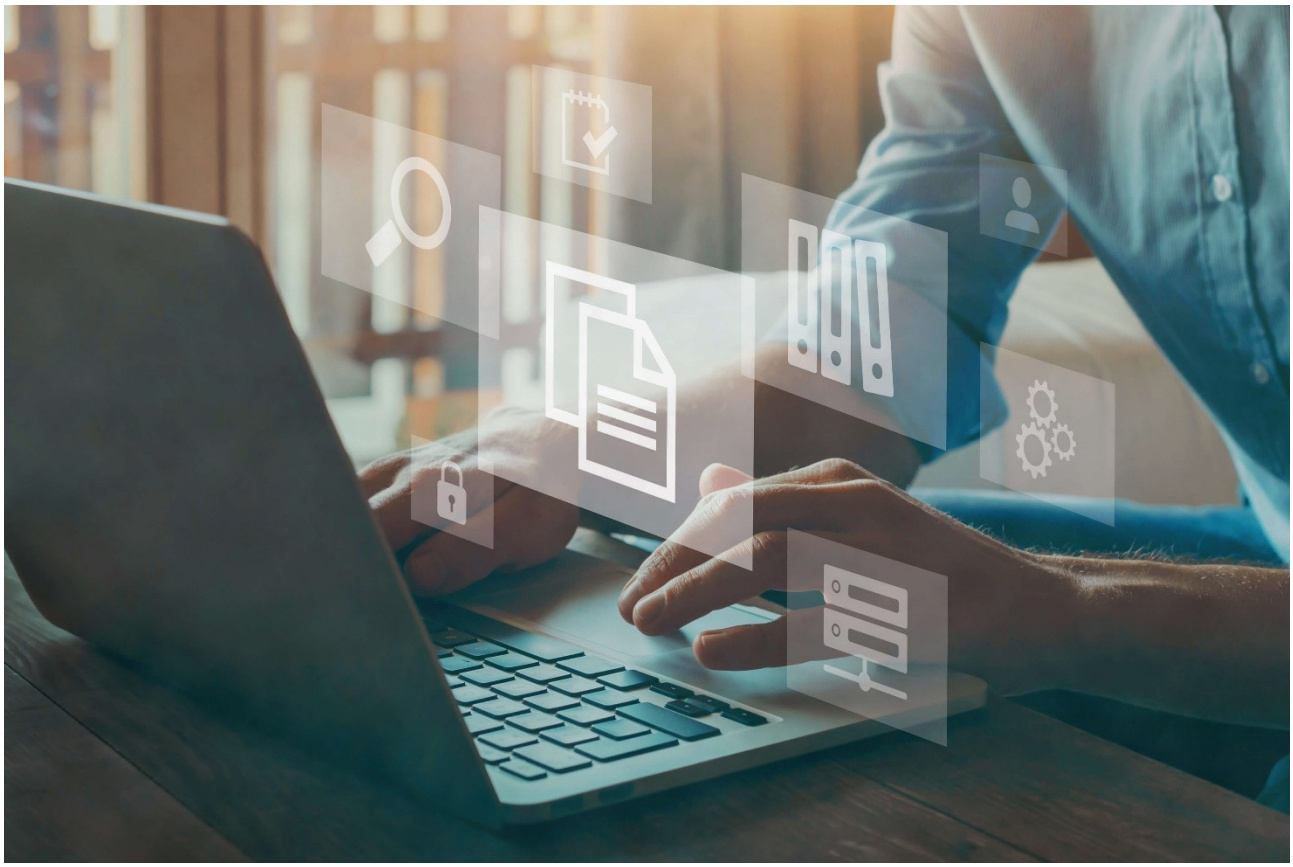
Istituto degli Innocenti

Manuale di gestione del protocollo informatico, dei documenti e degli archivi digitali

Approvato con Deliberazione del Consiglio di Amministrazione n. 61 del 28/12/2021



Versione	Data approvazione versione	Descrizione modifiche
1.0	28/12/2021	Prima stesura

Indice

1.1.

1. Principi generali

1.1. Premessa

Il manuale di gestione documentale descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, come previsto dal punto 3.5 delle Linee Guida sulla formazione gestione e conservazione dei documenti informatici, emesse da AgID il 09.09.2020 con determinazione dirigenziale n. 404/2020, in vigore dal 10.09.2020 ed in attuazione dal 01.01.2022 (di seguito "Linee Guida AgID").
La redazione e l'aggiornamento del manuale di gestione documentale, nonché la corretta applicazione di quanto in esso definito e descritto, è compito del responsabile della gestione documentale, così come definito dall'art. 61 del Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000, di seguito "TUDA") e dal punto 3.4 delle Linee Guida AgID.
L'adozione del manuale di gestione è prevista per tutte le amministrazioni di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82 e ss.mm.ii., Codice dell'Amministrazione Digitale (di seguito "CAD").
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. Le modalità operative di tenuta del protocollo informatico sono definite nel capo IV del TUDA.
Obiettivo del manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili per gli addetti al servizio e per i soggetti esterni che a diverso titolo interagiscono con l'Istituto. Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'attività dell'Istituto. 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'Istituto. Il manuale è articolato come definito al punto 3.5 delle Linee Guida AgID, seguendo il modello generale proposto dall'AgID stessa.

1.2. Ambito di applicazione del manuale

Il presente manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi del punto 3.5 delle Linee Guida AgID. Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'Istituto. Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e della spedizione di un documento.

1.3. Definizioni e norme di riferimento

Ai fini del presente manuale si intende per:

- "Istituto", l'Istituto degli Innocenti di Firenze;
- "TUDA", il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- "Linee Guida AgID", Linee Guida sulla formazione gestione e conservazione dei documenti informatici, emesse da AgID il 09.09.2020 con determinazione dirigenziale n. 404/2020, in vigore dal 10.09.2020 ed in attuazione dal 01.01.2022;
- "CAD", il decreto legislativo 7 marzo 2005, n. 82 e ss.mm.ii. - Codice dell'amministrazione digitale.

I termini e le definizioni utilizzate in questo manuale sono quelle dettagliata nell'allegato 1 (Glossario dei termini e degli acronimi) delle Linee Guida AgID, che qui si intende integralmente richiamato.
Di seguito si riportano gli acronimi utilizzati più frequentemente:

- AOO - Area Organizzativa Omogenea;
- MdG - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;
- RPA - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- RSP - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
- SdP – Servizio di protocollo informatico;
- UOP - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- UOR - Uffici Organizzativi di Riferimento (Servizi e Staff di Area) - un insieme di uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.

1.4. Aree Organizzative Omogenee

Per la gestione dei documenti l'Istituto ha creato un'unica Area Organizzativa Omogenea (AOO) dove è istituito un unico servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. All'interno dell'Istituto il sistema archivistico è unico. All'interno della AOO il sistema di protocollazione è centralizzato per la corrispondenza in ingresso, mentre la protocollazione della corrispondenza interna e di quella in uscita è delegata alle singole UOR.

1.5. Servizio per la gestione informatica del protocollo

Nella AOO è istituito il servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Al suddetto servizio è preposto il responsabile del servizio di protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RSP), che coincide con il Responsabile del Servizio di Segreteria generale sistemi IT e Museo degli Innocenti (cfr. cap. 3).
In relazione alla modalità di fruizione del servizio di protocollo adottata dalla AOO, è compito del servizio:

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

1.6. Conservazione del registro di protocollo

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

1.7. Firma digitale

Per l'espletamento delle attività istituzionali l'Istituto fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla.

1.8. Tutela dei dati personali

L'Istituto titolare dei dati di protocollo e dei dati personali, comuni, sensibili e/o giudiziari, contenuti nella documentazione amministrativa di propria competenza ha ottemperato al dettato del Regolamento UE 679/2016 (GDPR) e al decreto legislativo 10 agosto 2018, n. 101 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 679/2016) con atti formali aventi rilevanza interna ed esterna.

1.9. Caselle di Posta Elettronica

L'AOO è dotata di una casella di posta elettronica certificata istituzionale per la corrispondenza, sia in ingresso che in uscita: istitutodeglinnocenti@pec.it. Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UOR) che ad essa fanno riferimento.
In attuazione di quanto previsto dalla Direttiva del Ministro per l'Innovazione e le Tecnologie 18 novembre 2005 sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'Istituto munisce tutti i propri dipendenti compresi quelli per i quali non sia prevista la dotazione di un personal computer di una casella di posta elettronica ordinaria.

1.10. Sistema di classificazione dei documenti

Per consentire l'attività operativa del protocollo informatico è stato adottato un unico titolario di classificazione per l'archivio centrale unico dell'Istituto. Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base dell'organizzazione funzionale dell'AOO, consentendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.
La definizione del sistema di classificazione, nella sua versione aggiornata al 21 luglio 2021, è stata approvata con delibera del consiglio di amministrazione dell'Istituto degli Innocenti di Firenze n. 36 del 28 luglio 2021.
Al fine di agevolare e normalizzare, da un lato la classificazione archivistica e dall'altro l'assegnazione per competenza, sul SdP è stato predisposto un elenco delle UOR e dei dipendenti che, unitamente a quello di classificazione, permette l'immediata individuazione sia della classificazione e che delle competenze.

1.11. Formazione

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

1.12. Accreditamento dell'AOO all'IPA

L'AOO, come accennato si è dotata di una casella di posta elettronica certificata attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della UOP incaricata; quest'ultima procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta.
L'Istituto, 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'Istituto comunica tempestivamente all' IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa, in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività l'Istituto comunica la soppressione, ovvero la creazione di una AOO.
Il codice IPA dell'Istituto è: idi_fi
Il codice univoco dell'unica AOO è: AFAFD26

2. Utilizzo degli strumenti informatici per la formazione e lo scambio di documenti informatici

2.1. Formazione dei documenti - Aspetti operativi

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

- ricevuto;
- inviato;
- interno formale.

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

- informatico;
- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici. La redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità. Pertanto il documento amministrativo può essere disponibile anche nella forma analogica.

2.2. Documento ricevuto

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

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

Un documento analogico può essere recapitato:

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

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

2.3. Documento inviato

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma:

- per mezzo della posta elettronica certificata, se la dimensione del documento e/o di eventuali allegati, non supera la dimensione massima prevista dal sistema di posta utilizzato dall'AOO, che è di 30 Megabytes, e con un limite di 50 destinatari;
- per mezzo della posta elettronica ordinaria, se la dimensione del documento e/o di eventuali allegati, non supera la dimensione massima prevista dal sistema di posta utilizzato dall'AOO, che è di 50 Megabytes;
- per mezzo di un sistema telematico di trasferimento di file di grandi dimensioni, che garantisce la riservatezza dei contenuti e la certezza di consegna al destinatario corretto.

In caso sia necessario, il documento informatico potrebbe essere copiato su supporto digitale rimovibile e trasmesso al destinatario con altri mezzi di trasporto, ivi compresa la consegna a mano da parte di personale appositamente incaricato.

2.4. Sottoscrizione di documenti informatici

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale oppure con l'apposizione di un sigillo elettronico, entrambi conformi alle disposizioni dettate dalla

normativa vigente. I documenti informatici prodotti dall'AOO, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità (vedi Allegato 2 delle Linee Guida AgID).

2.5. Documento interno formale

I documenti interni sono formati con tecnologie informatiche e, dopo l'attribuzione di un numero di protocollo interno e la sottoscrizione con firma digitale qualificata o con sigillo elettronico, trasmessi per mezzo della posta elettronica interna oppure attraverso lo smistamento del SdP.

2.6. 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.

2.7. Il documento digitale

I documenti dell'Istituto sono prodotti con sistemi informatici, come previsto dalla vigente normativa e pertanto sono da considerarsi documenti digitali ab origine.
Ogni documento formato per essere inoltrato formalmente all'esterno o all'interno:

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

Le firme necessarie alla redazione e perfezione sotto il profilo giuridico del documento in partenza sono apposte prima della sua protocollazione.
Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabili dei singoli UOR.
Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della AOO e dell'UOR che ha prodotto il documento, con indirizzi e riferimenti.

Il documento deve inoltre recare almeno le seguenti informazioni:

- il luogo di redazione;
- la data di redazione;
- il numero degli allegati, se presenti;
- l'oggetto;
- firma elettronica avanzata o qualificata da parte del RPA e/o del responsabile del provvedimento finale.

2.8. Requisiti degli strumenti informatici di scambio

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

- l'integrità del messaggio;

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

2.9. Firma digitale, sigillo elettronico

Gli strumenti che soddisfano i primi due requisiti di cui al precedente paragrafo 2.8. sono la firma digitale o il sigillo elettronico utilizzati per sottoscrivere i documenti.

2.10. Verifica delle firme nel SdP

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

- Nel caso si tratti di un documento firmato CAdES, apertura della busta "virtuale" contenente il documento firmato (questa operazione non è necessaria per i documenti firmati PAdES e XAdES);
- verifica della validità del certificato alla data dichiarata di sottoscrizione; questa attività è realizzata verificando on-line le Certificate Revocation List (CRL);
- verifica della firma (o delle firme multiple) con funzioni informatiche standard; in particolare, viene calcolata l'impronta del documento e verificata con quella contenuta nella busta "logica" (formato CAdES) o nel documento stesso (formati PAdES e XAdES);
- verifica dell'utilizzo, nell'apposizione della firma, di un certificato emesso da una Certification Authority (CA) presente nell'elenco pubblico dei certificatori accreditati e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle CA accreditate presso l'AgID;
- attribuzione della segnatura di protocollo;
- nel caso di documento firmato CAdES, il sistema documentale del SdP permette la consultazione del documento in chiaro.

2.11. Uso della posta elettronica certificata

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.
Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo. Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura, in un formato compreso nell'allegato 2 alle Linee Guida AgID;
- inserire i dati del destinatario (almeno: denominazione, indirizzo della casella di posta elettronica);
- firmare il documento (ed eventualmente associare il riferimento temporale al documento firmato) o apporre il sigillo elettronico;
- assegnare il numero di protocollo in uscita a tale documento;
- invio del messaggio contenente il documento firmato o sigillato e protocollato in uscita alla casella di posta elettronica del destinatario.

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

- firmare elettronicamente il messaggio;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica certificata dichiarato dal destinatario;
- ricevere in automatico le "ricevute di accettazione" e le "ricevute di consegna" costituite da messaggi di posta elettronica generati dal sistema PEC.

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

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico certificato 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 raccomandata nei casi consentiti dalla legge.

3. UO responsabile del servizio di protocollo informatico

Il presente capitolo individua l'unità organizzativa responsabile delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti informatici all'interno della AOO. La tenuta dei documenti informatici all'interno della AOO è attribuita al servizio Segreteria Generale, Sistemi IT e Museo degli Innocenti, che è competente a gestire l'intera documentazione digitale, ai fini della sua corretta collocazione, classificazione e conservazione.

4. Flusso di lavorazione e regole di assegnazione ed inoltro

I flussi di lavorazione dei documenti all'interno della AOO sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico probatoria. Essi si riferiscono ai documenti:

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

4.1. Flusso dei documenti in uscita dalla AOO

I documenti in uscita sono generalmente inviati da una “sorgente interna all’AOO”. Per sorgente interna all'AOO si intende l'unità organizzativa mittente interna all'AOO che invia, tramite il SdP, nelle forme e nelle modalità più opportune, ad altra amministrazione oppure ad altro ufficio UOR della stessa AOO. Per "documenti in uscita" s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra amministrazione oppure ad altro ufficio UOR della stessa AOO. Il documento è in formato digitale composto secondo gli standard illustrati in questo manuale. I mezzi di recapito della corrispondenza considerati sono quelli definiti in questo manuale.
Nel caso di trasmissione interna di allegati al documento di cui sopra che possono superare la capienza della casella di posta elettronica si procede ad un riversamento (con le modalità previste dalla normativa vigente), su supporto rimovibile da consegnare al destinatario contestualmente al documento principale. I documenti in partenza possono contenere l'invito al destinatario a riportare i riferimenti della registrazione di protocollo della lettera alla quale si dà riscontro.

4.1.1 Verifica formale dei documenti

Tutti i documenti originali da spedire, siano essi in formato digitale o analogico, devono rispettare quanto enunciato ai paragrafi 2.6. e 2.7. di questo manuale. Il documento deve essere sottoscritto in modalità digitale o autografa.

4.1.2 Registrazione di protocollo e segnatura

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

4.1.3 Trasmissione di documenti informatici

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla normativa vigente.
I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno alla AOO).
Per la spedizione dei documenti informatici, l'AOO si avvale del servizio di "posta elettronica certificata", conforme a quanto previsto dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, offerto da

un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio delle ricevute di ritorno elettroniche.
Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non devono duplicare 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.

4.1.4 Trasmissione di documenti cartacei a mezzo posta

La UOR mittente provvede direttamente a tutte le operazioni di spedizione della corrispondenza:

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

La UOR mittente provvede all'attività di affrancatura.
Qualora si debba inviare un documento a più destinatari, verranno spedite solo copie dell'unico originale prodotto dall'UOR.
La minuta del documento cartaceo spedito e le eventuali ricevute delle raccomandate sono conservate all'interno del relativo fascicolo.
Le UOR curano anche l'archiviazione delle ricevute di ritorno delle raccomandate. Queste ultime sulle quali è stato trascritto sia il numero di protocollo attribuito al documento a cui esse si riferiscono, sia l'UOR mittente, sono consegnate alle UOR medesime

4.2. Flusso dei documenti in ingresso alla AOO

4.2.1 Provenienza esterna dei documenti

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

4.2.2 Provenienza di documenti interni formali

Per sorgente interna dei documenti si intende qualunque UOR che invia formalmente la propria corrispondenza ad altra UOR della stessa AOO. Il documento è, di norma, di tipo digitale e viene trasmesso attraverso il SdP.

4.2.3 Ricezione di documenti informatici sulla casella di posta istituzionale

Di norma, la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile alla UOP dell'AOO.
Quando i documenti informatici pervengono alla UOP, la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo ed alla assegnazione agli UOR di competenza.
Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente illustrate.
L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle Linee Guida AgID 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 e successivamente protocollato, smistato, assegnato e gestito. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quello di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA).

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

4.2.4 Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale

Nel caso in cui il messaggio venga ricevuto su una casella di posta elettronica non istituzionale o comunque non destinata al servizio di protocollazione, il messaggio stesso viene reindirizzato al SdP. I controlli effettuati sul messaggio sono quelli sopra richiamati.

4.2.5 Ricezione di documenti informatici su supporti rimovibili

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

Nei casi in cui con un documento cartaceo siano trasmessi gli allegati su supporto rimovibile, questi devono essere in formato conforme a quanto previsto dall'allegato 2 delle Linee Guida AgID.

Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e adempimenti del caso. L'acquisizione degli allegati digitali nel sistema SdP può avvenire solo se la grandezza totale di ogni allegato non supera il limite consentito dal sistema. Gli allegati che superano tale dimensione dovranno essere riversati in file di dimensioni più piccole, ciascuno firmato digitalmente ed inserito nel SdP.

4.2.6 Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti pervenuti a mezzo posta convenzionale sono consegnati alla UOP.

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

La corrispondenza destinata nominalmente a personale dell'Istituto viene aperta e protocollata, se sono soddisfatti i requisiti di protocollazione. La corrispondenza non viene aperta qualora la busta riporti una dicitura di riservatezza come, ad esempio: "SPM", "Riservata personale" o analoga dicitura.

La corrispondenza ricevuta via telegramma, per ciò che concerne la registrazione di protocollo, è trattata come un documento cartaceo.

Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione. La corrispondenza in ingresso viene, di norma, aperta il giorno lavorativo in cui è pervenuta, protocollata (se sono soddisfatti i requisiti di protocollazione) e assegnata al destinatario tramite il SdP.

4.2.7 Errata ricezione di documenti digitali

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

4.2.8 Errata ricezione di documenti cartacei

Se la busta è indirizzata ad altro destinatario viene restituita al servizio postale che provvede ad inoltrarla all'indirizzo corretto.

4.2.9 Attività di protocollazione dei documenti

Superati tutti i controlli precedentemente descritti i documenti, digitali o analogici, sono protocollati e gestiti secondo gli standard e le modalità indicate in questo manuale al paragrafo 7.10..

4.2.10 Rilascio di ricevute attestanti la ricezione di documenti informatici

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

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

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

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

- *messaggio di annullamento di protocollazione*: un messaggio che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza;
- *messaggio di aggiornamento di protocollazione*: un messaggio che contiene una comunicazione di aggiornamento riguardante un documento protocollato ricevuto in precedenza.

4.2.11 Rilascio di ricevute attestanti la ricezione di documenti cartacei

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

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

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

- fotocopiare gratuitamente la prima pagina del documento;
- apporre gli estremi della segnatura se contestualmente alla ricezione avviene anche la protocollazione;
- apporre sulla copia così realizzata il timbro dell'Istituto, con la data e l'ora d'arrivo e la sigla dell'operatore.

La consegna diretta da parte del mittente dovrà avvenire nell'orario di apertura dell'UOP. Qualora la consegna avvenga fuori da tali orari, la ricevuta sarà inviata successivamente, tramite posta elettronica, durante l'orario di apertura dell'UOP.

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

4.2.12 Conservazione dei documenti informatici

I documenti informatici ricevuti dall'Istituto sono archiviati sui supporti di memorizzazione del SdP, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo. Tali documenti sono resi disponibili alle UOR, attraverso il SdP stesso.

4.2.13 Conservazione delle copie per immagine di documenti cartacei

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

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

Le copie per immagine dei documenti cartacei sono archiviate sul SdP, secondo le regole vigenti, in modo non modificabile al termine del processo di scansione. I documenti cartacei dopo l'operazione di riproduzione in formato immagine vengono inviati alle UOR che provvedono alla loro conservazione. Qualora si decida di distruggere l'originale cartaceo, al fine di mantenere la validità e l'efficacia probatoria garantite dal comma 1-bis dell'art. 20 del CAD, è necessario assicurarsi che il documento, trasformato in copia digitale come sopra specificato, sia stato firmato digitalmente da colui che ha effettuato l'operazione.

4.2.14 Assegnazione, presa in carico dei documenti e classificazione

Gli addetti alla UOP provvedono ad inviare il documento all'UOR, la quale:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore restituisce il documento alla UOP mittente;
- in caso di verifica positiva, esegue l'operazione di presa in carico affidandolo al RPA;
- esegue la prima classificazione (o classificazione di primo livello) del documento sulla base del titolano di classificazione in essere presso l'AOO, a meno che non sia stato fatto precedentemente.

4.2.15 Conservazione dei documenti nell'archivio corrente

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

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

4.2.16 Conservazione dei documenti e dei fascicoli nella fase corrente

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

4.3. Regole di assegnazione dei documenti

L'assegnazione dei documenti in ingresso segue le regole qui descritte.

4.3.1 Attività di assegnazione

L'assegnazione dei documenti protocollati avviene sfruttando le funzionalità supportate dal SdP che, 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 della UOR. In questa sede viene perfezionata la classificazione del documento secondo le voci del titolario.

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

L'assegnazione può essere effettuata: per conoscenza o per competenza. L'UOR competente è incaricata della gestione del procedimento a cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento amministrativo, che prende avvio dal documento, decorrono comunque dalla data di protocollazione. Il SdP memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante permette di individuare i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

4.3.2 Corrispondenza di particolare rilevanza

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto e dal canale trasmissivo utilizzato, viene inviato direttamente al Direttore.

4.3.3 Assegnazione dei documenti ricevuti in formato digitale

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

L'UOR competente ha notizia dell'assegnazione di detti documenti tramite una notifica a video che compare nella scrivania del SdP. Ogni giorno il responsabile o un operatore di ciascuna UOR è tenuto ad accedere alla scrivania del SdP al fine di verificare l'eventuale presenza di documenti assegnati.

I componenti dell'UOR sono in grado di visualizzare i documenti, attraverso le funzionalità del SdP e, in base alle abilitazioni possedute, potranno:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento.

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

4.3.4 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 alla UOR di competenza per via informatica attraverso il SdP. L'originale cartaceo riceve il seguente trattamento:

- viene acquisito in formato immagine con l'ausilio di scanner;
- viene trasmesso alla UOR per essere conservato.

I documenti cartacei gestiti dalla UOP sono di norma messi a disposizione in appositi spazi 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'UOR competente ha notizia dell'arrivo del documento ad esso indirizzato tramite una notifica a video che compare nella scrivania del SdP. Ogni giorno il responsabile o un operatore di ciascuna UOR è tenuto ad accedere alla scrivania del SdP al fine di verificare l'eventuale presenza di documenti assegnati. I componenti dell'UOR sono in grado di visualizzare i documenti, attraverso le funzionalità del SdP e, in base alle abilitazioni possedute, potranno:

- visualizzare gli estremi del documento;
- visualizzare il contenuto 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.

4.3.5 Modifica delle assegnazioni

Nel caso di assegnazione errata, l'UOR che riceve il documento comunica l'errore alla UOP, che procederà ad una nuova assegnazione.
Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

5. Criteri di rilascio delle abilitazioni di accesso al sistema documentale

5.1. Utenti interni alla AOO

Il controllo degli accessi è assicurato dall'utilizzo delle credenziali per l'accesso, costituite da UserID e password, e dal sistema di autorizzazione basato sulla profilazione degli utenti. La profilazione consente di definire le autorizzazioni rilasciate ad un utente del servizio di protocollo e gestione documentale. Queste, in sintesi, sono:

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

Le regole per la composizione delle password e il blocco delle utenze valgono sia per gli amministratori, che per gli utenti delle AOO.
Le relative politiche di composizione, aggiornamento e, in generale di sicurezza, sono configurate sui sistemi di accesso come obbligatorie tramite il SdP.
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 singola registrazione di protocollo, all'atto del suo inserimento 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'organigramma, ciascun utente può accedere solamente alle registrazioni di protocollo che sono state assegnate al suo UOR, salvo che non vi siano assegnazioni ad personam.
Il SdP consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO.
Le registrazioni di protocollo non vengono mai visualizzate dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca *full text*.

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

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

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 al SdP;
- ruoli degli utenti, gestiti dall'amministratore di ente, per la specificazione delle macro-funzioni alle quali vengono abilitati.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di addetto all'UOP e limitatamente al registro dell'AOO sul quale è stato abilitato ad operare.
L'utente assegnatario dei documenti protocollati è invece abilitato ad una vista parziale sul registro di protocollo, che comprende le sole registrazioni di protocollo assegnate a lui o alla sua UOR.
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 sulla scheda di protocollo è possibile solo all'utente a cui il protocollo è stato assegnato per competenza e al protocollatore che ha effettuato la protocollazione riservata.

6. Formato dei documenti

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

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

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. I formati utilizzati devono essere conformi a quanto specificato nell'allegato 2 alle Linee Guida AgID.
Per la produzione di documenti non è consentito l'utilizzo di formati diversi da quelli elencati nell'allegato 2 delle Linee Guida AgID.
Si adottano preferibilmente i formati PDF, XML, JPEG e TIFF. I documenti informatici redatti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard appena citati, come previsto dalle Linee Guida AgID, 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 definiti nelle Linee Guida AgID.

7. Registrazioni di protocollo informatico

7.1. Unicità del protocollo informatico

Nell'ambito della AOO il registro generale di protocollo è unico al pari della numerazione progressiva delle registrazioni di protocollo.
La numerazione progressiva si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.
Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Il numero di protocollo è costituito da almeno sette cifre numeriche.
Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.
Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.
La documentazione che non è stata registrata nel SdP viene considerata giuridicamente inesistente presso l'Istituto.
Non è consentita la protocollazione di un documento già protocollato.
Il registro di protocollo è un atto pubblico originario, che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.
Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.
Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'Istituto e tutti i documenti informatici.

7.2. Registro giornaliero di protocollo

Il SdP provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.
Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è versato, entro la giornata lavorativa successiva, al sistema di conservazione digitale a norma.

7.3. 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, 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.
Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente che ha prodotto il documento;
- il destinatario del documento;
- l'oggetto del documento;
- tutti i metadati obbligatori definiti nell'allegato 5 alle Linee Guida AgID.

Le variazioni su "oggetto", "mittente" e "destinatario" vengono mantenute con un criterio di storicizzazione dall'SdP, evidenziando data, ora e utente che ha effettuato la modifica.
Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.
I documenti informatici sono ricevuti, e trasmessi, in modo formale attraverso la casella di posta elettronica istituzionale dell'AOO.

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma.
Nel caso di documenti informatici in partenza, l'operatore esegue anche la verifica della validità amministrativa della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato automaticamente dal SdP per tutti i file allegati al messaggio di posta elettronica ricevuto, o inviato.
La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, che si può riferire sia al corpo del messaggio che ad uno dei file ad esso allegati che può assumere la veste di documento principale.
Tali documenti sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.
Le UOR provvedono direttamente alla protocollazione dei documenti in uscita, siano essi a destinazione esterna che interna.
Nel caso di corrispondenza in uscita o interna, l'UOR esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali definiti in questo manuale.
I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza.
La registrazione di protocollo di un documento cartaceo ricevuto viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.

7.4. Elementi facoltativi delle registrazioni di protocollo

Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, il RSP, con proprio provvedimento, può modificare e integrare gli elementi facoltativi del protocollo informatico.
La registrazione degli elementi facoltativi del protocollo può essere modificata, integrata e cancellata in base alle effettive esigenze della UOP o degli UOR.
In caso di necessità, i dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

7.5. Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo. La segnatura di protocollo è l'apposizione, o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.
I dati della segnatura di protocollo di un documento informatico sono attribuiti, un'unica volta nell'ambito dello stesso messaggio e stampigliati sul documento stesso. Le informazioni minime incluse nella segnatura di protocollo sono le seguenti:

- codice identificativo dell'Istituto;
- data e numero di protocollo del messaggio ricevuto o inviato;
- classificazione secondo il titolario.

La struttura ed i contenuti della segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.
La segnatura di protocollo di un documento cartaceo avviene attraverso una stampigliatura sulla quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- data e numero di protocollo del messaggio ricevuto o inviato;
- classificazione secondo il titolario.

L'operazione di segnatura dei documenti in partenza viene integralmente eseguita dalla UOR. L'operazione di acquisizione dell'immagine dei documenti cartacei si conclude con la stampigliatura della segnatura di protocollo sul file prodotto. La segnatura di protocollo viene sull'originale.

7.6. Annullamento delle registrazioni di protocollo

La necessità di modificare anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrate in forma non modificabile, per correggere errori verificatisi in sede di immissione manuale di dati, comporta l'obbligo di annullare l'intera registrazione di protocollo. Le informazioni relative alla

registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RSP. In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie.
Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto. Solo il RSP è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo. L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RSP. Analoga procedura di annullamento va eseguita quando, stante le funzioni primarie di certificazione riconosciute dalle norme alla UOP, emerge che ad uno stesso documento in ingresso, ricevuto con mezzi di trasmissione diversi quali, ad esempio originale cartaceo, email, siano stati attribuiti più numeri di protocollo.

7.7. Livello di riservatezza

Il SdP applica automaticamente il livello di riservatezza "base" a tutti i documenti protocollati. I documenti classificati come riservati sono accessibili esclusivamente dai soggetti indicati nelle ACL delle singole schede di protocollo. Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti invece che hanno un livello di riservatezza superiore lo mantengono.

7.8. Casi particolari di registrazioni di protocollo

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

7.8.1 Circolari e disposizioni generali

Gli ordini di servizio, di norma, non vengono protocollati. Le circolari ricevute vengono protocollate nel registro ufficiale di protocollo. Le disposizioni generali e tutte le altre comunicazioni interne, di norma, si registrano con un solo numero di protocollo nel registro di protocollo interno.

7.8.2 Documenti cartacei in uscita con più destinatari

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

7.8.3 Documenti cartacei ricevuti a mezzo telegramma

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

7.8.4 Protocollazione di un numero consistente di documenti cartacei

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

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

La corrispondenza ricevuta con rimessa diretta dall'interessato, o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo. Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta. Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, gli stessi saranno accantonati e protocollati successivamente. In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

7.8.6 Fatture, assegni e altri valori di debito o credito

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

7.8.7 Protocolli urgenti

La richiesta di protocollare urgentemente un documento è collegata ad una necessità indifferibile e di tipo straordinario. Solo in questo caso il RSP si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale,

o cartaceo, da spedire. Tale procedura viene osservata sia per i documenti in ingresso che per quelli in uscita.

7.8.8 Documenti non firmati

L'operatore di protocollo, conformandosi alle regole stabilite dal RSP attesta la data, la forma e la provenienza per ogni documento. Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "mittente sconosciuto o anonimo" e "documento non sottoscritto". Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali. È poi compito dell'UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

7.8.9 Protocollazione dei messaggi di posta elettronica ordinaria

Considerato che il sistema di posta elettronica ordinaria 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.

7.8.10 Protocollazione di documenti 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.

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".

7.8.11 Copie per conoscenza

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

7.8.12 Differimento delle registrazioni

Le registrazioni di protocollo dei documenti pervenuti presso l'AOO destinataria sono, di norma, effettuate nella giornata di arrivo e comunque non oltre le 48 ore dal ricevimento di detti documenti. Qualora nei tempi sopra indicati non possa essere effettuata la registrazione di protocollo si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del RSP, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti. Il protocollo differito consiste nel rinvio dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento sopra citato.

7.8.13 Corrispondenza personale o riservata

La corrispondenza destinata nominalmente a personale dell'Istituto viene aperta e protocollata, se sono soddisfatti i requisiti di protocollazione. La corrispondenza non viene aperta qualora la busta riporti una dicitura di riservatezza come, ad esempio: "SPM", "Riservata personale" o analoga dicitura. Se il destinatario reputa che i documenti ricevuti devono essere comunque protocollati perché riguardano problematiche istituzionali, provvede a trasmetterli alla UOP per la protocollazione.

7.8.14 Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento e gli eventuali allegati. Tale verifica spetta al responsabile del procedimento amministrativo (RPA) che, qualora reputi necessario

acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento. I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel relativo fascicolo.

7.9. Registrazioni di protocollo

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono effettuate attraverso il SdP. Il sistema di sicurezza dell'Istituto garantisce la protezione di tali informazioni sulla base della relativa architettura tecnologica, sui controlli d'accesso e i livelli di autorizzazione realizzati.

7.9.1 Attribuzione del protocollo

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il SdP appone al documento protocollato una segnatura, come previsto dalla normativa vigente. Il SdP assicura l'esattezza del riferimento temporale contenuto nella segnatura con l'acquisizione periodica del tempo ufficiale di rete. Come previsto dalla vigente normativa in materia di protezione dei dati personali le UOR aderenti al SdP sono informate della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo.

7.9.2 Registro informatico di protocollo

Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo generale della AOO, il SdP provvede, entro il giorno lavorativo successivo alla chiusura dell'attività giornaliera di protocollo, ad effettuare la trasmissione della stampa del registro giornaliero di protocollo, in formato PDF, al sistema di conservazione digitale a norma. I meccanismi di conservazione a norma permettono di conferire validità e integrità ai contenuti del file del registro di protocollo.

È inoltre disponibile per le UOP del SdP una funzione applicativa di "Stampa registro di protocollo".

7.9.3 Modalità di utilizzo del registro di emergenza

Il RSP assicura che, ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura informatica del SdP, le operazioni di protocollo siano svolte sul registro di emergenza informatico su postazioni di lavoro operanti fuori linea. Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il RSP imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare. Sul registro di emergenza sono riportate: la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.

La numerazione progressiva del registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno. Qualora nel corso di un anno il registro di emergenza non venga utilizzato, il RSP annota sullo stesso il mancato uso. Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite sul registro di protocollo generale. Il registro di emergenza si configura come un repertorio del protocollo generale. Le registrazioni effettuate sul registro di emergenza vengono recuperate ed inserite nel SdP al momento del suo ripristino. Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione sono associati anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza. Al fine di ridurre la probabilità di commettere errori in fase di trascrizione dei dati riportati dal registro di emergenza a quello del protocollo generale e di evitare la duplicazione di attività di inserimento, le informazioni relative ai documenti protocollati in emergenza, su una o più postazioni di lavoro dedicate della AOO, sono inserite nel sistema informatico di protocollo generale utilizzando un'apposita funzione automatica.

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.

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro, il numero totale di operazioni registrate. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO. Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono gli stessi previsti dal protocollo generale.

7.10. Tipologie documentali escluse dalla registrazione di protocollo

Secondo quanto prescritto dal comma 5 dell'art. 53 del DPR 445/2000, sono esclusi dalla registrazione di protocollo: le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari e tutti i documenti già soggetti a registrazione particolare dell'amministrazione.

8. Sistema di classificazione, fascicolazione e piano di conservazione

8.1. Protezione e conservazione degli archivi pubblici

Il sistema di classificazione dei documenti, di formazione del fascicolo e di conservazione dell'archivio definisce i tempi e le modalità di aggiornamento, i criteri e le regole di selezione e scarto della documentazione, anche con riferimento all'uso di supporti sostitutivi e di consultazione e movimentazione dei fascicoli.
La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (titolario), cioè di quello che si suole definire "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti".
Il titolario e il piano di conservazione sono predisposti, verificati e confermati antecedentemente all'avvio delle attività di protocollazione informatica e di archiviazione, considerato che si tratta degli strumenti che consentono la corretta formazione, gestione e archiviazione della documentazione dell'Istituto. Il titolario e il piano di conservazione sono stati adottati dall'Istituto con atti formali.
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 ed interni) 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 Soprintendenza Archivistica e Bibliografica della Toscana. L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della suddetta Soprintendenza. Lo scarto dei documenti dell'archivio in parola è subordinato all'autorizzazione della Soprintendenza sopra citata. 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 analogici.

8.2. Titolario o piano di classificazione

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'Istituto. Il piano di classificazione si suddivide in titoli, classi, sottoclassi, dette anche voci di I livello, II livello, III livello. Il titolo individua funzioni primarie e di organizzazione dell'Istituto; le successive partizioni, classi e sottoclassi, corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato. Titoli, classi, sottoclassi sono nel numero prestabilito dal Titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del vertice dell'Istituto.
Il Titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'Istituto, soggette a modifiche in forza delle leggi e dei regolamenti statali.

L'aggiornamento del Titolario compete esclusivamente al vertice dell'Istituto, su proposta del RSP. La revisione, anche parziale, del Titolario viene proposta dal RSP quando 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. Il SdP garantisce la storicizzazione delle variazioni di Titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del Titolario vigente al momento della produzione degli stessi. Per ogni specifica voce viene riportata la data di inserimento e la data di variazione. Di norma le variazioni vengono introdotte a partire dal 1 gennaio dell'anno successivo a quello di approvazione del nuovo Titolario e hanno durata almeno per l'intero anno. Rimane possibile, se il sistema lo consente, di registrare documenti in fascicoli già aperti fino alla conclusione e alla chiusura degli stessi. Il Titolario è stato elaborato da un gruppo di lavoro appositamente costituito all'interno dell'AOO ed è stato approvato con delibera del Consiglio di Amministrazione dell'Istituto n. 36 del 28 luglio 2021, dopo preliminare verifica da parte della Soprintendenza Archivistica e Bibliografica della Toscana.
La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO. Essa è eseguita 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), il titolo del fascicolo ed eventualmente del sottofascicolo. Le operazioni di classificazione vengono svolte interamente dagli UOR.

8.3. Fascicolazione dei documenti

Tutti i documenti registrati nel SdP, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli. Ogni documento, dopo la classificazione, viene inserito nel fascicolo di riferimento. I documenti sono archiviati all'interno di ciascun fascicolo e all'occorrenza sottofascicolo.
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);
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'AOO;
- data di apertura del fascicolo;
- AOO e UOR;
- collocazione fisica, di eventuali documenti cartacei;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Il fascicolo viene chiuso al termine del procedimento amministrativo o con l'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto. Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.
Quando un nuovo documento viene recapitato all'AOO, l'UOR abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se il documento stesso debba essere ricollegato ad un affare o procedimento in corso e pertanto debba essere inserito in un fascicolo già esistente oppure se il documento si riferisce a un nuovo affare, o procedimento, per cui è necessario aprire un nuovo fascicolo. A seconda delle ipotesi, si procede come segue:

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

Quando si verifica un errore nell'assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'UOR di competenza. Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando, per ciascuno di essi, l'identificativo dell'operatore che effettua la modifica, con la data e l'ora dell'operazione.

8.4. Repertorio dei fascicoli

I fascicoli sono annotati nel repertorio dei fascicoli. Il repertorio dei fascicoli, ripartito per ciascun titolo del Titolario, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio rispecchia quella del Titolario di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo. Mentre il Titolario rappresenta in astratto le funzioni e le competenze che l'Ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività. Il repertorio dei fascicoli è costantemente aggiornato.

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

La richiesta di consultazione, e di conseguenza di movimentazione dei fascicoli, può pervenire dall'interno dell'Istituto, oppure da utenti esterni all'Istituto, per scopi giuridico amministrativi o per scopi storici.
Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15, che qui si intende integralmente richiamato.

8.5.1 Consultazione da parte di utenti esterni all'Istituto

La domanda di accesso ai documenti viene presentata al servizio archivistico che provvede a richiederne la protocollazione alla UOP. Le richieste di accesso ai documenti della sezione storica dell'Archivio possono essere inoltrate anche dai Tribunali per i minorenni.
Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale. In tal caso il responsabile del servizio archivistico provvede a rilasciare una copia conforme semplice o una trascrizione dell'intero documento o di una parte dello stesso. Il rilascio di copie dei documenti dell'archivio avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'Istituto.
I documenti riguardanti il diritto all'anonimato delle partorienti potranno essere consultati solo dopo 100 anni dalla loro formazione, come previsto dalle norme vigenti.
L'ingresso all'archivio di deposito, e storico, è consentito solo agli addetti del servizio archivistico. La consultazione dei documenti è possibile esclusivamente sotto la diretta sorveglianza del personale addetto all'interno dell'apposita sala di consultazione. In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione.

8.5.2 Consultazione da parte di personale interno all'Istituto

Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito, o storica.
L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito, o storico, ad un ufficio del medesimo UOR, od altro UOR, avviene solamente per il tempo strettamente necessario all'esaurimento di un affare o di un procedimento amministrativo.
Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, il suo UOR e la sua firma. Un esemplare della richiesta di consultazione viene conservata all'interno del fascicolo, un altro nella posizione fisica occupata dal fascicolo in archivio.
Tale movimentazione viene registrata a cura del responsabile del servizio archivistico in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna e quella di restituzione, nonché eventuali note sullo stato della documentazione, in modo da riceverla nello stesso stato in cui è stata consegnata. Il responsabile del servizio archivistico verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista. L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine degli stessi, rispettandone la sedimentazione archivistica e il vincolo. Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'AOO. In ogni caso, deve essere garantito

l'accesso conformemente a criteri di salvaguardia dei dati, dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

9. Misure di sicurezza e protezione dei dati personali

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.

9.1. Il piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dall'AOO sono disponibili, integre e riservate;
- i dati personali comuni, particolari e 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.

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

Il piano di sicurezza:

- si articola, di conseguenza, in due componenti: una di competenza del SdP, una di competenza della AOO;
- si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e i documenti trattati, rispettivamente, nei locali dove risiedono le apparecchiature utilizzate dal SdP e nei locali della AOO;
- si fonda sulle direttive strategiche di sicurezza stabilite;
- definisce:
    - le politiche generali e particolari di sicurezza da adottare all'interno, rispettivamente, del SdP e della AOO;
    - le modalità di accesso al SdP;
    - gli aspetti operativi della sicurezza, con particolare riferimento alle misure minime di sicurezza, di cui al GDPR (Regolamento UE 679/2016);
    - i piani specifici di formazione degli addetti;
    - le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione formale con cadenza almeno biennale. Esso può essere modificato a seguito di eventi gravi. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il SdP, saranno conservati secondo le vigenti norme e saranno consultati solo in caso di necessità.

9.2. Sicurezza dei documenti informatici

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

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

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Istituto e gli atti dallo stesso 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 protezione dei dati personali;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

9.3. Componente organizzativa della sicurezza

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte per l'erogazione del SdP. Il SdP è erogato da server presenti all'interno dell'infrastruttura informatica dell'Istituto.
All'interno dell'Istituto, l'erogazione dei servizi individua le seguenti figure:

- responsabile dei servizi di Information & Communications Technology;
- responsabile della sicurezza;
- responsabile della tutela dei dati personali;
- internai auditor;
- operatore dei sistemi ICT.

9.4. Componente fisica della sicurezza

Gli utenti esterni devono esplicare la procedura di registrazione per l'ingresso nei locali dell'Istituto.
Il controllo degli accessi fisici alle risorse ICT dell'Istituto è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;
- i visitatori occasionali devono essere accompagnati da personale ICT;
- ogni persona che accede alle risorse della sede in locali protetti è identificata in modo certo; gli accessi alla sede sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;
- il personale dell'Istituto ha l'obbligo di utilizzare il badge sia in ingresso che in uscita dalla sede.

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 locale, sono finalizzate a controllare l'accesso ai locali interni alla sede.

Il controllo degli accessi fisici alle risorse della sede dell'Istituto è regolato secondo i principi stabiliti dall'apposita UO dell'Istituto.

9.5. Componente logica della sicurezza

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente, nell'ambito del SdP, è stata realizzata attraverso:

- l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico:
  - identificazione, autenticazione ed autorizzazione degli addetti della AOO e degli operatori dell'erogatore del SdP;
  - riservatezza dei dati;
  - integrità dei dati;
  - integrità del flusso dei messaggi;
  - non ripudio dell'origine (da parte del mittente);
  - non ripudio della ricezione (da parte del destinatario);
  - audit di sicurezza;
- il ripristino in caso di guasto 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 della AOO, 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.

Il SdP ha al suo interno un sistema di identificazione, autenticazione e autorizzazione proprio, che mette in pratica i requisiti di sicurezza sopra richiamati.

9.6. Componente infrastrutturale della sicurezza

Presso la sede dell'Istituto sono disponibili i seguenti impianti:

- antincendio;
- rilevamento dell'allagamento nelle zone critiche rispetto a questa minaccia;
- luci di emergenza;
- continuità elettrica nelle zone critiche rispetto a questa minaccia;
- controllo degli accessi e dei varchi fisici.

Essendo la sede dell'Istituto lontana da insediamenti industriali e posta 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.

9.7. Gestione delle registrazioni di protocollo e di sicurezza

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

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

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 SdP sono elaborate tramite procedure automatiche dal sistema di autenticazione e di autorizzazione in esso contenuti;
- i supporti con le registrazioni di sicurezza sono conservati in locali ad accesso controllato;
- i log di sistema sono accessibili ai sistemisti in sola lettura al fine di impedirne la modifica;
- l'operazione di scrittura delle registrazioni del SdP è effettuata direttamente dall'applicativo;
- le registrazioni sono soggette a più copie giornaliere di salvataggio;
- il periodo di conservazione delle registrazioni è conforme alla normativa vigente in materia.

9.8. Sicurezza nella trasmissione di documenti informatici

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario. Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre AOO, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.
Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'AOO, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

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

Lo scambio per via telematica di messaggi protocollati tra AOO diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali come previsto dal GDPR (Regolamento UE 679/2016). 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.
Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture. Gli uffici organizzativi di riferimento (UOR) dell'AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica in attuazione di quanto previsto dalla Direttiva del Ministro per l'innovazione e le tecnologie del 18 novembre 2005, concernente l'impiego della posta elettronica nelle pubbliche amministrazioni.

9.9. Interoperabilità dei sistemi di protocollo informatico

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).
Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete. Il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi. La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal CAD.

10. Conservazione dei documenti

La conservazione dei documenti informatici avviene sulla base delle disposizioni riportate nelle Linee Guida AgID e in osservanza a quanto definito nel manuale di conservazione del conservatore che eroga il servizio di conservazione a norma. 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 Linee Guida AgID vigenti.

10.1. Servizio archivistico

Il responsabile del sistema archivistico dell'Istituto ha individuato nei locali al piano terra della sede istituzionale dell'Istituto e negli armadi in essi ubicati la sede dell'archivio storico dei documenti analogici. L'archivio di deposito è ubicato nei locali sotterranei dell'Istituto. Il responsabile del servizio in argomento ha effettuato la scelta, in accordo con il Servizio Patrimonio dell'Istituto, alla luce dei vincoli logistici imposti dall'edificio e della valutazione dei fattori di rischio che incombono sui documenti. Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio, in accordo con il Servizio Patrimonio dell'Istituto, ha adottato un piano di sicurezza dettagliato e documentato che individua i soggetti incaricati delle attività preventive e di quelle di mitigazione delle conseguenze di situazioni di emergenza. 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 e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.

10.2. Conservazione del registro di protocollo

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione a norma, 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. Tali modalità sono riportate nel manuale di conservazione del conservatore che eroga il servizio di conservazione a norma.
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 gli eventuali annullamenti occorsi.
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.
I metadati da inviare in conservazione unitamente alla copia del registro di cui sopra sono quelli definiti come obbligatori dall'allegato 5 alle Linee Guida AgID.
All'avvio del processo di creazione del pacchetto di versamento vengono elaborati i dati presenti nel registro di protocollo con segnalazione di eventuali anomalie durante il flusso. Il trasferimento del Pacchetto di versamento al sistema di conservazione avviene tramite canale WebServices. Al riguardo è previsto un processo automatico che si occupa di creare il pacchetto di versamento, inviarlo al sistema di conservazione e registrare lo stato del versamento stesso. Il processo provvede ad estrarre dal SdP 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.

11. Approvazione e aggiornamento di questo manuale

L'Istituto 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 dal RSP.

Con l'entrata in vigore del presente manuale sono annullati tutti i regolamenti interni all'AOO nelle parti contrastanti con lo stesso.
Il presente manuale è disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento. Copia del presente manuale è

- fornita a tutto il personale dell'AOO mediante la rete intranet;
- pubblicata sul sito istituzionale dell'Istituto.

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