MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DELL'AGENZIA PER L'ITALIA DIGITALE

Area Organizzativa Omogenea ADG

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione		Donatelle Vigevani	
Verifica		Marco Bani	
Approvazione		Antonio Samaritani	

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
3.1		Adeguamento al DPCM 3 dicembre 2013	

Indice

1 PRINCIPI GENERALI

1.1 Premessa

II decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 recante le "Regole tecniche per il protocollo informatico", all'articolo 3, comma 1, lettera d), prevede l'adozione del "Manuale di gestione del protocollo informatico, dei documenti e dell'archivio" 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, redatto secondo quanto previsto dal successivo art. 5, comma 1, del suddetto DPCM," descrive il sistema di gestione anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi". In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 50 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000).

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

Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale sulla quale 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 necessarie per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

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

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

1.2 Ambito di applicazione del manuale

II presente manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'articolo 3, comma 1, lettera d) del decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 recante le "Regole tecniche per il protocollo informatico".
Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'Agenzia per l'Italia Digitale – AgID.
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", l'Agenzia per l'Italia Digitale - AgID
- "Testo Unico", il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- "Regole tecniche", il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico";
- "Codice", il decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale.

Per le definizioni vedasi l'elenco riportato nell'allegato 1.

Di seguito si riportano gli acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea;
- **CGD** – Coordinatore della Gestione Documentale;
- **MdG** - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;
- **RPA** - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- **RSP** - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **SdP** – Servizio di protocollo informatico;
- **UOP** - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UOR** - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- **UU** - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal servizio di protocollo informatico; ovvero il soggetto, destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Per le norme ed i regolamenti di riferimento vedasi l'elenco riportato nell'allegato 2.

1.4 Aree Organizzative Omogenee

Per la gestione dei documenti l'amministrazione ha istituito un'unica Area Organizzativa Omogenea (AOO), denominata "ADG", nell'ambito della quale è istituito un unico servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi (allegato 4).

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

All'interno della AOO il sistema di protocollazione è centralizzato, e tutta la corrispondenza, in ingresso e in uscita, è gestita da una sola UOP.

1.5 Servizio per la gestione informatica del protocollo

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

Al suddetto servizio è preposto il Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RSP).

Le attività afferenti al Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi, sono coordinate da un dirigente, il Coordinatore della gestione documentale (di seguito CGD) .

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 Tutela dei dati personali

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

1.8 Caselle di Posta Elettronica

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

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

1.9 Sistema di classificazione dei documenti

Con l'inizio dell'attività operativa del protocollo informatico, è stato adottato un unico Titolario di classificazione per l'archivio centrale unico dell'amministrazione.

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

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

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

1.10 Formazione

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

1.11 Accreditamento dell'AOO all' IPA

L'AOO, come accennato, si è dotata di una casella di posta elettronica certificata attraverso la quale trasmette e riceve documenti informatici soggetti alla registrazione di protocollo. Tale casella è 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), 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'IPA è accessibile, tramite il relativo sito internet, a tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni modifica delle proprie credenziali di riferimento nonché la data a partire dalla quale la modifica stessa sarà operativa: sarà così garantita l'affidabilità dell'indirizzo di posta elettronica indicato. Con la stessa tempestività, l'amministrazione comunica la soppressione, ovvero la creazione di una AOO.

1.12 Dematerializzazione dei procedimenti amministrativi della AOO

L'amministrazione ha in fase di prossima realizzazione 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.

È 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 all'eliminazione dei registri di protocollo diversi dal protocollo informatico.

2.1 Piano di attuazione

In coerenza con quanto previsto e disciplinato dal presente manuale, tutti i documenti inviati e ricevuti dalla AOO sono registrati nel 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:

- il registro di protocollo delle circolari interne;
- il registro di protocollo degli ordini di servizio;
- eventuali registri per la protocollazione di corrispondenza riservata in uso esclusivo al Direttore generale.

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 e, attraverso controlli ed ispezioni mirate, la validità dei criteri di classificazione utilizzati.

3 PIANO DI SICUREZZA

II 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

II 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 vengano 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.

Il piano di sicurezza:

- si articola in due componenti: una di competenza del SdP, una di competenza della AOO;
- si basa sui risultati delle analisi dei rischi a cui sono esposti i dati e i documenti trattati, rispettivamente, nei locali dove risiedono le apparecchiature utilizzate dal SdP e nei locali della AOO;
- si fonda sulle direttive strategiche di sicurezza stabilite;
- definisce:
    - le politiche generali e particolari di sicurezza da adottare all'interno, rispettivamente, del Centro servizi e della AOO;

- le modalità di accesso al SdP;
- gli aspetti operativi della sicurezza, con particolare riferimento alle misure minime di sicurezza, *di cui al Disciplinare tecnico richiamato nell'allegato B) del D.lgs. 196/2003 - Codice in materia di protezione dei dati personali;*
- i piani specifici di formazione degli addetti;
- le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione formale con cadenza almeno biennale. Esso può essere modificato a seguito di eventi gravi.

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

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

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

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

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce 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 adottato.

Per la gestione dei documenti informatici all'interno dell'AOO, il RSP fa riferimento alle norme stabilite dal responsabile dall'Area "Sistemi, tecnologie e sicurezza informatica" dell'AgID.

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 Centro servizi destinato ad erogare il SdP, le qualifiche funzionali individuate sono le seguenti:

- responsabile del centro;
- responsabile della sicurezza;
- responsabile della tutela dei dati personali;
- responsabile dei sistemi e delle reti;
- internai auditor;
- responsabile del *call center;*
- operatore di sicurezza;
- operatore (sistemi e TLC);

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;
- *operativa sicurezza* ha il compito 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* ha il compito di controllare le misure di sicurezza adottate, verificandone l'efficacia e la coerenza con le politiche di sicurezza.

Relativamente alla componente fisica della sicurezza sono stati definiti i seguenti ruoli:

- responsabile della sicurezza;
- responsabile Centro servizi;
- operatori della sicurezza.

La componente organizzativa della sicurezza afferente l'AOO è articolata e gestita secondo quanto stabilito dall'Area "Sistemi, tecnologie e sicurezza informatica" dell'AgID.

3.4.2 Componente fisica della sicurezza

II controllo degli accessi fisici alle risorse della sede del Centro servizi è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;
- i meccanismi di controllo dell'accesso sono più selettivi all'aumentare del livello di protezione del locale;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti devono esplicare la procedura di registrazione. Essi non possono entrare e trattenersi nelle aree protette se non accompagnati da personale dell'erogatore del servizio autorizzato a quel livello di protezione;
- ogni persona che accede alle risorse della sede in locali protetti è identificata in modo certo con sistemi di autenticazione forte;
- gli accessi alla sede sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;
- il personale della sede ha l'obbligo di utilizzare il *badge* sia in ingresso che in uscita dalla sede stessa.

Le misure di sicurezza fisica hanno un'architettura multilivello così articolata:

- a livello di *edificio*, attengono alla sicurezza perimetrale e sono atte a controllare l'accesso alla sede in cui sono ospitate risorse umane e strumentali;
- a livello di *Centro di servizio*, sono destinate a controllare l'accesso ai locali del centro;
- a livello di *locale*, sono finalizzate a controllare l'accesso ai locali interni alla sede.

Il controllo degli accessi fisici alle risorse della sede dell'amministrazione/AOO è regolato secondo i principi stabiliti dal Servizio Logistica e affari generali dell'Area "Contabilità, finanza e funzionamento" dell'AgID.

3.4.3 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);
  - *audit* di sicurezza;
- la ridondanza dei sistemi di esercizio.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura "a strati multipli di sicurezza" conforme alle *best practices* correnti.

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 dall'Area "Sistemi, tecnologie e sicurezza informatica" dell'AgID.

3.4.4 Componente infrastrutturale della sicurezza

Presso il Centro servizi dell'erogatore sono disponibili i seguenti impianti:

- antincendio;
- rilevazione dell'allagamento;
- luci di emergenza;
- continuità elettrica;
- controllo degli accessi e dei varchi fisici.

Essendo il Centro servizi lontano da insediamenti industriali e posto all'interno di un edificio adibito ad uffici, le sue condizioni ambientali per quanto riguarda polvere, temperatura, umidità, vibrazioni meccaniche, interferenze elettriche e radiazioni elettromagnetiche e livelli di inquinamento chimico e

biologico, sono tali da non richiedere misure specifiche di prevenzione oltre quelle già adottate per le sedi di uffici di civile impiego.

Gli impianti e le considerazioni precedenti valgono anche per la componente infrastrutturale della sicurezza per l'AgID. In particolare:

- antincendio;
- luci di emergenza;
- continuità elettrica;
- controllo degli accessi e dei varchi fisici.

3.4.5 Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad esempio: dati, transazioni), presenti o transitate sul SdP che occorre mantenere, sia dal punto di vista regolamentare, sia in caso di controversie legali, che abbiano ad oggetto le operazioni effettuate sul SdP, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai *log* dei dispositivi di protezione periferica del sistema informatico *(intrusion detection system-IDS*, sensori di rete *e firewall),*
- dalle registrazioni dell'applicativo SdP, modulo GEDOC.

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:

- l'accesso alle registrazioni è limitato, esclusivamente, ai sistemisti o agli operatori di sicurezza addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- le registrazioni del modulo GEDOC sono elaborate tramite procedure automatiche dal sistema di autenticazione e di autorizzazione
- i supporti con le registrazioni di sicurezza sono conservati all'interno di un armadio ignifugo in un locale con controllo biometrico per l'accesso;
- i *log* di sistema sono accessibili ai sistemisti in sola lettura al fine di impedirne la modifica;
- l'operazione di scrittura delle registrazioni del SdP, modulo GEDOC è effettuata direttamente dagli applicativi;
- le registrazioni sono soggette a copia giornaliera su disco.

In questa sede viene espressamente richiamato quanto stabilito nell'ultimo capoverso paragrafo 3.2 del presente manuale.

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, 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 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 preventiva degli utenti.

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, effettuare una registrazione di protocollo ed associare i documenti;
- *Modifica* - per modificare i dati opzionali di una registrazione di protocollo;
- *Annullamento* - per annullare una registrazione di protocollo autorizzata dal RSP.

Le regole per la composizione delle *password* e il blocco delle utenze valgono sia per l'amministratore che per gli utentidella AOO .

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

Il SdP fruito dall'AOO:

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

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

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

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

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

3.6.1 Utenti interni alla AOO

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

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, ne' al momento della prima generazione, ne' 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;
- *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 limitatamente al registro dell'AOO sul quale è stato abilitato ad operare.

L'utente assegnatario dei documenti protocollati è invece abilitato ad una visione parziale sul registro di protocollo. Tale visione è definita dalle voci di Titolario associate alla lista di competenza in cui l'utente è presente (sia come singolo, sia come ufficio).

L'operatore che gestisce lo smistamento dei documenti può definire "riservato" una registrazione di protocollo ed assegnarla per competenza ad un utente assegnatario.

Nel caso in cui sia effettuata una protocollazione riservata, la visibilità completa del documento è possibile solo all'utente assegnatario per competenza e agli operatori di protocollo 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 - Altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui agli art. 72 e ss. del d.lgs 7 marzo 2005 n. 82.

Le AOO che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC, utilizzano funzioni di accesso per ottenere le seguenti informazioni:

- numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
- identificazione dell'UU di appartenenza del RPA.

3.6.4 Utenti esterni alla AOO - Privati

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 dell'Agenzia
- DPCM 3 dicembre 2013 per i documenti inviati in conservazione.

3.7.1 Servizio archivistico

Il CGD, in accordo con il RSP, ha individuato nei locali al piano -2, al primo e al terzo piano e negli armadi ubicati nei corridoi della sede istituzionale dell'amministrazione medesima, la sede del relativo archivio dell'amministrazione.

La scelta è stata effettuata alla luce dei vincoli logistici imposti dall'edificio e della valutazione dei fattori di rischio che incombono sui documenti. Per contenere i danni conseguenti a situazioni di emergenza, è in corso di perfezionamento un piano specifico che individui i soggetti incaricati di ciascuna fase.

Sono state altresì regolamentate le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.

Il CGD e il RSP sono a conoscenza, in ogni momento, della collocazione del materiale archivistico. A tal fine, sono stati predisposti, a cura dell'RSP, elenchi di consistenza del materiale afferente

all'archivio di deposito e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.

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

3.7.2 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.

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

3.7.3 Conservazione delle registrazioni di sicurezza

Un operatore di sicurezza dell'erogatore, provvede con periodicità almeno mensile, alla memorizzazione su supporto ottico dei seguenti oggetti:

- i *file* contenenti i *log* originali;
- le firme dei *file.*

I supporti sono archiviati in un armadio ignifugo dell'area sicurezza del Centro servizi e sono conservati per un periodo minimo di cinque anni ove specifiche disposizioni di legge non ne prevedano la conservazione per un più lungo periodo.

Le modalità di archiviazione sono regolamentate da procedure specifiche.

3.7.4 Riutilizzo e dismissione dei supporti rimovibili

All'interno del Centro servizi dell'erogatore del servizio di protocollo informatico non è previsto il riutilizzo dei supporti rimovibili. Al termine del periodo di conservazione prestabilito i supporti sono distrutti secondo una specifica procedura operativa.

3.8 Politiche di sicurezza adottate dalla AOO

Le politiche di sicurezza, riportate nell'allegato 5 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 della sicurezza e del responsabile della tutela dei dati personali procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.

Il 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 dall'AgID al fornitore del SdP, o a seguito dei risultati delle attività di *audit.*

In ogni caso, tale attività è svolta almeno con cadenza annuale.

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

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'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 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;
4. con consegna diretta da parte dell'interessato, 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 prevista, dal sistema di posta attualmente utilizzato dall'AOO, che è di 30 *Megabytes*, e un limite di 50 destinatari.

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

4.3 Documento interno formale

I documenti interni sono formati con tecnologie informatiche e, solo nella fase transitoria, lo scambio tra UOR/UU della AOO di documenti informatici di rilevanza amministrativa giuridico-probatoria, dopo averli trasformati in analogici, avviene per mezzo della posta interna cartacea.
In questo caso il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa sia sull'originale che sulla minuta e successivamente protocollato.
Per le richieste di parere prodotte già oggi interamente in formato digitale firmato la trasmissione avviene attraverso il SdP utilizzando la casella di posta elettronica certificata.

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

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

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

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

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

Il documento deve inoltre recare almeno le seguenti informazioni:

- il luogo di redazione[1];
- la data (giorno, mese, anno)[1];
- il numero di protocollo[1];
- 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.

[1] Questo valore è riportato all'interno dell'etichetta di segnatura del protocollo

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 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").

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, al fine di garantirne l'immodificabilità, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione (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 requisiti minimi di sicurezza di seguito richiamati:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno 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 (si vedano le norme pubblicate sul sito www.agid.gov.it)

4.11 Verifica delle firme nel SdP per i formati .p7m

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

- apertura della busta "virtuale" contenente il documento firmato;
- verifica della validità del certificato; questa attività è realizzata verificando *on-line* le *Certificate Revocation List* (CRL) con una periodicità predefinibile parametricamente nel modulo GEDOC. Una giacenza in memoria temporanea *(cache)* di un'ora è considerata accettabile;
- verifica della firma (o delle firme multiple) con funzioni Java standard; in particolare, viene calcolata l'impronta del documento e verificata con quella contenuta nella busta "logica";
- verifica dell'utilizzo, nell'apposizione della firma, di un certificato emesso da una *Certification Authority* (CA) presente nell'elenco pubblico dei certificatori accreditati e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle CA accreditate presso l'AgID con periodicità settimanale;
- trasformazione del documento in uno dei formati standard previsti dalla normativa vigente in materia (PDF o XML o TIFF) e attribuzione della segnatura di protocollo;
- inserimento nel sistema documentale del SdP (modulo GEDOC) sia del documento originale firmato, sia del documento in chiaro;
- archiviazione delle componenti verificate e dei dati dei firmatari rilevati dal certificato in una tabella del database del SdP per accelerare successive attività di verifica di altri documenti ricevuti.

E' in corso l'aggiornamento del SdP allo standard di firma in formato PDF.

4.12 Uso della posta elettronica certificata

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

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

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

- redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno: denominazione, indirizzo, casella di posta elettronica); firmare il documento (ed eventualmente associare il riferimento temporale al documento firmato); 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.

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

I messaggi di ritorno, che sono classificati in:

- conferma di ricezione;
- notifica di eccezione;
- aggiornamento di conferma;
- annullamento di protocollazione;

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

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

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

5 DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

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

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

5.1 Generalità

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

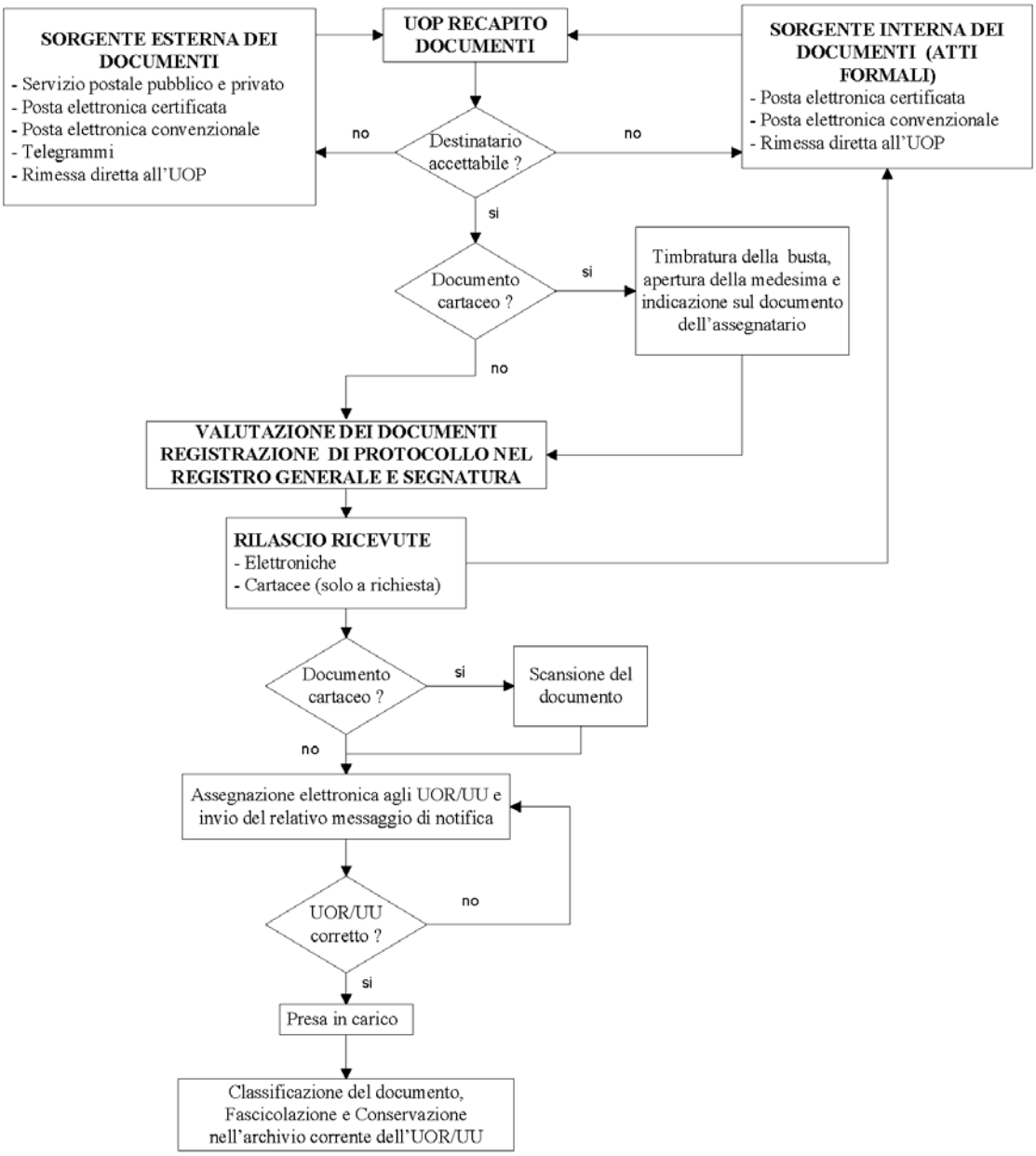
Tali flussi sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico probatoria. Essi si riferiscono ai documenti:

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

I flussi gestiti all'interno del sistema archivistico dell'amministrazione/AOO dalla Sezione di deposito e storica dell'archivio sono sviluppati, per omogeneità e completezza di trattazione, nel successivo capitolo 10 (Sistema di classificazione, fascicolazione e piano di conservazione).

Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni è ricevuto e trasmesso per posta elettronica interna e non interessa il sistema di protocollo.

5.2 Flusso dei documenti in ingresso alla AOO



5.2.1 Provenienza esterna dei documenti

Oltre quelli richiamati nel capitolo precedente, i documenti trasmessi da soggetti esterni all'AOO possono essere, tra gli altri, eventuali supporti digitali rimovibili allegati a documenti cartacei. Questi documenti sono recapitati alla UOP designata.

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

Le modalità di gestione della corrispondenza in ingresso, stabilite dal CGD in accordo con l'RSP, sono riportate nell'allegato 7.

5.2.2 Provenienza di documenti interni formali

Per sorgente interna dei documenti si intende qualunque UOR/UU che invia formalmente la propria corrispondenza alla UOP della AOO per essere, a sua volta, trasmessa, nelle forme opportune, ad altro UOR o UU della stessa AOO.

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

5.2.3 Ricezione di documenti informatici sulla casella di posta istituzionale

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

Quando i documenti informatici pervengono alla UOP, 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 non istituzionale o comunque non destinata al servizio di protocollazione, il messaggio stesso viene inoltrato alla casella di posta istituzionale.

I controlli effettuati sul messaggio sono quelli richiamati nel paragrafo precedente.

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 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.

L'acquisizione degli allegati digitali nel sistema SdP può avvenire attualmente solo se la grandezza totale di ogni allegato non supera il limite di 1 Megabyte.

Gli allegati che superano tale dimensione dovranno essere riversati su un apposito disco virtuale condiviso e visibile dagli utenti assegnatari.

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 del Servizio contratti dell'Area "Affari giuridici e contratti", 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 ne' protocollata, ma consegnata al destinatario: questi ne valuterà il contenuto e, nel caso dovesse riguardare l'amministrazione, provvederà a inoltrarla all'Ufficio protocollo per la registrazione.

La corrispondenza ricevuta via telegramma, per ciò che concerne la registrazione di protocollo, è trattata come un documento cartaceo con le modalità descritte nel successivo capitolo 11 (Modalità di produzione e di conservazione delle registrazioni di protocollo informatico).

Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.

La corrispondenza in ingresso viene timbrata sull'involucro all'arrivo alla UOP e, di norma, aperta lo stesso giorno lavorativo in cui è pervenuta. Essa viene assegnata contestualmente all'apertura, con indicazione manuale del destinatario sul documento medesimo, e 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 in una casella non istituzionale, messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore rispedisce il messaggio al mittente con la 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 per il recapito all'indirizzo corretto.

5.2.9 Attività di protocollazione dei documenti

Superati tutti i controlli precedentemente descritti i documenti, digitali o analogici, sono protocollati e gestiti secondo gli standard e le modalità indicate nel dettaglio nel capitolo 11 (Modalità di produzione e di conservazione delle registrazioni di protocollo informatico).

5.2.10 Rilascio di ricevute attestanti la ricezione di documenti informatici

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

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

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

- *messaggio di conferma di protocollazione:* un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto. Si differenzia da altre forme di ricevute di recapito generate dal servizio di posta elettronica dell'AOO in quanto segnala l'avvenuta protocollazione del documento, e quindi l'effettiva presa in carico;
- *messaggio di notifica di eccezione:* un messaggio che notifica la rilevazione di una anomalia in un messaggio ricevuto;
- *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 per la tenuta del protocollo sulla copia, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale della UOP in merito alla ricezione ed all'assegnazione del documento.

Quando il documento cartaceo è consegnato direttamente alla UOP 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'AgID sono archiviati sui supporti di memorizzazione del Centro servizio, 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, di norma non vengono inviati alle UOR ma rimangono alla UOP che provvede ad archiviarli in ordine sequenziale di protocollo. A questa regola fanno eccezione i documenti seguenti:

- richieste di parere (inviati al Servizio Pareri, Istruttorie e Modelli, dell'Area Studi, ricerca e pareri);
- corrispondenza riguardante il personale dipendente (inviata al Servizio Amministrazione del personale, dell'Area Amministrazione, controllo di gestione e Programmazione)
- originali delle lettere-contratto firmate per accettazione (inviate al Servizio Contratti dell'Area Affari giuridici e contratti)
- documentazione contabile da esibire per eventuali controlli (inviata alla Servizio Bilancio e contabilità, dell'Area Contabilità, finanza e funzionamento).

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

5.2.14 Assegnazione, presa in carico dei documenti e classificazione.

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

L'UOR:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, restituisce il documento alla UOP mittente;
- in caso di verifica positiva, esegue l'operazione di presa in carico riassegnandola, al proprio interno, ad un UU o direttamente al RPA;
- esegue la prima classificazione (o classificazione di primo livello) del documento sulla base del Titolario di classificazione in essere presso l'AOO, solo in assenza del meccanismo di assegnazione e classificazione automatica predisposto nel SdP.

5.2.15 Conservazione dei documenti nell'archivio corrente

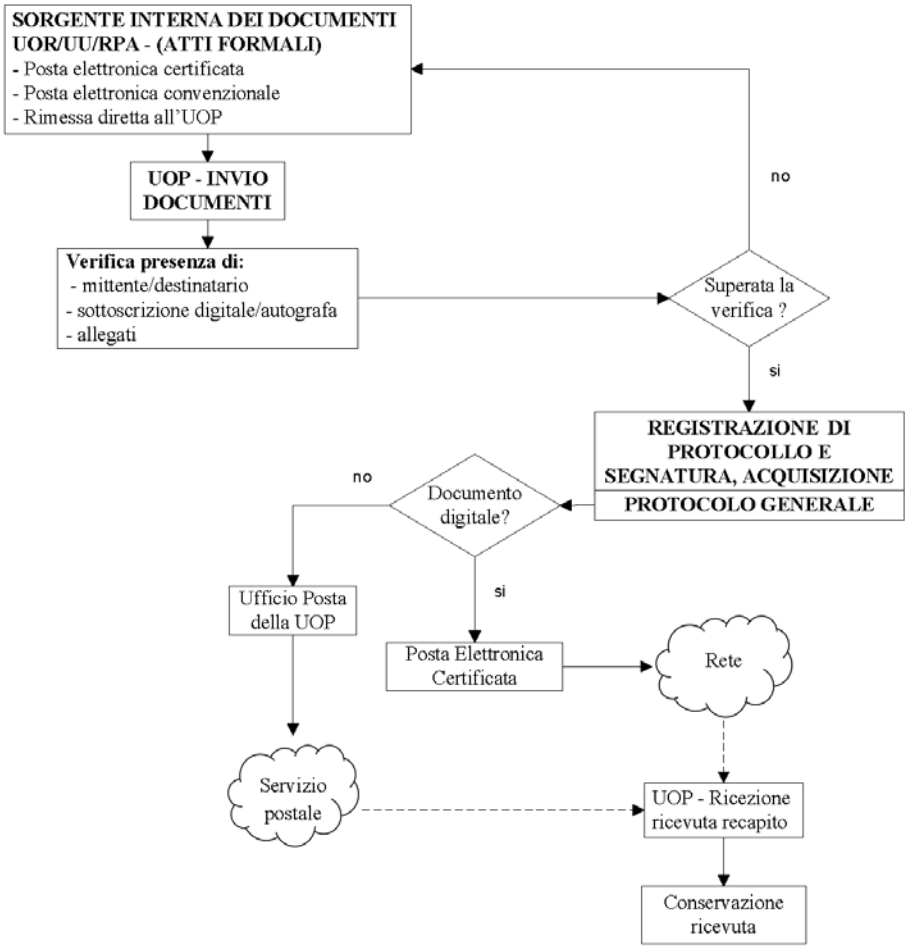
Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le seguenti attività:

- classificazione di livello superiore, sulla base del Titolario di classificazione adottato dall'AOO;
- fascicolazione del documento, secondo le procedure previste dall'AOO;
- inserimento del fascicolo nel repertorio dei fascicoli, nel caso di apertura di un nuovo fascicolo.

5.2.16 Conservazione dei documenti e dei fascicoli nella fase corrente

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

5.3 Flusso dei documenti in uscita dalla AOO



5.3.1 Sorgente interna dei documenti

Nel grafico di cui al paragrafo 5.3 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 formato secondo gli standard illustrati nei precedenti capitoli.

I mezzi di recapito della corrispondenza considerati sono quelli stessi richiamati nel paragrafo "4.12 - Uso della posta elettronica certificata".

5.3.2 Verifica formale dei documenti

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

- nella casella di posta elettronica interna dedicata alla funzione di "appoggio", nel caso di documenti digitali da trasmettere;
- 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). L'UOP verifica anche che siano indicati correttamente il mittente e il destinatario, che il documento sia sottoscritto in modalità digitale o autografa, e, se dichiarati, la presenza di allegati.

Se il documento è completo, viene registrato nel protocollo generale e ad esso viene apposta la segnatura; in caso contrario è restituito al UOR/UU/RPA proponente 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.

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

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.

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

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

5.3.5 Trasmissione di documenti cartacei a mezzo posta

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

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

5.3.6 Affrancatura dei documenti in partenza

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

Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla UOP secondo le regole richiamate nell'allegato 7.

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 dall'UOR/UU.

5.3.8 Inserimento delle ricevute di trasmissione nel fascicolo

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

Gli UOR/UU curano anche l'archiviazione degli avvisi di ricevimento delle raccomandate. Questi ultimi, sui quali, precauzionalmente, viene trascritto sia il numero di protocollo attribuito al documento al quale si riferiscono, sia l'UOR/UU mittente, sono inizialmente raccolte dalla UOP e, successivamente, consegnate alle UOR/UU medesime previo rilascio di ricevuta di consegna.

6 REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

II presente capitolo contiene le regole di assegnazione, adottate dalla UOP, per i documenti in ingresso.

6.1 Regole disponibili con il SdP

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

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

All'assegnazione segue la presa in carico del documento da parte del RPA, che provvede a inoltrarlo, se del caso, all'addetto istruttore della pratica. In questa sede viene eseguita la classificazione del documento secondo le voci del Titolario.

6.2 Attività di assegnazione

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

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

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

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

Una volta che al mittente iniziale (UOP) giunge notizia della presa in carico della corrispondenza, questo provvede ad inviare, con le tecnologie adeguate, il documento in questione, compilato nella parte segnatura (o timbro di segnatura), al UOR/UU/RPA di competenza.

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

L'UOR competente è incaricata della gestione del procedimento cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento amministrativo che si avvia con l'assegnazione del 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 per 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, è 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 in modo non modificabile su supporti informatici interni al Centro servizio.

L'UOR competente ha notizia dell'assegnazione di detti documenti tramite un messaggio di posta elettronica di "notifica di assegnazione".

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

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

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

I destinatari del documento per "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 e 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 viene trattato come di seguito indicato:

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

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

L'UOR competente ha notizia dell'arrivo/assegnazione del documento ad esso indirizzato tramite un messaggio di posta elettronica.

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

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

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

6.6 Modifica delle assegnazioni

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

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

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

7 REGOLE DI ASSEGNAZIONE DEI DOCUMENTI INVIATI

II presente capitolo riporta le regole di gestione dei documenti in uscita adottate dalla UOP.

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.

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

Il presente capitolo individua l'Unità Organizzativa Responsabile delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno della AOO.

In base al modello organizzativo adottato dall'amministrazione, nell'allegato 3 è riportata l'articolazione della AOO in UOR e UU.

Relativamente all'organizzazione e alla tenuta dei documenti della AOO è stato istituito il servizio archivistico.

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

8.1 Servizio archivistico

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

Al servizio archivistico preposto l'RSP. Le attività afferenti a tale servizio sono coordinate dal CGD in accordo con l'RSP.

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

9.1 Documenti esclusi

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53, comma 5, del dPR 28 dicembre 2000, n. 445 come riportato nell'Allegato 8.

9.2 Documenti soggetti a registrazione particolare

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati nell'Allegato 9.

La registrazione particolare consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione documentale avuto riguardo, nello specifico, alla classificazione, alla fascicolazione, all'indicizzazione.

10 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

10.1 Protezione e conservazione degli archivi pubblici

10.1.1 Caratteristiche generali

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

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del Piano di classificazione (Titolario). Il Titolario è definito come un "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti".

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

Il Titolario e il Piano di conservazione sono adottati dall'amministrazione con atti formali.

10.1.2 Misure di protezione e conservazione degli archivi pubblici

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

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

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

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

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

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

10.2 Titolario o Piano di classificazione

10.2.1 Titolario

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

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

Il titolo individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni, classi e sottoclassi, corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato, secondo lo schema riportato nell'allegato 12.

Titoli, classi, sottoclassi nonchè le rimanenti voci di livello, sono nel numero prestabilito dal Titolario e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del vertice dell'amministrazione.

Il Titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali.

L'aggiornamento del Titolario compete esclusivamente al vertice dell'amministrazione, su proposta del CGD.

La revisione, anche parziale, del Titolario viene proposta dal CGD, in accordo con l'RSP, quando necessario ed opportuno.

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

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

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

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

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

Rimane possibile, qualora il sistema lo consenta, la registrazione di documenti in fascicoli già aperti fino alla conclusione e alla chiusura degli stessi.

Il Titolario attualmente in uso è stato elaborato da un gruppo di lavoro appositamente costituito all'interno dell'AOO ed è stato approvato dai competenti organi dell'amministrazione archivistica statale.

10.2.2 Classificazione dei documenti

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

Essa è eseguita in base al Titolario di classificazione facente parte del Piano di conservazione dell'archivio.

Tutti i documenti ricevuti e prodotti dagli UOR dell'AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati secondo le voci del Titolario vigente.

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

Le operazioni di classificazione sono svolte interamente dagli UOR/UU destinatari/istruttori di atti.

10.3 Fascicoli e dossier

10.3.1 Fascicolazione dei documenti

Tutti i documenti registrati nel sistema di protocollo informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.

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

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

10.3.2 Apertura del fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'AOO, il RPA provvede all'apertura di un nuovo fascicolo.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

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

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

10.3.3 Chiusura del fascicolo

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

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

Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.

Gli elementi che individuano un fascicolo sono gestiti dal soggetto di cui al paragrafo precedente, primo capoverso, il quale è tenuto, pertanto, all'aggiornamento del repertorio dei fascicoli.

10.3.4 Processo di assegnazione dei fascicoli

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

A seconda delle ipotesi, si procede come segue:

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

10.3.5 Modifica dell'assegnazione dei fascicoli

Quando si verifica un errore nell'assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'UOR di competenza.

Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando, per ciascuno di essi, l'identificativo dell'operatore di UU che effettua la modifica, la data e l'ora dell'operazione.

10.3.6 Repertorio dei fascicoli

I fascicoli, sono annotati nel Repertorio dei fascicoli.

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

La struttura del Repertorio rispecchia quella del Titolario di classificazione e, di conseguenza, varia in concomitanza con l'aggiornamento di quest'ultimo.

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

Il Repertorio dei fascicoli è costantemente aggiornato.

10.3.7 Apertura del dossier

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

- il numero del *dossier,*
- la data di creazione;
- il responsabile del *dossier,*
- la descrizione o l'oggetto del *dossier,*
- la sigla della AOO e dell'UOR;
- l'elenco dei fascicoli contenuti;
- il livello di riservatezza del *dossier* (viene, di norma, assegnato dal livello di riservatezza del fascicolo a più alto livello di riservatezza).

10.3.8 Repertorio dei dossier

I *dossier,* di norma, sono annotati nel repertorio dei *dossier.*

Il repertorio dei *dossier* è lo strumento di gestione e reperimento dei *dossier.*

Nel repertorio sono indicati:

- il numero del *dossier,*
- la data di creazione;
- la descrizione o oggetto del *dossier,*
- il responsabile del *dossier.*

Il repertorio dei *dossier* è costantemente aggiornato.

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

10.4.1 Principi generali

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

10.4.2 Consultazione ai fini giuridico-amministrativi

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

"Esclusione dal diritto di accesso."

1. Il diritto di accesso è escluso:
    a. per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
    b. nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
    c. nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
    d. nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.
2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.
3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.
4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.
5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.
6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi:
    a. quando, al di fuori delle ipotesi disciplinate dall'articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione;
    b. quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
    c. quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;

d. quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono;
e. quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

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

10.4.3 Consultazione da parte di personale esterno all'amministrazione

La domanda di accesso ai documenti viene presentata/inviata alla UOP, che provvede a smistarla al servizio archivistico.

Presso la UOP, a cui fa capo il servizio archivistico, sono disponibili appositi moduli, come quelli riportati nell'Allegato 11.

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

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

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

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

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

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

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

10.4.4 Consultazione da parte di personale interno all'amministrazione

Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito, o storica, compilando appositi moduli, come quello riportato nell'Allegato 11.

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

Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa, redatta in duplice copia su un apposito modello, come quello riportato

nell'Allegato 11, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, il suo UOR/UU e la sua firma.

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

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

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

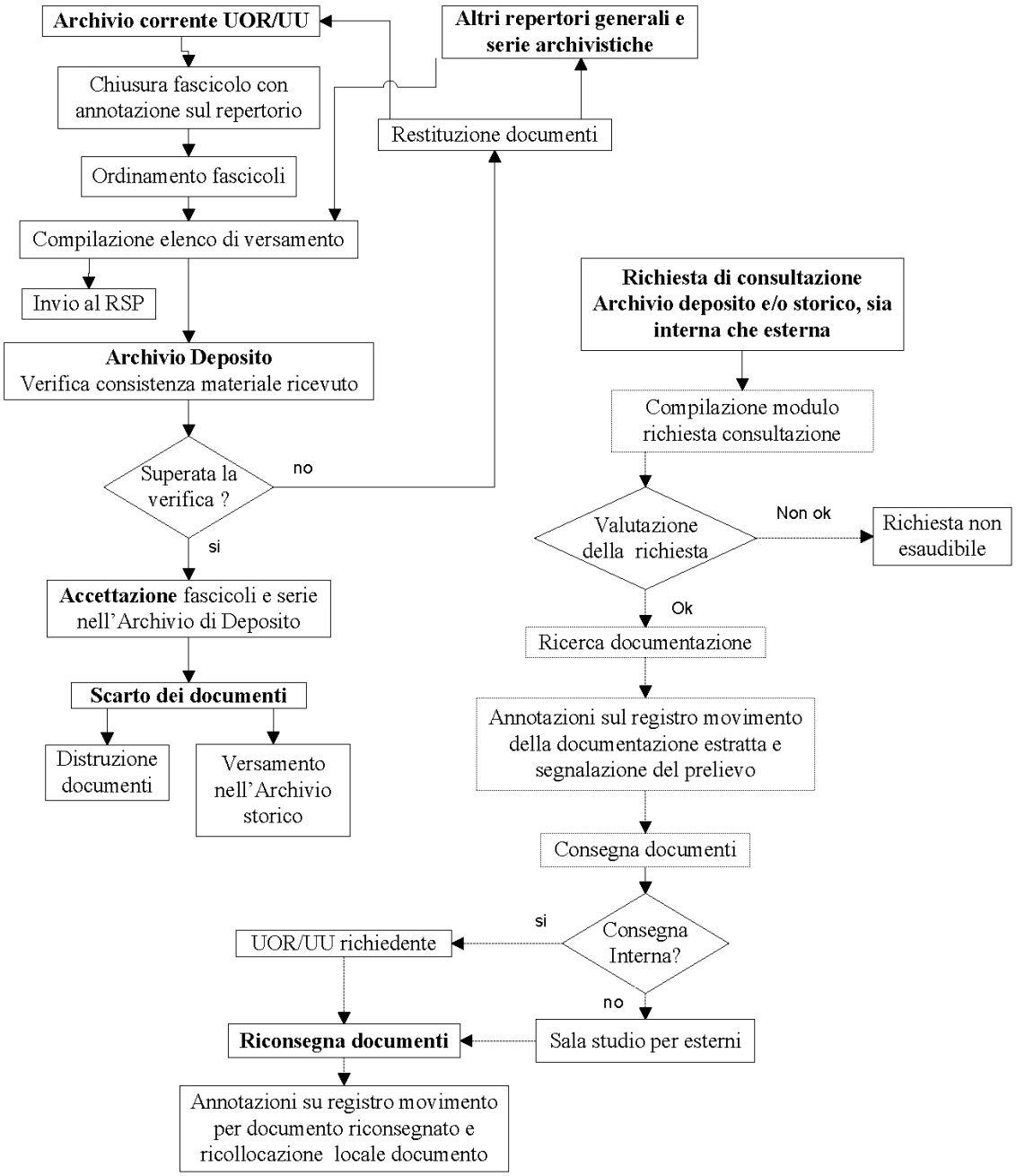
L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine degli stessi rispettandone la sedimentazione archivistica e il vincolo.

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

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

10.4.5 Schematizzazione del flusso dei documenti all'interno del sistema archivistico

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



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

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

11.1 Unicità del protocollo informatico

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

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

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

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

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

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

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

Non è consentita la protocollazione di un documento già protocollato.

Il registro di protocollo è un atto pubblico originario ed è idoneo a produrre effetti giuridici.

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

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

11.2 Registro giornaliero di protocollo

Il 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 Registro giornaliero di protocollo è inviato in conservazione. Tale operazione viene espletata automaticamente dal SdP.

11.3 Registrazione di protocollo

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

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

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

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

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

- l'oggetto del documento;

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

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

Tali dati facoltativi sono descritti nei paragrafi seguenti.

11.3.1 Documenti informatici

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

La registrazione di protocollo 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.

Le UOP ricevono i documenti informatici interni di tipo formale da protocollare all'indirizzo di posta elettronica interno preposto a questa funzione.

11.3.2 Documenti analogici (cartacei e supporti rimovibili)

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

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

Nel caso di corrispondenza in uscita l'UOP esegue la registrazione di protocollo e invia la copia dell'originale informatico sottoscritto digitalmente e protocollato.

11.4 Elementi facoltativi delle registrazioni di protocollo

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

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

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

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

- Il 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 e-mail in termini di privacy.

11.5 Segnatura di protocollo dei documenti

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

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

Essa consente di individuare ciascun documento in modo inequivocabile.

11.5.1 Documenti informatici

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

Le informazioni minime incluse nella segnatura sono le seguenti:

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

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

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

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

11.5.2 Documenti cartacei ricevuti

La segnatura di protocollo di un documento cartaceo ricevuto 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'etichetta autoadesiva ha il formato e il contenuto riportato nell'Allegato 12.

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.

11.6 Annullamento delle registrazioni di protocollo

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

11.7 Livello di riservatezza

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

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

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

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

11.8 Casi particolari di registrazioni di protocollo

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

11.8.1 Circolari e disposizioni generali

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

Le circolari ricevute vengono protocollate nel registro ufficiale di protocollo.

Le disposizioni generali e tutte le altre comunicazioni interne, di norma, si registrano con un solo numero di protocollo nel Registro di protocollo interno.

11.8.2 Documenti cartacei in uscita con più destinatari

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

11.8.3 Documenti cartacei ricevuti a mezzo telegramma

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

11.8.4 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.

11.8.5 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.

11.8.6 Fatture

Le fatture sono protocollate sul registro ufficiale di protocollo e inviate automaticamente al sistema di gestione contabile della UOR competente.

11.8.7 Assegni e altri valori di debito o credito

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

11.8.8 Protocollazione di documenti inerenti gare di appalto confezionate su supporti cartacei

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo", o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non viene aperta dalla UOP, ma viene timbrata dalla medesima che provvede ad inoltrarla alla UOR/UU competente; quest'ultima provvede a sottoscrivere il plico, a riportare sul medesimo la data, l'ora di arrivo ed a riconsegnarla alla UOP per la protocollazione del plico in questione.

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

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

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

11.8.9 Protocollazione delle domande di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata confezionate su supporti cartacei

La corrispondenza, dal cui involucro si evince che si tratta di una domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata, non viene aperta dalla UOP, ma protocollata con l'applicazione dell'etichetta autoadesiva di segnatura sulla confezione. Successivamente viene inoltrata alla UOR/UU competente. Quest'ultima, dopo l'apertura della busta, ha l'obbligo di riportare gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.

11.8.10 Protocolli urgenti

La richiesta di protocollare urgentemente un documento deve essere 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.

Tale procedura viene osservata sia per i documenti in ingresso che per quelli in uscita.

11.8.11 Documenti non firmati

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

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

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

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

11.8.12 Protocollazione dei messaggi di posta elettronica convenzionale

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

- caso di invio, come allegato, di un documento scansionato munito di firma autografa: fermo restando che il RPA deve verificare la provenienza certa dal documento, in caso di mittente non verificabile, il RPA valuta, caso per caso, l'opportunità di trattare il documento inviato via *e-mail;*
- caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale: il documento e/o il messaggio sono considerati come un documento elettronico inviato con qualunque mezzo di posta;
- caso di invio di una *e-mail* contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

11.8.13 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.

11.8.14 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".

11.8.15 Copie per "conoscenza"

Nel caso di copie “per conoscenza” si deve utilizzare la procedura descritta nel paragrafo 11.8.2. 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".

11.8.16 Differimento delle registrazioni

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

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

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

11.8.17.Corrispondenza personale o riservata

La corrispondenza personale non viene aperta ma consegnata al destinatario, il quale, dopo averne preso visione, qualora reputi che i documenti ricevuti debbano essere comunque protocollati perché riguardanti affari d'ufficio, provvede a trasmetterli alla UOP per la protocollazione.

11.8.18.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 sul protocollo generale e, a cura del RPA, sono inseriti nel relativo fascicolo.

11.9 Gestione delle registrazioni di protocollo con il SdP

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

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

11.10 Registrazioni di protocollo

11.10.1. Attribuzione del protocollo

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

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

Come previsto dalla normativa vigente in materia di protezione dei dati personali, le AOO aderenti al SdP sono informate della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo.

11.10.2 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. Tali modalità sono riportate nel manuale di conservazione dell'AgID.

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

Al termine delle operazioni giornaliere, o comunque entro il successivo giorno lavorativo, all'interno del centro servizi dell'erogatore del SdP sono effettuate le seguenti operazioni di garanzia:

- *export* delle tabelle contenenti i dati dei registri di protocollo delle AOO e loro acquisizione dai sistemi di esercizio sulla stazione di gestione dell'area sicurezza;
- cifratura dei file per i quali è prevista questa operazione;
- apposizione della firma digitale sui file da archiviare.

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

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

12.1 . Descrizione funzionale ed operativa

La descrizione completa delle funzionalità dell'applicativo di protocollo è disponibile e consultabile insieme ai manuali operativi nella intranet dell'Agenzia.

13 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

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

13.1 Il registro di emergenza

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

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

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

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

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

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

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

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

II SdP realizza il registro di emergenza con un applicativo specifico installato sulle postazioni di lavoro delle UOP in modalità *stand alone*, fuori linea.

13.2 Modalità di apertura del registro di emergenza

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

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

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

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

L'elenco delle UOP abilitate alla registrazione dei documenti sui registri di emergenza è riportato nell'allegato 3.

Le modalità operative di impiego dell'applicativo del registro di emergenza sopra richiamato sono dettagliatamente riportate nel documento "Modalità organizzative per la fruizione del registro di emergenza per gli utenti del servizio di protocollo in modalità ASP".

Servizio di gestione informatica del protocollo, dei documenti e degli archivi
Scheda di apertura/chiusura del registro di emergenza
AgID- Agenzia per l'Italia Digitale -
Area Organizzativa Omogenea ADG
Unità Organizzativa di registrazione di Protocollo

Causa dell'interruzione:

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

Ora dell'evento hh /mm Annotazioni:

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

Pagina n._____
Firma del responsabile del servizio di protocollo

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

13.3 Modalità di utilizzo del registro di emergenza

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

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

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

Durante il periodo di interruzione del SdP, il responsabile della gestione del Centro servizio (o persona da lui delegata) informa costantemente il "call center" sui tempi di ripristino del servizio in parola affinché possa fornire le informazioni aggiornate alle AOO che ne fanno richiesta.

13.4 Modalità di chiusura e di recupero del registro di emergenza

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

E' compito del RSP, o di un suo delegato, riportare dal registro di emergenza al registro di protocollo generale del SdP le protocollazioni relative ai documenti protocollati in emergenza attraverso le postazioni di lavoro abilitate, 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.

Le modalità operative di recupero dei dati acquisiti in emergenza con l'applicativo in parola, sono dettagliatamente riportate nell'omonimo documento "Modalità organizzative per la fruizione del registro di emergenza per gli utenti del servizio di protocollo in modalità ASP".

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

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

14 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI

14.1 Modalità di approvazione e aggiornamento del manuale

L'amministrazione adotta il presente "Manuale di gestione" su proposta del Coordinatore della Gestione Documentale, sentito il Responsabile del servizio di protocollo informatico.

Il presente manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;

- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.

14.2 Regolamenti abrogati

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

14.3 Pubblicità del presente Manuale

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

Copia del presente manuale è:

- fornita a tutto il personale dell'AOO e resa disponibile nella intranet dell'Agenzia;
- inviata all'organo di revisione;
- pubblicato sul sito istituzionale dell'amministrazione.

14.4 Operatività del presente manuale

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