PROCURA GENERALE DI TRIESTE

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEI DOCUMENTI E DEGLI ARCHIVI

INDICE

3. GESTIONE DEI FLUSSI DOCUMENTALI

3.1 Flussi documentali in ingresso
3.2 Flussi documentali in uscita

4. CLASSIFICAZIONE, FASCICOLAZIONE E ARCHIVIAZIONE DEI DOCUMENTI

4.1 Caratteristiche generali
4.2 Piano di classificazione e titolario
4.3 Accesso al patrimonio documentale
4.4 Accesso esterno al patrimonio documentale

5. PIANO DELLA SICUREZZA

5.1 Elementi di rischi cui sono soggetti i documenti informatici ed i dati contenuti nel sistema di protocollo
5.2 Requisiti minimi di sicurezza applicativa
5.3 Sicurezza delle reti di accesso al servizio
5.4. Accesso a SdP da parte di utenti interni all'AOO
5.5. Formazione e sottoscrizione dei documenti
5.6 Sicurezza delle registrazioni di protocollo
5.7 Backup e ripristino dell'accesso dei dati
5.8 Trascrizione e interscambio dei documenti
5.9 Piani formativi del personale
5.10 Monitoraggio periodico dell'efficacia delle misure di sicurezza

ATTO DI PPROVAZIONE

ALLEGATI

1. Titolario
2. Provvedimento di nomina figure di sistema

1. DISPOSIZIONI GENERALI

1.1 Premessa

Il presente documento costituisce il Manuale di gestione del protocollo informatico e del sistema documentale della Procura Generale di Trieste ed è redatto in conformità a quanto stabilito dalla normativa di riferimento, in particolare:

- articolo 2, comma 2, Codice dell'Amministrazione Digitale;
- par. 3.5 delle Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici, e 7 allegati tecnici, pubblicate in data 11 settembre 2020;
- articoli. 2,6, 9, 20 e 21 del DPCM 3 dicembre 2013 contenente le "Regole tecniche per il protocollo informatico";
- determinazione n. 371/2021, Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici;

Il Manuale di gestione descrive il sistema di gestione anche ai fini della conservazione dei documenti informativi e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50 del testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000).

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

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

Una volta adottato, il Manuale viene aggiornato periodicamente, in virtù del costante censimento e della progressiva razionalizzazione delle attività e delle prassi in essere, dell'individuazione e della definizione di nuovi aspetti organizzativi e gestionali, anche nel rispetto della normativa eventualmente sopraggiunta.

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

1.2 Ambito di applicazione

Il presente manuale di gestione del protocollo dei documenti e degli archivi è adottato ai sensi dell'articolo 3, comma 1, lett. d) del decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 recante le "Regole tecniche per il protocollo informatico".

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi della procura Generale di Trieste.

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

1.3. Norme di riferimento

- Testo Unico, il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445, Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA);
- Codice, il decreto legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione digitale (CAD);
- Regole Tecniche, il decreto del Presidente del Consigli dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico", artt. 2,6 ,9, 18, 20, 21;
- Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici pubblicate in data 11 settembre 2020;
- Determinazione n. 371/2021, Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici;

1.4. Definizioni

Ai fini del presente manuale, s'intende per:
Amministrazione: Procura Generale di Trieste;

Archivio digitale: il processo di memorizzazione su qualsiasi supporto di documenti digitali, anche informatici univocamente identificati mediante un codice di riferimento;

Archivio corrente: il complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussiste un interesse attuale;

Archivio di deposito: la parte di documentazione relativa a procedimento conclusi non più occorrenti quindi alla trattazione dell'attività in corso, ma non ancora destinata istituzionalmente alla conservazione permanente;

Archivio storico: il complesso di documenti selezionai per la conservazione permanente;

Area organizzativa omogenea (AOO): un insieme di funzioni e di strutture individuate che opera su tematiche omogenee e che presenta esigenza di gestione della documentazione in modo unitario e coordinato;

Assegnazione di un documento: l'individuazione dell'ufficio competente per la trattazione del procedimento amministrativo, cui i documenti si riferiscono;

Classificazione: l'attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati;

Documento amministrativo: ogni rappresentazione, comunque formata, del contenuto di atti, fatti o dati giuridicamente rilevanti anche interni, prodotto o acquisiti dall'Amministrazione o comunque utilizzati ai fini dell'attività amministrativa;

Documento analogico; un documento che può essere creato sia manualmente, sia con l'utilizzo di strumenti informatici in forma cartacea;

Documento informatico: qualsiasi supporto informatico contenente dati o informazioni aventi efficacia probatoria, cioè la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

Fascicolo: l'insieme ordinata di documenti che può fare riferimento ad uno stesso procedimento o ad una stessa materia o ad una stessa tipologia documentaria che si forma nel corso delle attività amministrative, allo scopo di riunire, ai fini decisionali o informativi, tutti i documenti utili allo svolgimento di tali attività;

Fascicolo informatico: l'aggregazione strutturata e univocamente identificata di atti, dati informatici prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento;

Firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica ed una privata, correlate tra loro che consente al titolare tramite la chiave privata ed al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti;

Gestione informatica dei documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonchè alla classificazione organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formali o acquisiti dall'Amministrazione, nell'ambito del sistema di classificazione adottato, effettuate mediante sistemi informatici;

Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (RSP), il dirigente o il funzionario in possesso di requisiti professionali o di professionalità tecnico-archivistica, dedicato al servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi;

Sistema di conservazione: il sistema di conservazione dei documenti informatici;

Servizio di protocollo informatico (SdP): l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dall'amministrazioni per la gestione dei documenti, ovvero tutte le risorse tecnologiche necessarie alla realizzazione di un sistema automatico dei documenti (DPR n. 445/2000);

Titolario di classificazione: un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base delle competenze della Procura Generale, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la sedimentazione secondo un ordine logico che rispetti storicamente lo sviluppo dell'attività svolta.

1.5 Aree Organizzative Omogenee

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

Tutte le strutture dell'Amministrazione comprese nella AOO devono utilizzare il presente manuale ed adeguare alle prescrizioni ivi contenute le procedure e le attività di loro competenza:

1.6 Figure di sistema e loro compiti

Questa AOO individua, con dedicato atto di nomina del Capo dell'Ufficio, successivamente trasmesso al Direttore Generale per i sistemi informativi automatizzati, le figure i cui compiti sono specificati nei paragrafi successivi;

- il responsabile di AOO del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (RSP);
- l'amministratore di AOO e suo vicario;
- referente per la gestione delle PEC e PEO e suo vicario

1.7 Responsabile della gestione documentale (RSP)

Compiti del RSP sono:

- presidiare la puntuale attuazione del presente Manuale;
- predisporre lo schema di Manuale di gestione di AOO, contenente regole integrative e/o attuative del Manuale;
- provvedere alla pubblicazione del Manuale sul sito istituzione della propria AOO;
- profilare i necessari utenti da inserire nel Servizio di Prococollo (SdP), inserendo per ciascuno di essi le funzioni più appropriate tra quelle disponibili;
- curare l'aggiornamento sul SdP dell'organigramma e affidare all'amministratore di AOO l'esecuzione operativa della modifica;
- presidiare il rispetto delle disposizioni normative inerenti alle operazioni di protocollo;
- organizzare la tenuta della copia del registro giornaliero di protocollo;
- autorizzare le operazioni di annullamento della registrazione di protocollo così come indicato dal manuale di AOO;
- disporre l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza secondo quanto previsto nel paragrafo 2.6;
- indicare tempi, modalità, misure organizzative e tecniche per l'eliminazione dei protocolli settoriali e dei relativi registri, specie se ancora cartacei;

1.8 Amministratore di AOO

E' la figura operativa di supporto al responsabile della gestione documentale (RSP).

Compiti dell'Amministratore di AOO sono:

- manutenere ed aggiornare gli elementi costitutivi di ciascuna AOO: registri, titolario di archivio, liste di competenza, uffici e utenti dell'AOO, rubriche ecc.;
- assicurare l'inserimento nel SdP degli utenti individuati dl RSP secondo il profilo e le funzioni secondo quanto stabilito dal Manuale di AOO;

- verificare in caso di cessazione dal servizio o trasferimento ad altro uffici di un utente del sistema di protocollo, che lo stesso abbia classificato tutti i documenti a suo carico o assegnare gli stessi ad altro utente e poi provvedere alla chiusura dell'utenza;
- formalizzare all'RSP la richiesta di abilitazione al servizio qualora formulata dai singoli utenti;
- monitorare il rispetto delle disposizioni inerenti al protocollo;
- garantire operativamente la conservazione della copia del registro giornaliero di protocollo secondo termini e modalità specificati dal RSP;
- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;
- curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza in attuazione delle disposizioni del RSP;
- supportare la redazione del Manuale di AOO;
- supportare il RSP nell'adozione delle misure organizzative e tecniche per l'eliminazione dei protocolli settoriali e relativi registri.

1.9 Referente per la PEC e la PEO istituzionali

E' la figura operativa di supporto.
Compiti del Referente sono:

- monitorare la gestione dei punti unici di accesso documentale gestiti a mezzo posta elettronica certificata e ordinaria;
- stimolare l'attuazione delle disposizioni normative e regolamentari vigenti in materia;
- disporre tempi, termini e modalità di gestione delle password di accesso alle caselle di posta non integrate egli applicativi ministeriali, oggetto di presidio e monitoraggio da parte dell'AOO, se non da altri gestiti (ad es. GSI)

2. PROTOCOLLAZIONE E REGISTRAZIOEN DEI DOCUMENTI

2.1 Il Protocollo informatico

L'Amministrazione avendo individuato una sola AOO, adotta un unico sistema di protocollo informatico.
.La numerazione delle registrazioni di protocollo è unica e progressiva, essa comincia il 1° gennaio e si chiude al 31 dicembre di ogni anno.
Tutti gli atti e documenti prodotti o ricevuti dall'AOO fanno parte del sistema documentale fanno parte del sistema documentale digitale dell'Amministrazione e sono protocollati in modalità informatica, nei versi di ingresso, interno ed uscita, secondo le norme sul protocollo informatico e sono conservati secondo la normativa vigente (art. 40bis CAD, art. 53 TU, DPCM 3 dicembre 2013, Regola Tecniche sul Protocollo Informatico).
Tutti gli atti e documenti analogici che entrano nel sistema documentale sono riprodotti in documenti informatici al fine di essere protocollati e conservati in modalità digitale.
Tramite il registro di protocollo è possibile registrare ufficialmente l'esistenza di un documento all'interno dell'AOO e tenere traccia delle sue movimentazioni.

2.2 Casella di Posta elettronica istituzionale

La comunicazione esterna istituzionale avente valore legale è gestita a mezzo una casella di posta elettronica certificata (PEC) istituzionale: prot.pg.trieste@giustiziacert.it;, integrata nel sistema di protocollo informatica e fornita dal Ministero della Giustizia. Tale casella costituisce il domicilio digitale dell'Amministrazione ex art. 6, c. 1 del Codice dell'Amministrazione Digitale.

2.3 Firme digitale

Il dirigente di quest'Amministrazione, a seconda delle competenze e delle necessità organizzative, ha dotato il personale di CNS per la sottoscrizione digitale di documenti atti inerenti all'espletamento delle attività istituzionali, ai processi, nonchè alla normativa relativa alla gestione dei documenti informatici.

I formati relativi alle firme elettroniche avanzate utilizzate per la firma sono i seguenti:

- **CADES**: è una firma digitale che può esser apposta su qualsiasi tipo di file generando una busta crittografica contenente il documento informativo originale e caratterizzata dal suffisso P7M che si aggiunge all'estensione del file;
- **PADES**: è una firma che può esser apposta solo su file PDF e in tal caso, l'apposizione prevalentemente nel caricamento di dati su piattaforma gestite da altre PP.AA. E da utilizzarsi in tutte le comunicazioni ordinarie aventi rilevanza esterna od interne.

Le firme digitali servono a:

- fissare la paternità dell'atto;
- autenticare la firma autografa di terzi;
- attestare la conformità di una copia originale;

2.4 Il sistema dei registri

Nell'Amministrazione sono presenti i seguenti registri:

il registro ufficiale di protocollo per registrare le comunicazioni ricevute e spedite dall'Amministrazione;

il registro di protocollo di emergenza, da attivare in caso di indisponibilità tecnica del di sistema di protocollo;

il registro interno utilizzato per tracciare le comunicazioni che si volgono tra strutture interne all'AOO.

2.5 Il registro ufficiale di protocollo

Ai sensi dell'art. 53 del TUDA, sono soggetti alla registrazione sul registro ufficiale di protocollo tutti i documenti in ingresso ed in uscita.

Il numero di protocollo attribuito dal sistema informatico individua un unico documento ed i suoi eventuali allegati e, di conseguenza, ogni documento reca un solo numero di protocollo.

Non è consentita l'attribuzione manuale di numero di protocollo.

Non è possibile attribuire ad un documento un numero già attribuito dal sistema informatico ad altri documenti anche se questi documenti sono strettamente correlati fra loro.

Di conseguenza, non è ammessa la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in entrata e per il documento in uscita, né tantomeno è consentita l'assegnazione di un solo numero di protocollo alla ricezione di una gran mole di documenti simili in risposta, ad esempio, ad un avviso di bando pubblico.

In caso di necessità di inviare più documenti è possibile procedere o con protocollazione singola di ciascuna istanza, o co protocollazione di una sola nota di trasmissione corredata delle istanze di cui trattasi.
Il protocollo serve ad attribuire ad un determinato documento data, forma e provenienza certa attraverso la registrazione di alcuni elementi rilevanti sul piano giuridico-probatorio e quindi è necessario ricordare le seguenti informazioni:

- data di registrazione, assegnata automaticamente dal sistema e registrata in forma non modificabile, corrispondente alla data del giorno in cui avviene la registrazione;
- numero di protocollo generato automaticamente dal sistema e registrato in forma non modificabile;
- mittente per il documento in arrivo, destinatario per il documento in partenza;
- oggetto del documento;
- data e numero di protocollo del documento ricevuto se disponibili;
- impronta di simboli binari in grado di identificare univocamente il contenuto, registrata in forma non modificabile

2.6. Il registro di emergenza

Il responsabile della gestione della gestione della conservazione autorizza eccezionalmente lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo sul registro di emergenza ogni qual volta per cause tecniche non sia possibile utilizzare il sistema.
In condizioni di emergenza si applicano le modalità di registrazione e di recupero dei dati descritte nell'art. 63 del TUDA, e precisamente:

- sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione, nonchè la data e l'ora del ripristino della funzionalità del sistema;
- qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre 24 ore, per cause di eccezionale gravità, il responsabile del servizio può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione;
- per ogni giornata di registrazione di emergenza è riportata sul registro di emergenza il numero totale di operazioni registrate;
- la sequenza numerica utilizzata su un registrato di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO;
- le informazioni relative ai documenti protocollarti in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dati, senza ritardo rispetto al ripristino delle funzionalità del medesimo. Durante la fase di ripristino, a ciascuno documento registrato in emergenza, viene attributo un numero di protocollo dal sistema informatico ordinario, che provvede a mantenere stabilmente la correzione con il numero utilizzato in emergenza.

Per l'avvio dei termini dei provvedimenti amministrativi relativi ai documenti così registrati, si fa riferimento alla data di effettiva ricezione.

2.7 Il registro interno

Il registro interno è utilizzato per registrare i documenti scambiati interamente aventi valore giuridico-probatorio nell'ambito dei procedimenti tra strutture interne (ordini di servizio, comunicazioni tra uffici interni, comunicazione al personale ecc.) dell'AOO e non destinati all'invio a soggetti esterni all'AOO stesso.
Il numero di registrazione e la data di registrazione sono attribuiti in automatico dal sistema; la numerazione progressiva delle registrazioni interne è unica e separata dal protocollo generale e si chiude al 31 dicembre di ogni anno e ricomincia dal 1° gennaio dell'anno successivo.

2.8 Il protocollo riservato

Sono previste particolari forme di riservatezza e di visibilità limitata (accesso controllato al protocollo) per:
a) documenti legati a vicende di persone o a fatti privati e particolari individuati dalla normativa vigente in merito alla tutela dei dati personali;
b) documenti di carattere politico e d'indirizzo, di competenza della segreteria della Presidenza, che, se trattati con i mezzi ordinari, potrebbero ostacolare il raggiungimento degli obiettivi prefissati individuati caso per caso;
c) documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi.
La funzionalità che permette di limitare l'accesso e ridurre la visibilità della registrazione è utilizzata dalle segreterie dell'AOO, responsabili del procedimento a cui tale documento si riferisce, con livelli di accesso stabiliti caso per caso.

Le procedure adottate per la gestione dei documenti e dei procedimenti amministrativi ad accesso riservato, comprese la protocollazione, la classificazione e la fascicolazione, sono le stesse adottate per gli altri documenti e procedimenti amministrativi, ad eccezione della scansione ottica (documento in arrivo) o dell'associazione del file (documento in partenza) che, non saranno effettuate a meno di espresse deroghe.
I documenti dell'archivio riservato divengono consultabili alla scadenza dei termini stabiliti dal dirigente responsabile e comunque potranno essere accolte prima della scadenza dei termini in applicazione della legge in vigore in materia di accesso agli atti amministrativi.

2.9 Protocollazione differita

Nel caso in cui non sia possibile procedere alla registrazione di protocollo nel giorno di ricevimento, ad es. per un eccezionale e imprevisto carico di lavoro, per una ricezione in chiusura dell'ufficio, e qualora dalla mancata registrazione del documento nel medesimo giorno possa venire meno n diritto di terzi, è possibile effettuare la registrazione differita di protocollo.
Il protocollo differito consente la normale registrazione a protocollo con l'evidenza della data effettiva di ricevimento. E'possibile esclusivamente per i documenti in attivo cui si possa inequivocabilmente associare la data di ricevimento e non si applica per i documenti informatici pervenuti via PEC essendo questi corredati delle ricevute e delle notifiche di accettazione e consegna che attestano la data certo di ricevimento dell'atto.
La richiesta di differimento va trasmessa al RSP completa di indicazioni d sulla nota in questione e sulla motivazione per la quale l'operazione sarebbe opportuna.
Nessun operatore può annullare in autonomia protocolli se non è pervenuta l'autorizzazione del suddetto RSP.

2.10 Protocolli urgenti

La protocollazione di atti avviene di norma secondo l'ordine cronologico di arrivo nella disponibilità delle risorse deputate al servizio.
La richiesta di differimento va trasmessa al RSP completa di indicazioni d sulla nota in questione e sulla motivazione per la quale l'operazione sarebbe opportuna.
Nessun operatore può annullare in autonomia protocolli se non è pervenuta l'autorizzazione del RSP.

2.11 Il registro giornaliero di protocollo

Le Linee Guida di cui in premessa prevedono la formazione del registro giornaliero di protocollo che può essere considerato come una sorta di rendicontazione, in quanto in esso devono essere riportate le registrazioni di tutti di documenti in entrata ed in uscita, mediante raggruppamento anche in via automatica di un insieme di dati o registrazioni secondo una struttura logica predeterminata e memorizzata in forma statica.
Nel registro devono essere riportate le informazioni fondamentali quali il numero di protocollo del documento, la data di registrazione di protocollo, il mittente per i documenti ricevuti ed il destinatario per i documenti inviati, l'oggetto del documento, la data e protocollo del documento ricevuto, l'impronta del documento informatico, se trasmesso per via telematica, l'indicazione del registro nel quale è stata effettuata la registrazione.
Il SdP genera automaticamente un file contenente le registrazioni di protocollo del giorno.

2.12 Livello di riservatezza

La riservatezza di alcuni documenti atta a tutelare il trattamento di dati sensibili è affare organizzativo a cui concorre, per la corretta definizione del processo di gestione, la tecnologia e la disponibilità di idonei applicativi tra cui il servizio di protocollo informatico (SdP).
Il SdP applica autonomamente il livello di riservatezza "base" a tutti i documenti protocollati. Ciascuno vede i documenti assegnati nella qualità di redattore, sottoscrittore o competente dell'evasione dell'affare.

2.13 Annullamento delle registrazioni di protocollo

I dati obbligatori della registrazione di protocollo sono inseriti in campi non modificabili e quindi, eventuali errori di immissione ad essi riferiti, non possono essere corretti ma comportano la necessità di annullare l'intera registrazione di protocollo Anche le registrazioni a protocollo di documenti erroneamente introdotti nel patrimonio documentale dell'AOO devono essere annullate.
La richiesta di annullamento, va trasmessa al RSP?? O all'Amministratore di AOO con indicazioni sulla nota in questione e sulla motivazione per la quale l'operazione sarebbe opportuna.
Nessun operatore può annullare in autonomia protocolli se non è pervenuta l'autorizzazione del RSP.

2.14 Documenti esclusi dalla registrazione di protocollo

L'art. 53, co. 5 del TUDA esclude dalla registrazione le seguenti tipologie documentali:

- gazzette ufficiali;
- bollettini ufficiali della PA,
- notiziari della PA;

- dati statistici;
- atti e corrispondenza interna di natura informativa scambiata tra uffici come ad esempio richieste di materiale di cancelleria, richieste di interventi di manutenzione hardware;
- materiale editoriale o pubblicitario, inviti a manifestazioni;
- documenti erroneamente indirizzati;
- certificati medici dei dipendenti;
- le richieste di ferie dei dipendenti;
- le richieste di permessi retribuiti;
- le comunicazioni da parte di enti diversi di bandi di concorso;
- le fatture elettroniche che vengono gestite attraverso il sistema di interscambio messo a disposizione della PA;
- i documenti unici di regolarità contributiva (DURC) dei fornitori di beni, servizi e lavori.

Inoltre, i documenti già destinati a registri informatici dell'Amministrazione (es. atti destinati ai registri penali o civili) non devono essere registrati a protocollo.

2.15 Segnatura 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. A tal fine, il sistema di protocollo informatico produce il file di segnatura, i cui dati saranno utilizzati a completamento automatico delle informazioni afferenti alla registrazione di protocollo.

Tali dati non saranno modificabili dall'addetto al protocollo successivamente alla registrazione o in caso di registrazione automatica, fatto salvo il campo "oggetto" il cui contenuto può essere integrato per inserire ulteriori informazioni necessarie alla AOO ricevente.

Sui documenti in entrata ed in uscita, l'etichetta di segnatura di protocollo viene impressa almeno sul primo foglio del documento informatico al fine di garantire la validità del documento informatico così prodotto.

Per migliorare l'efficacia e l'efficienza dell'azione amministrativa, il RSP, con proprio provvedimento può modificare, integrare o eliminare elementi facoltativi del protocollo, la modifica di dati facoltativi non comporta necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico registra tali modifiche.

2.16 Il documento

I documenti son distinguibili in:

a)analogici o informatici: in osservanza della normativa vigente, con particolare riguardo all'art. 40 del CAD, i documenti sono redatti con strumenti informatici dovendo essere ex lege nativi digitali. Pertanto, le produzioni documentali analogiche, es. lettera scritta a mano, sono da considerarsi casi straordinari di oggettiva impossibilità di generare documento elettronico. I documenti informatici in particolare devono essere convertiti in uno dei seguenti formati:

- pdf (compreso il foranto RDF/A);
- gif,jpg,tif;
- OOOXML, Office Open XML (principali estensioni:doc, xlsx, pptx);

- Open Document Format;
- Txt (codice unicode UTF 8);
- Zip (a condizione ce i file contenuti all'interno del file compresso siano prodotti in uno dei formati previsti nel presente elenco);
- P7m 8documenti firmati digitalmente con sottoscrizione di tipo CADES e a condizione che i file originali oggetto di sottoscrizione digitale siano prodotti in uno dei formati previsti nel presente elenco);

In ogni caso i documenti elettronici inviati o consegnati all'Amministrazione dovranno essere privi di elementi attivi, tra cui macro e campi variabili.

b) documenti digitali e misti: l'RSP può, in caso di corrispondenza pervenuta per canali diversi da quelli interoperabili, inviare via mail al mittente una comunicazione di invito all'uso dei canali di trasmissione PEC disponibili sul protocollo.
La ricezione dei documenti informatici può avvenire via posta elettronica certificata o ordinaria. Per questo, il personale della UO è tenuto a monitorate le caselle istituzionali di PEO e presidiare quelle di PEC, salvo diversa indicazione.
Si distinguono i seguenti casi:

- messaggio ricevuto su una casella istituzionale di posta elettronica di servizio integrata nel sistema di protocollo: questo verrà automaticamente protocollato;
- messaggio ricevuto su una casella istituzionale di posta elettronica di servizio non integrata nel sistema di protocollo: solo qualora esso abbia una rilevanza amministrativa, nei modi e termini indicati nel presente Manuale, va inoltrato all'UOP che provvederà alla protocollazione, inserendo correttamente il mittente d'origine nel sistema di protocollo;
- messaggio avente in allegato un documento scansionato e sottoscritto in maniera autografa: va verificata la provenienza certa del documento secondo le previsioni della normativa di settore vigente. Termini e modalità di verifica nonché di valutazione dei casi in cui i mittenti non sono verificabili, sono descritti nel presente Manuale. In mancanza, varranno le puntuali determinazioni del RSP comunicate a mezzo PEO istituzionale;
- messaggio firmato digitalmente o avente in allegato, un documento sottoscritto digitalmente: si provvederà a protocollarlo registrando come mittente il soggetto firmatario nel rispetto delle regole descritte nel presente Manuale;
- messaggio contenente un testo non sottoscritto: va verificata la provenienza certa del documento secondo le previsioni della normativa di settore vigente. Termini e modalità di verifica nonché di valutazione dei casi in cui i mittenti non sono verificabili, sono descritti nel presente Manuale. In mancanza, varranno le puntuali determinazioni del RSP comunicate a mezzo PEO istituzionale;

c) documenti analogici o cartacei: il documento pervenuto in formato cartaceo è acquisito in formato immagine (copia per immagine di documento analogico) attraverso un processo di scansione, secondo le fasi di seguito indicate:

- acquisizione delle immagini in unico file anche se il documento cartaceo sia composto da più pagine;
- verifica della leggibilità e della qualità delle immagini acquisite;

- registrazione di protocollo e rilascio del numero progressivo;

d)documenti interni: I documenti di rilevanza interna, sono quelli nei quali mittente e destinatario appartengono alla medesima AOO. Possono essere di natura prevalentemente informativa oppure di natura prevalentemente giuridico-probatoria.
I primi, quali mere comunicazione interne scambiate fra uffici, richieste di materiale di cancelleria, richieste di interventi di manutenzione ecc. non vanno protocollati. DI regola los cambio avviene per mezzo posta elettronica.
I documenti di natura giuridica-probatoria, ossia gli atti redatti dal personale nell'esercizio delle proprie funzioni, volti a documentare le proprie attività, possono essere protocollati secondo le indicazioni del RSP???

e)documenti in entrata e documenti in uscita:
-documenti in entrata: la registrazione di protocollo prevede la numerazione sequenziale annuale per gli atti in entrata ed in usciti, contraddistinti rispettivamente, dal simbolo E (entrata) oppure U (uscita).
La documentazione in entrata attivano un workflow diverso dipendente dalla natura dello stesso: analogico, digitale o "misto". La ricezione dei documenti informatici può avvenire per posta elettronica certificata o ordinaria, a tal fine è necessario monitorare le caselle istituzionale di PEO e presidiare quelle di PEC.
Il documento pervenuto in formato cartaceo è acquisito in formato immagine (copia per immagine di documento analogico) attraverso un processo di scansione.
Tra PPAA la trasmissione via fax dei documenti è esclusa ai sensi dell'art. 47 del CAD.
Nel caso di assegni o valori di debito o credito, va protocollata la lettera di trasmissione ed indicato nel campo "note" il luogo di custodia dell'originale ricevuto.
La corrispondenza che riposta l'indicazione "offerta" – "gara di appalto" e simili, si procede alla protocollazione per la successiva consegna al responsabile del procedimento.
Un documento perviene per errore quando reca un'errata definizione del destinatario o viene recapitato per errata esecuzione dei servizi di consegna.
-documenti in uscita: i documenti in uscita sono il risultato di un workflow proprio di questa AOO, ma non può mai essere cartaceo o analogico e quindi solo digitale o "misto", come da art. 40 del CAD.
Per i documenti in uscita, il protocollista verifica la corretta indicazione del mittente, del destinatario, l'avvenuta sottoscrizione e la presenza di eventuali allegati dichiarati, registra il documento generando la segnatura. In caso riscontri irregolarità restituisce la nota alla UO proponente con le osservazioni del caso. Se le dimensioni degli allegati superano quella massima consentita, lo segnala all'UO e procede copiando il documento informatico su idoneo supporto digitale e trasmesso al destinatario secondo modalità condivise con l'UO proponente.
Infine, collega gli eventuali documenti correlati e richiamati nel testo, già presenti nel protocollo al fine di evidenziare con immediatezza la concatenazione tra più atti di uno stesso affare.

2.17 Documenti non firmati – anonimi
Nel caso di ricevimento di documenti non firmati o anonimi, il protocollatore attesta la data, la forma e la provenienza per ciascuno di essi.

Le lettere anonime devono essere protocollate e identificate come tali, con la dicitura "mittente sconosciuto e anonimo".
Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e identificate come tal con la dicitura "documento non sottoscritto".

2.18 Tenuta dei documenti registrati

I documenti registrati sono tenuti nel SdP in modalità non modificabile per almeno dieci anni.
Sono resi disponibili alle UO competenti dopo l'operazione di assegnazione ed in base ai diritti di visibilità.
Il SdP rappresenta pertanto, il cosiddetto archivio corrente

3. GESTIONE DEI FLUSSI DOCUMENTALI

3.1 Flussi documentali in ingresso

la gestione dei flussi documentali che questa AOO acquisisce nell'espletamento della propria attività da altri enti pubblici o privati, da soggetti privati si svolge secondo le seguenti fasi:

1. ricezione;
2. protocollazione;
3. segnatura;
4. assegnazione;

1. Ricezione

a) i documenti possono pervenire in forma cartacea tramite il servizio postale, consegna diretta presso l'Ufficio; in forma elettronica attraverso la casella di posta elettronica certificata in formato pdf attraverso una casella di posta elettronica che consente in modo inequivocabile l'individuazione del mittente, con acclusa una copia del una copia del documento d'identità in corso di validità del mittente.
b) corrispondenza non soggetta ad apertura:
i plichi e le buste riconducibili alle seguenti categorie non devono essere aperti dall'operatore che li riceve;
c) corrispondenza sulla cui busta sia riportata la dicitura "riservato" o qualunque altra formula idonea a fare ritenere che il contenuto sia soggetto all'applicazione di particolari restrizioni all'accesso;
d) corrispondenza indirizzata nominativamente al dirigente o al capo dell'ufficio;
corrispondenza sulla cui busta sia riportata la dicitura "personale" o s.p.m., o qualunque altra formula idonea a fare ritenere che si tratti di corrispondenza di carattere personale;
e) corrispondenza proveniente da strutture appartenenti al servizio sanitario nazionale o comunque per la quale si possa ipotizzare un contenuto relativo ad informazioni sullo stato di salute del soggetto interessato, offerta in busta chiusa e sigillata relative alla partecipazione di gare.
Il protocollista che riceve la corrispondenza rientrante nelle suddette tipologie non procede all'apertura dei plichi e delle buste, ma provvede all'apposizione sulla busta del timbro con la data di ricezione e alla conseguente consegna al soggetto destinatario.
La protocollazione sarà effettuata successivamente su richieste del soggetto stesso.

2.Protocollazione

Alla registrazione in ingresso avviene presso l'AOO preposto al protocollo.

La protocollazione in entrata avviene di norma nella stessa giornata lavorativa per i documenti ricevuti entro le ore 14.00.

I documenti ricevuti oltre il suddetto orario possono essere protocollati entro il giorno lavorativo successivo, salvo casi di protollazione differita (vedi paragrafo 2.8).

I documenti analogici ricevuti tramite servizio postale sono protocollati e sono conservati in modalità digitale nel rispetto delle norme tecniche vigenti al fine di evitare la circolazione e l'eventuale duplicazione del supporto cartaceo. La digitalizzazione del documento avverrà a cura dei protocollisti.

Nel caso in cui un documento venga consegnato a mano dal mittente o da altra persona incaricata e venga contestualmente richiesto il rilascio di una ricevuta di avvenuta consegna, l'addetto al protocollo provvede a protocollare l'atto e rilascia la ricevuta prodotta dal sistema di protocollo.

Premesso che, a norma dell'art. 14 del decreto legge 21 giugno 2013 n. 69, convertito con modificazioni dalla legge 9 agosto 2013, n. 98, è escluso l'uso del fax per lo scambio di documenti tra pubbliche amministrazioni, mentre non vi sono preclusioni normative per lo scambio di documentazione tra pubbliche amministrazioni e cittadini ed imprese, il documento ricevuto tramite fax deve essere protocollato senza necessità di acquisizione del relativo documento cartaceo originale e nel caso non sia possibile accertare la fonte di provenienza, il documento sarà trattato come documento anonimo.

In caso di ricevimento anche dell'originale, l'addetto al protocollo, accertato che trattasi dello stesso documento, deve attribuisca quest'ultimo la stessa segnatura del documento pervenuto via fax, poiché ogni documento deve essere individuato con un solo numero di protocollo, indipendentemente dal supporto o dal mezzo di trasmissione.

I documenti trasmessi per mezzo delle caselle di posta elettronica di questa Amministrazione vengono registrati, segnati ed assegnati qualora sussista almeno una delle seguenti caratteristiche:

-siano sottoscritti mediante firma digitale o firma elettronica qualificata;

-quando l'autore sia identificato con l'uso della carta d'identità elettronico e della carta nazionale dei servizi;

-quando in allegato vi sia la scansione di un valido documento d'identità dell'autore;

-quando siano trasmessi mediante la PEC dell'autore stesso;

-in altri casi non contemplati previa autorizzazione del RSP.

3.Segnatura

A tutti i documenti protocollati deve essere associata la segnatura di protocollo come descritta al paragrafo 2.13.

4.Assegnazione

Il documento dopo essere stato sottoposto a registrazione di protocollo viene assegnato al settore di lavoro di competenza per la successiva trattazione.

A seconda del tipo, della materia e della rilevanza, i documenti devono essere portati all'attenzione delle risorse di quest'Amministrazione opportunamente già profilate sul SdP e quindi nell'organigramma in cui sono configurabili diversi livelli gerarchici per i seguiti di competenza.

Ogni documento in entrata, in uscita o interno può essere assegnato per competenza oppure per conoscenza ad una o più unità organizzative e/o a singole risorse. L'assegnazione per competenza individua il soggetto responsabili della trattazione della pratica e ne determina la presa in carico. Un'assegnazione può determinare l'attribuzione a diversi soggetti, oppure a singole risorse sia della competenza che della conoscenza di un determinato atto. E' sempre necessario che per ogni documento ci sia almeno un soggetto competente della conseguenziale trattazione. Per tale motivo il personale autorizzato ad accedere al SdP è tenuto alla consultazione quotidiana del protocollo.
Quest'Amministrazione consente di rendere disponibili gli atti protocollati in entrata secondo il seguente modello:

- **assegnazione di I livello**: i documenti in ingresso sono assegnati al vertice dell'AOO (segreteria);
- **assegnazione di II livello:** la segreteria provvede ad assegnarli ai responsabili dei settori di lavoro;
- **assegnazione di III livello**: i responsabili dei settori di lavoro provvederanno poi al loro smistamento finale assegnando la competenza e la conoscenza del documento alle risorse ritenuto competenti della trattazione o dell'evasione della pratica.

3.2 Flussi documentali in uscita

Il ciclo di produzione dei documenti destinati all'uscita prevede le seguenti fasi di lavorazione:

1. formazione e sottoscrizione del documento;
2. registrazione di protocollo;
3. spedizione;

1. Formazione e sottoscrizione del documento

I documenti in uscita vengono prodotti mediante strumenti informatici di elaborazione di testi; completa la fase di redazione, il documento viene sottoposto alla sottoscrizione di colui che è titolare del potere di firma o di un suo delegato.
I documenti prodotti possono essere sottoscritti con firma autografa quando l'originale del documento è prodotto in forma cartacea; con firma digitale nel caso in cui il documento originale in forma elettronica.

1. Registrazione di protocollo

Tutti i documenti in uscita devono essere registrati dopo la sottoscrizione nel registro ufficiale di protocollo; ogni registrazione deve identificarsi con un solo documento e quindi non è possibile attribuire a un documento in uscita lo stesso numero di protocollo attribuito all'eventuale documento in entrata dal quale è scaturita la lavorazione. La protocollazione è effettuata dal personale di questa AOO a ciò abilitati.
Anche la classificazione e la fascicolazione dei documenti protocollati sono di competenza dei protocollisti.

5,Spedizione

Il documento sottoscritto e protocollato viene inviato dai protocollisti al destinatario mediante La trasmissione che può avvenire per posta elettronica certificata PEC, attraverso il sistema Script@, posta elettronica ordinaria, raccomandata, fax o consegna a mano.

4. CLASSIFICAZIONE, FASCICOLAZIONE E ARCHIVIAZIONE DEI DOCUMENTI

4.1 Caratteristiche generali

La classificazione dei documenti amministrativi è un'operazione prevista dall'art. 56 del TUSDA, che consente all'Ufficio di organizzare gli atti amministrativi secondo un ordine logico in relazione alle funzioni ed alle proprie competenze, nonchè di rendere agevole l'identificazione e la tracciabilità all'interno dell'archivio documentale., Le operazioni di classificazione si svolgono utilizzando il pianto di classificazione o titolario, all'interno del quale è possibile creare fascicoli elettronici.
Il documento può essere associato alla voce corrispondente (operazione di classificazione ed inserito in un fascicolo o sotto fascicolo elettronico (operazione di fascicolazione).
Si possono associare allo stesso documento più voci di classifica, in funzione delle attività nell'ambito delle quali il documento protocollato viene trattato.
La classificazione non è legata necessariamente al momento della registrazione di protocollo, in ogni momento della lavorazione è possibile effettuare, modificare o integrare la classificazione associata al documento protocollato.

4.2 Piano di classificazione o titolario

Il piano di classificazione o titolario è l'elenco di cui all'allegato 1 quale sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzionai di quest'Ufficio al quale viene ricondotta la molteplicità dei documenti prodotti. Esso si suddivide in funzioni, macroattività, attività più comunemente dette voci di I,II e III livello.
Il titolario risulta già caricato nel SdP ed è definito, revisionato ed aggiornato centralmente. Nel caso in cui vengano apportate modifiche, l'onere di informare tutti i soggetti abilitati alla classificazione dei documenti ed impartire istruzione è in capo al RSP.

4.3 Fascicolazione

La fascicolazione è l'operazione conseguente alla classificazione mediante la quale ogni documento registrato nel protocollo viene inserito all'interno del titolario d'archivio, nel fascicolo di riferimento o all'occorrenza in sotto fascicoli. La creazione e alimentazione dei fascicoli elettronici ha la funzione di garantire l'ordinata sequenza degli atti procedimentali, in quanto il sistema provvede all'ordinamento cronologico dei documenti.
La creazione dei fascicoli è demandata ai soggetti che ricevono gli atti per competenza, individuati secondo le scelte organizzative di questa AOO, e per quanto possibile nel rispetto di quanto stabilito dal modello titolario.
Qualora un documento dia luogo all'avvio di più procedimenti amministrative o pratiche, potrà essere assegnato a più fascicoli che vanno formati secondi diversi criteri:

- per persona fisica/giuridica;
- per serie documentale, quando si tratti di documenti della stessa tipologia (contratti, verbali, circolari);

- per procedimento amministrativo, in questo caso nel fascicolo andranno inseriti via via tutti gli atti procedimentali prodotti;

I fascicoli esprimono una relazione amministrativa tra i documenti che sono destinati ad esservi contenuti. All'interno dei fascicoli possono essere creati sotto fascicoli destinati a contenere atti relativi a particolari aspetti dell'affare trattato nel fascicolo principale: in quanto caso, nessun atto dovrà essere inserito nel fascicola madre, ma tutti gli atti saranno sistemati nei sotto fascicoli appropriati.

Al termine del procedimento amministrativo o all'esaurimento della pratica, buona prassi è quella di procedere all'operazione di chiusura del fascicolo.

4.4 Accesso al patrimonio documentale

Li utenti interni possono accedere alla documentazione di protocollo in funzione del proprio ruolo all'interno di questa AOO, del conseguente profilo assegnato nel sistema e delle abilitazioni concesse.

I documenti non fascicolari sono visibili agli assegnatari, a coloro che li hanno ricevuti in conoscenza o trasmissione ed ai superiori gerarchici.

L'accesso ai documenti è consentito a seconda dei differenti livelli di accesso che gli utenti hanno in relazione agli affari trattati nel rispetto della riservatezza prevista dalle norme vigenti.

Ogni utente può procedere alle ricerche sulla porzione di archivio documentale assegnato.

4.5 Accesso esterno al patrimonio documentale

Secondo il principio di trasparenza, la normativa prevede che i soggetti esterni possano accedere alla documentazione dell'AOO, in particolare si fa riferimento alle prerogative previste dalla legge n. 241/90, nonchè all'istituto dell'accesso civico generalizzato di cui al D.lgs. n. 33/2013, come modificato dal D.lgs. n. 97/2016.

Quindi, il soggetto esterno può avviare un procedimento che inizia con l'atto di richiesta e si conclude, in via ordinaria, con l'esibizione, cioè l'operazione che consente di visualizzare il documento conservato o di estrarne copia.

Le istanze dovranno essere prese in carico dal servizio di protocollo che le tratterà secondo le disposizioni impartite dal dirigente amministrativo.

5. PIANO DELLA SICUREZZA

Il presente Piano della Sicurezza Informatica relativo alla formazione, gestione, trasmissione, interscambio e archiviazione elettronica dei documenti - redatto ai sensi del decreto del Presidente del Consigli dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico" ed in relazione alle norme sulla protezione dei dati personale previste dal D.lgs. n. 196/2003 - costituisce parte integrante e specifica del documento aggiornato relativo alle misure di sicurezza dei dati personali trattati con e senza l'ausilio di strumenti elettronici.

Scopo del Piano è descrivere le strategie che questa AOO intende adottare per potere soddisfare i requisiti minimi di sicurezza in relazione agli elementi di rischio a cui sono soggetti i documenti informatici e i dati contenuti nel sistema di protocollo.
Si specifica che, poiché il sistema del protocollo informatico è gestito centralmente, si riportano le misure e le politiche di sicurezza contenute nel Manuale di gestione dei flussi documentali per il Ministero della Giustizia redato in dato 4 gennaio 2020 dalla Direzione Generale per sistemi informativi automatizzati.

5.1 Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel sistema di protocollo.

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'applicativo utile a informatizzare il servizio di protocollo, sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al SdP o come accesso ai documenti, dati e unita archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati presenti sul SdP;
- perdita dei documenti e dei dati contenuti nel SdP;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, DGSIA adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

5.2 Requisiti minimi di sicurezza applicativa

Con nota avente prot. n. 6281.Idell'01.06.2020, l'Amministrazione nell'ambito dell'esecuzione dei contratti di sviluppo in essere, ha assicurato la compliance del SdP alle seguenti misure:
1. Il sistema di protocollo deve essere conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).
2. Il sistema di protocollo deve assicurare l'accesso sia dalla propria postazione di lavoro connessa in rete locale, che da remoto secondo stringenti condizioni di sicurezza;
3. Il sistema di protocollo deve assicurare l'accesso per il tramite di credenziali già disponibili alla risorsa ministeriale (c.d. "di ADN");
4. Il sistema di protocollo deve assicurare la protezione della sessione di lavoro dell'utente. In particolare, devono essere attivati meccanismi non più deboli dei seguenti:

a) la comunicazione tra la stazione di lavoro e i sistemi di elaborazione che realizzano il Servizio di Protocollo è crittografata tramite il protocollo SSL a 128 bit;

b) è configurato un time-out per la disconnessone automatica delle utenze dal servizio dopo 30 minuti di inattività;

c) non sono consentite le sessioni multiple con la stessa user-id.

5. Il sistema di protocollo deve assicurare soddisfare i seguenti requisiti:

a) garanzia della disponibilità, riservatezza e integrità dei documenti e del registro di protocollo;

b) garanzia della corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;

c) possibilità di reperimento delle informazioni riguardanti i documenti registrati;

d) accesso in sicurezza alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;

e) garanzia della corretta organizzazione dei documenti nell'ambito del sistema di classificazione adottato.

6. Il sistema di protocollo deve assicurare che Titolare e Responsabile del Trattamento dei dati personali possano trattare tutti i dati personali raccolti e trattati perché contenuti nei documenti elettronici oggetto del servizio di Protocollo e/o di Scrivania digitale siano trattati solo per le finalità proprie dell'applicativo e della gestione e manutenzione sua e dell'infrastruttura ospitante.

7. Il servizio di protocollo assicurare la disponibilità delle registrazioni di sicurezza rappresentate da:

a) dai log di sistema generati dal sistema operativo;

b) dai log dei dispositivi di protezione periferica del sistema informatico (Intrusion Detection System (IDS), sensori di rete e firewall), se disponibili

c) dalle registrazioni del sistema di Protocollo.

8. Il sistema di protocollo deve assicurare la disponibilità di almeno i seguenti livelli di autorizzazione per l'accesso alle funzioni del sistema di Protocollo:

a) abilitazione alla consultazione;

b) abilitazione all'inserimento;

c) abilitazione alla cancellazione;

d) abilitazione alla modifica delle informazioni;

e) abilitazione all'annullamento delle registrazioni;

f) abilitazioni alla classificazione dei documenti;

5.3 Sicurezza della rete di accesso al servizio

La Rete Unitaria di Giustizia è protetta da una rete di circa 600 firewall.

Questa robusta protezione perimetrale assicura la messa in sicurezza delle comunicazioni Untrusted che avvengono tra l'esterno della rete (tipicamente Internet/Extranet) ed il resto dell'infrastruttura.

I server su cui alloggia il SdP è in una zona filtro, denominata "DMZ".

Le contromisure necessarie per proteggere le comunicazioni che avvengono all'interno dell'organizzazione sono attuate tramite l'adozione di un dominio di Active Directory e a un sistema centralizzato di Antivirus.

Da un punto di vista generale, qualsiasi accesso esterno alla rete ministeriale ed in particolare al protocollo, può costituire una minaccia per l'organizzazione.

Tuttavia, la necessità di avere costantemente a disposizione dati e documenti ministeriali, anche quando non è possibile fisicamente accedere al SdP dall'interno della RUG, impone l'utilizzo di tecnologie in grado di fornire un accesso diretto al SdP con connessioni a qualsiasi punto del mondo ed indipendentemente dall'orario locale. Per far fronte a tale necessita si è strutturato un sistema che prevede l'inserimento all'interno della DMZ di un everse proxi come ulteriore protezione dal WEB per permettere l'accesso remoto al portale di protocollazione.

Il SdP è alloggiato su storage e server ad alta affidabilità costantemente aggiornato e manutenuto.

5.4 Accesso al SdP da parte di utenti interni all'AOO

L'accesso a computer e reti informatiche è normalmente autorizzato solo per i soggetti che superano un processo di autenticazione dell'utente, inteso come il riconoscimento dell'identità dichiarata, via ADN.

L'accesso di cui trattasi avviene attraverso l'utilizzo di credenziali di autenticazione c.d. di ADN; i profili di abilitazione alle funzionalità del SdP sono attribuiti a ciascun utente sulla base di quanto stabilito dal titolare della AOO e dal RSP. Le credenziali di autenticazione consistono in un codice (User-Id), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (Password), conosciuta solamente dal medesimo tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione/autenticazione (ADN), il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente. Alle risorse incaricate a vario titolo per l'accesso al SdP è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della Password; quest'ultima è composta da almeno otto caratteri, tra cui almeno un numero e un carattere speciale e non contiene riferimenti agevolmente riconducibili al titolare.

La Password deve essere modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza semestrale. L'User-Id non è assegnato a nessun altro incaricato per nessuna motivazione. Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità (intesa come efficacia sulla sicurezza) che consente all'incaricato l'accesso ai dati personali. Qualora l'utente medesimo dimenticasse la propria password si procederà all'assegnazione di una nuova chiave di accesso. Gli incaricati a vario titolo al SdP non devono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento dei documenti ministeriali.

Le credenziali di accesso al SdP di ciascun operatore devono essere consegnate in busta chiusa e sigillata al RSP. In caso di prolungata assenza o impedimento del soggetto incaricato del trattamento di specifici documenti di una certa rilevanza e qualora si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il RSP è autorizzato ad utilizzare le credenziali contenute nella suddetta busta per procedere al trattamento, comunicandolo al titolare.

Di ciò va depositata a protocollo una relazione a firma del RSP che dettagli quanto sopra in grassetto. Il soggetto titolare delle credenziali provvederà, al momento del proprio rientro in servizio, alla sostituzione della Password, provvedendo all'inserimento della stessa in altra busta sigillata da riconsegnare al suddetto RSP.

5.5 Formazione e sottoscrizione dei documenti

I documenti dell'AOO sono prodotti utilizzando i formati indicati al punto 2.14 della sezione 2 dedicata alla protocollazione e registrazione dei documenti.del presente Manuale. L'apposizione della firma digitale, volta a garantire l'attribuzione certa della titolarità del documento e la sua integrità, avviene previa conversione in un formato che garantisca la leggibilità, l'interscambiabilità, la non alterabilità, l'immutabilità nel tempo del contenuto e della struttura del documento medesimo (ad esempio il formato PDF); l'acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati avente le medesime caratteristiche. L'apposizione delle varie tipologie di sottoscrizioni elettroniche, l'apposizione della firma digitale, nonché la validazione temporale del documento sottoscritto digitalmente deve avvenire in conformità a quanto sancito dalle richiamate Linee guida

emanate ai sensi dell'art. 71 del D. Lgs. 82/05. La sottoscrizione del documento con firma digitale deve avvenire prima dell'effettuazione della registrazione di protocollo.

5.6 Sicurezza delle registrazioni di protocollo

L'accesso al registro di protocollo al fine di effettuare le registrazioni o di apportare modifiche è consentito soltanto al personale abilitato alla protocollazione. L'accesso in consultazione al registro di protocollo è consentito sulla base dell'organizzazione dell'AOO: di norma, ciascun operatore è abilitato ad accedere esclusivamente ai documenti e ai dati di protocollo dei documenti che ha prodotto, che gli sono stati assegnati o, comunque, di competenza del proprio ufficio di riferimento. Ogni registrazione di protocollo viene memorizzata dal SdP unitamente all'identificativo univoco dell'autore che l'ha eseguita insieme alla data e l'ora della stessa. Eventuali modifiche, autorizzate nei termini e nelle modalità fissate dal presente manuale, vengono registrate per mezzo di log di sistema che mantengano traccia dell'autore, della modifica effettuata, nonché della data e dell'ora; il SdP mantiene leggibile la precedente versione dei dati di protocollo,
permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione. Il SdP non consente la modifica del numero e della data di protocollo; in tal caso l'unica possibile modifica è l'annullamento della registrazione stessa di cui, analogamente al caso precedente, il SdP manterrà traccia. L'annullamento di una registrazione di protocollo deve sempre essere accompagnato da autorizzazione scritta del RSP e il SdP deve recare, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione o la motivazione dell'annullamento. L'impronta digitale del documento informatico, associata alla registrazione di protocollo del medesimo è generata utilizzando una funzione di hash, conforme a quanto previsto dalla normativa vigente. Al fine di garantire l'immodificabilità delle registrazioni di protocollo, il SdP permette, al termine della giornata lavorativa, la produzione del registro giornaliero delle registrazioni di protocollo, in
formato digitale. Il SdP consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il SdP consente il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni sono protette al fine di non consentire modifiche non autorizzate. Il Sistema e tutti i documenti e/o dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici dannosi in quanto è impegno costante di DGSIA, attraverso l'attività del Centro Gestione Firewall, del Tavolo per la Governance della Sicurezza Informatica di Giustizia e l'attuazione del Piano Strategico per la sicurezza informatica ministeriale, il rendere ragionevolmente sicuri gli accessi al SdP ed alla RUG e quindi a tutti i documenti e dati in esso contenuti. Ciò anche in virtù del presidio del processo di apertura delle porte in uscita (LAN to AN) del firewall che avviene esclusivamente verso indirizzi preventivamente individuati da personale interno qualificato.
Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dal SdP e dagli applicativi ministeriali, vengono costantemente tenuti aggiornati per mezzo dell'istallazione degli aggiornamenti periodici che i fornitori rendono disponibili.

5.7 Backup e ripristino dell'accesso ai dati

Il backup dei dati contenuti nel SdP su supporti mobili portanti i dati sensibili o giudiziari, quando presenti, devono essere custoditi, sotto chiave, a cura del RSP del Ministero della Giustizia, vista la

gestione centralizzata del sistema del protocollo informatico, al fine di evitare accessi non autorizzati e trattamenti non consentiti. Cessato lo scopo per cui sono stati memorizzati, se non riscrivibili devono essere necessariamente distrutti, se riscrivibili possono venire cancellati e riutilizzati esclusivamente nel caso in cui le informazioni in essi contenute non siano intelligibili e in alcun modo ricostruibili.
Il backup full dei dati del SdP deve consentire, attuando best practise vigenti, il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, entro 24/36 ore lavorative in caso di generico malfunzionamento, entro 72 ore lavorative in caso di disastro (si ricorda che va redatto il Piano di Continuità Operativa e Disaster Recovery del SdP).

5.8 Trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici tra questa A00 ed il Ministero deve avvenire esclusivamente per mezzo del SdP; nessun'altra modalità è consentita, al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati.

5.9 Piani formativi del personale

In conformità a quanto disposto dall'art. 13 del D.lgs. 82/2005, ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione, DGSIA rappresenterà alle articolazioni competenti in materia la necessità di predispone apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del SdP;
- fascicolazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione in materia di protezione dei dati personali.

5.10 Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

Considerata la gestione centralizzata del sistema del protocollo informatico, è compito dell'amministratore di Ente del SdP controllare mensilmente i log di sistema mantenendoli per 6 mesi, al fine di verificare eventuali violazioni del Sistema.
Il Coordinatore Ministeriale della gestione documentale effettua periodiche verifiche sul corretto funzionamento del SdP.

48/21 Prot. PG 28 SET. 2021

ATTO DI APPROVAZIONE

IL PROCURATORE GENERALE

Esaminata la seguente normativa:

- Testo Unico, il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445, Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA);
- Codice, il decreto legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione digitale (CAD);
- Regole Tecniche, il decreto del Presidente del Consigli dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico", artt. 2,6 ,9, 18, 20, 21;
- Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici pubblicate in data 11 settembre 2020;
- Determinazione n. 371/2021, Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici;

Rilevato che il presente Manuale di gestione rappresenta un atto di organizzazione che descrive le varie fasi operative del sistema di gestione del protocollo informatico, dei flussi documentali e degli archivi, individuando ogni azione del processo ed i rispettivi livelli di esecuzione, responsabilità e controllo;

Evidenziato che il Manuale persegue le finalità di disciplinare il sistema di gestione documentale, a partire dalla fase di protocollazione della corrispondenza in ingresso, in uscita ed interna e quella di determinare le funzionalità disponibili agli utenti interni ed ai soggetti esterni che a diverso tiolo interagiscono con la Procura Generale di Trieste;

Esaminato lo schema del Manuale predisposto dal Responsabile della gestione documentale, dott.ssa Ombretta D'Amato, dirigente amministrativo della Procura Generale di Trieste;

Ritenuto di procedere all'approvazione del predetto Manuale;

APPROVA
IL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEI DOCUMENTI E DEGLI ARCHIVI

Redatto in conformità alla vigente normativa in materia dal Responsabile della gestione documentale.

Trieste, 27 settembre 2021

Il Procuratore Generale
Dario Grohmann