FONDAZIONE PTV
POLICLINICO TOR VERGATA

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DEL POLICLINICO TOR VERGATA

Area organizzativa omogenea "Protocollo generale"

Revisione	Data	Causale	Redazione RSP/P	Approvazione RSP/AAGG	Validazione Servizio informatico	Emissione IQ AAGG
1	30/10/2020	Nuova emissione	Dr. M. Guerrieri Wolf	Dr. F. Cosi	Dr. G. Guarnieri	Dr. M. Guerrieri Wolf
			Firmato	Firmato	Firmato	Firmato

Sommario

1 PRINCIPI GENERALI

1.1 Premessa

II Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "*Regole tecniche per il protocollo informatico*", all'articolo 3, comma 1, lettera d), prevede l'adozione del manuale di gestione di cui all'art. 5 per tutte le amministrazioni di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione digitale.

Il manuale di gestione, disciplinato dal successivo art. 5, comma 1, "*descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi*".

In conformità con quanto previsto dall'articolo 61 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445), l'art. 3, comma 1, lettere a) e b) dispone che ogni amministrazione pubblica individui una o più aree organizzative omogenee, all'interno delle quali sia nominato un responsabile della gestione documentale.

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

Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'attività dell'amministrazione.

Il manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente la gestione documentale.

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

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

1.2 Ambito di applicazione del manuale

II presente manuale di gestione è adottato ai sensi dell'articolo 3, comma 1, lettera d) del decreto del Presidente del Consiglio del 3 dicembre 2013 concernente le "*Regole tecniche per il protocollo informatico*". Esso descrive le attività di formazione e registrazione dei documenti, oltre alla gestione dei flussi documentali relativi ai procedimenti amministrativi del Policlinico Tor Vergata. Nelle more dell'elaborazione del titolario, non vengono, invece, effettuate le operazioni di classificazione e fascicolazione dei documenti, la cui archiviazione viene effettuata a livello decentrato a cura delle singole unità organizzative di riferimento.
Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e della spedizione di un documento.

1.3 Definizioni e norme di riferimento

Ai fini del presente manuale si intende per:

- "**amministrazione**", il Policlinico Tor Vergata;
- "**Testo Unico**", il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- "**Regole tecniche**", il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "*Regole tecniche per il protocollo informatico*";
- "**Codice**", il decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale.

Di seguito si riportano gli acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea;
- **MdG** - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;
- **RPA** - Responsabile del procedimento amministrativo - colui che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- **RSP** - Responsabile della gestione documentale;
- **SdP** – Servizio di protocollo informatico;
- **UOP** - Unità organizzative di protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UOR** - Unità organizzativa di riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- **UU** - Ufficio utente - un settore della UOR che utilizza i servizi messi a disposizione dal servizio di protocollo informatico.

1.4 Aree organizzative omogenee

Per la gestione dei documenti l'Amministrazione ha istituito un'unica Area Organizzativa Omogenea (AOO) denominata "*Area del Protocollo generale*", definita con separato atto del responsabile della gestione documentale, che ne individua le UOR e i relativi acronimi e che è sempre suscettibile di aggiornamento.

All'interno della AOO il sistema di protocollazione della posta in entrata è centralizzato presso una sola UOP, mentre quello della posta in uscita è ripartito tra più UOP all'uopo abilitate. Eccezionalmente, limitatamente alle domande di concorso o alle offerte di gara, è possibile autorizzare le UOR interessate alla protocollazione in entrata.

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. (di seguito SdP).

Al suddetto servizio è preposto il responsabile della gestione documentale (di seguito RSP), individuato secondo le regole vigenti presso l'ente.

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

- predisporre lo schema del manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del manuale sul sito istituzionale dell'amministrazione;
- abilitare gli utenti dell'AOO all'utilizzo del SdP e definire per ciascuno di essi il tipo di funzioni più appropriate tra quelle disponibili;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta conservazione della copia del registro giornaliero di protocollo;
- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;
- garantire il buon funzionamento degli strumenti interni all'AOO e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
- autorizzare le eventuali operazioni di annullamento della registrazione di protocollo;
- vigilare sull'osservanza delle disposizioni delle norme vigenti da parte del personale autorizzato e degli incaricati;
- curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza con gli strumenti e le funzionalità disponibili nel SdP.

1.6 Conservazione delle copie di riserva

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

1.7 Firma digitale

Per l'espletamento delle attività istituzionali l'amministrazione può fornire la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla. In tal caso viene istituito l'elenco delle persone titolari di firma digitale.

1.8 Tutela dei dati personali

L'amministrazione, titolare del trattamento dei dati personali contenuti nella documentazione amministrativa di propria competenza, si conforma alle norme del GDPR (UE) 2016/679 e del decreto legislativo 30 giugno 2003, n. 196 e ss.mm.ii.

1.9 Caselle di posta elettronica

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

In attuazione di quanto previsto dalla Direttiva del Ministro per l'Innovazione e le Tecnologie 18 novembre 2005 sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione munisce tutti i propri dipendenti compresi quelli per i quali non sia prevista la dotazione di un *personal computer* di una casella di posta elettronica convenzionale.

1.10 Sistema di classificazione dei documenti

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

Allo stato il titolario di classificazione non è adottato. L'Azienda si riserva di adottarlo in futuro.

1.11 Formazione

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

1.12 Accreditamento dell'AOO all'IPA (Indice delle P.A.)

L'AOO, come accennato si è dotata di una casella di posta elettronica certificata attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della UOP incaricata; quest'ultima procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta.

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'indice delle pubbliche amministrazioni (IPA), tenuto e reso pubblico dalla medesima fornendo le informazioni che individuano l'amministrazione e l'articolazione delle sue AOO.

Il codice identificativo dell'amministrazione è stato generato e attribuito autonomamente dall'amministrazione.

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

1.13 Dematerializzazione dei procedimenti amministrativi dell'AOO

L'Amministrazione favorisce la progressiva realizzazione di procedure tali da consentire, in coerenza con le disposizioni normative e regolamentari in materia, che nella AOO siano prodotti, gestiti, inviati e conservati solo documenti informatici.

E' prevista la riproduzione su carta degli originali informatici firmati e protocollati solo nel caso in cui il destinatario 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.

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

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

2.1 Piano di attuazione

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

Fanno eccezione esclusivamente i registri delle fatture, tenuti dalle UOR cui compete la gestione delle risorse economiche e finanziarie e dell'ALPI.

Il RSP esegue comunque, periodicamente, dei controlli a campione sugli UOR/UU per verificare la corretta esecuzione del piano e l'utilizzo regolare dell'unico registro ufficiale di protocollo.

3. PIANO DI SICUREZZA

Il presente capitolo riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

3.1 Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dall'AOO siano disponibili, integre e riservate;
- i dati personali comuni, sensibili e/o giudiziari vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

3.2 Generalità

Considerata la particolare modalità di fruizione del servizio di gestione del protocollo, gran parte delle funzioni/responsabilità di sicurezza sono demandate all'erogatore del SdP. All'AOO, in quanto fruitrice del servizio, è demandata la componente "locale" della sicurezza, poiché attraverso la propria organizzazione, nonché le sue misure e le politiche di sicurezza, essa contribuisce a stabilire adeguati livelli di sicurezza proporzionati al "valore" dei dati/documenti trattati.

I dati personali registrati nel *log* del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il SdP, saranno conservati secondo le vigenti norme e saranno consultati solo in caso di necessità.

3.3 Formazione dei documenti - Aspetti attinenti alla sicurezza

Il documento informatico, identificato in modo univoco e persistente, è memorizzato nel sistema di gestione informatica dei documenti in uso nella AOO che ne garantisce l'inalterabilità, la riservatezza e la fruibilità da parte di persone dotate di adeguate autorizzazioni.

L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'allegato 2 del DPCM 13 novembre 2014 in modo da assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la durata nel tempo dei dati in termini di accesso e di leggibilità.

3.4 Gestione dei documenti informatici

II sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente.

Il sistema operativo del *server* che ospita i *file* utilizzati come deposito dei documenti è configurato in maniera da consentire:

- l'accesso esclusivamente al *server* del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- può fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di *privacy*, con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio, ove adottato.

Per la gestione dei documenti informatici all'interno dell'AOO, il RSP fa riferimento alle disposizioni stabilite dal responsabile del sistema informativo del PTV.

3.4.1 Componente organizzativa della sicurezza

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte per l'erogazione del SdP.

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

- *sicurezza informatica* - si occupa principalmente della definizione dei piani di sicurezza e della progettazione dei sistemi di sicurezza;
- *sicurezza operativa* – si occupa di realizzare, gestire e mantenere in efficienza le misure di sicurezza così da soddisfare le linee strategiche di indirizzo definite dalla funzione *sicurezza informatica;*
- *revisione* – si occupa di controllare le misure di sicurezza adottate, verificandone l'efficacia e la coerenza con le politiche di sicurezza.

La componente organizzativa della sicurezza è articolata e gestita secondo quanto stabilito dai competenti uffici del PTV.

3.4.2 Componente logica della sicurezza

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, nell'ambito del SdP, è stata realizzata attraverso l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico:

- identificazione, autenticazione ed autorizzazione degli addetti delle AOO e degli operatori dell'erogatore del SdP;
- riservatezza dei dati;
- integrità dei dati;
- integrità del flusso dei messaggi;
- non ripudio dell'origine (da parte del mittente);
- non ripudio della ricezione (da parte del destinatario);

L'architettura realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione degli addetti delle AOO e degli operatori dell'erogatore del SdP, con le seguenti caratteristiche:

- unico *login server* per la gestione dei diritti di accesso ai servizi applicativi;
- unico sistema di *repository* delle credenziali di accesso degli utenti;
- unico database delle anagrafiche contenente tutti i profili di utenza.

La componente della sicurezza logica dell'AOO viene descritta nelle politiche di sicurezza definite dall'amministrazione aziendale.

3.4.3 Componente infrastrutturale della sicurezza

Presso il PTV sono disponibili i seguenti impianti:

- antincendio;
- luci di emergenza;
- continuità elettrica;

3.4.4 Gestione delle registrazioni di protocollo e di sicurezza

Il SdP garantisce la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

3.5 Trasmissione e interscambio dei documenti informatici

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

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

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

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

- accesso all'indice dei gestori di posta elettronica certificata, allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel *file* di *log* della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal GDPR (UE) 2016/679 e dal decreto legislativo del 30 giugno 2003, n. 196.

Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

3.5.1 All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).

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

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

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

3.5.2 All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.
Gli uffici organizzativi di riferimento (UOR) dell'AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica in attuazione di quanto previsto dalla Direttiva del Ministro per l'innovazione e le tecnologie del 18 novembre 2005 concernente l'impiego della posta elettronica nelle pubbliche amministrazioni.

3.6 Accesso ai documenti informatici

II controllo degli accessi è assicurato utilizzando le credenziali di accesso, pubblica *(UserID)* e privata *(Password)* ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

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

- *consultazione,* per visualizzare in modo selettivo, le registrazioni di protocollo eseguite da altri;
- *inserimento,* per inserire gli estremi di protocollo e effettuare una registrazione di protocollo ed associare i documenti;
- *modifica,* per modificare i dati opzionali di una registrazione di protocollo;
- *annullamento,* per annullare una registrazione di protocollo autorizzata dal RSP.

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

Il SdP fruito dall'AOO:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente, o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

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

Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca *full text.*

3.6.1 Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RSP dell'AOO.

Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti principi operativi:

- gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta esplicita dell'amministratore dell'AOO o per errori di inserimento)
- la credenziale privata degli utenti e dell'amministratore AOO non transita in chiaro sulla rete, né al momento della prima generazione, né successivamente al momento del *login.*

3.6.2 Accesso al registro di protocollo per utenti interni alla AOO

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

- *liste di competenza,* gestite dall'amministratore di AOO, per la definizione degli utenti abilitati ad accedere a determinate voci del titolario, ove presente (attualmente non applicabile);
- *ruoli degli utenti,* gestiti dall'amministratore di ente (amministrazione), per la specificazione delle macro-funzioni alle quali vengono abilitati;
- *protocollazione "particolare o riservata",* gestita dall' amministratore di ente, relativa a documenti sottratti alla consultazione da parte di chi non sia espressamente abilitato.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di "Responsabile del registro" e agli operatori della UOP.

Gli altri utenti del SdP sono invece abilitati ad una visione parziale sul registro di protocollo. Tale visione è definita dall'appartenenza a uno o più gruppi di utenti afferenti alle UOR ed è limitata ai documenti che transitano sulle relative scrivanie.

L'operatore della UOP, per segnalare la delicatezza di un documento, può definire come "*riservato*" ovvero "*altamente riservato*" un protocollo ed assegnarlo per competenza a una UOR o a un utente affidatario.

Nel caso in cui sia effettuata una protocollazione "altamente riservata", la visibilità completa sul documento è possibile solo a utenti preventivamente indivduati e autorizzati, oltre che ai protocollisti che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo).

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

3.6.3 Utenti esterni alla AOO

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

3.7 Conservazione dei documenti informatici

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

- DPCM 13 novembre 2014, per quanto attiene ai documenti informatici presenti nell'archivio corrente del PTV
- DPCM 3 dicembre 2013, per i documenti inviati in conservazione.

3.7.1 Servizio archivistico

Il PTV non dispone di un servizio archivistico, avendo optato per un sistema di archiviazione decentrato in luogo della centralizzazione, demandando alle singole UOR la custodia e l'archiviazione dei documenti cartacei assegnati per competenza.

La scelta è stata effettuata alla luce dei vincoli logistici imposti dall'edificio e della valutazione dei fattori di rischio che incombono sui documenti. L'Azienda si riserva di effettuare, in futuro, una valutazione circa l'opportunità di procedere all'istituzione di un servizio archivistico centralizzato.

3.7.2 Conservazione del registro giornaliero di protocollo

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

3.8 Politiche di sicurezza adottate dalla AOO

Le politiche di sicurezza stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure consuntive per la gestione degli incidenti informatici.

È compito del responsabile del servizio informatico e del responsabile della tutela dei dati personali procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.

II riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti attinenti alla sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dal PTV al fornitore del SdP, o a seguito dei risultati delle attività di *audit.*

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

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

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

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

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

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

- informatico;
- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "*1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71*" e "*2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità*".

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

4.1 Documento ricevuto

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

Un documento informatico può essere recapitato:

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

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;

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

A fronte delle tipologie descritte ne esiste una terza denominata "*ibrida*", composta da un documento analogico (lettera di accompagnamento) e da un documento digitale.

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, se la dimensione del documento e/o di eventuali allegati non supera la dimensione massima e il limite numerico di destinatari previsti dal sistema di posta utilizzato dall'AOO.
In caso contrario, il documento informatico viene copiato su supporto digitale rimovibile non modificabile e trasmesso al destinatario con altri mezzi di trasporto.

4.3 Documento interno formale

I documenti interni di rilevanza amministrativa giuridico-probatoria sono formati con tecnologie informatiche e lo scambio tra UOR/UU della AOO avviene mediante il SdP. Solo nella fase transitoria, dopo la trasformazione in analogici, avviene per mezzo della posta interna cartacea, che può anche, in ogni caso, accompagnare quella digitale.
In questo caso il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa sia sull'originale che sulla minuta e successivamente protocollato e acquisito mediante scansione.

4.4 Documento interno informale

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

4.5 Il documento analogico - cartaceo

Per documento analogico si intende un documento amministrativo formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale.

Di seguito si farà riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o *text editor*) e poi stampata.

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

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

4.6 Formazione dei documenti - Aspetti operativi

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

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

- deve trattare un unico argomento, indicato in maniera sintetica ma esaustiva dall'autore nello spazio riservato all'oggetto;
- deve essere identificato univocamente da un solo numero di protocollo,
- può fare riferimento a più fascicoli.

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

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabili delle singole UOR.

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

- la denominazione e il logo dell'amministrazione
- l'indirizzo della sede dell'amministrazione ed eventuali altri riferimenti (sito *web*, etc.)
- il codice fiscale dell'amministrazione
- l'indicazione dell'UOR che ha prodotto il documento e i recapiti (telefono, *email*)

Il documento deve inoltre recare almeno le seguenti informazioni:

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

4.7 Formazione dei documenti informatici - Aspetti operativi

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, XML e TIFF.

I documenti informatici redatti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati *standard* (PDF, XML e TIFF), come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Al documento informatico immodificabile vengono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo dei metadati, come definiti nell'allegato 5 al DPCM 13 novembre 2014 ("*Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici*"), è costituito da:
a) l'identificativo univoco e persistente;
b) il riferimento temporale di cui al comma 7;
c) l'oggetto;
d) il soggetto che ha formato il documento;
e) l'eventuale destinatario;
f) l'impronta del documento informatico.

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

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

- l'identificabilità del soggetto che ha formato il documento e l'AOO 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 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, la sua integrità e, se del caso, la riservatezza, 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 al decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 recante "*Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici*".

4.8 Sottoscrizione di documenti informatici

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.
I documenti informatici prodotti dall'AOO, indipendentemente dal *software* utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati *standard* previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità (vedi Allegato 2 del decreto del Presidente del Consiglio dei Ministri 13 novembre 2014).

4.9 Requisiti degli strumenti informatici di scambio

Scopo degli strumenti informatici di scambio e degli *standard* di composizione dei messaggi è garantire sia l'interoperabilità, sia i re+

quisiti minimi di sicurezza di seguito richiamati:

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

4.10 Firma digitale

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 4.9 è la firma digitale utilizzata per inviare e ricevere documenti per l'AOO per sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro *file* digitale con valenza giuridico-probatoria.

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

4.11 Uso della posta elettronica certificata

Il rispetto degli *standard* di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo (cfr. par. 3.5 Trasmissione e interscambio dei documenti informatici).

Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;

- inserire i dati del destinatario (almeno: denominazione, indirizzo, casella di posta elettronica); firmare il documento (ed eventualmente associare il riferimento temporale al documento firmato) e inviare il messaggio contenente il documento firmato digitalmente alla casella interna del protocollo;
- 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 istituzionale del destinatario.

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

- firmare elettronicamente il messaggio;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti alla stessa e ad altre amministrazioni.

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

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

Nel caso di trasmissione interna di allegati al documento di cui sopra che possono superare la capienza della casella di posta elettronica, si procede ad un riversamento (con le modalità previste dalla normativa vigente), su supporto rimovibile da consegnare al destinatario contestualmente al documento principale.
I documenti in partenza contengono l'invito al destinatario a riportare i riferimenti della registrazione di protocollo della lettera alla quale si dà riscontro.

Durante la fase transitoria di migrazione all'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere in formato analogico. I mezzi di recapito della corrispondenza in quest'ultimo caso sono il servizio postale, nelle sue diverse forme.

5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, e le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.

L'UOP non effettua fotocopie della corrispondenza trattata, sia in ingresso che in uscita.

5.1. Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento a quanto descritto nelle pagine seguenti.

Tali flussi sono stati elaborati 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.

5.2. Flusso dei documenti in ingresso alla AOO

5.2.1. Sorgente esterna dei documenti

Per sorgente esterna dei documenti si intende il servizio postale (pubblico o privato), la posta elettronica certificata o convenzionale, il telefax e la rimessa diretta alla UOP.

I documenti che transitano attraverso il servizio postale (pubblico o privato), indirizzati a tutta l'amministrazione, sono consegnati quotidianamente alla UOP, che si fa carico di selezionare e smistare la corrispondenza.

5.2.2. Sorgente interna dei documenti

Per sorgente interna dei documenti si intende qualunque UOR/UU che invia formalmente la propria corrispondenza ad altro UOR o UU della stessa AOO. Di norma, le UOR sono abilitate a registrare direttamente i propri documenti con il protocollo interno.

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

5.2.3. Ricezione di documenti informatici sulla casella di posta istituzionale

Di norma, la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile solo alla UOP dell'AOO. I documenti pervenuti sulla PEC vengono riversati in automatico nel SdP. Qualora tale funzione venga meno per motivi tecnici, la UOP vi provvede manualmente.

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

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

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

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

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

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

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

Nel caso in cui il messaggio viene ricevuto su una casella di posta elettronica certificata (PEC) non istituzionale o comunque non destinata al servizio di protocollazione, il messaggio stesso viene inoltrato alla casella di posta elettronica certificata istituzionale. I controlli effettuati sul messaggio sono quelli sopra richiamati.

I messaggi ricevuti su caselle di posta elettronica ordinaria sono stampati e trattati come cartacei.

5.2.5. Ricezione di documenti informatici su supporti rimovibili

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

Nei casi in cui con un documento cartaceo sono trasmessi gli allegati su supporto rimovibile, considerata l'assenza di *standard* tecnologici e formali in materia di registrazione di *file* digitali, la AOO si riserva la

facoltà di acquisire e trattare tutti quei documenti informatici così ricevuti che riesce a decodificare e interpretare con le tecnologie a sua disposizione.

Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e adempimenti del caso.

5.2.6. Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti pervenuti a mezzo posta sono consegnati alla UOP.

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

La corrispondenza relativa a bandi di gara non viene aperta, ma, dopo essere stata esaminata dal personale dell'UOP, che appone sulla busta la data e l'ora di arrivo della busta medesima, viene registrata al protocollo con la segnatura applicata sull'esterno del plico e successivamente riconsegnata chiusa all'Ufficio competente.

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

La corrispondenza ricevuta via telegramma, per ciò che concerne la registrazione di protocollo, è trattata come un documento cartaceo con le modalità descritte nel successivo capitolo 8.

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

5.2.7. Errata ricezione di documenti digitali

Nel caso in cui pervengano sulla casella di posta istituzionale dell'AOO, o anche su una casella non istituzionale, messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore rispedisce il messaggio al mittente con la dicitura "***Messaggio pervenuto per errore -non di competenza di questa AOO***".

5.2.8. Errata ricezione di documenti cartacei

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

5.2.9. Attività di protocollazione dei documenti

Superati tutti i controlli precedentemente descritti i documenti, digitali o analogici, sono protocollati e gestiti secondo gli *standard* e le modalità indicate nel dettaglio nel capitolo 8.

5.2.10. Rilascio di ricevute attestanti la ricezione di documenti informatici

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

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

Il sistema di protocollazione informatica dei documenti prevede la possibilità di formare e inviare al mittente di uno dei seguenti messaggi:

- *messaggio di conferma di protocollazione:* un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto. Si differenzia da altre forme di ricevute di

recapito generate dal servizio di posta elettronica dell'AOO in quanto segnala l'avvenuta protocollazione del documento, e quindi l'effettiva presa in carico;

● *messaggio di notifica di eccezione:* un messaggio che notifica la rilevazione di una anomalia in un messaggio ricevuto;

● *messaggio di annullamento di protocollazione:* un messaggio che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza;

● *messaggio di aggiornamento di protocollazione:* un messaggio che contiene una comunicazione di aggiornamento riguardante un documento protocollato ricevuto in precedenza.

5.2.11. Rilascio di ricevute attestanti la ricezione di documenti cartacei

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

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

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

● fotocopiare gratuitamente la prima pagina del documento;

● apporre gli estremi della segnatura se contestualmente alla ricezione avviene anche la protocollazione;

● apporre sulla copia così realizzata il timbro dell'amministrazione, con la data e l'ora d'arrivo e la sigla dell'operatore.

Nel caso di corrispondenza pervenuta ad una UOR, questa deve consegnarla alla UOP allo scopo di ottenere una ricevuta valida.

5.2.12. Conservazione dei documenti informatici

I documenti informatici ricevuti dall'AOO sono archiviati sui supporti di memorizzazione del centro servizi, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.
Tali documenti sono resi disponibili agli UOR/UU, attraverso la rete interna dell'amministrazione subito dopo l'operazione di assegnazione.

5.2.13. Conservazione delle copie per immagine di documenti cartacei

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

● acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico *file;*
● verifica della leggibilità e della qualità delle immagini acquisite;
● collegamento del *file* delle immagini alle rispettive registrazioni di protocollo, in modo non modificabile;
● memorizzazione del *file* delle immagini su supporto informatico, in modo non modificabile.

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

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

Gli originali dei documenti cartacei ricevuti vengono inviati alle UOR.

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

Gli addetti alla UOP provvedono ad inviare il documento all'UOR, che identifica l'UU di destinazione.

L'UOR:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore restituisce il documento alla UOP mittente;
- in caso di verifica positiva, esegue l'operazione di presa in carico smistandola al proprio interno ad un UU o affidandola direttamente ad uno o più operatori singoli;
- esegue la prima classificazione (o classificazione di primo livello) del documento, solo in assenza del titolario di classificazione dell'AOO e del meccanismo di assegnazione e classificazione automatica predisposto nel SdP.

5.2.15. Conservazione dei documenti nell'archivio corrente

Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso, ove presente il titolario di classificazione, vengono svolte le seguenti attività:

- classificazione di livello superiore sulla base del titolario;
- fascicolazione del documento;
- inserimento del fascicolo nel repertorio dei fascicoli nel caso di apertura di un nuovo fascicolo.

5.2.16. Conservazione dei documenti e dei fascicoli nella fase corrente

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

5.3. Flusso dei documenti in uscita dalla AOO

5.3.1. Sorgente interna dei documenti

Per "sorgente interna (all'AOO) dei documenti" si intende l'unità organizzativa mittente interna all'AOO che invia, tramite il RPA, la corrispondenza alla UOP della AOO stessa affinché sia trasmessa, nelle forme e nelle modalità più opportune, ad altra amministrazione o altra AOO della stessa amministrazione, ovvero ad altro ufficio (UU o UOR) della stessa AOO.
Per "documenti in uscita" s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra amministrazione o altra AOO della stessa amministrazione, ovvero ad altro ufficio (UU o UOR) della stessa AOO. Il documento è in formato digitale secondo gli *standard* illustrati nei precedenti capitoli. I mezzi di recapito della corrispondenza considerati sono quelli stessi richiamati nel paragrafo 4.2.

5.3.2. Verifica formale dei documenti

Tutti i documenti originali da spedire, siano essi in formato digitale o analogico, sono inoltrati alla UOP istituzionale:

- nella casella di posta elettronica interna dedicata alla funzione di "appoggio" per i documenti digitali da trasmettere nel caso di documenti informatici;
- in busta aperta per le operazioni di protocollazione e segnatura nel caso di documenti analogici, tranne i documenti contenenti dati personali sensibili o giudiziari.

L'UOP provvede ad eseguire le verifiche di conformità della documentazione ricevuta (per essere trasmessa) allo *standard* formale richiamato nel capitolo precedente (logo, descrizione completa dell'amministrazione e della AOO, etc.); verifica anche che siano indicati correttamente il mittente e il destinatario, che il documento sia sottoscritto in modalità digitale o autografa nonché la presenza di allegati, se dichiarati.

Se il documento è completo, viene registrato nel protocollo generale e ad esso viene apposta la segnatura; in caso contrario è rispedito al mittente UOR/UU/RPA con le osservazioni del caso.

5.3.3. Registrazione di protocollo e segnatura

Le operazioni di registrazione e di apposizione della segnatura del documento in uscita sono effettuate presso la UOP istituzionale. In nessun caso gli operatori di protocollo sono autorizzati a riservare numeri di protocollo per documenti non ancora resi disponibili. La compilazione di moduli, se prevista, come, ad esempio, nel caso di spedizioni per raccomandata con ricevuta di ritorno, posta celere, corriere, è a cura della UOR.

5.3.4. Trasmissione di documenti informatici

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

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

Per la spedizione dei documenti informatici l'AOO si avvale dei servizi di autenticazione e marcatura temporale propri di certificatore accreditato iscritto nell'elenco pubblico tenuto dall'AgID nonché del servizio di "posta elettronica certificata", conforme a quanto previsto dal Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione e di dare certezza sulla data di spedizione e di consegna dei documenti, attraverso una procedura di rilascio delle ricevute di ritorno elettroniche.

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

5.3.5. Trasmissione di documenti cartacei a mezzo posta

La UOP provvede alla spedizione della corrispondenza consegnando al servizio postale tutta la corrispondenza, mentre la UOR provvede alla chiusura delle buste e alla predisposizione delle ricevute di invio e di ritorno per le raccomandate, unitamente alla distinta delle stesse da rilasciare al servizio postale.

5.3.6. Affrancatura dei documenti in partenza

Tutte le attività di affrancatura della corrispondenza inviata per posta vengono svolte dal servizio postale.

5.3.7. Documenti in partenza per posta convenzionale con più destinatari

Qualora i destinatari siano più di uno, vengono inviate solo le copie dell'unico originale prodotto dalla UOR/UU. Tali copie devono essere prodotte dalla stessa UOR.

5.3.8. Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito e le ricevute di ritorno delle raccomandate, ovvero sono conservate all'interno del relativo fascicolo a cura delle UOR/UU. Le ricevute di ritorno, sulle quali viene precauzionalmente trascritto sia il numero di protocollo attribuito al documento a cui esse si riferiscono, sia l'UOR/UU mittente, sono inizialmente raccolte dalla UOP e successivamente consegnate alle UOR/UU.

Le ricevute digitali del sistema di posta certificata, utilizzata per lo scambio dei documenti digitali, vengono associate in automatico dal SdP al documento cui si riferiscono e restano disponibili a sistema.

6. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI

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

6.1. Regole disponibili con il SdP

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

Il SdP, per abbreviare il processo di assegnazione dei documenti, utilizza l'elenco delle UOR e degli acronimi di cui all'organigramma dell'AOO.

All'assegnazione segue la presa in carico del documento da parte del RPA, che provvede a smistarlo a un UU ovvero ad affidarlo, se del caso, all'addetto istruttore della pratica. In questa sede viene eseguita la classificazione del documento secondo le voci del titolario, ove presente.

6.2. Attività di assegnazione

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

L'attività di assegnazione di un documento, che compete al RSP ovvero agli operatori della UOP da lui delegati, può essere effettuata per competenza e per conoscenza.

Essa consiste nell'attribuzione della competenza del procedimento amministrativo cui il documento si riferisce ad una delle UOR destinatarie e, quindi, al suo RPA. Tale attribuzione può anche non coincidere con l'indicazione effettuata dal mittente e persino investire una UOR non destinataria. In casi eccezionali, ove si ravvisi una competenza trasversale a più UOR, anche se non tutte indicate dal mittente come destinatarie, è ammessa una competenza plurima.

L'assegnazione può prevedere, altresì, l'inoltro per conoscenza a destinatari ulteriori rispetto a quelli già indicati dal mittente.

In ogni caso, nessun destinatario indicato dal mittente può essere escluso dall'assegnazione.

Una volta assegnato, il documento viene protocollato e inviato tramite la piattaforma informatica alle UOR destinatarie e/o assegnatarie. L'eventuale formato originale cartaceo viene posto a disposizione della sola UOR assegnataria per competenza in apposito velinario.

Preso atto dell'assegnazione, il RPA verifica la competenza e, se esatta, prende in carico il documento che gli è stato assegnato, mediante l'accettazione.

I termini per la definizione del procedimento amministrativo che prende avvio dal documento decorrono comunque dalla data di protocollazione.

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

6.3. Corrispondenza di particolare rilevanza

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto utilizzato, viene inviato in busta chiusa direttamente al Direttore generale.

6.4. Assegnazione dei documenti ricevuti in formato digitale

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

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

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare come affidatario il RPA competente per la materia a cui si riferisce il documento o smistarlo a un UU.

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

I destinatari del documento per "competenza" e/o "per conoscenza" lo ricevono esclusivamente in formato digitale.

6.5. Assegnazione dei documenti ricevuti in formato cartaceo

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

- viene acquisito in formato immagine con l'ausilio di *scanner.;*
- viene successivamente trasmesso/ritirato al/dal RPA (non è mai conservato dalla UOP).

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

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

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento
- individuare come affidatario il RPA competente per la materia a cui si riferisce il documento o smistarlo a un UU.

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

6.6. Modifica delle assegnazioni

Nel caso di assegnazione errata, l'UOR/UU che riceve il documento può respingerlo alla UOP mediante il rifiuto motivato. La UOP procederà ad una nuova assegnazione.

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

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

6.7. Assegnazione dei documenti inviati

L'UOP, dopo aver protocollato in uscita il documento, lo assegna all'ufficio proponente. Tale assegnazione è generata automaticamente dal SdP ed è la conferma dell'avvenuta protocollazione del documento.

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

7.1. Documenti esclusi

Sono, esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53, comma 5, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 come riportato di seguito:

- Gazzetta ufficiale, Bollettino Ufficiale e notiziari della pubblica amministrazione;
- note di ricezione di circolari e altre disposizioni;
- materiali statistici;

- atti preparatori interni;
- giornali, riviste, libri, materiali pubblicitari (opuscoli, *depliant*);
- inviti a manifestazioni (che non attivino procedimenti amministrativi);

Si considerano assimilabili ai primi i seguenti documenti:

- documenti personali e note informali
- certificati medici
- esiti di visite fiscali al domicilio
- moduli per richiesta ferie, recupero ore, permessi, e simili
- programmazione e modifica dei turni del personale
- fogli-firme di presenza del personale
- lettere di accompagnamento di fatture e documenti di trasporto/doganali, quando non contengano informazioni aggiuntive rilevanti sotto il profilo amministrativo
- conferme di invio dei telegrammi e ricevute di ritorno di raccomandate
- richieste di informazioni o appuntamenti da parte di utenti esterni
- moduli per richieste interne di utilizzo sale riunioni, intervento tecnico, duplicato chiavi, e simili.

7.2. Documenti soggetti a registrazione particolare

Ai sensi dell'ultimo periodo dell'art. 53, comma 5, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono escluse dalla registrazione di protocollo generale, in quanto "*già soggette a registrazione particolare dell'ente*", le fatture attive e passive nonché le note di credito e di debito.

Tale tipo di registrazione consente, comunque, di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti.

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

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

8.1. Unicità del protocollo informatico

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

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

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

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

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

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

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

Non è consentita la protocollazione di un documento già protocollato.

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

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

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

8.2. Registro giornaliero di protocollo

II 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 e reso disponibile in formato PDF.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è inviato in conservazione, ai sensi dell'art. 7, comma 5, del DPCM 3 dicembre 2013. Tale operazione viene espletata automaticamente dal SdP.

8.3. Registrazione di protocollo

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

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

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

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

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma on modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente che ha prodotto il documento;
- il destinatario del documento;
- l'oggetto del documento;

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

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.

Tali dati facoltativi sono descritti nei paragrafi seguenti.

8.3.1. Documenti informatici

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

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma.

Nel caso di documenti informatici in partenza, l'operatore esegue anche 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.

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

I documenti informatici interni di tipo formale sono protocollati, di norma, dalla UOR che li produce.

8.3.2. Documenti analogici (cartacei e supporti rimovibili)

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

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

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

8.4. Elementi facoltativi delle registrazioni di protocollo

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

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

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

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

- II numero di protocollo e la data o solo data se presente;
- ulteriori informazioni sul mittente/destinatario, soprattutto se persona giuridica;
- l'indirizzo completo del mittente/destinatario (via, numero civico, CAP, città, provincia, stato civile, sesso);
- il numero di matricola (se dipendente interno dell'amministrazione);
- il codice fiscale;
- il numero della partita IVA;
- il recapito telefonico;
- gli indirizzi di posta elettronica;
- la chiave pubblica della firma digitale;
- il consenso all'uso della *email* in termini di *privacy*.

8.5. Segnatura di protocollo dei documenti

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

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

Essa consente di individuare ciascun documento in modo inequivocabile.

8.5.1 Documenti informatici

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

Le informazioni minime incluse nella segnatura sono le seguenti:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- codice identificativo del registro;
- data e numero di protocollo del messaggio ricevuto o inviato;
- oggetto;
- mittente;
- destinatario/destinatari.

E' facoltativo riportare le seguenti informazioni:
- denominazione dell'amministrazione;
- codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo.

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

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

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

8.5.2. Documenti cartacei

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

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

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

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

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

8.6. Annullamento delle registrazioni di protocollo

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

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RSP. In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.

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

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

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

8.7. Livello di riservatezza

Il SdP applica automaticamente il livello di riservatezza "base" a tutti i documenti protocollati.

E' possibile applicare un livello intermedio, selezionando l'opzione "*riservato*", che non limita la visibilità del documento, ma fornisce una indicazione ai destinatari circa la delicatezza del contenuto.

Infine, è possibile applicare l'opzione "*altamente riservato*", che limita la visibilità del documento ai soli operatori della UOP e agli altri utenti espressamente designati dal RSP sentita la Direzione.

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

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

8.8. Casi particolari di registrazioni di protocollo

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

8.8.1. Documenti cartacei in uscita con più destinatari

Qualora i destinatari siano più d'uno, il protocollo è unico e viene riportato solo sull'originale. I destinatari sono indicati sul documento con i recapiti *email*/PEC, con esclusione degli indirizzi di abitazione privata.

8.8.2. Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma inoltrati al servizio protocollo come documenti senza firma, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

8.8.3. Protocollazione di un numero consistente di documenti cartacei

Quando si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso (ad es. scadenza di gare o di concorsi) che in uscita, deve esserne data comunicazione all'ufficio protocollo con almeno due giorni lavorativi di anticipo, onde concordare tempi e modi di protocollazione e di spedizione.

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

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

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

Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, gli stessi saranno accantonati e protocollati successivamente. In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

8.8.5. Assegni e altri valori.

Gli assegni o altri valori di debito o credito sono protocollati sul registro ufficiale di protocollo e inviati quotidianamente, in originale, alla UOR competente.

8.8.6. Protocollazione di documenti inerenti gare di appalto su supporti cartacei

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo", o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non viene aperta dalla UOP, ma viene timbrata e protocollata dalla medesima, che provvede poi a riportare sul plico il numero di protocollo, la data l'ora di arrivo.

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

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

8.8.7. Protocolli urgenti

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

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

8.8.8. Documenti privi di firma o anonimi

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

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

Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali, con la dicitura "documento non firmato".

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

8.8.9. Protocollazione dei messaggi di posta elettronica convenzionale

Considerato che l'attuale sistema di posta elettronica convenzionale non consente di interfacciarsi con quella certificata e non è quindi possibile reindirizzare le *email* alla PEC del Protocollo, queste, ai fini della registrazione, devono essere trattate come documenti cartacei e, quindi, stampate e presentate alla UOP.

Le *email* di solo testo in uscita devono essere presentate alla UOP prima dell'invio o comunque in pari data.

8.8.10. Protocollazione di documenti digitali pervenuti erroneamente

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all'AOO non competente, l'addetto al protocollo, previa autorizzazione del RSP, provvede o ad annullare il protocollo stesso o a protocollare il documento in uscita indicando nell'oggetto "***protocollato per errore***" e rispedisce il messaggio al mittente.

8.8.11. Ricezione di documenti cartacei pervenuti erroneamente

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

8.8.12. Copie per "conoscenza"

Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nel paragrafo 8.8.1. In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, registra sul registro di protocollo a chi sono state inviate le copie "per conoscenza".

8.8.13. Differimento delle registrazioni

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

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

Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee indicate dal RSP.

8.8.14. Corrispondenza personale o riservata

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

8.8.15. Integrazioni documentarie

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

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

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

8.9. Gestione delle registrazioni di protocollo con il SdP

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

II sistema di sicurezza del centro servizi garantisce la protezione di tali informazioni sulla base della relativa architettura tecnologica, sui controlli d'accesso e i livelli di autorizzazione realizzati.

8.10. Registrazioni di protocollo

8.10.1. Attribuzione del protocollo

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

Il SdP assicura l'esattezza del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.

Come previsto dalla vigente normativa in materia di protezione dei dati personali, gli utenti abilitati a inserire dati nel SdP sono informati della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo.

8.10.2. 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 di informatico con l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire l'immodificabilità della registrazione medesime.

Il SdP provvede all'esecuzione automatica della stampa su *file*, in formato .PDF, del Registro giornaliero di protocollo. Il documento così creato riporta su un unico *file* il riepilogo di tutte le registrazioni di protocollo

eseguite nell'ambito della stessa giornata e, a seguire, gli eventuali annullamenti (parziali o totali) occorsi ai protocolli acquisiti nel corso dei giorni precedenti.

I metadati da inviare in conservazione, unitamente alla copia del registro di cui sopra, sono stati suddivisi in tre sottogruppi:

- *Metadati di identificazione*. Contengono le informazioni relative all'ente che sta inviando il documento (*file* PDF) al conservatore e quelle del protocollo che identificano univocamente il documento. Sono memorizzati tra le proprietà del sistema (Ente, struttura, ecc.) e sulla registrazione del documento;
- *Metadati di profilo generali*. Contengono le informazioni generali sul documento, come oggetto e data. Sono memorizzati sulla registrazione di protocollo;
- *Metadati di profilo specifici*. Contengono le informazioni specifiche del tipo di documento, come numero di protocolli effettuati nella giornata, numero iniziale e numero finale. Sono memorizzati sulla registrazione di protocollo e tra le proprietà dell'Area Organizzativa Omogenea.

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

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

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

Il trasferimento del pacchetto di versamento al sistema di conservazione avviene tramite canale *web services*. Al riguardo è previsto un processo automatico che si occupi di creare il pacchetto di versamento, inviarlo al sistema di conservazione e registrare lo stato del versamento stesso. Il processo provvede a:

1. Estrarre dal registro giornaliero il documento da inviare in conservazione. *In generale è presente un solo documento da inviare ma, nel caso si sia verificato un problema nei giorni precedenti, la procedura effettua l'invio di tutti i documenti in attesa;*
2. Predisporre il pacchetto di versamento estraendo le informazioni necessarie dal documento e dal sistema;
3. Inviare il pacchetto in modalità sincrona;
4. Indicare nel documento lo stato "conservato", in caso di esito positivo;
5. Indicare nel documento lo stato "errore" ed inviare una notifica al responsabile della conservazione, in caso di esito negativo.

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

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

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

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

9.1. Descrizione funzionale ed operativa - Rinvio

La descrizione completa delle funzionalità dell'applicativo di protocollo è disponibile e consultabile nella specifica sezione della piattaforma informatica in uso presso l'ente.

10. IL 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. Tenuta del registro di emergenza

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

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

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

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

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

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

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

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

10.2. Modalità di apertura del registro di emergenza

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

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

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

Solo la UOP del Protocollo generale è abilitata alla registrazione dei documenti sul registro di emergenza.

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

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'AOO.

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

Durante il periodo di interruzione del SdP, il responsabile del Servizio informatico (o persona da lui delegata) informa costantemente il RSP sui tempi di ripristino del servizio in parola affinché possa fornire le informazioni aggiornate a chi ne faccia richiesta.

10.4 Modalità di chiusura e di recupero del registro di emergenza

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

E' compito del RSP, o di un suo delegato nella UOP, riportare dal registro di emergenza al registro di protocollo generale del SdP le protocollazioni relative ai documenti protocollati in emergenza attraverso le postazioni di lavoro abilitate, entro cinque giorni dal ripristino delle funzionalità del SdP.

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

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

11 ARCHIVIAZIONE E SCARTO DEI DOCUMENTI CARTACEI

11.1 Tipologie di archivi

Per "archivio" è da intendersi l'insieme di documenti prodotti o acquisiti dall'Azienda nello svolgimento dell'attività istituzionale.

Esistono i seguenti tre tipi di archivi:

- **archivio corrente**: insieme dei documenti relativi a procedimenti/attività in corso; per quanto riguarda l'attività amministrativa; l'archivio corrente è istituito presso la struttura competente che ne è la responsabile; per quanto riguarda l'attività sanitaria, l'archivio corrente è istituito presso la struttura che eroga la prestazione;
- **archivio di deposito**: insieme di documenti relativi a procedimenti/attività conclusi; gli archivi di deposito sono istituiti presso la struttura aziendale competente, che ne è la responsabile, ad eccezione dell'archivio delle cartelle cliniche, che è istituito presso il locale individuato dalla Direzione Sanitaria; in seguito dell'affidamento dell'appalto del servizio di archiviazione e gestione dei documenti dell'Azienda, la documentazione conservata negli archivi di deposito suddetti è di regola quella degli ultimi due anni, mentre quella degli anni antecedenti viene conservata presso l'archivio esterno gestito dalla ditta appaltatrice;
- **archivio storico**: documenti contenuti nell'archivio di deposito relativi a procedimenti conclusi da oltre 40 anni; tale documentazione è archiviata presso l'archivio esterno gestito dalla ditta appaltatrice.

Archivi correnti

Gli archivi correnti sono gestiti:

- per quanto riguarda l'attività amministrativa, dal Responsabile del procedimento/Referente;
- per quanto riguarda l'attività sanitaria da coloro che sono incaricati dal Responsabile della struttura.

Per quanto riguarda i documenti relativi all'attività amministrativa:

a) il Responsabile del procedimento/Referente inserisce il documento nel fascicolo del procedimento/pratica; sulla copertina del fascicolo è indicato l'oggetto; i fascicoli sono inseriti in faldoni, sul cui dorso sono indicati l'oggetto e l'anno o gli anni di riferimento;

b) i documenti sono conservati secondo le indicazioni del Responsabile della struttura;

c) almeno una volta l'anno il Responsabile del procedimento/Referente della pratica:

- deposita i faldoni dei documenti relativi a procedimenti/attività conclusi da meno di due anni presso l'archivio di deposito interno;
- fa depositare i faldoni dei documenti relativi a procedimenti/attività conclusi da più di due anni presso l'archivio esterno gestito dalla ditta appaltatrice.

Per quanto riguarda i documenti relativi all'attività sanitaria:

a) sono conservati secondo le indicazioni del Responsabile della struttura che gestisce l'archivio;

Archivi di deposito

Gli archivi di deposito interni sono gestiti dal Responsabile della struttura competente o da uno o più referenti da lui nominati.

Archivio storico

I documenti contenuti nell'archivio di deposito relativi a procedimenti conclusi da oltre 40 anni sono archiviati presso l'archivio esterno gestito dalla ditta appaltatrice.

11.2 Responsabili dell'archiviazione

Sono responsabili dell'archiviazione e della corretta tenuta dell'archivio i Responsabili delle strutture competenti alla gestione del procedimento cui i documenti oggetto di archiviazione si riferiscono.

11.3 Scarto dei documenti

I periodi di conservazione dei documenti sono indicati nel "*Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere*" redatto dal Ministero per i beni e le Attività Culturali. Il Prontuario indica, per ciascuna voce, quali documenti debbano essere conservati permanentemente e quali invece possono essere destinati alla distruzione trascorsi i tempi minimi di conservazione indicati; l'applicazione dei tempi minimi di conservazione prescritti dal Prontuario sarà comunque effettuata in riferimento al caso concreto e alle esigenze di servizio.

Il rispetto dei termini massimi di conservazione della documentazione costituisce misura di prevenzione in materia di trattamento dei dati personali, in attuazione del principio di *accountability* sancito dal regolamento UE 2016/679.

11.4 Criteri per la selezione della documentazione da scartare

Lo scarto di documenti viene proposto periodicamente da ciascun Responsabile di Struttura quando si verifichino le seguenti condizioni: 1) esaurimento dell'utilità giuridico- amministrativa dei documenti; 2) mancanza di apprezzabile interesse come fonte storica; 3) scadenza dei tempi minimi di conservazione previsti dal Prontuario.

11.5 Procedura di scarto della documentazione conservata presso gli archivi di deposito interni

Il responsabile della struttura, una volta verificato il materiale da eliminare (tenendo conto delle condizioni sopra richiamate), trasmette alla UOC Affari Generali la proposta di scarto e l'elenco delle tipologie di documentazione che si ritiene non abbiano più utilità giuridico-amministrativa. L'elenco, in testa al quale è indicato il numero di pagine di cui esso si compone, verrà predisposto avendo cura di garantire la congruità dell'elenco e la corrispondenza dei dati riportati alle tipologie documentarie e agli anni di conservazione previsti dal Prontuario. L'elenco deve comprendere:

a) la descrizione delle tipologie dei documenti, facendo riferimento alla terminologia riportata nell'elenco o Prontuario;

b) l'anno o gli anni di riferimento;

c) la quantità del materiale (in numero di faldoni, scatole, pacchi e, ove possibile, in peso/volume in metri cubi approssimativo);

d) l'intestazione dell'Azienda, la data e la firma del Dirigente della Struttura che richiede lo smaltimento;

e) i l luogo nel quale sono conservati i documenti.

La UOC Affari Generali provvede successivamente ad inviare alla Soprintendenza archivistica e bibliografica del Lazio la richiesta di nulla osta, allegando l'elenco dei documenti da scartare trasmessi dai Dirigenti responsabili dello smaltimento.

La Soprintendenza archivistica restituisce una copia dell'elenco vistato con approvazione totale o parziale (c.d. nulla osta).

Il PTV adotta, su proposta della UOC Affari Generali, la deliberazione di scarto, facendo riferimento all'elenco autorizzato dalla Soprintendenza archivistica e Bibliografica per il Lazio, che costituisce parte integrante dell'atto. La gestione del processo di smaltimento sarà affidata alla struttura competente per la gestione del contratto di smaltimento rifiuti.

Al termine dell'operazione di smaltimento, il PTV richiede alla ditta copia del verbale di consegna del materiale da eliminare, con indicazione del relativo peso qualora possibile, nonché l'attestazione dell'avvenuta distruzione del materiale consegnato, da inviare poi alla UOC Affari Generali.

L'UOC Affari Generali trasmette successivamente alla Soprintendenza archivistica e bibliografica per il Lazio copia del verbale di consegna del materiale da eliminare e l'attestazione dell'avvenuta distruzione.

12 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI

12.1 Modalità di approvazione e aggiornamento del manuale

L'Amministrazione adotta il presente "Manuale di gestione" su proposta del RSP e 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.

12.2 Pubblicità del Manuale

Il presente Manuale è disponibile alla consultazione del pubblico e del personale mediante pubblicazione sulla *intranet* aziendale e sul sito istituzionale del PTV.

12.3 Operatività del Manuale

Il presente Manuale è operativo dal giorno della sua adozione.