REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ATSSardegna
Azienda Tutela Salute

Azienda per la tutela della salute

Partita Iva 00935650903

# Manuale di Gestione del Protocollo Informatico, dei Documenti e dell'Archivio

**Autori**

| *Autori del documento* | *Struttura di appartenenza* | *Parte del documento* | *Note* |
|---|---|---|---|
| Mario Cubadda | AOU Cagliari | tutte | Redazione |
| Marisa Udella | ASL8 | tutte | Redazione |
| Roberta Manutza | AO Brotzu | tutte | Redazione |
| Donatella Gallistru | SardegnaIT | tutte | Redazione |
| Danilo Anolfo | SardegnaIT | tutte | Redazione |

**Storia delle modifiche**

| *Vers.Rev.* | *Data* | *Autore* | *Descrizione modifiche* |
|---|---|---|---|
| 00.01 | 30.09.2016 | Daniele Farci (SardegnaIT) | Revisione |
| 00.01 | 02.11.2016 | Antonio Roscigno (ENG) | Revisione |
| 00.01 | 14.04.2017 | Danilo Anolfo (SardegnaIT) | Validazione Revisioni ambito regionale |
| 00.01 | 17.05.2017 | Cesare Delussu | Commenti per revisione ats |
| 00.01 | 19.05.2017 | Iolanda Spano | Commenti per revisione ats |
| 00.01 | 22.05.2017 | Danilo Anolfo (SardegnaIT) | Modifiche per revisione ats |
| 00.01 | 09.11.2017 | Giuseppe Pintor | Modifiche per revisione ats |
| 00.01 | 09.11.2017 | Luca Pisano | Modifiche per revisione ats |
| 00.01 | 09.11.2017 | Cesare Delussu | Modifiche per revisione ats |
| 00.01 | 11.12.2017 | Giuseppe Prevosto | Revisione normative di legge |
| 00.01 | 20.12.2017 | Danilo Anolfo (SardegnaIT) | Validazione Revisioni |
| 00.01 | 29.06.2018 | Luca Pisano<br>Vincenza Costeri | Revisione su nuovo assetto organizzativo ATS |
| 00.01 | 02.07.2018 | Luca Pisano<br>Vincenza Costeri<br>Giuseppe Pintor | Validazione revisioni |

**Sommario**.....Errore. Il segnalibro non è definito.

# 1 INTRODUZIONE

## 1.1 PREMESSA

II decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico", articolo 3, comma 1, lettera d), prevede l'adozione del manuale di gestione per tutte le amministrazioni di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale. Il Manuale, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi".

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000 (già art.12 del citato DsPR n. 428 del 20 ottobre 1998).

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 agli addetti al servizio e ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

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

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti. Il presente documento pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

Esso disciplina:

- la migrazione dei flussi cartacei verso quelli digitali, ovvero in via transitoria, i flussi cartacei in rapporto al protocollo informatico;
- i livelli di esecuzione, le responsabilità ed i metodi di controllo dei processi e delle azioni amministrative l'uso del titolario di classificazione e del massimario di selezione e di scarto;
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo ed interesse, in attuazione del principio di trasparenza dell'azione amministrativa.

## 1.2 AMBITO DI APPLICAZIONE DEL MANUALE E ACRONIMI UTILIZZATI

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 del 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico".

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione

ai procedimenti amministrativi dell'Azienda per la Tutela della Salute (ATS Sardegna) individuata ai sensi del presente manuale quale AOO (Area Organizzativa Omogenea).

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

Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno dell'amministrazione anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa.

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

La Legge Regionale 27 luglio 2016, n. 17 modificando l'assetto istituzionale del Servizio sanitario regionale della Sardegna, ha istituito l'Azienda per la Tutela della Salute (ATS) nata dalla fusione per incorporazione delle sette ASL nell'azienda incorporante di Sassari. Nell'ambito di tale processo la ATS ha ereditato il sistema informativo per la gestione del Protocollo denominato E-Grammata (SISAR-Protocollo informatico), sviluppato nell'ambito del progetto regionale per la realizzazione di un Sistema Informativo Sanitario Integrato Regionale (SISAR) ed in uso nelle ASL oggetto del processo di incorporazione nella ATS. Il sistema informativo E-Grammata (SISAR Protocollo) rappresenta il PdP - Prodotto di Protocollo informatico descritto nel presente manuale.

Al fine di una corretta lettura del presente Manuale si riportano, di seguito, gli acronimi utilizzati più frequentemente:

- ACL - Access Control List
- AOO - Area Organizzativa Omogenea;
- CED - Centro Elaborazione Dati
- IPA - Indice delle pubbliche amministrazioni
- MdG - Manuale di Gestione del protocollo informatico e gestione documentale e degli archivi;
- PEC – Posta Elettronica Certificata
- 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
- PdP - Prodotto di Protocollo informatico – l'applicativo acquisito dall'amministrazione per implementare il servizio di protocollo informatico;
- UOP - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- UOR = Unità Organizzative Responsabili: un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi

e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinate;

- UO - Unità Operativa - un insieme di uffici che, per tipologia di mandato istituzionale e di 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 sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

## 1.3 DEFINIZIONI E NORME DI RIFERIMENTO

Vedi allegato 3

## 1.4 MODELLO ORGANIZZATIVO

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

All'interno dell'AOO il sistema di protocollazione è unico, articolato in UO (Unità Operative) che la compongono con la loro articolazione in UU (Ufficio Utente), come da allegato 1.

L'allegato con la descrizione delle strutture di protocollazione e relativi sottolivelli (articolazione UO e UU) è suscettibile di modifica in caso di inserimento di nuove strutture o di riorganizzazione delle medesime. Le modifiche sono proposte ai vertici dell'amministrazione dal *Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi* (RSP). L'amministrazione si riserva la facoltà di autorizzare, in via transitoria e del tutto eccezionale, altre UUOO allo svolgimento dell'attività di protocollazione.

Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del RSP. Nelle UO sarà utilizzato il medesimo sistema di numerazione di protocollo e l'operatore incaricato dell'attività di protocollazione dovrà essere previamente abilitato, su richiesta del Responsabile della struttura di assegnazione, secondo le modalità previste dal presente documento.

## 1.5 GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI: FIGURE COINVOLTE NELLA GESTIONE DEL "SERVIZIO PROTOCOLLO"

Nella AOO precedentemente individuata è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Alla guida del suddetto servizio è posto il Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito R.S.P.). Le altre figure/Servizi che concorrono alla corretta Gestione del Sistema Protocollo sono il Servizio Sistemi Informativi Amministrativi (SIA), e il Data Privacy Officer (DPO), ognuno dei quali interviene nella gestione del Servizio Protocollo nelle materie/attività di propria competenza così come dettagliate nel presente manuale.

**Responsabile del Servizio di Protocollo informatico (RSP)**

Egli è funzionalmente nominato con atto deliberativo del Direttore Generale.

Al servizio è preposto un dirigente ovvero un funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.

Sono compiti propri, non delegabili, del Responsabile del Servizio di Protocollo informatico:

- 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 INTERNET e INTRANET dell'amministrazione;
- impartire disposizioni e direttive sul rispetto della normativa vigente durante le operazioni di registrazione e di segnatura di protocollo;
- verificare il rispetto delle normative vigenti da parte dei dirigenti delle UU.OO.;
- segnalare alla Direzione Generale di eventuali omissioni nella gestione del protocollo;
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico;
- attività inerenti la sicurezza di cui al punto 3.2.1

Sono compiti propri, eventualmente delegabili, del Responsabile del Servizio di Protocollo informatico:

- collaborare con i Servizi Informativi Aziendali per la redazione del piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;
- esprimersi in merito alle segnalazioni trasmesse dal SIA su richieste di abilitazione presentate da Responsabili di Struttura che paiano in contrasto con le disposizioni organizzative vigenti;
- ammissione di uno o più documenti alla registrazione differita di cui al punto 11.3.3
- autorizzare le operazioni di annullamento della registrazione di protocollo di cui al punto 11.3.4;
- autorizzare la registrazioni nel protocollo riservato nelle situazioni in cui non ne emerga in maniera palese la necessità (punto 11.4)
- aprire e chiudere il registro di protocollazione di emergenza;
- segnalare ai Sistemi Informativi Aziendali, eventuali malfunzionamenti degli strumenti;

- tutte le altre attività ad esso riconosciute e previste dal presente manuale.

**Servizio Sistemi Informativi Amministrativi (SIA)**

Sono compiti propri del Servizio Sistemi Informativi Amministrativi (SIA)

- abilitare gli addetti dell'amministrazione all'utilizzo del PdP (Prodotto di Protocollo Informatico) e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, modifica ecc.) secondo quanto richiesto dal Responsabile della struttura di assegnazione;
- attività inerenti la sicurezza di cui al punto 3.2.2
- sottoporre al RSP (o suo delegato) la valutazione in merito a richieste di abilitazione presentate da Responsabili di Struttura che paiano in contrasto con le disposizioni organizzative vigenti;
- referente IPA (indice delle pubbliche amministrazioni) per l'ATS;
- redazione e aggiornamento, di concerto con DPO, della procedura per la composizione delle password e il blocco delle utenze
- definizione e aggiornamento procedura per riutilizzo e dismissione dei supporti rimovibili
- monitora la regolare produzione del registro giornaliero di protocollo e il conseguente invio al Sistema di Conservazione Sostitutiva, secondo quanto disposto dalle normative vigenti;

**Data Privacy Officer (DPO)**

Sono compiti propri del Data Privacy Officer (DPO)

- Il DPO di concerto con il Responsabile del servizio protocollo individua i documenti che, in ragione della necessità di protezione dei dati/informazioni ivi contenuti, sono sottratti alla procedura di scansione ovvero soggetti a registrazione particolare di cui al successivo punto 10.2.

## 1.6 FIRMA DIGITALE

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'amministrazione fornisce idoneo strumento per la firma digitale ai soggetti da essa delegati a rappresentarla.

## 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 pertinenza dà attuazione alla vigente normativa in materia di trattamento dei dati con atti formali aventi rilevanza interna ed esterna.

Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, devono essere incaricati dal titolare dei dati e, se nominato, dal responsabile.

Relativamente agli adempimenti esterni, l'amministrazione si è organizzata per garantire che i certificati ed i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente.

In relazione alla protezione dei dati personali trattati al proprio interno l'amministrazione ottempera a quanto previsto dalla vigente normativa in materia di trattamento dei dati, con particolare riferimento:

- al principio di necessità nel trattamento dei dati;
- al diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.

## 1.8 CASELLE DI POSTA ELETTRONICA

Ai fini del presente manuale si intende per:

- casella di posta elettronica istituzionale PEC: casella di posta elettronica certificata (PEC) avente dominio @pec.atssardegna.it.
- casella di posta elettronica istituzionale tradizionale: casella di posta elettronica "non PEC" avente dominio @atssardegna.it

L'AOO e le UO identificate sono dotate di casella di Posta Elettronica Certificata per la corrispondenza, sia in ingresso che in uscita, che costituisce l'indirizzo virtuale di riferimento per la corrispondenza di competenza della Struttura da e verso l'esterno. Ad ogni casella di Posta Elettronica Certifica, integrata nel Sistema di Protocollo mediante l'interoperabilità, corrisponde un punto di protocollazione.

Gli indirizzi PEC sono pubblicati sull'Indice delle Pubbliche Amministrazioni (IPA) a cura dei Sistemi Informativi Amministrativi.

Le UO sono inoltre dotate di una casella di posta elettronica istituzionale tradizionale, attraverso la quale veicolare la corrispondenza interna di preminente carattere informativo non sottoposta a protocollazione, secondo l'esemplificazione di cui al successivo paragrafo 4.5.

La casella di posta elettronica è inoltre utilizzata dai singoli operatori per trasmettere i documenti digitali alla postazione di protocollazione di prossimità, al fine della successiva trasmissione verso altra UO ovvero verso l'esterno.

In attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione dota tutti i propri dipendenti, compresi quelli per i quali non sia prevista la dotazione di un personal computer, di una casella di posta elettronica istituzionale.

Non è ammesso l'utilizzo da parte dei dipendenti, per fini connessi all'attività e ai procedimenti lavorativi, utilizzo di caselle di posta elettronica, tradizionali o certificata, diverse da quelle istituzionali.

Eventuali caselle di posta elettronica certificata (PEC) aventi dominio nome.cognome@pec.atssardegna.it rilasciate per soddisfare adempimenti e/o necessità procedimentali specifiche previste dalla normativa vigente sono escluse dall'integrazione con il Sistema di Protocollo mediante l'interoperabilità e non rappresentano pertanto un punto virtuale di protocollazione. Qualora necessario acquisire al Protocollo eventuale documentazione trasmessa/ricevuta a mezzo di tali strumenti, la stessa dovrà essere gestita secondo le regole definite nel presente manuale (punto 5.2.5).

## 1.9 SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI

Per l'attività operativa del protocollo informatico viene adottato un unico titolario (vedi allegato 2) di classificazione per l'archivio centrale unico (logico) dell'amministrazione valido per tutte le AOO in cui è articolata l'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, permettendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.

In via transitoria, avendo l'AOO (ATS) ereditato il titolario predisposto ed in uso al momento del passaggio dalle ex-ASL all'attuale ATS, rimane vigente il titolario in uso (allegato 2) fino alla adozione del nuovo titolario predisposto e strutturato sul nuovo assetto organizzativo della AOO in via di definizione.

Al fine di agevolare e normalizzare, da un lato la classificazione archivistica e dall'altro l'assegnazione per competenza, sul PdP è stato predisposto un elenco degli Uffici Utente e dei dipendenti unitamente a quello di classificazione come riportato nell'allegato 1. L'elenco oltre ad essere una guida rapida di riferimento, permette l'immediata e univoca individuazione della classificazione e delle competenze.

## 1.10 FORMAZIONE

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

## 1.11 ACCREDITAMENTO DELL' AOO ALL' IPA

L’AOO e le UU.OO. individuate, come accennato, sono dotate di caselle di posta elettronica certificata attraverso cui trasmettono e ricevono documenti informatici soggetti alla registrazione di protocollo. La responsabilità della registrazione della corrispondenza è affidata al responsabile della UO incaricata; quest'ultima procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta. L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'indice delle pubbliche amministrazioni (IPA), tenuto e reso pubblico dalla medesima fornendo le informazioni che individuano l'amministrazione e l'articolazione delle sue AOO.

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

## 2 ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

In coerenza con quanto previsto e disciplinato dall'art. 3 comma 1 lettera e del DPCM 03/12/2013, tutti i documenti inviati e ricevuti dall'amministrazione sono registrati all'interno del registro di protocollo informatico. Pertanto tutti i registri particolari di protocollo sono aboliti ed eliminati. Il piano di attuazione del protocollo informatico prevede l'eliminazione dei diversi protocolli di settore, di reparto e multipli. A tal fine sono state e/o saranno svolte le seguenti attività:

- censimento preliminare dei diversi protocolli esistenti;
- analisi dei livelli di automazione;
- definizione degli interventi organizzativi, procedurali e tecnici da effettuare per adottare il protocollo informatico;
- valutazione dei tempi di sostituzione;
- stima dei costi derivanti.

Il RSP esegue periodicamente dei controlli a campione sulla corretta esecuzione del piano e sull'utilizzo regolare di un unico registro di protocollo, verificando, attraverso controlli ed ispezioni mirate nelle varie UO, la validità dei criteri di classificazione utilizzati.

# 3 PIANO DI SICUREZZA

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

## 3.1 OBIETTIVI

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'amministrazione/AOO/UO siano resi disponibili, integri e riservati;
- 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 ATTIVITÀ

3.2.1 Considerata la complessità e la pluralità di competenze necessarie in funzione della organizzazione propria della AOO nonché delle misure e delle politiche di sicurezza, necessarie per stabilire adeguati livelli di sicurezza proporzionati al 'valore' dei dati/documenti trattati, le funzioni/responsabilità inerenti la sicurezza del SdP, sono assicurate attraverso l'azione coordinata, diretta e responsabile delle diverse figure (punto 1.5) coinvolte nella gestione del "servizio protocollo".

In particolare RSP-DPO-SIA concorrono congiuntamente ad elaborare e definire:

- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui alla normativa vigente, in caso di trattamento di dati personali;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza a livello di accessi.
- i piani specifici di formazione degli addetti;
- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le misure tecniche e organizzative necessarie per assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

3.2.2 Al Servizio Informativo Aziendale (nei casi in cui ricorre), è demandata la componente 'locale' della sicurezza e le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza interna della rete informatica

Compete altresì al SIA:

- l’assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- eventuali reset delle password durante la fase di esercizio;
- creazione e chiusura scrivanie e utenze di Protocollo;
- attivazione delle postazioni per la gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate per l’uso del protocollo di emergenza;
- verifica che l'accesso sia consentito soltanto al personale autorizzato per motivi di servizio;
- stabilire e controllare la selettività degli accessi a livello di protezione locale.

3.2.3 Il piano di sicurezza, si basa sui risultati dell’analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e deve tenere conto ed integrarsi a tutte le disposizioni in materia previste dal DPO.

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

3.2.4 Al fornitore del servizio sono demandate le seguenti attività:

- archiviazione giornaliera su nastro, dei backup del database e file system, con conservazione dei nastri come da specifiche di progetto (30 giorni solari)
- archiviazione giornaliera, in formato .pdf, delle copie del registro di protocollo;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie dei dati su nastro e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei “moduli” (patch e service pack) correttivi dei sistemi operativi lato server.

Il controllo degli accessi fisici ai locali protetti è regolato secondo i seguenti principi:

- 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 è regolato secondo i principi stabiliti dall'Area "Funzionamento" Sezione Logistica e sicurezza.

La componente logica della sicurezza 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:

- riservatezza dei dati;
- integrità dei dati;
- integrità del flusso dei messaggi;
- 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.

Presso il centro servizi del fornitore sono disponibili i seguenti impianti:

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

Il centro servizi è 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 aziendale. In particolare:

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

L'accesso dall'esterno da parte di persone non autorizzate non è consentito in base

all'architettura stessa del servizio, essendo controllato dal fornitore.

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:

- dalle registrazioni dell'applicativo Protocollo.

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 sono elaborate tramite procedure automatiche dal sistema di autenticazione e di autorizzazione;
- i log di sistema sono accessibili esclusivamente ai sistemisti autorizzati l'operazione di scrittura delle registrazioni del Protocollo è effettuata direttamente dagli applicativi;
- le registrazioni sono soggette a copia giornaliera su disco e a salvataggio su nastro;
- il periodo di conservazione del nastro è conforme alle specifiche di progetto.

## 3.3 FORMAZIONE DEI DOCUMENTI - ASPETTI ATTINENTI ALLA SICUREZZA

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

- l'identificabilità del soggetto che ha formato il documento;
- 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. 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.

I documenti informatici redatti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (preferibilmente PDF), 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.

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

Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 (**"**Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23- ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005").

## 3.4 GESTIONE DEI DOCUMENTI INFORMATICI

II sistema 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 f
- i 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 nel l'ambito del sistema di classificazione d'archivio adottato.

## 3.5 TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sul l'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 dalla normativa vigente.

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.

## 3.6 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.

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

## 3.7 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 già indicate.

Gli uffici organizzativi di riferimento (UO) dell'AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica istituzionali o registrazioni con repertorio NP, 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.

## 3.8 ACCESSO AI DOCUMENTI INFORMATICI

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

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale. Queste, in sintesi, sono definite nell'Allegato 5: "Elenco tipologia profilazione".

Le regole per la composizione delle password e il blocco delle utenze valgono sia per gli amministratori dell'AOO che per gli utenti e sono disciplinate da opportuna procedura redatta e aggiornata dai sistemi informativi aziendali.

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 UO, 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 nel l'archivio o di una ricerca cosiddetta "full text".

## 3.9 UTENTI INTERNI ALLA AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal SIA previa formale richiesta del Responsabile della struttura di assegnazione. Nel caso in cui la richiesta evidenzi la presenza di elementi di profilazione in contrasto con le disposizioni organizzative vigenti il SIA potrà sottoporre la valutazione preventiva alla profilazione al RSP o suo delegato.

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

La gestione delle utenze rispetta i seguenti principi operativi:

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

## 3.10 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.

L'utente assegnatario dei documenti protocollati è invece abilitato ad una vista parziale sul registro di protocollo. Tale vista 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 un protocollo ed assegnarlo per competenza ad un utente assegnatario.

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

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).

## 3.11 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 del l'UU di appartenenza del RPA.

## 3.12 UTENTI ESTERNI ALLA AOO - PRIVATI

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

## 3.13 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La conservazione dei documenti informatici deve avvenire sulla base delle disposizioni riportate nel DPCM 13 novembre 2014, per quanto attiene ai documenti informatici presenti nell'archivio corrente del Fornitore e dal DPCM 3 dicembre 2013 per i documenti inviati in conservazione.

## 3.14 SERVIZIO ARCHIVISTICO

Il responsabile del sistema archivistico dell'intera amministrazione, definisce le regole per la corretta archiviazione e allocazione della documentazione dell'amministrazione in base ai 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, il responsabile del servizio ha, in corso di perfezionamento, un piano specifico individuando, i soggetti incaricati di ciascuna fase.

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

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

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

Per quanto riguarda le procedure operative si rimanda ai regolamenti e alle disposizioni interne in materia.

## 3.15 CONSERVAZIONE DEL REGISTRO GIORNALIERO DI PROTOCOLLO

Il registro giornaliero di protocollo viene prodotto giornalmente da una procedura informatica. Tale automatismo produce la stampa in formato pdf del registro di protocollo ed eventuali repertori, e registra la stessa con apposito repertorio con sigla RGP il cui accesso è riservato solo agli amministratori di sistema e/o loro delegati. In tale stampa vengono riportate anche le impronte digitali di eventuali file allegati alle registrazioni. Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Al riguardo di seguito si descrivono le modalità di produzione di invio in conservazione delle registrazioni di protocollo informatico con l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire l'immodificabilità della registrazione medesime.

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

Per quanto attiene ai 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 al giorno successivo in modo che nessun altro documento possa essere protocollato nel registro della giornata precedente né in modalità manuale né in modalità automatica.

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

1. Ottenere i 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. In caso di anomalia durante il flusso inviare una notifica al responsabile della conservazione.

Il trasferimento del Pacchetto di versamento al sistema di conservazione avviene tramite canale 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 sia avvenuto 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. In caso di esito positivo indicare nel documento lo stato "conservato".

5. In caso di esito negativo indicare nel documento lo stato "errore" ed inviare una notifica al Sistema di conservazione e al Conservatore.

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'AOO a tutela della immodificabilità del medesimo ai sensi dell'art.3, comma 4, lettera d), del D PCM 13 novembre 2014.

### 3.16 CONSERVAZIONE DELLE REGISTRAZIONI DI SICUREZZA

Un operatore di sicurezza dell'erogatore, provvede quotidianamente alla memorizzazione su nastri magnetici dei seguenti oggetti:

● i file contenenti i log applicativi e del server;

● le registrazioni di protocollo e file allegati alle stesse.

I supporti sono archiviati all'interno della Tape Library sita in un'area di sicurezza riservata all'interno del centro servizi. Le modalità di archiviazione sono regolamentate da procedure specifiche.

### 3.17 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 definita dal SIA.

### 3.18 POLITICHE DI SICUREZZA ADOTTATE DALLA AOO

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

È compito del responsabile della sicurezza e del responsabile della tutela dei dati personali-DPO 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'Amministrazione al RTI, o a seguito dei risultati delle attività di *audit.*

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

# 4 DOCUMENTO

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

## 4.1 DOCUMENTO AMMINISTRATIVO

Per documento amministrativo si intende ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale (art. 22 L. n. 241/1990, art. 1 DPR n. 445/2000).

All'interno del AOO, ciascun **documento amministrativo** risulta caratterizzato dai seguenti fattori:

- **supporto** (cartaceo, informatico ecc.).
- **natura/destinazione** (in ingresso, in uscita, interno informale, interno formale)
- **uso/ambito** (interno/esterno)

## 4.2 DOCUMENTO INFORMATICO

In coerenza a quanto previsto nell' art. 22 L. n. 241/1990 si intende per documento informatico la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Secondo quanto disposto negli artt. 22 e 57 del predetto D.Lgs. 82/2005, il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti informatici, sono da ritenersi validi e rilevanti a tutti gli effetti di legge, purché coerenti alle disposizioni normative contenute del DPR stesso.

Inoltre secondo quanto disposto dal c.1 dell'art.9 del citato DPR, gli atti formati con strumenti informatici, i dati ed i documenti informatici delle pubbliche amministrazioni, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

Il documento informatico prodotto dalle pubbliche amministrazioni, laddove redatto anche in conformità alle regole tecniche, soddisfa il requisito legale della forma scritta ed ha, quindi, efficacia probatoria ai sensi dell'art. 2712 del Codice Civile.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "1. Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.

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.

## 4.3 DOCUMENTO IN INGRESSO

Si intende per documento in ingresso un documento pervenuto o acquisito dall'AOO nell'esercizio delle proprie funzioni e, quindi, sottoposto all'operazione di registrazione presso uno dei punti di protocollazione in entrata. Al termine dell'operazione di registrazione e di classificazione del documento, i documenti in arrivo nell'AOO sono assegnati al destinatario

desunto dal documento stesso o, in alternativa, alla UO di competenza che, nella persona del Responsabile o suo incaricato, ne individua il destinatario; questi provvederà, quindi alle operazioni di fascicolazione del documento, intese come corretto inserimento all'interno del fascicolo relativo al procedimento di afferenza del documento.

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, 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 al servizio di protocollo e/o alle UO aperte al pubblico.

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

Per quanto riguarda le procedure operative si rimanda ai regolamenti e alle disposizioni interne in materia.

### 4.4 DOCUMENTO IN USCITA

Si intende per documento in uscita un documento predisposto all'interno dell'AOO e trasmessi ad altre amministrazioni o a privati.

Le operazioni di protocollazione con contestuale classificazione dei documenti in uscita e attribuzione ad un fascicolo relativo allo specifico procedimento di afferenza, sono effettuate all'interno dell'area di riferimento da parte dello scrivente, nel caso sia un soggetto a ciò abilitato presso il sistema di protocollo informatico della AOO.

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma, per mezzo della sola posta elettronica certificata se la dimensione del documento e/o di eventuali allegati, non supera la dimensione massima prevista dal sistema di posta utilizzato dal l'AOO, che viene fissata in 100 MB, e con un limite massimo di 500 destinatari.

In caso contrario, il documento informatico viene copiato, su supporto digitale rimovibile non modificabile e trasmesso al destinatario con altri mezzi di trasporto o a mezzo posta su supporto cartaceo secondo il principio della maggiore economicità.

Per quanto riguarda le procedure operative si rimanda ai regolamenti e alle disposizioni interne in materia.

## 4.5 DOCUMENTO INTERNO

Si intende per documento interno un documento generato/prodotto all'interno di una UO e trasmesso ad altra UO comunque afferente all'AOO.

I documenti interni si distinguono in:

a) documenti di preminente carattere informativo;

b) documenti di preminente carattere giuridico-probatorio.

Si intendono per documenti interni di preminente carattere informativo le memorie informali, gli appunti, le brevi comunicazioni di rilevanza meramente informativa scambiati tra le UO.

Tali tipologie di documenti non sono sottoposti, di norma, a protocollazione.

Si intendono invece per documenti interni di preminente carattere giuridico-probatorio i documenti prodotti al fine di documentare atti o provvedimenti amministrativi dai quali emergano diritti, doveri o legittime aspettative di terzi. Proprio in virtù di dette finalità tali tipologie documentali sono sempre sottoposte a registrazione su un repertorio separato dal protocollo generale (repertorio NP). Analogamente a quanto già espresso con riferimento ai documenti in uscita, le operazioni di protocollazione con contestuale classificazione dei documenti interni e attribuzione ad un fascicolo relativo allo specifico procedimento di afferenza, sono effettuate all'interno dell'UO da parte dello scrivente, nel caso sia un soggetto a ciò abilitato presso il sistema di protocollo informatico.

Tali documenti, compresi di eventuali allegati, dovranno essere visualizzati attraverso la lista lavoro documenti della UO destinataria o per mezzo della sola posta elettronica con l'utilizzo della casella di posta aziendale.

In base alle normative vigenti NON è consentito stampare su carta le note NP/PG per invii o consegne destinate a uffici interni alla AOO ovvero ad altre Pubbliche Amministrazioni o Imprese.

## 4.6 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 nelle apposite linee guida.

## 4.7 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 al l'interno:

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

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

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

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

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

Nel documento trasmesso dovranno altresì essere riportate/allegate, secondo le possibilità consentite dall'SdP, le seguenti informazioni:

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

## 4.8 IL DOCUMENTO DIGITALE

### 4.8.1 FIRMA DIGITALE

La firma digitale è uno strumento utilizzato per sottoscrivere documenti da inviare/archiviare 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 secondo le modalità descritte al successivo paragrafo.

### 4.8.2 VERIFICA DELLE FIRME DIGITALI

Nel Sistema di protocollo 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 sistema di protocollo
- 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 *Certification Authority* accreditate presso l'AOO;
- trasformazione del documento in uno dei formati standard previsto dalla normativa vigente in materia DPCM del 13 novembre 2014 e attribuzione della segnatura di protocollo;
- inserimento nel sistema documentale del Sistema di Protocollo 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 Sistema di Protocollo per accelerare successive attività di verifica di altri documenti ricevuti.

Per quanto riguarda le procedure operative si rimanda ai regolamenti e alle disposizioni interne in materia.

### 4.8.3 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/UO, nel caso di documenti interni formali;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

### 4.8.4 USO DELLA POSTA ELETTRONICA CERTIFICATA

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

Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo. Allo scopo di effettuare la trasmissione di un documento utilizzando l'interoperabilità dei sistemi di protocollo è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno: denominazione, indirizzo, casella di posta elettronica);
- firmare il documento (ed eventualmente associare il riferimento temporale al documento firmato);
- assegnare il numero di protocollo in uscita al documento firmato (digitalmente o olograficamente);
- trasmettere il documento firmato e protocollato in uscita alla casella di posta istituzionale del destinatario di regola attraverso la procedura di interoperabilità del sistema di protocollo.

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

- 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:

- Accettazione del sistema
- Avvenuta consegna;
- 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. e alle UO.

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

Per quanto riguarda le procedure operative si rimanda ai regolamenti e alle disposizioni interne in materia.

# 5 FLUSSO DEI DOCUMENTI RICEVUTI

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. Il servizio di protocollo non effettua fotocopie della corrispondenza trattata, sia in ingresso che in uscita salvo specifici casi previsti da norme vigenti.

## 5.1 GENERALITÀ

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

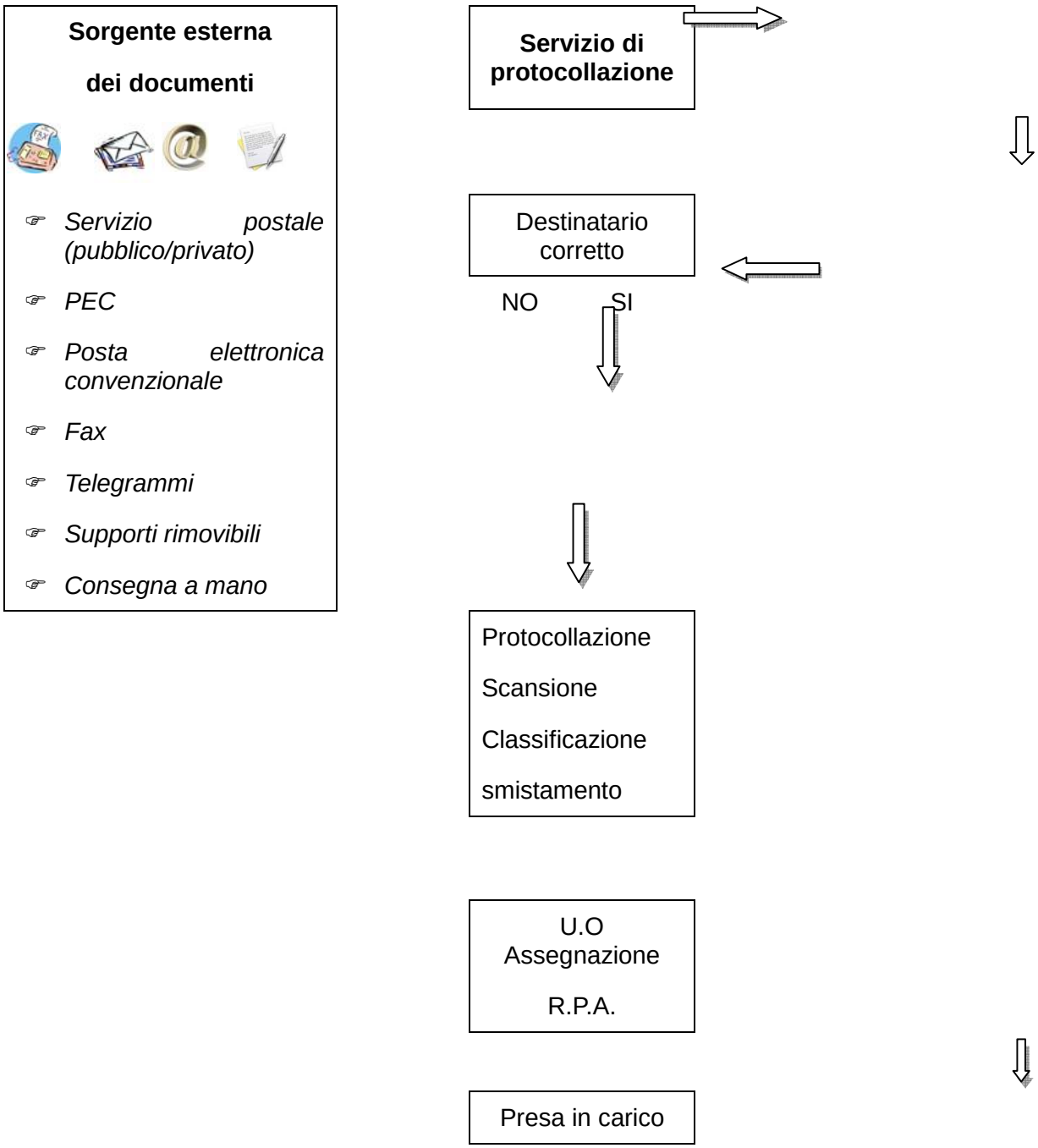
Tali flussi sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico probatoria. Essi si riferiscono ai documenti:

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

I flussi gestiti all'interno del sistema archivistico dell'amministrazione/AOO dalla sezione di deposito e storica dell'archivio sono sviluppati, per omogeneità e completezza di trattazione, nel successivo capitolo 10.

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

## 5.2 FLUSSO DEI DOCUMENTI IN INGRESSO




### 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 UO designata.

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

### 5.2.2 Ricezione Documenti Informatici sulla Casella di Posta Elettronica Istituzionale (PEC)

Per casella di posta elettronica istituzionale si intende una casella di posta elettronica certificata (PEC) avente dominio @pec.atssardegna.it.

Di norma la ricezione dei documenti informatici è assicurata tramite le caselle di posta elettronica certificate istituzionali che sono accessibile solo alle U.O. in cui si è organizzata l'AOO.

Quando i documenti informatici pervengono alle UO, le stesse unità, previa verifica della validità della firma apposta e della leggibilità del documento procedono alla registrazione di protocollo.

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 del SDP controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale PEC e verifica se sono da protocollare.

### 5.2.3 Ricezione Documenti Informatici sulla Casella di Posta elettronica istituzionale tradizionale (non PEC)

Per casella di posta elettronica istituzionale tradizionale si intende una casella di posta elettronica "non PEC" avente dominio @atssardegna.it

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 ricevente dovrà inviare al mittente un messaggio con l'indicazione della casella di posta corretta. Il messaggio comunque ricevuto previa verifica dei presupposti richiesti viene stampato e gestito secondo le procedure previste per il documento cartaceo di cui al punto 5.2.5.

Il ricevente, se appartenente ad una UO in cui non è attivo il SdP dovrà rivolgersi al punto di protocollazione ad esso più prossimo che procederà alle verifiche sul documento e alla conseguente protocollazione.

### 5.2.4 Ricezione di Documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica. Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile 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 gli adempimenti del caso.

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

### 5.2.5 Ricezione di Documenti Cartacei a mezzo posta convenzionale o con consegna a mano presso punto fisico di protocollazione

I documenti consegnati a mano presso un punto "fisico" di protocollazione vengono da questo direttamente gestiti.

I documenti pervenuti a mezzo posta o ritirati dagli uffici postali sono consegnati al servizio protocollo (UOP) di prossimità/riferimento (ATS/ASSL/Dipartimento/SC/SSD/SS).

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

La corrispondenza relativa a bandi di gara e concorsi è registrata e successivamente consegnata chiusa all'ufficio responsabile della gara/concorso, qualora la corrispondenza sia recapitata a mano dovrà essere ritirata dal servizio competente presso il quale è istituita apposita UOP.

La corrispondenza personale non deve essere ritirata in assenza di delega da parte del destinatario e in ogni caso non deve essere aperta, né protocollata ma deve essere consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, provvederà a inoltrarla all'ufficio protocollo (UOP) di prossimità/riferimento per la registrazione. 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 arrivo è aperta il giorno lavorativo in cui è pervenuta e, di norma, contestualmente protocollata. La busta si allega al documento per la parte relativa ai timbri postali.

### 5.2.6 Documenti cartacei ricevuti a mezzo posta convenzionale e tutela dei dati personali

Qualora una AOO sia organizzata per ricevere documenti su carta attraverso qualsiasi UO aperta al pubblico, oltre, ovviamente alle unità di protocollo istituzionali, ovvero se per errore la corrispondenza viene recapitata ad un UO quest'ultima, a tutela dei dati personali eventualmente contenuti nella missiva, non apre le buste o i contenitori ricevuti ma rilascia ricevuta al mittente nelle forme stabilite dal Responsabile del Servizio Protocollo, e invia, nella stessa giornata, prima della chiusura del protocollo, la posta a una delle UO abilitate e "incaricate" dell'apertura della corrispondenza e della protocollazione.

Il personale preposto alla apertura della corrispondenza è appositamente autorizzato al trattamento dei dati personali.

### 5.2.7 Errata ricezione di documenti digitali

Nel caso in cui pervengano su una casella di posta istituzionale PEC o in una casella di posta tradizionale (non PEC), messaggi dal cui contenuto si rileva che gli stessi sono stati erroneamente trasmessi alla AOO (es. messaggi destinati ad altri Enti/soggetti destinatari diversi da ATS), l'operatore attraverso la funzione eccezione rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa ATS".

### 5.2.8 Errata ricezione di documenti cartacei

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

## 5.3 PROTOCOLLAZIONE

Superati tutti i controlli precedenti, i documenti, digitali o analogici, sono protocollati e “segnati” nel protocollo generale o particolare (riservato)

### 5.3.1 Ricevute

*Ricevute attestanti ricevimento documenti informatici*

La ricezione di documenti comporta l’invio al mittente di due tipologie diverse di ricevute:

una legata al servizio di posta certificata, una 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.

*Ricevute attestanti la ricezione di documenti cartacei*

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

- apporre gli estremi della segnatura se contestualmente alla ricezione avviene anche la protocollazione.
- Stampare la ricevuta in duplice copia, che dovranno essere sottoscritte dal mittente e dalla persona incaricata della ricezione.

Nel caso in cui non fosse possibile procedere alla protocollazione contestualmente alla ricezione del documento, l'operatore del protocollo provvederà, su richiesta del mittente, a fotocopiare gratuitamente la prima pagina del documento e ad apporre sulla copia cosi realizzata il timbro dell'amministrazione con data e ora di arrivo unitamente alla propria sottoscrizione.

# 6 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

I documenti informatici sono archiviati su supporti di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo. I documenti ricevuti per via telematica sono resi disponibili alle UO, attraverso la rete interna dell'amministrazione/AOO, subito dopo l'operazione di smistamento e di assegnazione.

## 6.1 CONSERVAZIONE DELLE RAPPRESENTAZIONI DIGITALI DI DOCUMENTI CARTACEI

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato PDF attraverso un processo di scansione.

Il processo di scansione avviene in diverse fasi:

- 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 delle immagini alle rispettive registrazioni di protocollo in modo non modificabile;
- memorizzazione delle file delle immagini su supporto informatico, in modo non modificabile.

Le rappresentazioni digitali dei documenti cartacei sono archiviate, secondo le regole vigenti, su supporti di memorizzazione, in modo non modificabile al termine del processo di scansione.

Nei casi in cui uno o più documenti cartacei vengano recapitati ad un punto di protocollazione diverso dai Servizi destinatari gli stessi dopo le operazioni di registrazione e segnatura vengono, di norma, trattenuti per l'archiviazione da parte del soggetto ricevente secondo le indicazioni e sulla base dell'organizzazione dell'attività di archiviazione data dal Responsabile del Servizio interessato e nel rispetto delle linee guida e/o direttive di carattere generale impartite dall'Azienda per la Tutela della Salute.

Fanno eccezione rispetto alla regola di cui al punto precedente i casi in cui per esigenze di servizio e/o procedurali il Responsabile del Servizio destinatario del documento richieda espressamente la trasmissione del documento originale cartaceo. In tale ipotesi il documento verrà conservato a cura del servizio richiedente l'originale cartaceo.

Il DPO di concerto con il Responsabile del servizio protocollo individua i documenti che, in ragione della necessità di protezione dei dati/informazioni ivi contenuti, sono sottratti alla procedura di scansione ovvero soggetti a registrazione particolare di cui al successivo punto 10.2.

## 6.2 CLASSIFICAZIONE, ASSEGNAZIONE E PRESA IN CARICO

Gli addetti alla protocollazione eseguono la prima classificazione (o classificazione di primo livello) del documento sulla base del titolario di classificazione adottato presso l'AOO e provvedono ad inviarlo all'UO di destinazione che:

• esegue una verifica di congruità in base alle proprie competenze;

• in caso di errore, il documento è ritrasmesso al servizio di protocollo di origine;

• in caso di verifica positiva, esegue l’operazione di presa in carico smistandola al proprio interno ad una UU o direttamente al responsabile del procedimento amministrativo.

*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 dal l'AOO;
- fascicolazione del documento secondo le procedure previste dal l'AOO;
- inserimento del fascicolo nel repertorio dei fascicoli nel caso di apertura di un nuovo fascicolo.

## 6.3 CONSERVAZIONE DEI DOCUMENTI E DEI FASCICOLI NELLA FASE CORRENTE

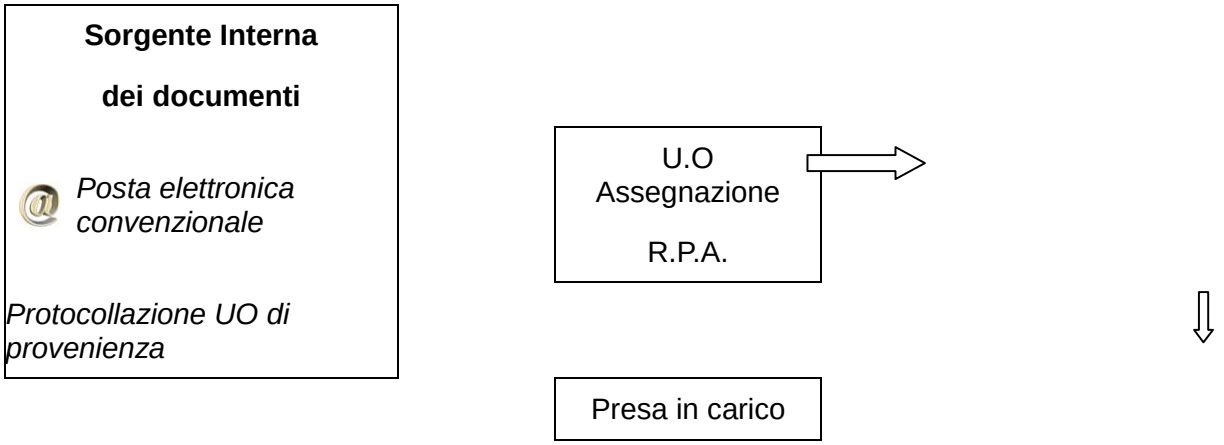
All'interno di ciascun Ufficio Utente (UU) di ciascun UO della AOO sono individuati gli addetti alla organizzazione e alla tenuta dei fascicoli "attivi" (e chiusi in attesa di riversamento nel l'archivio di deposito) e alla archiviazione dei documenti al loro interno.

# 7 CORRISPONDENZA INTERNA

## 7.1 PROVENIENZA DI DOCUMENTI INTERNI FORMALI

Per sorgente interna dei documenti si intende qualunque UO che invia formalmente la propria corrispondenza attraverso il servizio di protocollo della AOO per essere, a sua volta, trasmessa, nelle forme opportune, ad altro UO o UU della stessa AOO.

Il documento è, di norma, di tipo digitale secondo i formati standard illustrati nel precedente capitolo. In questo caso, il mezzo di recapito della corrispondenza considerato è di norma la "scrivania di protocollo" nonché, qualora ritenuto necessario o opportuno la mail aziendale del servizio della UO di Appartenenza.




Nel caso di trasmissione interna di allegati al documento di cui sopra che possono superare la capienza della casella di posta elettronica si procede ad un riversamento (con le modalità previste dalla normativa vigente), su supporto rimovibile da consegnare al destinatario contestualmente al documento principale.

## 7.2 PROVENIENZA DI DOCUMENTI INTERNI INFORMALI

Tutta la corrispondenza interna informale, sia digitale che analogica, è esclusa dalla protocollazione.

# 8 FLUSSO DOCUMENTI IN USCITA

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

Il documento in formato digitale formato secondo gli standard illustrati nei precedenti capitoli potrà essere spedito secondo le procedure indicate nei paragrafi successivi.

I documenti in partenza devono contenere l'invito al destinatario a riportare i riferimenti della registrazione di protocollo della lettera alla quale si da riscontro.

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

## 8.1 VERIFICA FORMALE DEI DOCUMENTI PROTOCOLLAZIONE IN USCITA

Ogni UO è autorizzata dall'AOO per il tramite del servizio protocollo a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita qualora la stessa sia a firma del Responsabile della UO o del Responsabile del Procedimento Amministrativo. Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati dalle UO.

Le UO provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.

Se la verifica da esito positivo, il documento viene registrato nel registro di protocollo generale o particolare; in caso contrario è restituito al mittente UU/RPA con le osservazioni del caso.

Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatura della missiva da inviare sono effettuate dal RPA. Il documento registrato presso il protocollo riservato/sensibile è contrassegnato apponendo la spunta nel flag riservato.

## 8.2 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'indice PA

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

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi

trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.

## 8.3 TRASMISSIONE DOCUMENTI CARTACEI A MEZZO POSTA

I documenti da spedire su supporto cartaceo, nell'ambito della AOO, sono trasmessi all'ufficio addetto allo smistamento della posta dove previsto, abilitato alla spedizione "fisica" della corrispondenza.

### 8.3.1 Affrancatura dei documenti in partenza

Tutte le attività di affrancatura della corrispondenza inviata per posta vengono svolte dal servizio spedizioni attivo presso ciascuna ASSL/ATS.

Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata al servizio spedizioni secondo le regole da questo definite.

Documenti in partenza per posta convenzionale con più destinatari: qualora i destinatari siano più di uno vengono inviate solo le copie del l'unico originale prodotto dall' UO.

### 8.3.2 Inserimento delle ricevute di trasmissione nel fascicolo

Copia 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.

Le UO/UU curano anche l'archiviazione delle ricevute di ritorno delle raccomandate. Queste ultime, sulle quali, precauzionalmente, è stato trascritto sia il numero di protocollo attribuito al documento a cui esse si riferiscono, sia l'UO/UU mittente, sono inizialmente raccolte dal Servizio Spedizioni e successivamente consegnate alle UO/UU medesime.

### 8.3.3 Invio cartaceo dati sensibili.

Nel caso di invio di documentazione cartacea contenente dati sensibili, nella busta dovrà essere riportata la dicitura "contiene dati sensibili soggetti alla tutela della privacy ai sensi della vigente normativa in materia di trattamento dei dati apribile solo da personale autorizzato".

## 8.4 TRASMISSIONE DOCUMENTI CARTACEI A MEZZO FAX

Di norma è esclusa la trasmissione di documenti a mezzo fax fatta eccezione nel caso in cui un privato cittadino richieda espressamente riscontro a precedente comunicazione con lo stesso mezzo. E' in ogni caso esclusa la comunicazione via fax tra pubbliche amministrazioni.

# 9 REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

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.

## 9.1 ATTIVITÀ DI ASSEGNAZIONE

L'attività di assegnazione consiste nell'operazione di inviare direttamente dai punti di protocollazione in entrata il documento protocollato e assegnato all'UO competente e la contestuale trasmissione del materiale documentario oggetto di trattazione compilato nella parte segnatura.

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

Con l'assegnazione tramite il SdP la struttura assume la presa in carico della documentazione. La responsabilità del relativo procedimento è individuato in base alla regolamentazione aziendale vigente (funzionigramma, atti di attribuzione di attività/funzioni ecc.).

L'UO competente è incaricata della gestione del procedimento a cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento amministrativo decorrono dalla data certa di recezione del documento da parte dell'amministrazione.

Il Responsabile della UO provvede ad individuare il soggetto preposto alla gestione del documento nell'ambito del relativo procedimento assegnandogli lo stesso nel rispetto del principio di dematerializzazione. Da tale momento decorre in capo al soggetto assegnatario la responsabilità in ordine alla gestione del documento e del relativo procedimento

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

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.

### 9.1.1 Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'UO competente attraverso i canali telematici dell'AOO.

L'UO competente ha notizia dell'assegnazione di detti documenti attraverso la consultazione quotidiana della lista lavoro documenti.

Il responsabile dell'UO 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 UO 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.

### 9.1.2 Assegnazione dei documenti ricevuti in formato cartaceo

Al termine delle operazioni di registrazione, segnatura dei documenti ricevuti dall'AOO in formato cartaceo, i documenti medesimi sono assegnati tramite il SdP al'UO di competenza.

L'originale cartaceo riceve il seguente trattamento:

- viene acquisito in formato immagine con l'ausilio di *scanner;*
- viene trattenuto per l'archiviazione da parte del soggetto ricevente secondo le indicazioni e sulla base dell'organizzazione dell'attività di archiviazione data dal Responsabile del Servizio interessato e nel rispetto delle linee guida e/o direttive di carattere generale impartite dall'Azienda per la Tutela della Salute
- viene trasmesso/ritirato al/dal RPA su espressa richiesta del Responsabile del Servizio destinatario del documento motivata da esigenze di servizio e/o procedurali.

In ogni caso gli atti giudiziari saranno trasmessi in originale, a cura del Responsabile della Struttura alla quale afferisce il punto di protocollazione ricevente, alla SC Affari Legali,a mezzo corriere interno, con cadenza bisettimanale, salvo esigenze particolari di acquisizione immediata rappresentate dal Direttore della Struttura Affari Legali.

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

L'UO competente ha notizia dell'arrivo del documento ad esso indirizzato attraverso le funzioni del SdP e qualora ritenuto opportuno o necessario tramite un messaggio di posta elettronica. In base alle abilitazioni previste il responsabile dell'UO potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento
- individuare l'RPA competente sulla materia oggetto del documento.

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

### 9.1.3 Modifica delle assegnazioni

Nel caso di assegnazione errata, l'UO/UU che riceve il documento comunica l'errore al servizio protocollo, 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 UO, l'abilitazione al relativo cambio di assegnazione è attribuita anche al dirigente della UO medesima, o a persona da questi incaricata.

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

## 9.2 REGOLE DI ASSEGNAZIONE DEI DOCUMENTI INVIATI

Il Servizio Protocollo dopo aver protocollato in uscita il documento lo assegna all'ufficio proponente. Tale assegnazione è generata automaticamente dal Servizio Protocollo ed è la conferma dell'avvenuta protocollazione del documento.

### 9.2.1 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 1 è riportata l'articolazione della AOO in UO e UU.

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

# 10 ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

### 10.1.1 Documenti Esclusi

Ai sensi dell'art. 53 del DPR n. 445/2000 sono esclusi dalla registrazione a protocollo:

- gazzette ufficiali
- bollettini ufficiali della pubblica amministrazione
- notiziari della pubblica amministrazione
- note di ricezione di circolari
- note di ricezione di altre disposizioni
- materiali statistici
- atti preparatori interni
- giornali
- riviste
- libri
- materiali pubblicitari
- inviti a manifestazioni
- tutti documenti soggetti a registrazione particolare dell'Amministrazione

Sono parimenti esclusi dalla registrazione di protocollo:

- certificati medici dipendenti
- richieste ferie
- richieste permessi retribuiti (art. 30 c. 1-4 CCNL, l. 104/92)
- richieste di rimborso spese e missioni di interni ed esterni
- comunicazioni da parte di enti di bandi di concorso, di domande da presentare entro data da definire

### 10.1.2 Documenti Soggetti a Registrazione Particolare

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le seguenti tipologie di documenti:

- Documentazione Sanitaria
- Procedimenti disciplinari
- Contenziosi e atti giudiziari
- Altra documentazione valutata caso per caso dalla Direzione

- Delibere Direttore Generale e Determine Dirigenziali
- Contratti e Convenzioni
- Verbali di ispezione, sopralluogo e contestazione illeciti
- Ordinanze
- Verbali Commissioni di gara/cocorso/varie
- fatture (attive e passive)
- certificazioni (di servizio, di situazioni retributive e contributive) meccanizzate e non meccanizzate
- documentazione gestita da eventuali procedure meccanizzate

Tale tipo di registrazione consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertoriazione.

# 11 MODALITÀ DI PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO

## 11.1 UNICITÀ DEL PROTOCOLLO INFORMATICO

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica.

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.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro. Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

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

Non è consentita la protocollazione di un documento già protocollato. Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento (fatto salvo quanto previsto da normativa specifica in materia di posta elettronica certificata), indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

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

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

## 11.2 REGISTRO 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 trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).

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

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

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

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

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

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

Tali dati facoltativi sono descritti nei paragrafi seguenti.

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.

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

### 11.3.1 Documenti Informatici

I documenti informatici sono ricevuti e trasmessi in modo formale sulle/dalle caselle di posta elettronica certificata dell'amministrazione. 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, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati.

I documenti informatici 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.

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;
- data e numero di protocollo del messaggio ricevuto o inviato
- l'oggetto
- il mittente
- il destinatario o i destinatari
- denominazione dell'amministrazione;
- codice identificativo del l'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo.

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

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

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

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

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

### 11.3.2 Documenti Analogici

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza, (il servizio postale pubblico e/o privato o con consegna diretta alla UOP). La registrazione di protocollo di un documento analogico cartaceo ricevuto, così come illustrato nel seguito, viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.

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

**Elementi Facoltativi nella Registrazione di Protocollo**

Il RSP, con proprio provvedimento e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può modificare e integrare gli elementi facoltativi del protocollo. La registrazione degli elementi facoltativi del protocollo, con determinazione del RSP può essere modificata, integrata e cancellata in base alle effettive esigenze delle UOR o degli UOP. In caso di

necessità i dati facoltativi sono modificabili senza obbligatorietà 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 sistema di protocollo sono previste specifiche funzionalità che consentono di gestire:

- Il numero di protocollo corrispondenza ricevuta 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 recapito telefonico;
- gli indirizzi di posta elettronica;
- la chiave pubblica della firma digitale;
- il consenso all'uso della *email* in termini di *privacy.*
- *Eventuali note e chiavi di ricerca*

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un "segno" grafico sul 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;
- indice di classificazione;

Il "segno" grafico è realizzato con una etichetta autoadesiva corredata di codice a barre; nel caso non fosse disponibile verrà eseguito con un timbro tradizionale. L'operazione di acquisizione dell'immagine dei documenti cartacei è eseguibile 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.

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

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

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

### 11.3.3 Protocollo Differito

Nel caso di un temporaneo ed eccezionale carico di lavoro che non permetta di evadere la corrispondenza ricevuta nella medesima giornata lavorativa (ad es. nel caso di un consistente numero di domande di partecipazione ad un concorso) e qualora dalla mancata registrazione a

protocollo del documento nel medesimo giorno lavorativo di ricezione possa derivare un pregiudizio a diritti o legittime aspettative di terzi, con motivato provvedimento del responsabile del servizio protocollo dell'AOO, o suo delegato, si differiscono i termini di registrazione.

Nel provvedimento di differimento dei termini devono essere individuati i documenti da ammettere alla registrazione differita, le cause della stessa nonché il termine entro il quale la registrazione a protocollo deve comunque essere effettuata.

Possono essere ammessi alla procedura di protocollo differito soltanto i documenti in arrivo, distinti in tipologie omogenee da indicarsi nel provvedimento di differimento.

### 11.3.4 Annullamento Protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrati 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 o suo delegato. 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, o suo delegato, 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, o suo delegato .

Il registro riporta i motivi dell'annullamento e, se il documento è stato protocollato nuovamente, il nuovo numero di protocollo assegnato.

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, email, siano stati attribuiti più numeri di protocollo.

## 11.4 CASI PARTICOLARI DI REGISTRAZIONE PROTOCOLLO

### 11.4.1 Protocollo Riservato

All'interno dell'AOO è istituito il protocollo riservato - sottratto alla consultazione da parte di chi non sia espressamente abilitato - nel quale sono riportati:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa.

La registrazione nel protocollo particolare, quando non sia palesemente evidente la necessità, può essere disposta dal RSP, o suo delegato, con l'apposizione, sul documento, della seguente dicitura: "Da registrare sul protocollo particolare".

### 11.4.2 Circolari e Documenti con più destinatari

Le circolari, le disposizioni generali e tutte le altre comunicazioni interne alla ATS che abbiano più destinatari si registrano con un solo numero di protocollo generale. Tutti i destinatari sono indicati in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo secondo le modalità previste dalla gestione anagrafica del sistema.

Al fine di garantire l'efficienza, l'efficacia e la tempestività dell'azione amministrativa:

- laddove il numero di destinatari, comunque definiti, sia in numero maggiore di 20 l'operatore di protocollo potrà a seconda del caso:

- assegnare il documento nel sistema di protocollo secondo le normali procedure in uso;
- assegnare il documento nel sistema di protocollo alle sole macrostrutture di appartenenza (es. Dipartimenti / Aree Socio Sanitarie Locali ecc.) dei singoli destinatari che a loro volta provvederanno a recapitare con modalità telematica (assegnazione nel SdP o trasmissione a mezzo mail) il documento ai destinatari;
- trasmettere il documento protocollato alle mail dei destinatari (istituzionali ovvero altre mail espressamente indicate quale indirizzo di recapito) riportando nel campo note associato al numero di protocollo acquisito l'avvenuta trasmissione a mezzo mail con indicazione della data e dell'ora di invio).

- laddove la comunicazione sia rivolta ad una pluralità indefinita di soggetti interni anche raggruppati per categorie (es. "a tutto il personale ATS", "Al personale del Comparto", "Al personale del P.O. _____" ecc.) l'operatore di protocollo potrà a seconda del caso:

- assegnare il documento nel sistema di protocollo alle macrostrutture di appartenenza dei singoli destinatari che a loro volta provvederanno a recapitare il documento ai destinatari con modalità telematica (assegnazione nel SdP o trasmissione a mezzo mail) ovvero mediante affissione del documento in punti di passaggio/bacheche ad ampia visibilità;
- trasmettere il documento protocollato alle mail dei destinatari (istituzionali ovvero altre mail espressamente indicate quale indirizzo di recapito) mediante sistemi di trasmissione massiva, riportando nel campo note associato al numero di protocollo acquisito l'avvenuta trasmissione a mezzo mail con indicazione della data e dell'ora di invio);
- pubblicare il documento in apposita sezione dedicata della INTRANET aziendale riportando nel campo note associato al numero di protocollo acquisito l'avvenuta pubblicazione con indicazione della sezione della Intranet e della data di pubblicazione.

### 11.4.3 Documenti ricevuti a mezzo Telegramma

I telegrammi vengono registrati nel SdP come documenti senza firma, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

### 11.4.4 Documenti cartacei ricevuti a mezzo Telefax

Il documento ricevuto a mezzo telefax è un documento analogico (cartaceo) a tutti gli effetti e come tale dovrà essere gestito. Il documento trasmesso da chiunque alla AOO tramite telefax, qualora ne venga accertata la fonte di provenienza, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale. L'accertamento

della fonte di provenienza spetta al RPA e avviene, di norma, per le vie brevi o con l'uso di sistemi informatici.

Qualora non sia possibile accertare la fonte di provenienza, sul telefax viene apposta la dicitura *"Documento ricevuto via telefax"* e successivamente il RPA provvede ad acquisire l'originale.

Nel caso che al telefax faccia seguito l'originale, poiché ogni documento viene individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione, l'addetto alla registrazione a protocollo, dopo aver registrato il telefax, deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax ed apporre la seguente dicitura: "*Già pervenuto via fax il giorno……."*.

Il RSP accerta comunque che si tratta del medesimo documento ricevuto via fax: qualora dovesse riscontrare una differenza, anche minima, deve procedere alla registrazione con un nuovo numero di protocollo in quanto si tratta di un documento diverso.

Il fax ricevuto con un terminale telefax dedicato (diverso da un PC) è fotocopiato dal ricevente qualora il supporto cartaceo non fornisca garanzie per una corretta e duratura conservazione. Su di esso o sulla sua foto-riproduzione va apposta, a cura del ricevente, la dicitura "Documento ricevuto via telefax".

Fermo restando l'espresso divieto di utilizzo del fax per le comunicazioni interne alla AOO ovvero tra qualsiasi UO delle AOO e altre Pubbliche Amministrazioni esterne e che gli operatori ATS potranno ricorrere all'utilizzo del fax solo quando non sia possibile raggiungere il destinatario con altri mezzi telematici (e.mail/PEC) e su sua espressa richiesta, eventuali documentI in partenza a mezzo recano una delle seguenti diciture:

- *"Anticipato via telefax"* se il documento originale viene successivamente inviato al destinatario;
- *"La trasmissione via fax del presente documento non prevede l'invio del documento originale»* nel caso in cui l'originale non venga spedito. Il RPA è comunque tenuto a spedire l'originale qualora il destinatario ne faccia motivata richiesta.

La segnatura viene apposta sul documento e non sulla copertina di trasmissione. La copertina del telefax ed il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione. Il fax ricevuto direttamente su una postazione di lavoro (esempio un PC con l'applicativo per invio e ricezione di fax) è la rappresentazione informatica di un documento che può essere, sia stampato e trattato come un fax convenzionale come è stato descritto nei paragrafi precedenti, sia visualizzato e trattato interamente con tecniche informatiche. In questo secondo caso il "file" rappresentativo del fax, viene inviato al protocollo generale, per essere sottoposto alle operazioni di protocollazione e segnatura secondo gli standard XML vigenti e poi, trattato secondo le regole precedentemente specificate per la gestione dei documenti informatici.

### 11.4.5 Documenti non firmati/Documenti anonimi

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

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

### 11.5 PROTOCOLLAZIONE DEI MESSAGGI DI POSTA ELETTRONICA TRADIZIONALE NON PEC

Considerato che l'attuale sistema di posta elettronica tradizionale non PEC 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.

### 11.6 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.

### 11.7 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 COPIE PER "CONOSCENZA"

Nel caso di copie per conoscenza si deve utilizzare la procedura prevista dal sistema di protocollo. 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".

Le UO destinatarie delle copie per conoscenza avranno cura di verificare la corrispondenza ricevuta dalle proprie liste lavoro senza ulteriori invii da parte del servizio di protocollo

### 11.9 CORRISPONDENZA PERSONALE

La corrispondenza personale è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura “riservata” o “personale”.

In quest’ultimo caso, la corrispondenza con la dicitura “riservata” o “personale” non è aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli al più vicino ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

**Integrazioni Documentarie**

L’addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed 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 fascicolo relativo.

# 12 SISTEMA DI CLASSIFICAZIONE E PIANO DI CONSERVAZIONE

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente. Il piano di classificazione si suddivide in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello, etc. Il titolo (o la voce di 1° livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) 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 2.

Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito della funzione di governo 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 e/o regionali.

L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RSP (oppure, su proposta del responsabile dell'archivio generale dell'amministrazione e/o dalle autorità competenti per materia).

La revisione anche parziale del titolario viene proposta dal RSP quando è necessario ed opportuno.

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

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

Viene garantita 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 modifica di una voce viene riportata la data di introduzione 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 valgono almeno per l'intero anno. Rimane possibile, se il sistema lo consente, registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.

Il titolario è elaborato da un gruppo di lavoro appositamente costituito all'interno dell'amministrazione/AOO e approvato dai competenti organi dell'amministrazione archivistica statale.

## 12.1 MISURE DI PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI

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

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

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

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

Lo scarto dei documenti dell'archivio in parola è subordinato all'autorizzazione della direzione generale per gli archivi,

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.

## 12.2 CLASSIFICAZIONE

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO. Essa è eseguita a partire dal 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 in base al sopra citato titolario.

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

Qualora l'ente lo ritenga opportuno, le operazioni di classificazione possono essere svolte in momenti diversi: l'addetto alla registrazione di protocollo può inserire la voce di livello più alto, mentre l'attribuzione delle voci di dettaglio è demandata all'incaricato della trattazione della pratica.

## 12.3 FASCICOLAZIONE

Tutti i documenti registrati nel sistema informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli. Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento. I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza, sottofascicolo o inserto, secondo l'ordine cronologico di registrazione.

### 12.3.1 Apertura Fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'AOO, il soggetto preposto (quale, ad esempio, RPA, RSP, responsabile del servizio archivistico addetto alla protocollazione, etc.) 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, etc.);
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'amministrazione/ AOO;

- data di apertura del fascicolo;
- AOO e UOR;
- collocazione fisica, di eventuali documenti cartacei;
- collocazione logica, dei documenti informatici;

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

### 12.3.2 Chiusura del Fascicolo

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento

dell'affare.

### 12.3.3 Inserimento del Documento nel Fascicolo

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

A seconda delle ipotesi, si procede come segue:

- Se il documento si ricollega ad un *affare o procedimento in corso*, l'addetto:
- seleziona il relativo fascicolo;
- collega la registrazione di protocollo del documento al fascicolo selezionato;
- invia il documento all'UOR cui è assegnata la pratica. (Se si tratta di un documento su supporto cartaceo, assicura l'inserimento fisico dello stesso nel relativo fascicolo).
- Se il documento dà avvio ad un *nuovo fascicolo*, il soggetto preposto:
- esegue l'operazione di apertura del fascicolo;
- collega la registrazione di protocollo del documento al nuovo fascicolo aperto;
- assegna il documento ad un istruttore su indicazione del responsabile del procedimento;
- invia il documento con il relativo fascicolo al dipendente che dovrà istruire la pratica per competenza.

### 12.3.4 Processo di assegnazione dei fascicoli

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

ipotesi, si procede come segue:

- se il documento si ricollega ad un *affare o procedimento in corso,* l'addetto:
    - seleziona il relativo fascicolo;
    - collega la registrazione di protocollo del documento al fascicolo selezionato;
    - invia il documento all'1.11.1 cui è assegnata la pratica;
- se il documento da avvio ad un *nuovo fascicolo,* il soggetto preposto:
    - esegue l'operazione di apertura del fascicolo;
    - collega la registrazione di protocollo del documento al nuovo fascicolo aperto;
    - assegna il documento ad un istruttore su indicazione del RPA;
    - invia il documento con il relativo fascicolo, al dipendente, che dovrà istruire la pratica per competenza.

### 12.3.5 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'UO 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, con la data e l'ora dell'operazione.

# 13 REGISTRO DI EMERGENZA

Qualora non fosse disponibile fruire del PdP per una interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza secondo il modello allegato n. 6.1 al presente manuale.

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

Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite su registro di 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 è associato 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

## 13.1 APERTURA REGISTRO EMERGENZA

Il RSP, o suo delegato, assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica, le operazioni di protocollo sono svolte manualmente sul registro di emergenza, sia esso cartaceo o informatico, su postazioni di lavoro operanti fuori linea. Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, su richiesta presentata dal Direttore/Responsabile del servizio interessto (da presentarsi utilizzando il modello 6.2 allegato al presente Manuale), il RSP, o suo delegato, 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.

## 13.1 CHIUSURA DEL REGISTRO EMERGENZA

È compito del RSP, o suo delegato, verificare la chiusura del registro di emergenza. È compito del RSP, o suo delegato, verificare l'avvenuto inserimento dal registro di emergenza al sistema di protocollo generale (PdP) delle protocollazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.

Una volta ripristinata la piena funzionalità del PdP, il RSP, o suo delegato, provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.

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

## 14.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

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

Il presente manuale potrà essere aggiornato a seguito di:

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

## 14.2 REGOLAMENTI ABROGATI

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

## 14.3 PUBBLICITÀ DEL PRESENTE MANUALE

II presente manuale è disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento sul sito istituzionale dell'AOO ed è pubblicato a disposizione degli operatori nella INTRANET aziendale.

Inoltre copia del presente manuale è inviata ai direttori delle UO;

## 15 ALLEGATI

Allegato n. 1: Strutture di protocollazione e relativi sottolivelli (articolazione UO – UU)

Allegato n. 2: Titolario di classificazione

Allegato n. 3: Riferimenti Normativi

Allegato n. 4: Definizioni

Allegato n. 5: Elenco Abilitazioni

Allegato n. 6: Registro protocollo di emergenza e modelli per richiesta attivazione/chiusura.