struttura ricevente non deve procedere alla protocollazione, in quanto il documento è già protocollato, ma solo alla presa in carico e completamento con la fascicolazione o eventuale smistamento al nodo competente per materia.

5.2.7. PROVENIENZA DI DOCUMENTI INTERNI INFORMALI

Per documento interno informale si intende qualunque documento prodotto e inviato informalmente da una struttura ad un'altra dell'Ente.

Il documento interno deve essere solo in formato digitale, non protocollato e il mezzo di trasmissione può essere lo smistamento interno alla gestione documentale oppure la posta elettronica ordinaria.

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 per il recapito 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 del capitolo 9 "Modalità di produzione e di conservazione delle registrazioni di protocollo informatico".

5.2.10. RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI INFORMATICI

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

Il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, gestisce i messaggi scambiati tra le pubbliche amministrazioni seguendo le indicazioni dell'AgID

5.2.11. RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI CARTACEI

Il Segretariato generale, le Direzioni non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione come art. 53 del 28/12/2000 TU 445.

La semplice apposizione del timbro datario della struttura sulla copia non ha alcun valore giuridico, in quanto non sostituisce la protocollazione.

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

- fotocopiare gratuitamente la prima pagina del documento;
- apporre sulla copia il timbro dell'amministrazione, con la data, l'ora di arrivo e la

sigla del/della funzionario/funzionaria ricevente.

Nel caso di corrispondenza pervenuta ad un ufficio, quest'ultimo dopo aver rilasciato la ricevuta di avvenuta ricezione deve consegnarla alla Direzione per l'assegnazione e protocollazione.

5.2.12. ASSEGNAZIONE, PRESA IN CARICO DEI DOCUMENTI E CLASSIFICAZIONE.

Il Segretariato generale, le Direzioni procedono alla verifica della ricevibilità del documento, sia cartaceo che informatico, e alla sua assegnazione alla struttura competente per materia.

Iter relativo la documentazione istituzionale:

- La documentazione istituzionale PDL, PTR, ITR, OdG, ITRRI, ITP, Mozioni, PDCR, Pareri viene inserita nella piattaforma "Scrivania del Consigliere" e, a seguito della verifica di ricevibilità da parte del Segretario generale, il sistema crea il fascicolo relativo all'atto. I DDL e le DGR, pervenuti dalla Giunta regionale via PEC, vengono protocollati dal PG che effettua l'eventuale repertoriazione e gestisce gli inviti sul fascicolo creato nel sistema documentale verso gli uffici competenti smistando per competenza il documento al nodo responsabile della struttura.
- In generale la documentazione ricevuta viene smistata al nodo responsabile della struttura che individua il nodo operativo a cui smistare il documento per competenza.
- Il nodo operativo dopo aver preso in carico il documento individua la voce del titolario, dell'eventuale serie di fascicoli o di dossier o di tipologie documentarie e procede alla fascicolazione.
- In caso di smistamento errato l'ufficio destinatario contatta l'ufficio mittente, il quale revoca lo smistamento. In caso di rifiuto del documento, per evitare che il documento resti senza assegnazione, bisogna contattare l'ufficio mittente per permette di effettuare lo smistamento.

5.2.13. CONSERVAZIONE DEI DOCUMENTI INFORMATICI NELL'ARCHIVIO CORRENTE

I documenti informatici ricevuti dall'Ente sono archiviati nel sistema di gestione documentale dedicato, in modo non modificabile e, laddove normato, sono conservati presso il conservatore accreditato come definito nel manuale della conservazione.

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 non costituisce un sistema informatico documentale, con documenti digitali e pertanto è necessario conservare gli originali dei documenti cartacei nell'archivio corrente per il tempo indicato nel Titolario e piano di conservazione (allegato n. 1).

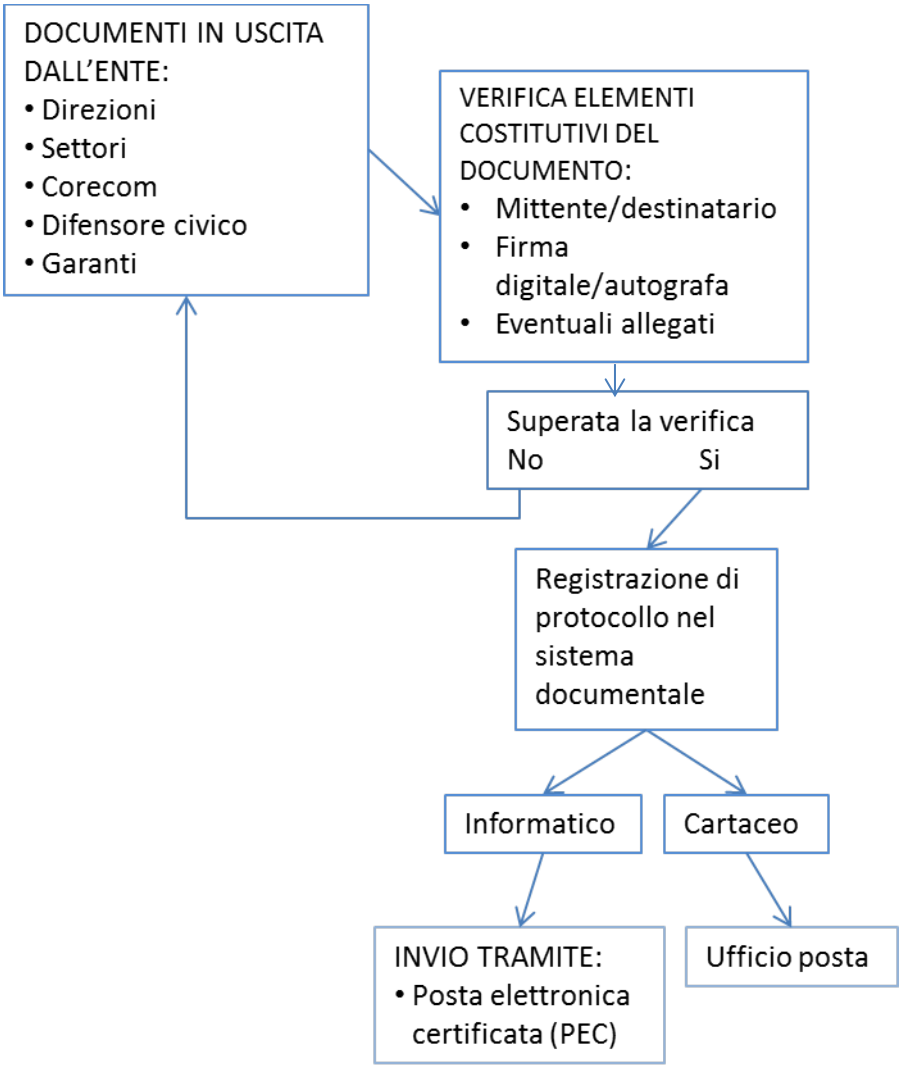
Il processo di scansione avviene secondo le fasi di seguito indicate:

- 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;
- scansione separata degli allegati;

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

Gli originali dei documenti cartacei ricevuti vengono inviati alle strutture competenti che provvedono ad archiviarli e conservarli in quanto la copia per immagine di documento analogico, non avendo l'attestazione di conformità e non essendo firmata digitalmente, non può avere la stessa efficacia probatoria dell'originale da cui è tratta.

5.3. FLUSSO DEI DOCUMENTI IN USCITA DALL'ENTE



L'opzione "Cartaceo" presente nel diagramma si riferisce all'eventuale invio al cittadino di copie analogiche di documenti informatici in assenza di domicilio digitale ai sensi dell'art 3-bis, commi 4-bis, 4-ter e 4-quater del "Codice".

5.3.1. SORGENTE INTERNA DEI DOCUMENTI

Per "sorgente interna dei documenti in uscita" s'intende la documentazione prodotta dal personale degli uffici dell'Ente, nell'esercizio delle proprie funzioni, avente rilevanza giuridico-probatoria e destinata ad essere trasmessa, tramite Pec, all'esterno dell'Ente (altre Amministrazioni, ditte, etc).

5.3.2. TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO POSTA

La Struttura responsabile provvede direttamente alle operazioni di spedizione della corrispondenza:

- predisposizione delle ricevute di invio e di ritorno per le raccomandate, unitamente alla distinta delle medesime da rilasciare all'ufficio postale;
- consegna all'ufficio postale di tutta la corrispondenza;

Qualora i/le destinatari/destinatarie siano più di uno/una vengono inviate solo le copie dell'unico originale (che resta agli atti dell'ufficio) prodotto dalle strutture responsabili.

5.3.3. SMISTAMENTO PER VERIFICA FORMALE DEI DOCUMENTI E FIRMA

Tutti i documenti originali da spedire, in formato digitale, sono smistati per firma attraverso la procedura documentale alla Struttura Nodo Responsabile che verifica la conformità della documentazione ricevuta allo standard formale (logo, descrizione completa dell'amministrazione, mittente, destinatario e, se dichiarati, la presenza di allegati). Se il documento è completo, viene firmato digitalmente e smistato per la registrazione di protocollo, nel caso contrario rifiutato/restituito all'ufficio mittente con le osservazioni del caso.

Tutti i documenti originali da spedire, in formato analogico, dopo le verifiche di conformità e la firma autografa sono descritti a livello di metadati con segnaposto nella procedura documentale, i dati inseriti sono smistati alla Struttura Nodo Responsabile per la protocollazione seguiti dal cartaceo che sarà scansionato e collegato al numero di registrazione (cfr. 6.2).

5.3.4. REGISTRAZIONE DI PROTOCOLLO E SEGNATURA

Le operazioni di registrazione e di apposizione della segnatura del documento in uscita sono effettuate dagli uffici individuati dalle strutture apicali.

La compilazione di moduli, se prevista (ad esempio: per spedizioni per raccomandata con avviso di ricevimento, posta celere, corriere) è a cura delle strutture responsabili.

5.3.5. AFFRANCATURA DEI DOCUMENTI IN PARTENZA

Tutte le attività di affrancatura della corrispondenza inviata per posta vengono svolte dall'Ufficio posta dell'Ente.

Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata all'Ufficio posta.

5.3.6. 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 dal destinatario, ovvero abilitato alla ricezione della posta per via telematica.

Per la spedizione dei documenti informatici, l'Ente si avvale dei servizi PEC e di firma

digitale di un certificatore accreditato iscritto nell'elenco pubblico tenuto dall'AgID.

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici, non possono 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.

5.3.7. INSERIMENTO DELLE RICEVUTE DI TRASMISSIONE NEL FASCICOLO

Le ricevute delle raccomandate del documento cartaceo spedito sono conservate all'interno del relativo fascicolo.

Per quanto concerne le ricevute del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, la procedura in uso la associa automaticamente alla registrazione di protocollo.

REGOLE DI ASSEGNAZIONE E PROTOCOLLAZIONE DEI DOCUMENTI RICEVUTI

II presente capitolo contiene le regole di assegnazione, adottate dalle strutture responsabili per i documenti in ingresso.

6.1. ASSEGNAZIONE DEI DOCUMENTI

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 effettuata dai Direttori, o loro delegati, consiste nell'operazione di individuare l'ufficio competente per materia.

Con l'assegnazione si provvede ad attribuire la responsabilità ad un soggetto fisico che si identifica nel Responsabile designato del Procedimento Amministrativo o del semplice processo.

Nel caso di documento informatico:

- PEC: inserimento nella Inbox del Protocollo generale o del Segretariato generale/Direzione/Settore competente
- Cartaceo: apposizione sul documento dell'assegnazione (per competenza o per conoscenza) con sigla del responsabile o suo delegato all'ufficio competente e consegna al Protocollo generale o al Segretariato generale/Direzione/Settore competente.

6.2. PROTOCOLLAZIONE DEI DOCUMENTI

Di seguito all'assegnazione i documenti sono protocollati e, sfruttando le funzionalità del sistema documentale, possono essere smistati per competenza/conoscenza ai diversi nodi responsabili che avranno cura di fascicolarli.

I documenti in formato cartaceo sono acquisiti dal sistema nel formato immagine con l'ausilio di scanner e l'originale consegnato all'ufficio competente.

L'operazione di acquisizione dell'immagine dei documenti cartacei deve essere effettuata prima che l'operazione di segnatura sia stata eseguita, dopodichè si devono riportare gli elementi minimi ed essenziali della registrazione sul documento cartaceo (data, n. protocollo e assegnazione es. 0001/A0300).

Preso atto dell'assegnazione, il/la Responsabile del Procedimento amministrativo verifica la competenza e, se esatta, provvede:

- alla presa in carico del documento che gli è stato assegnato/assegnata e all'inserimento nel fascicolo secondo le voci del titolario;

oppure

- a inoltrarlo, se del caso, al Nodo organizzativo che provvederà alla presa in carico e al completamento della fascicolazione.

In caso di errata assegnazione l'ufficio destinatario contatta l'ufficio mittente il quale revoca lo smistamento. In caso di rifiuto del documento, per evitare che il documento resti senza assegnazione, bisogna contattare l'ufficio mittente per permette di effettuare il corretto smistamento

Il Sistema documentale 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 risultante serve anche per individuare i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità, tenendo conto che i termini per il procedimento amministrativo decorrono dalla data di protocollazione ad eccezione dei casi disciplinati da altri regolamenti (es. Accesso civico, Gare).

La "presa in carico" dei documenti informatici è registrata dal sistema in modo automatico.

RESPONSABILE DEL SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Il presente capitolo individua la struttura Organizzativa Responsabile delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno dell'Ente, denominato Servizio Archivistico.

Il servizio in argomento è stato identificato e formalizzato con DUP n. 28 del 2 marzo 2009 e ha la competenza di gestire l'intera documentazione archivistica - ovunque trattata, distribuita o conservata - ai fini della sua corretta collocazione, classificazione e conservazione.

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

8.1. DOCUMENTI ESCLUSI

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53, comma 5, del DPR 28 dicembre 2000, n. 445 come gli esempi di seguito riportati:

- le gazzette ufficiali;
- i bollettini ufficiali e i notiziari della pubblica amministrazione;

- le note di ricezione delle circolari, delle pec e altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali, le riviste, i libri, i materiali pubblicitari;
- gli inviti a manifestazioni ad eccezione di quelli con rilevanza di procedimento;
- tutti i documenti già soggetti a registrazione particolare dell'amministrazione (es. determinazioni …). La registrazione particolare consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione documentale avuto riguardo, nello specifico, alla classificazione, alla fascicolazione, all'indicizzazione.

8.2. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

8.2.1 ARCHIVIO CORRENTE DI DEPOSITO E STORICO DELLA DOCUMENTAZIONE

L'archivio corrente è costituito dall'insieme organico dei documenti relativi ad attività in corso di trattazione ed è curato dai/dalle funzionari/funzionarie responsabili, in stretto raccordo con il/la responsabile del servizio archivistico.
All'inizio di ogni anno e di ogni legislatura il/la responsabile del servizio archivistico provvede a monitorare lo stato dei fascicoli aperti, esegue la chiusura per quelli relativi all'attività conclusa su indicazione dei/delle funzionari/funzionarie responsabili e procede all'istruzione dei nuovi fascicoli in stretto raccordo con i/le funzionari/funzionarie responsabili.

L'archivio di deposito è costituito dalla documentazione relativa ad attività concluse ed ancora utili all'Ente.
Il/La responsabile del servizio archivistico d'intesa con i/le funzionari/funzionarie responsabili organizza periodicamente il versamento della documentazione dall'archivio corrente all'archivio di deposito del materiale cartaceo, lasciando in consultazione comunque le strutture archivistiche costituite da documenti informatici e analogici.

I/Le funzionari/funzionarie responsabili predispongono gli elenchi della documentazione da versare all'archivio di deposito compilando l'apposito modulo presente sulla Intranet.

La consultazione dei fascicoli versati in deposito può avvenire dopo aver compilato l'apposito modulo, presente sulla Intranet, previa autorizzazione da parte del/della responsabile della struttura competente per materia e attraverso il/la responsabile del servizio archivistico.

Un fascicolo conservato nell'archivio di deposito può essere consultato anche per periodi lunghi ma non può più far parte nuovamente dell'archivio corrente; qualora si dovessero riattivare i termini del procedimento è necessario istruire un nuovo fascicolo nel quale saranno riferiti i dati identificativi del vecchio fascicolo per creare il vincolo archivistico. Nel fascicolo informatico sarà la nota formale a riportare i dati identificativi del vecchio fascicolo.

I fascicoli, siano essi cartacei o informatici o ibridi, possono essere consultati e può esserne richiesta copia conforme qualora ci sia un interesse legittimo.
Il sistema documentale consente di estrarre le così dette rendition di documentazione

nativa informatica confermando l’autenticità del documento.

8.3. PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI

8.3.1. CARATTERISTICHE GENERALI

Il presente capitolo illustra il sistema di classificazione dei documenti, di formazione del fascicolo e di tenuta 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).
Il Titolario è definito come un "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'Ente, al quale viene ricondotta la molteplicità dei documenti prodotti".

Il Titolario 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 Titolario e il Piano di conservazione sono adottati dall'amministrazione con atti formali a firma del/della direttore/direttrice competente in materia.
In caso di modifica del Titolario allegato non è obbligatorio riapprovare il Manuale.

8.3.2. 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'Ente, 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 (Ministero/Soprintendenza ai beni archivistici del Piemonte e Valle d’Aosta).

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 conservati nell’archivio dell’Ente è subordinato all'autorizzazione della struttura competente per materia in base al nullaosta rilasciato dalla Soprintendenza ai beni archivistici del Piemonte e Valle d’Aosta.

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

8.4. TITOLARIO E PIANO DI CONSERVAZIONE

8.4.1. TITOLARIO

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

Il Titolario si suddivide, di norma, in titoli e livelli gerarchicamente ordinati;

Il titolo individua per lo più funzioni primarie e di organizzazione dell'Ente (macrofunzioni); le successive voci corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato, secondo lo schema riportato nell'allegato Titolario.

Il Titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche anche in forza della normativa nazionale.

L'aggiornamento del Titolario compete esclusivamente alla Direzione competente per materia, quando necessario e opportuno.

Dopo ogni modifica del Titolario, il Servizio Archivistico 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 voci.

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

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

Per ogni specifica voce viene riportata, automaticamente, la data di inserimento e la data di variazione.

Di norma, le variazioni vengono introdotte immediatamente per permettere all'utenza l'immediata organizzazione della documentazione.

Rimane possibile la registrazione di documenti in fascicoli già aperti fino alla conclusione e alla chiusura degli stessi.

8.4.2. CLASSIFICAZIONE DEI DOCUMENTI

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze dell'Ente.

Essa è eseguita in base al Titolario di classificazione al quale è integrato il Piano di conservazione dell'archivio.

Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, voce, sottovoce), il numero del fascicolo e, eventualmente, del sottofascicolo.

La classificazione è applicata interamente dagli/dalle operatori/operatrici.

8.5. STRUTTURE ARCHIVISTICHE

8.5.1. SERIE

La serie è un raggruppamento omogeneo di documenti, fascicoli o dossier. Sono definite tre tipologie di serie:

- serie tipologica di documenti, con gli eventuali volumi;
- serie di fascicoli, con gli eventuali sottofascicoli;
- serie di dossier, con gli opportuni fascicoli all'interno.

8.5.2. REPERTORI

L'elenco dei fascicoli per AOO presenti sotto una certa voce di titolario costituisce il repertorio dei fascicoli che si può ottenere con la funzione di ricerca di fascicoli, presente nel sistema di gestione documentale, partendo da una determinata voce di titolario.
Mentre il titolario 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.

8.5.3. VOLUMI

Il volume è una suddivisione di strutture aggregative realizzata per ragioni di ergonomia.
I volumi sono creati per risolvere problematiche di gestione di strutture aggregative particolarmente voluminose o per suddividere temporalmente strutture aperte per lunghi intervalli temporali.
Il volume è visto come una porzione di un fascicolo, di un sottofascicolo, di una serie tipologica di documenti o di una serie di fascicoli.

8.5.4. FASCICOLAZIONE DEI DOCUMENTI

Tutti i documenti registrati nel sistema di protocollo informatico, indipendentemente dal supporto sul quale sono formati e dalla registrazione, sono riuniti in fascicoli.
Ogni documento, dopo la classificazione, viene inserito nel fascicolo di riferimento e all'occorrenza nel sottofascicolo secondo l'ordine cronologico di registrazione.

8.5.5. APERTURA DEL FASCICOLO

Quando un nuovo documento viene recapitato all'Ente, il/la funzionario/funzionaria abilitato/abilitata all'operazione di fascicolazione stabilisce, se il documento stesso debba essere ricollegato ad un'attività o procedimento in corso - e pertanto debba essere inserito in un fascicolo già esistente - oppure se il documento si riferisce a una nuova attività, o procedimento, per cui è necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

- ✓ se il documento si ricollega ad una attività o procedimento in corso, l'addetto/addetta prende in carico il documento smistato e lo inserisce nel fascicolo di materia già esistente.
- ✓ se il documento non è ricollegabile ad alcuna attività in corso l'addetto/addetta procede attraverso l'operazione di "apertura", a creare un nuovo fascicolo nella voce di titolario relativa alla materia.

Il fascicolo comprende la registrazione di alcune informazioni essenziali (metadati):

- ✓ indice di classificazione (titolo e voci attinenti la materia);
- ✓ numero del fascicolo (assegnato in automatico dal sistema);
- ✓ oggetto del fascicolo, individuato sulla base della materia indicata nelle voci;
- ✓ data di apertura del fascicolo (assegnata in automatico dal sistema);
- ✓ Nodo Responsabile (indicato automaticamente dal profilo con il quale l'operatore/operatrice accede al sistema);
- ✓ livello di riservatezza, se diverso da quello standard applicato dal sistema.

8.5.6. MODIFICA DELL'ASSEGNAZIONE DEI FASCICOLI

Nell'eventualità si verifichi una variazione nelle competenze e attività dei nodi operativi (es. riorganizzazioni) e sia necessario modificare l'assegnazione di un fascicolo, il Servizio archivistico provvede a variare la responsabilità del fascicolo.

Il sistema documentale tiene traccia di questi passaggi, memorizzando, per ciascuno di essi, l'identificativo dell'operatore/operatrice che effettua la modifica, la data e l'ora dell'operazione, storicizzando i diversi passaggi di responsabilità.

8.5.7. APERTURA DEL DOSSIER

La formazione di un nuovo dossier avviene attraverso l'operazione di "apertura", che prevede l'inserimento delle seguenti informazioni essenziali:

- ✓ indice di classificazione (titolo e voci attinenti la materia);
- ✓ il numero del dossier (assegnato in automatico dal sistema);
- ✓ la data di creazione (assegnato in automatico dal sistema);
- ✓ il/la responsabile del dossier;
- ✓ la descrizione o l'oggetto del dossier;
- ✓ livello di riservatezza, se diverso da quello standard applicato dal sistema.

8.5.8. CHIUSURA DELLE STRUTTURE ARCHIVISTICHE

La chiusura delle strutture archivistiche è effettuata alla fine della relativa attività e il sistema congela la data dell'azione di chiusura.

Nell'eventualità si verificasse l'esigenza di inserire ulteriori documenti le strutture archivistiche possono essere riaperte e nell'azione di chiusura il sistema storicizza la data.

8.6. CONSULTAZIONE E MOVIMENTAZIONE DELL'ARCHIVIO CORRENTE, DI DEPOSITO E STORICO

8.6.1. PRINCIPI GENERALI

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

8.7. ACCESSO ALLA DOCUMENTAZIONE

8.7.1. CONSULTAZIONE DOCUMENTAZIONE IN ARCHIVIO

Le strutture responsabili, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i documenti conservati, sia su supporto cartaceo sia informatico, compilando apposito modulo pubblicato sulla Intranet, contenente gli estremi identificativi della documentazione richiesta, il nominativo del/della richiedente e la firma del/della responsabile di materia.

La visibilità temporanea di un documento conservato avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.

Tale movimentazione viene registrata a cura del/della responsabile del servizio archivistico in una serie tipologica 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/La responsabile del servizio archivistico verifica che la restituzione dei documenti affidati temporaneamente avvenga alla scadenza prevista.

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

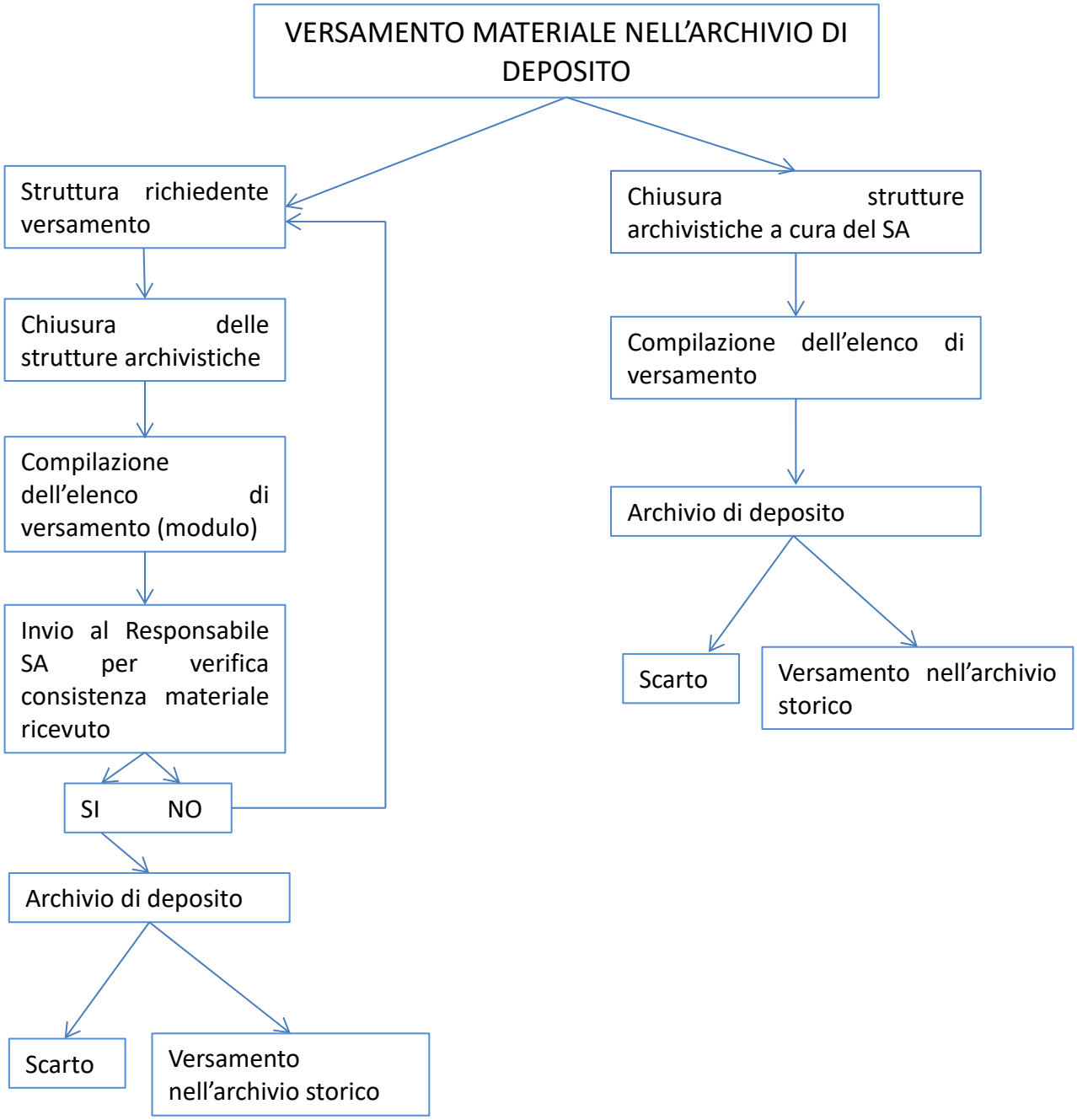
Nel caso di accesso ad archivi informatici il SA procede ad invitare la struttura richiedente al fascicolo, oppure ad estrarre copia del documento che verrà inviato mezzo posta elettronica.

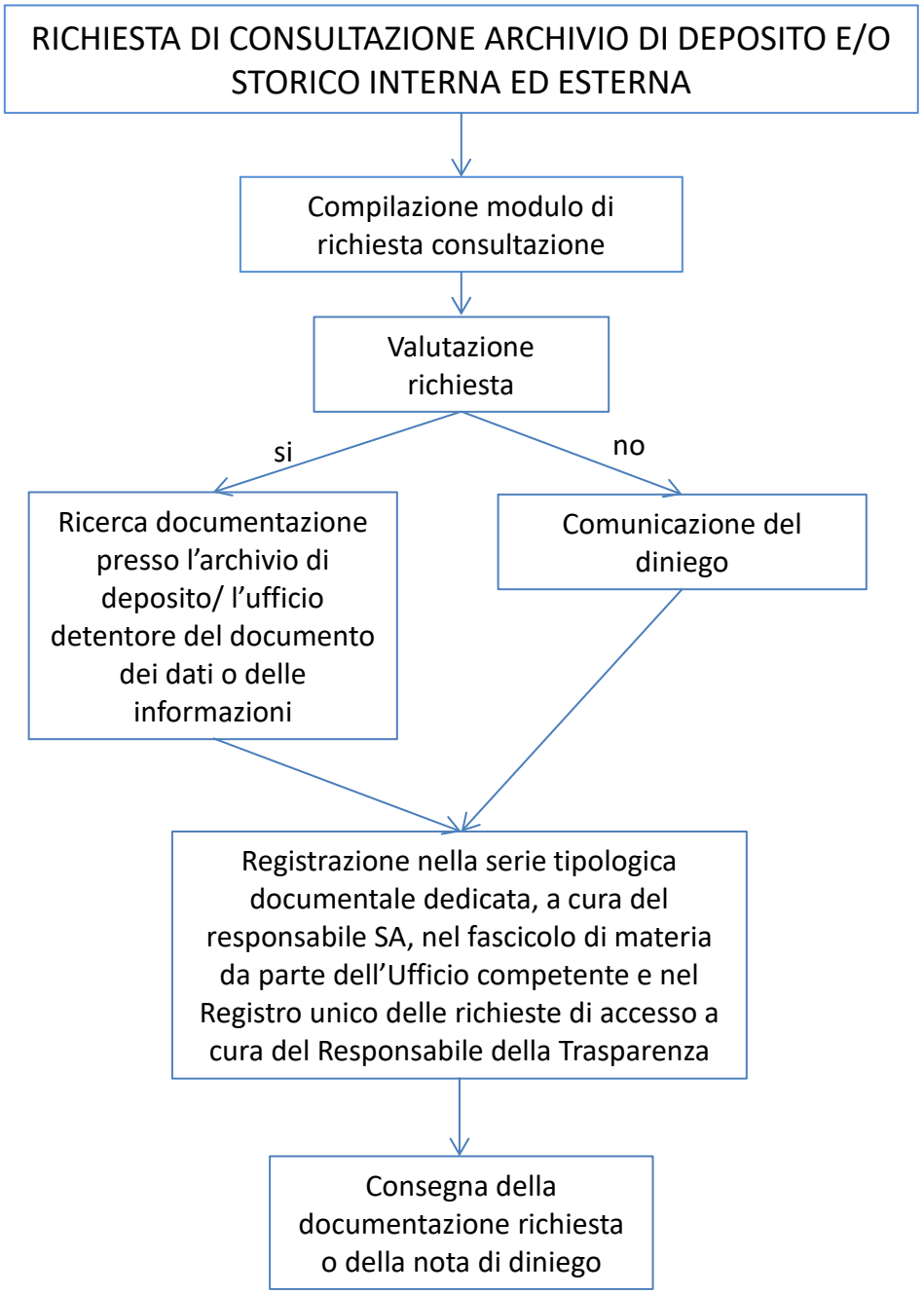
In ogni caso, deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

Se le richieste pervengono dall’esterno dell’Ente il/la richiedente segue le indicazioni pubblicate sulla pagina internet www.consiglioregionale.piemonte.it sezione amministrazione trasparente nella pagina dedicata all’accesso civico http://trasparenza.csi.it/web/crp/altri-contenuti-accesso-civico.

8.7.2. SCHEMATIZZAZIONE DEL FLUSSO DEI DOCUMENTI ALL'INTERNO DEL SISTEMA ARCHIVISTICO

Nella figura seguente viene riportata una rappresentazione grafica sintetica del complesso delle attività, delle norme e delle responsabilità illustrate nel presente capitolo che, nella loro totalità, costituiscono una funzione strategica dell'amministrazione.


VERSAMENTO MATERIALE NELL'ARCHIVIO DI DEPOSITO
Struttura richiedente versamento
Chiusura delle strutture archivistiche
Compilazione dell'elenco di versamento (modulo)
Invio al Responsabile SA per verifica consistenza materiale ricevuto
SI
NO
Archivio di deposito
Scarto
Versamento nell'archivio storico
Chiusura strutture archivistiche a cura del SA
Compilazione dell'elenco di versamento
Archivio di deposito
Scarto
Versamento nell'archivio storico


RICHIESTA DI CONSULTAZIONE ARCHIVIO DI DEPOSITO E/O STORICO INTERNA ED ESTERNA
Compilazione modulo di richiesta consultazione
Valutazione richiesta
si
no
Ricerca documentazione presso l'archivio di deposito/ l'ufficio detentore del documento dei dati o delle informazioni
Comunicazione del diniego
Registrazione nella serie tipologica documentale dedicata, a cura del responsabile SA, nel fascicolo di materia da parte dell'Ufficio competente e nel Registro unico delle richieste di accesso a cura del Responsabile della Trasparenza
Consegna della documentazione richiesta o della nota di diniego

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 nell'ambito di ogni sessione di attività di registrazione.

9.1 UNICITÀ DEL PROTOCOLLO INFORMATICO

Nell'ambito dell'Ente 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 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.

Non è consentita la protocollazione di un documento già protocollato.

Il registro di protocollo è un atto pubblico originario 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'Ente sia in formato cartaceo sia in formato elettronico, ad eccezione dei documenti elencati all'art. 53 del Testo Unico n. 445/2000.

9.2. REGISTRO GIORNALIERO DI PROTOCOLLO

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso viene prodotto automaticamente dal SdP attraverso il sistema di gestione documentale in formato XML con opportuno foglio di stile e reso disponibile anche in formato PDF.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il Registro giornaliero di protocollo viene automaticamente archiviato dal SdP.

9.3. REGISTRAZIONE DI PROTOCOLLO

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo, valide per tutti i tipi di documenti informatici trattati dall'Ente (ricevuti, trasmessi e interni formali). Come previsto dalla normativa vigente in materia di protezione dei dati personali, le

strutture responsabili sono informate della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo, si inserisce invece il Cognome e il Nome della persona interessata.

Su ogni documento ricevuto o spedito dall'Ente 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/operatrice, di inserire le informazioni successivamente.

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/la mittente che ha prodotto il documento;
- ✓ il/la destinatario/destinataria del documento;
- ✓ l'oggetto del documento;

Le variazioni su "oggetto", "mittente" e "destinatario" non si possono più effettuare dopo aver confermato la protocollazione.

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

9.3.1. DOCUMENTI INFORMATICI E ANALOGICI (CARTACEI E SUPPORTI RIMOVIBILI)

I documenti informatici e analogici sono ricevuti e trasmessi, in modo formale, sulle/dalle caselle di posta elettronica certificata istituzionale dell'Ente o trasmessi con i mezzi tradizionali della corrispondenza.

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore/operatrice del protocollo ne ha accertato l'integrità ed ha verificato la validità della firma.

Nel caso di documenti informatici in partenza il sistema di protocollazione esegue la verifica della validità amministrativa della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti *i file* allegati al messaggio di posta elettronica ricevuto o inviato.

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.

Per la registrazione di protocollo di un documento cartaceo ricevuto l'operatore/operatrice esegue la verifica della presenza della sottoscrizione del/della mittente e dell'assegnazione all'ufficio competente.

Per la documentazione cartacea in partenza l'operatore/operatrice esegue la verifica della presenza del/della destinatario/destinataria e la sottoscrizione da parte del/della dirigente.

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

Le Strutture ricevono i documenti interni di tipo formale da protocollare all'interno del sistema documentale attraverso lo smistamento per protocollazione.

9.4. ELEMENTI FACOLTATIVI DELLE REGISTRAZIONI DI PROTOCOLLO

Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, il SA con una circolare interna, può modificare e integrare gli elementi facoltativi del protocollo.

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 registri tali modifiche.

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

- ✓ Il numero di protocollo del/della mittente e la data del documento se presenti;
- ✓ ulteriori informazioni sul/sulla mittente/destinatario/destinataria, soprattutto se persona giuridica;
- ✓ l'indirizzo completo del/della mittente/destinatario/destinataria (via, numero civico, CAP, città, provincia);
- ✓ il codice fiscale;
- ✓ il numero della partita IVA;
- ✓ il recapito telefonico;
- ✓ gli indirizzi di posta elettronica;
- ✓ registrazione precedente se presente;
- ✓ data timbro postale e numero di raccomandata da inserire nella annotazione formale.

9.5. SEGNATURA DI PROTOCOLLO DEI DOCUMENTI

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo. Essa consente di individuare ciascun documento in modo inequivocabile.

9.5.1. 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'Ente;
- ✓ codice identificativo della Struttura;
- ✓ codice identificativo del registro;

- ✓ data e numero di protocollo del messaggio ricevuto o inviato;
- ✓ oggetto;
- ✓ mittente;
- ✓ destinatario/destinatari.
- ✓ denominazione dell'amministrazione;
- ✓ codice identificativo del Nodo Responsabile a cui il documento è destinato/assegnato o che ha prodotto il documento;
- ✓ numero di fascicolo.
- ✓ indice di classificazione;
- ✓ annotazioni per l'individuazione degli allegati.

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

9.5.2. DOCUMENTI CARTACEI RICEVUTI

La segnatura di protocollo di un documento cartaceo ricevuto è apposta sul documento sulla quale vengono riportate le seguenti informazioni relative alla registrazione:

- ✓ codice identificativo dell'Ente;
- ✓ codice identificativo della Struttura;
- ✓ data e numero di protocollo del documento;

Nel sistema documentale viene comunque associato, al documento scansionato, *un file* conforme alle specifiche *dell'Extensible Markup Language* (XML) e compatibile con il *Document Type Definition* (DTD) reso disponibile dagli organi competenti.

9.6. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

L'annullamento di una registrazione di protocollo generale deve essere richiesto con mail, adeguatamente motivata, indirizzata al SA.

Solo il SA è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni 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, l'autore/autrice dell'annullamento e la motivazione dell'annullamento del protocollo. In tale ipotesi, la procedura riporta la dicitura "annullato" 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.

Un esempio di annullamento è quando emerge che ad uno stesso documento in ingresso, ricevuto con mezzi di trasmissione diversi quali, ad esempio originale cartaceo e con mail, siano stati attribuiti più numeri di protocollo.

9.7. LIVELLO DI RISERVATEZZA

Il SdP garantisce un livello di riservatezza di base prevedendo la visibilità dei documenti in base ai profili assegnati agli/alle utenti. Per i documenti che richiedono una maggiore riservatezza la procedura dispone delle funzioni di riservato/sensibile da poter selezionare in base alla tipologia di dati da tutelare.

In modo analogo, il/la Responsabile del Procedimento Amministrativo 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.

9.7.1. DOCUMENTI CARTACEI IN USCITA CON PIÙ DESTINATARI

Qualora i/le destinatari/destinatarie siano in numero maggiore di uno, la registrazione di protocollo è unica ed è quella associata al documento informatico originale da cui sono state prodotte le copie cartacee da inviare a più destinatari.

9.7.2. DOCUMENTI CARTACEI RICEVUTI A MEZZO TELEGRAMMA

I telegrammi ricevuti esclusivamente da privati vanno di norma protocollati come documenti senza firma, specificando tale modalità di trasmissione nel sistema di protocollo informatico (annotazione formale).

9.7.3. DOCUMENTI NON FIRMATI

L'operatore/operatrice di protocollo, conformandosi alle regole stabilite dal SA, 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”.

È poi compito della struttura di competenza e, in particolare, del/della Responsabile del Procedimento Amministrativo valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

9.7.4. PROTOCOLLAZIONE DEI MESSAGGI DI POSTA ELETTRONICA CONVENZIONALE

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

- ✓ Ricezione di un documento scansionato sottoscritto con firma autografa deve essere accompagnato da fotocopia di un documento di riconoscimento valido, fermo restando che il/la RPA deve verificarne la provenienza certa;
- ✓ Ricezione di un documento sottoscritto con firma digitale non richiede altre conferme di validità come documento elettronico;
- ✓ Ricezione di una e-mail contenente un testo non sottoscritto quest'ultima sarà

considerata come missiva anonima.

9.7.5. PROTOCOLLAZIONE DI DOCUMENTI DIGITALI O CARTACEI PERVENUTI ERRONEAMENTE

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all'Ente, l'addetto/addetta al protocollo, previa autorizzazione del SA, provvede ad annullare il protocollo e a rispedire il messaggio al/alla mittente indicando in oggetto "Pervenuto erroneamente".

9.7.6. CORRISPONDENZA PERSONALE O RISERVATA

La corrispondenza personale non viene aperta ma consegnata al/alla destinatario/destinataria, il/la quale, dopo averne preso visione, qualora reputi che i documenti ricevuti debbano essere comunque protocollati, provvede a trasmetterli alla Direzione competente per la protocollazione.

9.7.7. INTEGRAZIONI DOCUMENTARIE

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

Tale verifica spetta al/alla responsabile del procedimento amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al/alla 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 e collegati alla registrazione precedente relativa alla stessa attività, dalla struttura competente e, a cura del/della RPA, sono inseriti nel relativo fascicolo.

9.8. REGISTRO DI PROTOCOLLO

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

Di seguito sono descritte le modalità di produzione e di invio in conservazione, entro la giornata lavorativa successiva, del Registro giornaliero informatico con l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire l'immodificabilità delle registrazioni medesime.

Il SdP provvede all'esecuzione automatica della stampa su file, in formato XML con opportuno foglio di stile e reso disponibile anche in formato PDF, del Registro giornaliero di protocollo. Il documento così creato riporta su un unico file il riepilogo di tutte le registrazioni di protocollo eseguite nell'ambito della stessa giornata e, a seguire, gli eventuali annullamenti occorsi ai protocolli acquisiti nel corso dei giorni precedenti.

I metadati da inviare in conservazione, unitamente alla copia del registro di cui sopra,

sono:

- Identificativo del documento;
- Oggetto;
- Destinatario;
- Data cronica;
- Data di chiusura del documento;
- Indice di classificazione;
- Codice del registro di protocollo;
- Anno del registro di protocollo;
- Numero della prima registrazione presente nel registro giornaliero;
- Data della prima registrazione presente nel registro giornaliero;
- Numero dell'ultima registrazione presente nel registro giornaliero;
- Data dell'ultima registrazione presente nel registro giornaliero;

Ogni giorno, in maniera automatica il sistema di gestione documentale effettua la generazione e l'archiviazione del registro giornaliero di protocollo, che deve avvenire entro le ore 24:00:00 del primo giorno lavorativo successivo al giorno sul quale si considera l'estrazione.

MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

II presente capitolo illustra le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente, prevista dal SdP.

10.1. 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 SA 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.

II SdP realizza il registro di emergenza, composto da tutti i dati previsti per la registrazione sul protocollo corrente (con mezzi di office automation o cartaceo).

10.2 MODALITÀ DI APERTURA DEL REGISTRO DI EMERGENZA

Il SA assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica, le operazioni di protocollo siano svolte sul registro di emergenza informatico su postazioni di lavoro operanti fuori linea centralizzato per l'Ente presso il SA.

Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il SA imposta la causa, la data e l'ora di inizio dell'interruzione del funzionamento della procedura di protocollo.

10.3. 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'Ente.

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

10.4. MODALITÀ DI CHIUSURA E DI RECUPERO DEL REGISTRO DI EMERGENZA E' COMPITO DEL SA VERIFICARE LA CHIUSURA DEL REGISTRO DI EMERGENZA.

E' compito del SA inviare ai rispettivi nodi responsabili i report da riportare dal registro di emergenza al registro di protocollo corrente. Le registrazioni relative ai documenti protocollati in emergenza, entro cinque giorni dal ripristino delle funzionalità, devono essere integrate nel SdP.

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

APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI

11.1. MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

L'Ente adotta il presente "Manuale di gestione" su proposta del Servizio archivistico, sentito il/la Direttore/Direttrice competente.

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.

11.2. REGOLAMENTI ABROGATI

Il presente Manuale sostituisce quello adottato con deliberazione dell'Ufficio di Presidenza n. 41 del 2018 ed ha tra i suoi allegati il Titolario con Piano di conservazione integrato.

11.3. PUBBLICITÀ DEL PRESENTE MANUALE

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

Copia del presente manuale è:

- ✓ resa disponibile nella intranet dell'Ente;
- ✓ inviata alla Soprintendenza ai beni archivistici per il Piemonte e la Valle d'Aosta;
- ✓ pubblicata sul sito istituzionale dell'amministrazione, nella sezione "Amministrazione Trasparente".

11.4. OPERATIVITÀ DEL PRESENTE MANUALE

Il presente manuale è operativo il primo giorno del mese successivo a quello della sua approvazione.

INDICE DEL DOCUMENTO

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale dei processi di formazione e conservazione elettronica dei documenti (di seguito anche "Manuale della Conservazione") ai sensi dell'articolo 8 del DPCM 3/12/2013 (G.U. 12/03/2014).

Il Manuale ha lo scopo di raccogliere le diverse normative in materia e di documentare il processo di conservazione dei documenti elettronici.

Inoltre, descrive tutte le procedure e le prassi seguite dal Consiglio regionale del Piemonte in materia di gestione della sicurezza del servizio, dei documenti e delle informazioni trattate: questa parte costituisce il regolamento operativo di tutti i processi di digitalizzazione dei documenti di conservazione digitale.

In caso di ispezione da parte delle Autorità di Vigilanza o di altri organismi a ciò deputati, il Manuale permette un agevole svolgimento di tutte le attività di controllo e costituisce un'importante dimostrazione dell'impegno del Consiglio regionale del Piemonte al rispetto delle norme.

Nell'ambito del Catalogo dei servizi del CSI Piemonte è disponibile il servizio di «Conservazione digitale documenti». Il CSI Piemonte ha individuato il fornitore per la conservazione che è Infocert SpA, il servizio di cui ci si avvale è Legaldoc.

Il Consiglio regionale si avvale di servizi di conservazione a partire dal 2011 limitatamente alla filiera documentale dei mandati di pagamento, delle reversali e delle quietanze (rif. D.U.P. n. 96/2011 e D.D. 582/2011).

L'invio in conservazione, secondo le modalità del 2011, è stato disattivato a partire dal giorno 11 aprile 2017, poiché si è resa necessaria la sottoscrizione di un nuovo affidamento del procedimento di conservazione (il fornitore è il medesimo ma sono variate le specifiche tecniche del servizio).

Il documento si applica dunque al servizio LegalDoc fornito in modalità ASP (Application Service Providing) da InfoCert SpA integrato con i sistemi documentali offerti da CSI.

Il sistema di integrazione è realizzato attraverso funzioni di base che possono essere arricchite di moduli specifici per ciascun conservatore, per rispondere ad eventuali scelte differenti da parte dell'ente.

Il conservatore, in virtù della delega ricevuta dal Consiglio regionale, assume il ruolo di responsabile del processo di conservazione grazie al riconoscimento della qualifica di Conservatore Accreditato presso l'Agenzia per l'Italia Digitale, garantendo così l'integrità, la leggibilità e l'autenticità dei documenti nel tempo.

In particolare viene resa disponibile al Consiglio regionale la soluzione per la conservazione digitale e per l'indicizzazione e ricerca dei documenti secondo parametri stabiliti. I documenti da conservare sono organizzati per tipologie omogenee nel sistema di gestione documentale (fatture, determinazioni dirigenziali, delibere, registri di protocollo, ecc…), caratterizzate dai rispettivi metadati (indici) che ne permettono l'invio automatico al sistema di conservazione. Il servizio web di consultazione dei documenti conservati viene erogato in modalità ASP (Application Service Providing) e per il suo utilizzo non è richiesta alcuna installazione specifica sulla postazione dell'utente (è

sufficiente un browser web di ultima generazione e l'accesso ad internet). Gli utenti abilitati potranno, ricercare ed esibire formalmente i documenti conservati tramite le opportune funzionalità disponibili via web.

Il Manuale è organizzato per sezioni:

1. la prima sezione (capitoli 1-4) contiene una panoramica di tutte le leggi e i decreti che regolano la materia, fornisce il profilo del Consiglio regionale del Piemonte, il profilo di InfoCert e dettaglia la configurazione dei sistemi utilizzati per l'erogazione;
2. la seconda sezione (capitoli 5-9) descrive il servizio LegalDoc, il responsabile della conservazione, descrive i macro flussi operativi definiti per la gestione della documentazione elettronica. Inoltre, è dettagliato il procedimento di conservazione posto sotto la responsabilità di InfoCert in virtù della delega allo svolgimento delle attività di competenza del Responsabile della Conservazione, sottolineando input, output e responsabilità di ogni fase. Infine, vengono descritti i controlli effettuati e i processi di ricerca e esibizione a norma dei documenti conservati.
3. L'allegato A contiene la descrizione degli oggetti conservati. L'allegato B descrive i formati dei file accettati.

2. TERMINOLOGIA (GLOSSARIO,ACRONIMI)

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
Archiviazione	E' il processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.
CA	Certification Authority
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione, successivamente DigitPA ora Agenzia per l'Italia Digitale
Conservazione	Il processo che consente di conservare i documenti in modalità informatica a norma di legge e che risponde a quanto stabilito nel DPCM 03/12/2013
Dati sensibili	ai sensi dell'articolo 4, comma 1, lettera d) del Decreto Legislativo 30 giugno 2003, n.196 e la seguente deliberazione del Consiglio dei Ministri del 25 maggio 2012, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale
Documento Analogico Originale	documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
Documento informatico	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
DPCM	Decreto del Presidente del Consiglio dei Ministri
EXTENSIBLE MARKUP LANGUAGE	linguaggio derivato dall'SGML (Standard Generalized Markup Language), metalinguaggio che permette di creare altri linguaggi. Mentre l'HTML è un'istanza specifica dell'SGML, XML costituisce a sua volta un metalinguaggio, più semplice dell'SGML, largamente utilizzato per la descrizione di documenti sul Web. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei

	marcatori (markup tags). Diversamente dall'HTML, l'XML consente all'utente di definire marcatori personalizzati, dandogli il controllo completo sulla struttura di un documento. Si possono definire liberamente anche gli attributi dei singoli marcatori.
Evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (all. 1 DPCM 03/12/2013)
Firma digitale	un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1 comma 1 lettera s) Decreto Legislativo del 7 marzo 2005 n. 82)
Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art. 1 comma 1 lettera q) Decreto Legislativo del 7 marzo 2005 n. 82)
Firma elettronica qualificata	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1 comma 1 lettera r) Decreto Legislativo del 7 marzo 2005 n. 82)
Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1 comma 1 lettera q-bis) Decreto Legislativo del 7 marzo 2005 n. 82). Si vedano anche le regole tecniche, pubblicate nella G.U. il 21 maggio 2013.
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP

HARDWARE SECURITY MODULE	dispositivo crittografico ad alte prestazioni utilizzato per apporre automaticamente la firma digitale e la validazione temporale ad elevati volumi di documenti informatici
HSM	Hardware Security Module
IdP:	strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
Impronta di una sequenza di simbolo binari (HASH)	la sequenza dei simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (all. 1 DPCM 03/12/2013).
MARCA TEMPORALE	il riferimento temporale che consente la validazione temporale, così come definita all'art. 1 comma 1 lettera i) DPCM del 30 marzo 2009. La marca temporale è opponibile ai terzi, definita anche nel DPCM 22 febbraio 2013, titolo IV
POSTA ELETTRONICA CERTIFICATA (PEC)	sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici
PORTABLE DOCUMENT FORMAT (PDF)	formato di file creato da Adobe Systems nel 1993 per lo scambio di documenti. Il PDF è un formato a schema fisso basato su un linguaggio di descrizione di pagina che permette di rappresentare documenti in modo indipendente dall'hardware, dal software e dal sistema operativo; ogni PDF incapsula una descrizione completa del documento, che include testo, caratteri, immagini e grafica. PDF è uno standard aperto; recentemente la versione PDF/A (PDF Reference Version 1.4) è stata riconosciuta dall'International Organization for Standardization (ISO) con la norma ISO 19005:2005.
RESPONSABILE DELLA CONSERVAZIONE	il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione ottica sostitutiva conformemente a quanto previsto all'art. 7 del DPCM 03/12/2013.
RIFERIMENTO	informazione, contenente la data e l'ora, che viene

TEMPORALE	associata ad uno o più documenti informatici, così come definito all'art. 1 comma 1 lettera m) DPCM del 30 marzo 2009, definito anche nel DPCM 22 febbraio 2013.
SG	Sistema di Gestione
SGD	Sistema di Gestione Documentale
SSL	Secure Socket Layer
TSA	Time Stamping Authority
TU	Testo Unico
URL	Uniform Resource Locator

3. NORMATIVA E STANDARD DI RIFERIMENTO

1.1 Normativa di riferimento

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3

e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

1.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1o ottobre 2014. La coerenza del sistema di conservazione a tali standard è obbligatoria per i soggetti accreditandi e accreditati.

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

4. RUOLI E RESPONSABILITÀ

In questo capitolo sono individuati i differenti soggetti che intervengono a vario titolo nelle diverse fasi del processo di creazione dei documenti elettronici, digitalizzazione dei documenti cartacei e conservazione elettronica documentale.

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	Graziella Miraudo	Consiglio regionale Direzione Amministrazione, Personale, Sistemi informativi e Corecom Responsabile servizio archivistico	In carica	Infocert Spa Antonio Dal Borgo (p18 manuale Infocert)
Responsabile Sicurezza dei sistemi per la conservazione	Infocert Alfredo Esposito (p19 manuale Infocert)	Responsabile Sicurezza dei sistemi per la conservazione	In carica	
Responsabile funzione archivistica di conservazione	Graziella Miraudo	Consiglio regionale Direzione Amministrazione, Personale, Sistemi informativi e Corecom Responsabile servizio archivistico	In carica	
Responsabile sistemi informativi per la conservazione	Infocert Massimo Biagi (p.20 manuale Infocert)	Responsabile sistemi informativi per la conservazione	In carica	
Responsabile sviluppo e manutenzione del sistema di conservazione	Infocert Nicola Maccà (p21 manuale Infocert)	Responsabile sviluppo e manutenzione del sistema di conservazione	In carica	

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

1.3 Organigramma

Gli enti/aziende coinvolti nel servizio di conservazione sono:

Consiglio regionale del Piemonte – soggetto produttore

Le direzioni del Consiglio regionale producono i documenti, il servizio archivistico (che risponde alla Direzione Amministrazione, personale, sistemi informativi e Corecom) gestisce il piano di conservazione dei documenti, il settore Sistemi informativi (che risponde alla medesima direzione) gestisce gli aspetti informatici e i rapporti con il CSI Piemonte

CSI Piemonte – gestione e governo del sistema informativo del Consiglio regionale (società in house)

Infocert SpA – conservatore accreditato

1.4 Strutture organizzative

Sono ora descritte le strutture organizzative, comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione, quali:

- attività proprie del contratto di servizio di conservazione:
- attivazione del servizio di conservazione: il servizio è stato acquisito nell'ambito della convenzione con CSI Piemonte da parte del Consiglio regionale;
- il CSI Piemonte eroga il servizio tramite il fornitore Infocert Spa
- Il responsabile del servizio di conservazione del Consiglio regionale ha delegato Infocert Spa in qualità di conservatore accreditato presso Agid
- acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento: Infocert riceve il pacchetto di versamento prodotto dal sistema di gestione documentale gestito da CSI, provvede alla verifica, acquisizione e gestione con la creazione del pacchetto di archiviazione;
- preparazione e gestione del pacchetto di archiviazione: Infocert dopo le verifiche positive sul pacchetto di versamento, genera il pacchetto di archiviazione e acquisisce i documenti da conservare;
- preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta: Infocert SpA;
- scarto dei pacchetti di archiviazione: servizio archivistico del Consiglio regionale tramite Infocert SpA;
- chiusura del servizio di conservazione (al termine del contratto): come

attivazione.

- attività proprie di gestione dei sistemi informativi: svolte da Infocert SpA
- conduzione e manutenzione del sistema di conservazione;
- monitoraggio del sistema di conservazione;
- change management;
- verifica periodica di conformità a normativa e standard di riferimento.

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Descrizione delle tipologie degli oggetti e dei pacchetti in essi contenuti sottoposti a conservazione.

I pacchetti (versamento/archiviazione/distribuzione) sono contrattualizzati tra il Consiglio regionale (soggetto produttore) e InfoCert S.p.a. (conservatore accreditato) e si basano sui documenti che fanno parte delle 'Specificità del Contratto'.

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione. Ad ogni documento il Sistema di conservazione associa un file XML, detto Indice del Pacchetto di Archiviazione (Indice di Conservazione UNI SInCRO). L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

Per "pacchetto di distribuzione" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta, ovvero è la risposta alla ricerca effettuata dal Soggetto Produttore tramite interfaccia disponibile, che porta all'esibizione del documento conservato. Il documento da esibire è accompagnato sempre dall'IPdA.

Nel sistema, ad oggi, il "pacchetto di distribuzione" coincide con il "pacchetto di archiviazione".

1.5 Oggetti conservati

Le tipologie di documenti sottoposti a conservazione e le relative politiche di conservazione sono elencate e descritte nell'allegato A del presente manuale (rif. 1.1 e 1.2).

1.6 Pacchetto di versamento

Le tipologie di pacchetto di versamento gestite sono elencate e descritte nell'allegato A del presente manuale (rif. 1.3).

1.7 Pacchetto di archiviazione

Rif. Manuale conservazione Infocert v.5.1 Cap. 6

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione. Ad ogni documento il Sistema di conservazione associa un file XML, detto Indice del Pacchetto di Archiviazione. L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

L'Indice del Pacchetto di Archiviazione è un file in formato XML, marcato temporalmente e firmato digitalmente dal Responsabile del servizio della Conservazione, generato dal sistema, che contiene i metadati in formato UNI SInCRO e le informazioni di conservazione del documento e viene con esso conservato.

In particolare nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA
- il token del documento (ovvero il suo identificativo univoco)
- l'operazione eseguita (conservazione, rettifica, scarto e cancellazione)
- il bucket (ovvero l'area di conservazione) associato al Soggetto Produttore e la policy utilizzata
- il nome dei file che compongono il pacchetto, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte
- eventuali informazioni relative al documento rettificante e rettificato
- il tempo di creazione (timestamp) del file IPdA
- l'impronta di Hash del documento.

L'insieme degli IPdA di un pacchetto di versamento formano il Rapporto di versamento di cui all'art. 9, comma d) del DPCM del 3 dicembre 2013.

Il file IPdA è reso disponibile con il documento di riferimento ad ogni operazione di conservazione e richiesta di esibizione.

1.8 Pacchetto di distribuzione

Rif. Manuale conservazione Infocert v.5.1 Cap. 6

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione.

Le procedure di esibizione permettono di estrarre dal sistema un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione utilizzando il relativo token (ovvero l'identificativo univoco del documento da esibire) o utilizzando uno o più metadati versati. Insieme ai file costituenti il pacchetto di

distribuzione, sono rese disponibili anche le informazioni che qualificano il processo di conservazione, ossia il file IPdA e un'Attestazione di corretta conservazione e datacertazione firmata dal Responsabile del servizio di Conservazione.

Non è possibile esibire parti singole di documento.

L'esibizione può restituire il documento in due modalità differenti: in un unico pacchetto di distribuzione in formato zip, oppure un file alla volta. Quest'ultima modalità deve essere compatibile con il client di esibizione dell'utente.

Le procedure del sistema mantengono e aggiornano ad ogni nuovo invio il database di tutti i token; il database viene interrogato ad ogni richiesta di rettifica, scarto e cancellazione, ricerca ed esibizione confrontando il token inviato con quelli memorizzati. La procedura assicura di agire solamente sul documento richiesto, e solamente se in possesso dei dovuti profili di autorizzazione.

L'esibizione del pacchetto di distribuzione ottenuto tramite interrogazione al sistema di conservazione rappresenta un'esibizione completa, legalmente valida ai sensi del secondo comma dell'articolo 10 del DPCM del 03 dicembre 2013 e dell'articolo 5 del DMEF del 17 giugno 2014.

Un apposito strumento di esibizione e verifica, anche detto "Esibitore a Norma", permette di richiamare agevolmente un documento conservato e consente di ottenere in modo automatico sia la verifica delle firme digitali e delle marche temporali apposte che le verifiche di integrità dei documenti conservati e di tutti gli altri elementi conservati.

7. IL PROCESSO DI CONSERVAZIONE

Rif. Manuale conservazione Infocert v.5.1 Cap. 7

Il sistema di conservazione è erogato in modalità SaaS (Software as a Service) secondo uno schema di Business Process Outsourcing (BPO) e permette di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

Il sistema consente le funzionalità di:

• accettazione del pacchetto di versamento, formato dal documento da conservare e dai metadati ad esso associati;

• conservazione del pacchetto di archiviazione: il documento, ricevuto nei Data Center di InfoCert in formato digitale statico non modificabile, viene conservato a norma di legge per tutta la durata prevista ed è contenuto in un pacchetto di archiviazione;

• rettifica del pacchetto di archiviazione: un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica è una modifica logica, nel pieno rispetto del principio di tracciabilità e la rettifica si applica al pacchetto di archiviazione;

• scarto /cancellazione del pacchetto di archiviazione: in caso un documento sia stato versato per errore. La cancellazione è una modifica logica, nel pieno rispetto del principio di tracciabilità e si applica al pacchetto di archiviazione; per la cancellazione fisica di pacchetti di archiviazione ritenuti privi di valore amministrativo e di interesse

storico-culturale dal Produttore, occorre formulare apposita richiesta a InfoCert (scarto archivistico);

• ricerca dei documenti conservati: l'utente autorizzato può eseguire una ricerca tra i documenti conservati trasversalmente sulle classi documentali, utilizzando uno o più metadati popolati in fase di caricamento;

• esibizione del pacchetto di distribuzione: il documento richiesto via web viene richiamato direttamente dal sistema di conservazione digitale ed esibito, con garanzia

della sua opponibilità a terzi; attraverso l'Esibitore di LegalDoc è possibile visualizzare e scaricare sia il documento conservato che gli altri documenti a corredo della corretta conservazione (file di indici, file di parametri, Indice del Pacchetto di Archiviazione);

• visualizzazione delle statistiche di conservazione;

• caricamento dei visualizzatori: è previsto il deposito dei visualizzatori da parte del Soggetto Produttore qualora la tipologia dei file conservati non sia quella standard, definita in fase di attivazione del sistema.

Il sistema di conservazione, quindi, integra il sistema di gestione del Soggetto Produttore, sia esso un'azienda o un ente locale, e ne estende i servizi con funzionalità di stoccaggio digitale (archivio di deposito).

Le fasi di creazione, utilizzo e archiviazione dei documenti sono organizzate liberamente, in quanto il servizio interviene solamente nella fase di conservazione e solamente per i documenti che il Soggetto Produttore sceglie di conservare.

1.9 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Rif. Manuale conservazione Infocert v.5.1 Cap. 7.1

Di seguito è riportata la tabella che descrive l'acquisizione dei pacchetti, seguendo lo schema: input\dettaglio delle attività\output.

ATT.1 Invio al sistema di conservazione del pacchetto di versamento

INPUT	*Documento da inviare al sistema di conservazione tramite il pacchetto di versamento*
Sistema di gestione documentale del Soggetto Produttore	Invocazione del sistema di conservazione da parte del sistema di gestione, secondo lo standard descritto nelle SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc.
	Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di sessione (ldSessionId)
	Trasmissione del pacchetto di versamento costituente il documento (file di dati, il file di indici del documento e il file dei parametri di conservazione) secondo le modalità di trasmissione descritte nelle SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc.
OUTPUT	*pacchetto di versamento inviato*

1.10 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Rif. Manuale conservazione Infocert v.5.1 Cap. 7.2

ATT.1 Validazione del pacchetto di versamento

INPUT	*Pacchetto di versamento*
Sistema di conservazione	Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal Soggetto Produttore, a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema di gestione del Soggetto Produttore dell'errore intercorso. In questo caso, termine del flusso.
	Controllo dei valori indicati dal Soggetto Produttore nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
	Controllo dei valori indicati dal Soggetto Produttore nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione, non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.
	Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.
OUTPUT	*pacchetto di versamento verificato*

1.11 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Rif. Manuale conservazione Infocert v.5.1 Cap. 7.3

Le fasi previste sono la memorizzazione, la creazione del file IPDA e la marcatura temporale dello stesso.

ATT.1 Generazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*
Sistema di conservazione	Eventuale apposizione della firma digitale sul file di dati, cioè sul documento da conservare (se prevista da accordi contrattuali appositi esplicitati nei 'Dati Tecnici di attivazione', che fanno parte delle 'Specificità del contratto')
	Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy ed il bucket (area di conservazione) utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo (token) assegnato al documento.
	Marcatura e firma da parte del Responsabile del servizio della Conservazione del file IPdA. Copia del file sul supporto primario.
	Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.
OUTPUT	*pacchetto di archiviazione*

ATT.2 Memorizzazione e creazione copia di sicurezza

INPUT	*Pacchetto di archiviazione*
	Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali
	Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito.
	La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
OUTPUT	*Documenti conservati*

ATT.3 Invio dell'IPdA al soggetto Produttore

INPUT	*File IPdA*
	Invio dell'esito e del file IPdA al soggetto Produttore.
OUTPUT	*Esito conservazione inviato*

1.12 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Rif. Manuale conservazione Infocert v.5.1 Cap. 7.4

All'interno delle "Specificità del Contratto" SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc è presente la griglia riassuntiva dei codici errore che il servizio LegalDoc restituisce in seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto.

1.13 Preparazione e gestione del pacchetto di archiviazione

Rif. Manuale conservazione Infocert v.5.1 Cap. 7.5

1.14 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

Rif. Manuale conservazione Infocert v.5.1 Cap. 7.6

1.15 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

Rif. Manuale conservazione Infocert v.5.1 Cap. 7.7

Per duplicato si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Per copia si intende il documento informatico avente contenuto identico al documento da cui è tratto, ma con forma diversa.

La conservazione avviene su supporto primario e su supporto secondario, quindi con duplicazione automatica. Come descritto in seguito, tali supporti sono magnetici ad alte capacità e performance, che garantiscono la ridondanza interna del dato. È inoltre eseguito un backup periodico su tape magnetico.

La creazione di copie informatiche, invece, in caso di adeguamento del formato rispetto all'evoluzione tecnologica sarà presa in carico dal Responsabile del servizio della Conservazione e dalle figure professionali coinvolte nel processo di conservazione in base alle specifiche del formato in questione e al know-how tecnologico a disposizione. A fronte di questa analisi sarà progettata una soluzione di concerto con il Soggetto Produttore del formato più idoneo per permettere la leggibilità del documento conservato.

Possono essere generati anche duplicati o copie attraverso l'Esibitore o su supporto ottico, su specifica richiesta del Soggetto Produttore.

Nel primo caso il Produttore/Utente agisce autonomamente con apposite credenziali attraverso l'Esibitore di LegalDoc. Nel secondo caso il Soggetto Produttore inoltra la richiesta ai suoi riferimenti abituali (help desk o account) che poi provvedono alla veicolazione verso gli operatori interni.

L'intervento di un Pubblico Ufficiale per attestare la conformità di una copia all'originale avviene secondo quanto previsto dagli articoli 22 e 23 del Codice e dalle Regole Tecniche del DPCM del 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al

decreto legislativo n. 82 del 2005.

1.16 Scarto dei pacchetti di archiviazione

Rif. Manuale conservazione Infocert v.5.1 Cap. 7.8

Descrizione analitica della funzione di scarto dei pacchetti di archiviazione secondo quanto previsto dalle regole tecniche (Art. 9, comma 1, lettera k).

In LegalDoc esistono due diverse metodologie di 'cancellazione':

1. Cancellazione logica: eliminazione di un documento versato in conservazione per errore materiale, gestita in autonomia solo dal Soggetto Produttore (attraverso apposite chiamate WS), per cui il documento cancellato è ancora consultabile dall'Utente (compare con lo 'stato': 'cancellato'), in ossequio al principio di tracciabilità

informatica.

2. Cancellazione fisica o scarto archivistico: eliminazione vera e propria di un documento o di un pacchetto di archiviazione e di qualsiasi duplicato prodotto durante le attività di conservazione, sia dal punto di vista logico che dal punto di vista fisico, per cessata rilevanza ai fini amministrativi, legali o di ricerca storica, ai sensi del Codice Privacy e del Codice dei beni culturali. Questa attività è espressamente richiesta a InfoCert dal Soggetto Produttore, mediante apposita lista debitamente firmata.

Per gli enti pubblici e per gli archivi privati dichiarati di notevole interesse storico, le proposte di scarto sono sottoposte a nulla osta delle soprintendenze archivistiche o delle commissioni di sorveglianza di competenza. La stesura di 'Piani di Conservazione' (detti anche 'Massimari di selezione e scarto'), la selezione dei documenti da scartare e la procedura di sdemanializzazione e approvazione ministeriale sono in capo al Consiglio regionale (soggetto produttore).

InfoCert, in quanto Conservatore, attiva la procedura di scarto sempre per richiesta e approvazione del Soggetto Produttore.

La distruzione degli eventuali supporti ottici rimovibili di back-up è effettuata mediante strumentazione adeguata e seguendo le procedure definite per lo smaltimento dei rifiuti prodotti.

Il Responsabile del servizio della Conservazione mantiene traccia delle richieste di scarto ricevute e correttamente eseguite, con l'indicazione a margine di eventuali errori occorsi durante lo svolgimento del processo, dei rimedi attuati e delle altre informazioni che ritiene meritevoli di annotazione.

1.17 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

Rif. Manuale conservazione Infocert v.5.1 Cap. 7.9

Descrizione delle funzioni, delle strutture dei dati e degli standard adottati a garanzia dell'interoperabilità e trasferibilità tra i sistemi di conservazione.

Nel caso il Soggetto Produttore decida di rescindere o interrompere il contratto di affidamento del servizio di conservazione, il Responsabile del servizio della Conservazione provvede a comunicare al Soggetto Produttore la lista dei pacchetti di archiviazione conservati.

Il soggetto produttore può effettuare il download dei propri Pacchetti di Distribuzione in autonomia, attraverso la procedura di esibizione, o richiedendo il servizio di restituzione al proprio commerciale di riferimento (su supporto da concordare in base a volume ed esigenze).

Se i supporti sono removibili, i documenti contenuti sono criptati e compressi con password apposita e non devono contenere nel dorso o nella custodia nessun riferimento al soggetto produttore o al contenuto.

Il soggetto produttore provvederà a inviare anche copia della liberatoria denominata 'MODULO DI RESTITUZIONE DATI – SERVIZIO LEGALDOC' sottoscritta digitalmente

dal Responsabile della Conservazione interno. Al termine della procedura di hand over verso il nuovo Conservatore per rescissione o risoluzione del contratto di servizio, i pacchetti conservati verranno cancellati da LegalDoc.

Insieme ai veri e propri documenti conservati, sono rese disponibili anche le informazioni e i documenti a corredo della corretta conservazione.

8. IL SISTEMA DICONSERVAZIONE

Rif. Manuale conservazione Infocert v.5.1 Cap. 8

La descrizione dell'architettura generale del sistema di conservazione è stata depositata da parte di Infocert SpA in AgID in fase di accreditamento.

Il sistema è organizzato su più siti (a Padova e a Modena).

Il sistema di conservazione è implementato da un'applicazione software appositamente sviluppata a tale scopo (applicazione Java in architettura distribuita, ossia costituita da molteplici componenti) e da una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, PEC).

Il sistema è reso in modalità SaaS (Softwareas a Service) e consente al Soggetto Produttore di accedere ai sistemi di conservazione dei documenti informatici su un elaboratore elettronico, gestito da InfoCert e fisicamente posto nei locali di quest'ultima, in conformità a quanto descritto nei documenti delle 'Specificità del Contratto'.

Il sistema è accessibile dalla apposita URL di rete e il Soggetto Produttore richiama il sistema di conservazione secondo le modalità concordate.

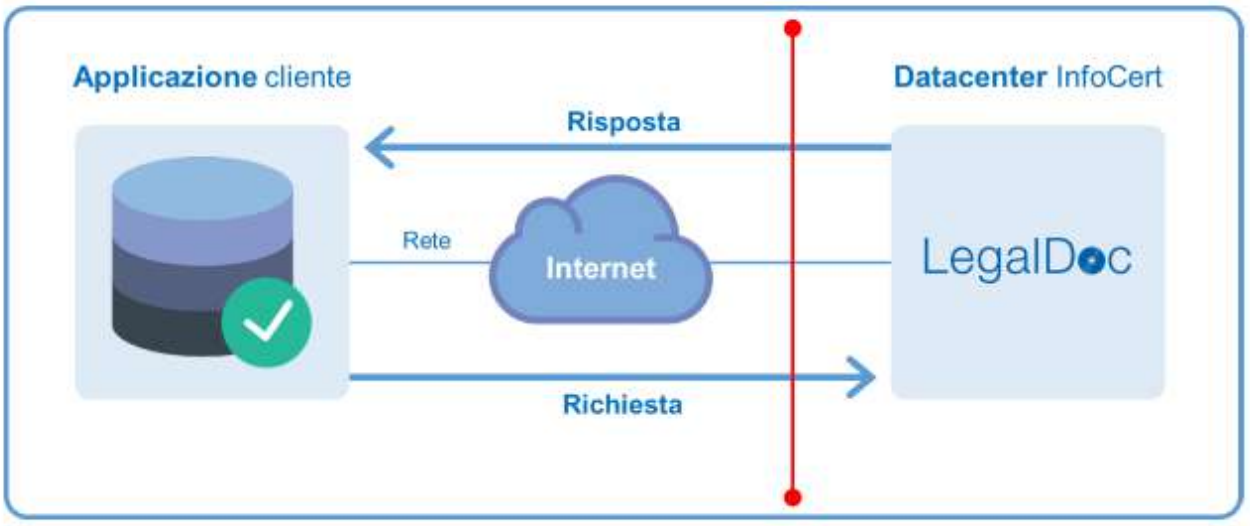


Figura1: Rappresentazione del servizio attraverso la rete

Dal punto di vista architetturale LegalDoc è realizzato utilizzando la tecnologia dei Web Services.

I Web Services di LegalDoc sono implementati secondo architettura REST su

protocollo HTTPS.

LegalDoc è dotato anche di un'interfaccia (LegalDoc WEB) utilizzata sia per il versamento manuale di alcune tipologie documentali, sia per la ricerca e l'esibizione a norma di documenti conservati.

L'esibitore è un'applicazione in tecnologia web, che permette ad un utente, precedentemente definito e in possesso delle debite autorizzazioni e credenziali, di accedere al sistema di conservazione LegalDoc da un qualsiasi computer, purché collegata in rete.

Attraverso l'esibizione a norma diventa possibile:

- estrarre un documento e visualizzarlo a video;
- produrre copia cartacea o su altro supporto informatico del documento;
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione;
- prendere visione dei file a corredo che formano il pacchetto di distribuzione e che qualificano il processo di conservazione attestandone il corretto svolgimento (Indice di Conservazione UNI SINCRO, altrimenti detto Indice del Pacchetto di Archiviazione, File di parametri, File di indici, File di dati, Attestato di conservazione);
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione;
- verificare l'integrità del documento.

Il sistema è protetto da firewall ed implementa un sistema di back-up dei dati memorizzati.

1.18 Componenti Logiche

Il servizio LegalDoc è basato su tecnologia REST e svolge le operazioni di conservazione, esibizione, rettifica, cancellazione e ricerca.

1.19 Componenti Tecnologiche

1.19.1 Firewall

I firewall assicurano la difesa del perimetro di sicurezza tra il sistema e il mondo esterno, nonché tra i sistemi dedicati all'erogazione del sistema e i sistemi che interfacciano i dispositivi sicuri per la generazione della firma digitale.

I firewall sono configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile.

1.19.2 Back-up

L'intero sistema di conservazione viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria per la sicurezza.

1.19.3 Servizio di marcatura temporale

Per l'emissione delle marche temporali il sistema si avvale del servizio di marcatura di InfoCert, Certification Authority accreditata, compliant eIDAS. Il Piano per la Sicurezza del Certificatore è depositato presso AgID.

La marca temporale viene richiesta al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert. Il root-certificate della TSA è depositato presso AgID.

Il TSS è sincronizzato via radio con l'I.N.RI.M di Torino (Istituto Nazionale di Ricerca Metrologica, già Istituto Elettrotecnico Nazionale "Galileo Ferraris") ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

1.19.4 Posta Elettronica Certificata

Il sistema di conservazione si avvale del servizio di posta elettronica certificata di InfoCert: in sede di attivazione del sistema, viene definita per il Soggetto Produttore una casella di posta certificata (PEC) tramite la quale richiedere supporto alla casella di amministrazione del sistema.

La PEC configurata all'attivazione è utilizzata, inoltre, per ogni comunicazione al Soggetto Produttore che interessa il funzionamento del sistema.

1.20 Componenti Fisiche

Rif. Manuale conservazione Infocert v.5.1 Cap. 8.3

InfoCert, in accordo con i Soggetti Produttori e come previsto dalle Condizioni Generali del Contratto si avvale di partner tecnologici per le componenti fisiche del data center.

1.20.1 Dispositivo HSM di firma digitale

Il sistema si avvale dei servizi di firma digitale forniti dalla CA InfoCert. In particolare, il servizio di firma automatica (firma massiva) permette di apporre automaticamente la firma digitale e la validazione temporale ad elevati volumi di documenti informatici, senza che sia necessaria la presenza del titolare nel momento preciso della firma.

I dispositivi utilizzati rispondono ai requisiti di sicurezza previsti per i dispositivi sicuri di firma.

1.20.2 Sistema Storage

Il sistema di conservazione di InfoCert, e dei suoi partner tecnologici, utilizza storage magnetici ad alte performance come sistema primario e secondario per la memorizzazione dei dati. Tali storage, scelti tra i primari fornitori di tecnologie presenti sul mercato, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato.

Tali storage rispondono all'esigenza di memorizzazione a lungo termine dei fixed content, ossia dei files che devono essere conservati con garanzia nel tempo di integrità e disponibilità del contenuto.

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni. Nel caso di documenti che contengono dati sensibili i dati vengono memorizzati cifrati con chiave in disponibilità al solo Responsabile del servizio della Conservazione.

I sistemi di storage sono stati valutati da InfoCert e dai suoi partner tecnologici sotto molteplici profili e, in virtù delle loro caratteristiche fisiche e architetturali, sono ritenuti idonei ad essere utilizzati nel sistema di conservazione.

Nell'ambito del sistema di conservazione, lo storage rappresenta sia il supporto primario di conservazione posto fisicamente presso la sede InfoCert di Padova, sia il supporto secondario posto nel sito di disaster recovery di Modena. I due sistemi sono interconnessi mediante collegamenti ad alta velocità dedicati, completamente ridondati e protetti da misure di sicurezza. I collegamenti consentono la replicazione dei dati conservati eliminando il rischio di distruzione di tutte le copie delle informazioni in caso di danno irreparabile a livello di sito.

Questo secondo sistema funge anche da copia di sicurezza.

L'allineamento tra il sito primario e il sito secondario avviene coerentemente con le politiche generali di Disaster Recovery definite in InfoCert che garantiscono RTO e RPO inferiori alle 48 ore.

1.20.3 Sincronizzazione dei sistemi

Tutti i server di InfoCert, attraverso il protocollo NTP (Network Time Protocol), sono sincronizzati sul "tempo campione" fornito dall'Istituto di Ricerca Metrologica – INRIM (già Istituto Elettrotecnico Nazionale "Galileo Ferraris"), abilitato a fornire il "tempo campione" ai sensi dell'articolo 2, comma 2, lettera b) del D.M. 30 novembre 1993, n.

591 "Regolamento concernente la determinazione dei campioni nazionali di talune unità di misura del Sistema internazionale (SI) in attuazione dell'art. 3 della L. 11 agosto 1991, n.273. La sincronizzazione è protetta da misure di sicurezza fisiche e logiche documentate per impedirne la manomissione.

Il meccanismo di allineamento temporale tra i sistemi fornisce la certezza della successione temporale degli avvenimenti nel sistema. La sincronizzazione delle macchine, infatti, genera dei file di log temporalmente omogenei tra loro, che permettono di ricostruire con certezza l'ordine di accadimento degli eventi intervenuti a tutti i livelli del sistema, e di individuare la sequenza di svolgimento delle varie operazioni.

1.21 Procedure di gestione e di evoluzione

Rif. Manuale conservazione Infocert v.5.1 Cap. 8.4

Il sistema di conservazione di InfoCert e il processo da questi implementato rispondono interamente alle norme di legge che regolano la materia.

La progettazione e il continuo miglioramento del sistema di conservazione sono il

frutto di una intensa opera di confronto tra le professionalità e le competenze delle diverse funzioni aziendali, al fine di giungere all'erogazione di un sistema pienamente conforme alle norme, architetturalmente stabile, affidabile, e che garantisca elevati livelli di servizio all'utente in condizioni di assoluta sicurezza, certezza degli accessi e tracciabilità delle operazioni.

Punto fondante del processo di progettazione è l'attenta disamina delle norme, al fine di definire puntualmente i requisiti legali che il sistema deve possedere per assicurare la corretta implementazione della conservazione.

Il rispetto dei requisiti di legge è la condizione imprescindibile per l'erogazione del servizio. Oltre a questi sono definiti ulteriori requisiti funzionali, di architettura e di connettività e interoperabilità. I requisiti funzionali, individuati dal gruppo di competenza, rispondono all'obiettivo di offrire al Soggetto Produttore le funzionalità da questi richieste, mentre i requisiti di architettura e di interoperabilità rispondono alla necessità di sviluppare e mantenere un sistema stabile, in linea con le evoluzioni tecnologiche e capace di interfacciarsi con gli altri sistemi sviluppati dall'azienda, sfruttando le economie di scala e di conoscenza.

9. MONITORAGGIO E CONTROLLI

Rif. Manuale conservazione Infocert v.5.1 Cap. 9

InfoCert ha scelto di introdurre in azienda un Service Management System - SMS conforme alla norma ISO/IEC 20000 [standard internazionale per l'IT Service Management] allo scopo di mantenere e migliorare l'allineamento e la qualità dei servizi di business erogati, attraverso un ciclo costante di monitoraggi, reporting e revisione degli SLA concordati.

InfoCert ha individuato nella Certificazione ISO 20000 un obiettivo di qualificazione dell'offerta in grado di conferire valore aggiunto ai servizi offerti e una maggiore garanzia dei livelli di servizio concordati con i propri clienti.

L'adozione di un modello di Service Management System – SMS InfoCert ha permesso di:

- mappare ed integrare i Livelli di Servizio (SLA) garantiti ai clienti in relazione ai Livelli di servizio operativi garantiti internamente e quelli contrattuali garantiti dai fornitori;
- governare la catena di composizione del valore dei servizi;
- ottimizzare la gestione dei processi aziendali integrando processi produttivi con processi di business fornendo un modello per la gestione sui servizi erogati;
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti evitando di assecondare aspettative cliente non erogabili;
- garantire un controllo dei fornitori che concorrono alla erogazione dei nostri servizi;
- migliorare la qualità dei servizi di business erogati.

Le attività di istituzione, attuazione, monitoraggio e sviluppo del Service Management System-SMS seguono il modello ciclico PDCA che si sviluppa nelle seguenti fasi:

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche

e i requisiti per la gestione dei servizi inerenti il campo di applicazione;
- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement dei servizi sulla base di quanto definito nel *service management plan;*
- azioni di monitoraggio e revisione del sistema-SMS (Check);
- attuazione di misure a miglioramento del sistema-SMS (Act) ove sono pianificate e attuate idonee azioni correttive sulla base dei risultati della fase precedente.

Il processo di gestione dei Livelli di Servizio [Service Level Management] è considerato un processo cardine del Service Management System in quanto ha effetto sui tre obiettivi principali quali:

- allineare i servizi di business con i bisogni correnti e futuri del cliente
- coordinare i requisiti del mercato sui servizi offerti con gli obbiettivi aziendali
- migliorare la qualità dei servizi di business erogati
- fornire attraverso gli SLA una base per la determinazione del valore del servizio.

Nello specifico InfoCert ha definito degli SLA baseline di riferimento in relazione ai

seguenti KPI (Key Performance Indicator):

- Orario di servizio
- Disponibilità di servizio.

9.1 Procedure di monitoraggio

La soluzione di monitoraggio, nel seguito denominata TMS, è fornita dal Gruppo Sintesi che si occupa della completa gestione di tutta la piattaforma.

TMS si occupa di monitorare e misurare tutto lo stack tecnologico usato per erogare i servizi InfoCert, infatti non è solo in grado di dire se un servizio o un particolare componente hardware stanno funzionando correttamente, ma è anche in grado di misurarne le risorse utilizzate e le performance.

La piattaforma è costruita a partire da una versione customizzata del noto software open source Nagios e per rilevare i dati dai diversi componenti utilizza diverse tecnologie (SNMP, NRPE, Sahi, ecc.). I monitoraggi possono essere eseguiti in modalità attiva (quindi la piattaforma interroga puntualmente le diverse componenti) oppure in modalità passiva (ovvero sono le singole componenti che inviano dati alla piattaforma, senza il bisogno di venire interrogate da essa).

L'infrastruttura di monitoraggio, ad oggi, è composta da:

- due apparati fisici (denominati probe) posizionati all'interno del Data Center,
- una probe posizionata all'interno dei locali della CA,
- un'altra probe posizionata nel sito di DR.

Alle quattro probe fisiche si aggiunge un pool di macchine virtuali posizionate nella server farm di Clouditalia.

Le probe fisiche si occupano di effettuare i monitoraggi sull'infrastruttura ed i servizi ospitati nei locali nei quali sono installate mentre le macchine virtuali si occupano di effettuare le navigazioni dei servizi sia da rete interna che tramite internet. Tutti i dati raccolti vengono infine centralizzati su una piattaforma resa disponibile online per una veloce e facile consultazione degli stessi.

Oltre alle misurazioni effettuate sull'infrastruttura, il sistema di monitoraggio è in grado di misurare anche le performance dei servizi, infatti tramite le navigazioni effettuate dalle macchine virtuali si riesce a capire se un servizio è disponibile e anche quanto tempo impiega per effettuare una certa elaborazione.

Con tutti i dati raccolti si popola una base di dati in ottica di Business Intelligence che risulta di fondamentale importanza per la redazione della reportistica riguardante gli SLA dei vari servizi ma anche, e soprattutto, per supportare i processi di decisione aziendale.

La soluzione di monitoraggio fin qui descritta risulta indispensabile per individuare tempestivamente eventuali anomalie sui servizi erogati da InfoCert, ma soprattutto è in grado di segnalarci su quale dei molti componenti che compongono un servizio andare a concentrare l'azione correttiva per una rapida risoluzione degli incident.

9.1.1 Processi di monitoraggio del sistema di conservazione

Il monitoraggio del sistema di conservazione si esplica su due diversi livelli operativi:

- sistema di monitoring della disponibilità del sistema
- sistema di monitoring dell'integrità degli archivi.

9.1.2 Monitoring della disponibilità del sistema

Tale operazione viene svolta coerentemente con le procedure di monitoring generali di InfoCert. In particolare, tutte le componenti costituenti il sistema di conservazione, ovvero i servizi applicativi, i processi di elaborazione batch e le interfacce per l'utente finale sono

monitorate con i tool definiti nella piattaforma di monitoraggio TMS precedentemente descritta.

A fronte di anomalie rilevate lo strumento invia delle segnalazioni al Service Desk InfoCert che le gestisce in conformità ai processi di Incident Management e, se necessario, Problem Management. Tali processi sono descritti nelle procedure che definiscono il Sistema di gestione integrato InfoCert.

9.2 Verifica dell'integrità degli archivi

Il sistema di memorizzazione utilizzato, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architetturale e alle procedure di memorizzazione permanente dei dati, garantisce l'immodificabilità, l'integrità, la leggibilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione.

Il sistema mantiene traccia di tutte le operazioni effettuate sui documenti in appositi file di log.

Inoltre, è garantita la tracciatura di tutti i documenti richiamati dal Soggetto Produttore mediante interrogazione al sistema e conseguentemente esibiti, che rappresenta un'ulteriore prova di leggibilità, effettuata direttamente dal Soggetto Produttore.

In aggiunta, come descritto dall'art. 7 comma 1 lettera g) del DPCM del 3 dicembre 2013, "al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta

funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati", InfoCert, per rispondere a tali richieste, ha attivato sottosistemi di controllo automatico dedicati alla simulazione della navigazione nel sistema e delle operazioni che effettua l'utente, svolgendo controlli di coerenza dei dati e attività di ripristino da situazioni di errore.

In ogni occasione in cui il file viene copiato o spostato di posizione, funzionalità automatiche verificano che le sue dimensioni non siano mutate durante lo spostamento e che non siano intervenute alterazioni, che possano inficiarne la visualizzazione.

Il Responsabile del servizio della Conservazione, come descritto nell'art. 7 comma 1 lettera f) "assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità" dei documenti conservati con procedure automatiche e manuali, al fine di prevenire il rischio che i documenti non possano essere visualizzabili, inficiando il mantenimento della loro validità legale nel tempo.

L'apposita procedura, detta **verificatore**, esegue il test di leggibilità binaria mediante il continuo calcolo delle impronte dei documenti conservati, con successivo confronto con l'hash del documento contenuto nel file delle direttive della conservazione inviato dal Soggetto Produttore. Se la procedura non registra differenze tra i due hash, il documento è inalterato rispetto a quanto trasmesso dal Produttore. Vengono eseguiti i seguenti passi operativi:

- verifica della validità della firma digitale e della marcatura temporale apposte all'atto della conservazione dal Responsabile del servizio della Conservazione sul file IPdA e, se presenti, verifica della firma digitale e della marcatura temporale del documento;
- calcolo dell'impronta del documento e confronto con quella contenuta all'interno del file IPdA;
- generazione di un report che viene automaticamente sottoposto alla conservazione nell'area dedicata al Responsabile del servizio della Conservazione (quindi a sua volta firmato e marcato temporalmente dal Responsabile del servizio della Conservazione stesso).

La procedura appena descritta viene applicata sia sul supporto primario sia su quello secondario.

In caso di anomalie, se il documento risulta corrotto in uno dei due repository, il sistema tenta il ripristino automatico con il dato presente nel repository integro. Se invece ambedue le copie sono alterate, viene inviato un alert al Responsabile del servizio della Conservazione, che tenterà il ripristino manuale partendo da un'altra sorgente (per esempio le copie di backup). Se nessuna sorgente è disponibile viene redatto un verbale di incidente, sottoscritto e conservato dal Responsabile del servizio della Conservazione per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.

Periodicamente, il sistema produce dei report di sintesi dell'attività di verifica svolta. In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio della Conservazione e i suoi Responsabili incaricati sono dotati di apposita strumentazione (detta **CORE, Console del Responsabile**), con credenziali dedicate, con la quale procedono manualmente e periodicamente ad una verifica campionaria di leggibilità dell'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.

Viene poi redatto automaticamente un verbale che attesta l'elenco dei documenti visualizzati, successivamente sottoscritto e conservato dal Responsabile del servizio della Conservazione nell'area appositamente creata nel sistema di conservazione.

9.3 Controlli

Oltre ai monitoraggi appena descritti, il sistema di conservazione implementa numerosi sotto-processi dediti al controllo del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al Soggetto Produttore o al personale incaricato dell'amministratore del sistema.

I controlli effettuati si distinguono nelle tre tipologie: controlli di versamento, controlli di processo e controlli periodici.

9.3.1 Controlli di versamento

In fase di versamento dei pacchetti in LegalDoc vengono automaticamente eseguiti dei controlli, preventivamente concordati con il soggetto Produttore nelle "Specificità del contratto" all'attivazione del servizio:

- Formato del documento da conservare (in coerenza con i 'Dati Tecnici di

attivazione' e con la configurazione degli ambienti);

- Correttezza della struttura del file di Parametri (contenente le informazioni per la leggibilità nel tempo del documento da conservare);
- Correttezza della struttura del file di Indici (contente i metadati del documento da conservare, alcuni dei quali obbligatori, in coerenza con i 'Dati Tecnici di attivazione');
- Presenza in conservazione sul medesimo path di un documento con lo stesso nome-file del documento da conservare;
- Abilitazione Utenza all'attività di versamento in quel dato ambiente; l'associazione tra utenza (username e password) e singola persona fisica è in capo al Produttore. La password di accesso è inviata da InfoCert al Produttore tramite canale PEC.
- Validità sessione in uso (di default della durata di un'ora tra login e logout);
- Dimensione massima del documento da conservare (di default 256 megabyte, variabile su richiesta);
- Validità del certificato qualificato di firma digitale con cui è sottoscritto il documento da conservare (su richiesta).

InfoCert NON effettua controlli sull'eventuale presenza di virus nei pacchetti di versamento, che sono conservati in LegalDoc alla stregua di tutti gli altri file.

9.3.2 Controlli di processo di progettazione e sviluppo dei servizi

L'organizzazione garantisce che non vengano rilasciati prodotti/servizi per i quali non siano state completate le attività di controllo della qualità citate nelle relative procedure di rilascio.

Per maggiori dettagli si rimanda a "PR/235 Progettare e sviluppare un servizio informatico InfoCert", "PR/225- Change Management InfoCert", "Service Management System-SMS".

9.3.3 Monitoraggio e registrazioni durante il ciclo produttivo

Lungo l'intero ciclo produttivo si effettuano i controlli al fine di verificare la conformità del prodotto e del processo a quanto previsto dalle procedure applicabili.

Nelle procedure "PR/235 Progettare e sviluppare un servizio informatico InfoCert" e "PR/225- Change Management InfoCert" sono indicate le fasi specifiche per i controlli, i test e le misurazioni del prodotto/servizio in termini di ciclo di vita, tecniche, metriche del SW, gestione dei controlli, dello "sforzo/effort", tenuta in controllo dei costi e dei tempi di realizzazione, la definizione dei mezzi e delle risorse necessarie.

Il prodotto/servizio è oggetto di un processo progressivo di accettazione: le registrazioni documentano la conformità del prodotto ai criteri di accettazione e indicano la persona che autorizza il rilascio.

Il prodotto/servizio è predisposto per la consegna al cliente ad esito positivo delle prove, controlli e collaudi. I prodotti che non superano le prove, i controlli e i collaudi sono sottoposti alla procedura per il trattamento dei prodotti non conformi.

9.3.4 Monitoraggio e registrazioni per collaudo finale

Il prodotto/servizio corrispondente ai requisiti contrattuali è oggetto di un processo progressivo di accettazione che viene attivato in occasione di ogni consegna ufficiale al Produttore, o di una accettazione globale fatta alla fine del processo produttivo secondo quanto previsto dalla procedura.

9.3.5 Controlli periodici

In InfoCert è attiva una struttura appositamente preposta alla supervisione e controllo della gestione dei problemi e del rispetto dei livelli del sistema per tutte le applicazioni.

La struttura si avvale di un gruppo di lavoro trasversale all'azienda ed effettua la raccolta dei dati relativi al funzionamento dei servizi.

Il gruppo si riunisce con una periodicità mensile al fine di individuare le cause dei malfunzionamenti registrati nel periodo, analizzare le soluzioni contingenti adottate per il superamento del problema e sviluppare eventuali proposte per rimedi strutturali.
Torna al sommario

9.4 Soluzioni adottate in caso di anomalie

Ad ogni semestre il Responsabile del servizio della Conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema

al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).

Torna al sommario

9.4.1 Auditing generale del sistema

Il Piano delle verifiche ispettive è definito annualmente dal gestore della qualità e approvato dal Rappresentante della direzione.

Le verifiche ispettive sono condotte all'interno della società sulla base della procedura "MG/325 Gestire Verifiche Ispettive InfoCert" volte a determinare se i processi aziendali ed i risultati ottenuti:

- sono orientati alle politiche per la qualità e al raggiungimento degli obiettivi
- sono in accordo con quanto previsto nei documenti di riferimento
- sono compliance alla normativa di riferimento
- sono compliance agli standard adottati dal sistema di conservazione
- sono attuate efficacemente
- sono idonee al conseguimento degli obiettivi della Qualità e miglioramento servizi

In ogni processo aziendale, le modalità di audit sono improntate alle indicazioni dello standard UNI EN ISO 19011 ed hanno per oggetto:

• strutture organizzative • risorse utilizzate • procedure • processi • prodotti e i

risultati dell'attività • documentazione • addestramento
• le segnalazioni dei clienti e terze parti.
Gli audit sono coordinati dall'Esecutivo Qualità ed eseguiti direttamente o da personale interno o esterno qualificato e debitamente addestrato.

Oltre alle verifiche ispettive sopra descritte indirizzate al Sistema Gestione Qualità, sono pianificati e condotti audit su tutti gli altri componenti del Sistema di Gestione Integrato (SGSI-ISO 27001, SMS-ISO 20000, SGA-ISO14001, Verifiche di interoperabilità condotte da AgID, Privacy, Sicurezza Fisica, M231/01 ecc.). Relativamente al SGA-ISO14001 l'attività di audit comprende anche la verifica di conformità legislativa.

Il processo prevede inoltre la gestione controllata di tutti gli Audit esterni svolti dagli Enti istituzionali, relativi ai Sistemi di Gestione ed ai Prodotti/Servizi certificati.

A fronte di non conformità rilevate in sede di verifica ispettiva, il Responsabile della Struttura Organizzativa valutata definisce un piano di attuazione delle azioni correttive o migliorative richieste.

Il Responsabile delle verifiche e ispezioni (auditing) pianifica e implementa processi di audit che coinvolgono aspetti di processo, organizzazione, tecnologici e logistici. L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto, alla documentazione generale del sistema, ai principi che ispirano il sistema qualità e al presente Manuale della Conservazione.

L'audit è un processo fondamentale per lo screening del sistema, in quanto consente l'individuazione delle aree critiche d'intervento e la pianificazione dei necessari interventi sul sistema, ragion per cui è svolto periodicamente.

9.4.2 Incident management

L'ambito completo del processo si applica alla gestione degli incidenti informatici che possono interessare uno o più servizi tecnologici eventualmente interconnessi ed è formalmente

descritto dalla procedura 'PR455-Incident Management InfoCert'. La procedura definisce anche la metodologia di assegnazione della gravità di un incidente e della relativa priorità di gestione in base alla matrice di analisi di impatto/urgenza effettuata utilizzando le informazioni sul servizio di riferimento e sui relativi SLA del servizio o nelle istruzioni /policy specifiche relative alla sicurezza informatica.

L'impatto è definito in base alla BIA [Business Impact Analisys] del servizio.

L'urgenza è dettata dallo SLA di disponibilità del servizio.

Il processo di gestione degli incidenti, condotto secondo le raccomandazioni delle Best Practice ITIL e in conformità alle norme ISO 27001, si focalizza sulle modalità di gestione e di ripristino tempestivo degli incidenti informatici. La funzione InfoCert coinvolta in tale processo è il Service Desk che opera anche come interfaccia per gli altri processi, quali il Change Management, il Problem Management e il Configuration Management.

Il modello organizzativo prevede che il supporto specialistico sistemistico sia fornito dalla funzione di Service Desk InfoCert (SD) che gestisce il ciclo di vita dell'incidente con lo strumento per la tracciatura dell'evento e che si avvale della collaborazione di tutte le strutture aziendali coinvolte.

Il processo d'Incident Management è supportato dall'attività di Problem Management (procedura PR456) che mira a ridurre gli impatti negativi a seguito di incidenti che possono essere provocati da errori/malfunzioni nelle infrastrutture IT e a prevenire il verificarsi e il ripetersi di tali errori.

A tale scopo il Problem Management cerca di individuare la causa degli incidenti e ne attua le opportune azioni preventive, correttive e/o migliorative.

La gestione dei problemi può essere sia reattiva che proattiva e riguarda l'identificazione e la risoluzione di problemi prima che si verifichino degli incidenti.

InfoCert è impegnata nel continuo affinamento e aggiornamento del sistema di conservazione, in modo da individuare ogni potenziale causa d'incidente e provvedere alla sua rimozione, scongiurando il blocco del sistema o il danneggiamento dei file in esso contenuti.

Il Responsabile del servizio della Conservazione mantiene il verbale degli incidenti e delle contromisure attuate, che divengono oggetto della successiva riunione di riesame e sono inviate al sistema di conservazione.

10. OPERATIVITÀ DEL PRESENTE MANUALE

Il presente manuale è operativo il primo giorno del mese successivo a quello della sua approvazione.

CONSIGLIO REGIONALE DEL PIEMONTE

ALLEGATO AL MANUALE DI CONSERVAZIONE DEL CONSIGLIO REGIONALE DEL PIEMONTE

11. ALLEGATO A – OGGETTI SOTTOPOSTI A CONSERVAZIONE

Oggetti sottoposti a conservazione

Le tipologie documentali inviate in conservazione sono le seguenti:

- Fattura elettronica
- Registro giornaliero di protocollo
- Determinazione dirigenziale
- Visto di conformità contabile
- Lotto di ordinativi

METADATI DEI DOCUMENTI DA INVIARE IN CONSERVAZIONE

I metadati validi per tutte le tipologie documentali da inviare in conservazione sono i seguenti:

Metadato	**Formato**	**Significato**	**Corrispondenza nel sistema di gestione documentale**
Identificativo	Stringa (50)	Sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione	Corrisponde all'Unique Identifier del documento (UUID) generato dal sistema, corrisponde all'attributo uuid_documento del Documento (non deve cambiare tra archivio corrente e archivio secondario/deposito).
Oggetto	Stringa (1000)	Riassume brevemente il contenuto e la natura del documento	Corrisponde al metadato "Oggetto" del Documento.
Soggetto produttore	Stringa (400)	Soggetto che ha autorità e competenza a produrre il documento informatico. Formatoda denominazione e codice fiscale	Corrisponde al metadato di identità "Soggetto produttore" del Documento.
Data cronica	Data (dd-mm-yyyy)	È la data in cui il documento è perfezionato (firmato, emesso, …). È la data che appare sul documento.	Corrisponde al metadato di identità "Data cronica" del Documento.

Destinatario	Stringa (800)	Soggetto che ha autorità e competenza a ricevere il documento informatico. Può essere fisico o giuridico, nel caso di destinatario fisico è possibile avere anche il codice fiscale	Corrisponde ai metadati di identità "Destinatario giuridico" e/o "Destinatario fisico" del Documento.
Data chiusura	Data (dd-mm-yyyy)	Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.	Corrisponde al metadato di identità "Data di chiusura" del Documento.
Indice di classificazione esteso	Stringa (1000)	Si definisce indice di classificazione esteso associato ad un documento, l'esplicitazione dell'intero percorso in cui è posizionato l'oggetto all'interno dell'archivio.	Corrisponde al metadato "Indice di classificazione esteso" del Documento.
Numero di protocollo	Stringa (50)	È il numero di protocollo assegnato al documento.	Corrisponde al numero della registrazione di protocollo più vecchia e non annullata.
Data di protocollo	Data (dd-mm-yyyy hh:mm:ss.)	È la data e l'ora di protocollazione.	Corrisponde al metadato "data protocollo" della Registrazione di protocollo più vecchia e non annullata.
Numero di repertorio	Stringa (100)	È il numero che, ove presente, identifica il documento (Es. il numero del contratto, il numero della fattura, il numero della determina, …).	Corrisponde al metadato di identità "Numero repertorio" del Documento.
Firma detached	Booleano	Indica se il documento si riferisce ad una firma detached	Ricavabile dal fatto che si sta inviando in conservazione una firma detached. Valorizzarlo a SI se si sta inviando una firma detached, a NO altrimenti
Marca detached	Booleano	Indica se il documento si riferisce ad una marca detached	Ricavabile dal fatto che si sta inviando in conservazione una marca detached. Valorizzarlo a SI se si sta inviando una marca detached, a NO altrimenti

Allegato di	Stringa (50)	Indica lo Unique Identifier del documento principale (UUID) a cui l'allegato fa riferimento	Corrisponde all'attributo uuid_documento del Documento principale a cui l'allegato fa riferimento.

Metadato	**Formato**	**Significato**	**Corrispondenza nel sistema di gestione documentale**
			Valorizzarlo con l'UUID del documento principale se il documento che SI sta inviando è un allegato, a NO altrimenti.

Per la sola tipologia ***Registro giornaliero di protocollo***, oltre ai metadati sopra definiti, si aggiungono i seguenti:

Metadato	**Formato**	**Significato**	**Corrispondenza in ACTA**
Codice registro	String a (100)	Codice identificativo del registro.	Corrisponde al metadato "Codice registro" del Documento di tipo registro.
Anno registro	Stringa (4)	Anno a cui il registro si riferisce.	Corrisponde al metadato "Anno registro" del Documento di tipo registro.
Numero prima registrazione	String a (20)	Indicazione del numero della prima registrazione effettuata sul registro.	Corrisponde al metadato "Numero prima registrazione" del Documento di tipo registro.
Data prima registrazione	Data (dd-MM-yyyy)	Indicazione della data della prima registrazione effettuata sul registro.	Corrisponde al metadato "Data prima registrazione" del Documento di tipo registro.
Numero ultima registrazione	String a (20)	Indicazione del numero dell'ultima registrazione effettuata sul registro.	Corrisponde al metadato "Numero ultima registrazione" del Documento di tipo registro.
Data ultima registrazione	Data (dd-MM-yyyy)	Indicazione della data dell'ultima registrazione effettuata sul registro.	Corrisponde al metadato "Data ultima registrazione" del Documento di tipo registro.

TIPOLOGIE DOCUMENTALI

Fattura elettronica

Le fatture elettroniche sono archiviate in:

Voce di titolario	Strutture aggregative	
5.5.2 Risorse Finanziarie e risorse contabili\Gestione delle uscite\Mandati,	**Serie tipologica di documenti** Una serie per ogni Ufficio (Codice Univoco Ufficio IPA)	**Volume** Un volume per ogni anno

I documenti possono essere nei seguenti formati:

TIPOLOGIA	FORMATO	MIME TYPE	CONTENUTO BUSTA	NOTE
Fattura elettronica	XML.P7M	application/pkcs7-mime	application/xml	File XML firmato CAdES
	XML	application/xml	NA	File XML firmato XAdES

La forma documentaria è *FatturaPA*.

Registro giornaliero di protocollo

I documenti registro giornaliero di protocollo sono archiviati in:

Voce	Strutture aggregative	
6.2.3 Sistema Informativo\Sistema Documentale\Gestione del protocollo e dell'archivio	**Serie tipologica di documenti** REG_PROT_GIORN/CR – Registro giornaliero di protocollo	**Volume** Un volume per ogni anno

I documenti sono nel seguente formato:

TIPOLOGIA	FORMATO	MIME TYPE	CONTENUTO	NOTE
Registro giornaliero di protocollo	XML	application/xml	NA	File XML non firmato

La forma documentaria è *Registro giornaliero*.

Determinazione dirigenziale

Le determinazioni dirigenziali sono archiviate in:

Voce	Strutture aggregative	
3.12 Organizzazione, patrimonio e risorse strumentali\Determinazioni e visti contabili	**Serie tipologica di documenti** Una serie per ogni Settore e per ogni anno	**Non sono presenti Volumi**

Le determinazioni dirigenziali possono contenere degli allegati, nei seguenti formati:

TIPOLOGIA	FORMATO	MIME TYPE	CONTENUTO	NOTE
Determinazione	PDF	application/pdf	NA	File PDF firmato PAdES
Allegato alla Determinazione dirigenziale	PDF	application/pdf	NA	File PDF

Le forme documentarie sono *Determinazione dirigenziale* e *Allegato alla determinazione dirigenziale*.

Visto di conformità contabile

I documenti sono archiviati in:

Voce	Strutture aggregative	
3.12 Organizzazione, patrimonio e risorse	**Serie tipologica di documenti** Una serie per ogni Settore e per ogni anno	**Non sono presenti Volumi**

I documenti sono nel seguente formato:

TIPOLOGIA	FORMATO	MIME TYPE	CONTENUTO	NOTE
Visto di conformità contabile	PDF	application/pdf	NA	File PDF firmato PAdES.

La forma documentaria è *Visto di conformità contabile*.

Lotto di ordinativi

I documenti relativi al lotto di ordinativi sono archiviati in:

Voce	Strutture aggregative	
5. Risorse Finanziarie e risorse contabili	**Serie tipologica di documenti** STDCO/CR – Conservazione degli ordinativi elettronici	**Volume** Un volume per ogni anno

I documenti sono nel seguente formato:

TIPOLOGIA	FORMATO	MIME TYPE	CONTENUTO	NOTE
Lotto di ordinativi	XML.P7M	application/pkcs7-mime	application/xml	File XML firmato CAdES

La forma documentaria è *Lotto di ordinativi*.

Pacchetto di versamento

Il sistema di gestione documentale DoQui ACTA, per i documenti appartenenti alle tipologie documentali definite nel paragrafo *1.2 Tipologie documentali*, genera il pacchetto di versamento e lo trasferisce al sistema di conservazione sulla base di quanto definito:

a) nel paragrafo *1.1 Metadati dei documenti da inviare in conservazione*;
b) nelle specifiche tecniche di configurazione LegalDoc PA definito con il conservatore InfoCert;
c) dal DPCM 3 dicembre 2013 "Regole tecniche in materia di sistema di conservazione".

Il sistema di conservazione restituisce:

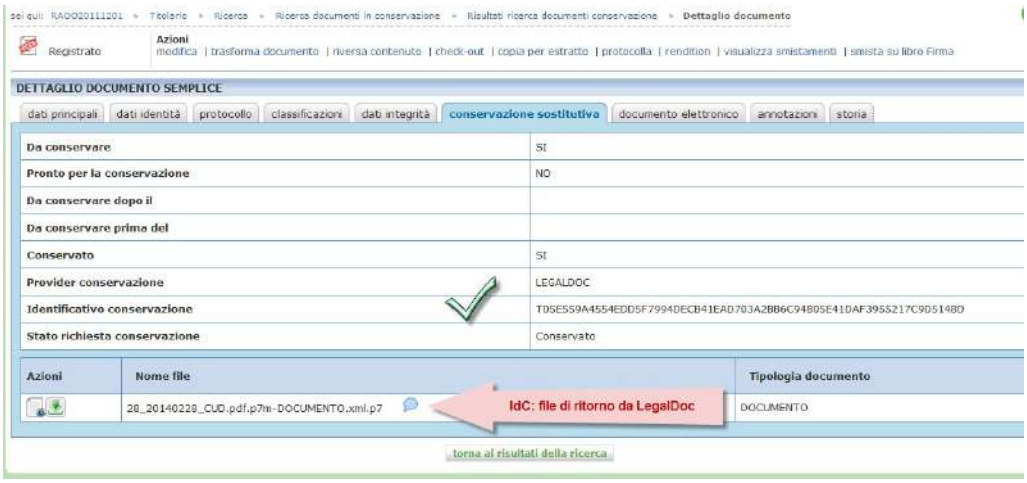
1. l'*Indice del pacchetto di archiviazione* IPdA (IdC - *Indice di Conservazione* nello standard SInCRO) in formato XML firmato dal responsabile della conservazione e marcato temporalmente

un esmpio di IdC (frammento)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<IdC>
  <SelfDescription>
    <ID>TD330A311A4749C1B1C3F3A87EF533280A47DD5CE35F4C40095274D484038CF11</ID>
    <CreatingApplication>
      <Name>Legaldoc</Name>
      <Version>1.0</Version>
      <Producer>Infocert</Producer>
    </CreatingApplication>
  </SelfDescription>
  <VdC>
    <ID>TD330A311A4749C1B1C3F3A87EF533280A47DD5CE35F4C40095274D484038CF11</ID>
    <MoreInfo>
      <EmbeddMetadata>
        <additionalInfo key="token">
            TD330A311A4749C1B1C3F3A87EF533280A47DD5CE35F4C40095274D484038CF11
        </additionalInfo>
        <additionalInfo key="bucket">B1</additionalInfo>
```

2. l'*identificativo di conservazione* del documento, un numero univoco che identifica il documento all'interno del sistema di conservazione.

Questi due elementi sono memorizzati all'interno del sistema di gestione documentale DoQui ACTA e sono reperibili, nel dettaglio del documento all'interno del folder "conservazione sostitutiva".



ALLEGATO B - FORMATI DOCUMENTI INFORMATICI

B.1 DOCUMENTI INFORMATICI

I documenti informatici devono essere formati utilizzando formati portabili statici non modificabili che non possano contenere macro istruzioni o codici eseguibili.

Nella scelta sono preferiti gli standard documentali ISO e gli standard che consentono il WYSIWYG (What You See Is What You Get), ovvero che forniscono sulla carta una disposizione grafica uguale a quella rappresentata sullo schermo del computer.

Sono accettate e protocollate le comunicazioni in cui i documenti allegati rispettano le seguenti condizioni:

- Si suggerisce l'utilizzo del formato PDF – PDF/A, perché di maggior diffusione e leggibilità.
- Sono comunque accettati i formati TIFF, JPG, XML, p7m, TXT, EML.
  Allegati in formati diversi (per esempio .doc, .xls, dvg,) verranno rifiutati.

Nel caso di file compressi (.zip, .rar…), dopo la loro decompressione si procederà alla verifica degli stessi ed alla successiva acquisizione solo nel caso di formati ammessi.

B.2 DOCUMENTI INFORMATICI FIRMATI

Sono accettate e protocollate le comunicazioni in cui i documenti allegati firmati o marcati digitalmente rispettano le seguenti condizioni:

- Le firme si appongono a documenti nei formati sopra indicati (il formato dei documenti deve essere convertito in uno dei formati ammessi prima della sottoscrizione con firma digitale),
- Le firme siano valide al momento della ricezione da parte dell'Ente.

B.3 DIMENSIONE DEI DOCUMENTI

Ciascun file componente il documento informatico deve avere una dimensione massima non superiore a 2 Mb. La somma delle dimensioni dei file inviati in un messaggio non deve superare i 20 Mb.