MINISTERO DELLA DIFESA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE DEGLI ARMAMENTI

DIREZIONE DEGLI ARMAMENTI NAVALI

SERVIZIO DEL PROTOCOLLO INFORMATICO E GESTIONE DEL FLUSSO DOCUMENTALE

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO

DEI DOCUMENTI E DEGLI ARCHIVI

Area Organizzativa Omogenea GNAV

Codice univoco AOO: A16D511

A cura del Responsabile del Servizio

Dott. Ing. Francesco ACQUARO

MINISTERO DELLA DIFESA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE DEGLI ARMAMENTI

DIREZIONE DEGLI ARMAMENTI NAVALI

ATTO DI APPROVAZIONE

Approvo il

"Manuale di gestione del protocollo informatico, dei documenti e degli archivi della DIREZIONE DEGLI ARMAMENTI NAVALI"

IL DIRETTORE DEGLI ARMAMENTI NAVALI

Amm. Isp. Capo Giuseppe Abbamonte

Firmato Digitalmente da/Signed by:
GIUSEPPE ABBAMONTE

In Data/On Date:
giovedì 20 febbraio 2025 18:58:31

Il presente documento abroga e sostituisce il manuale approvato in data 06/07/2022

L'ESTENSORE

IL RESPONSABILE DEL SERVIZIO

Dott. Ing. Francesco ACQUARO

FRANCESCO ACQUARO
Ministero della Difesa/97355240587
21.01.2025 14:55:36
GMT+02:00

1 - PRINCIPI GENERALI

1.1 - Premessa

1.2 - Definizione dell'ambito di applicazione del manuale

1.3 - Norme principali di riferimento

1.4 - Acronimi utilizzati nel manuale

1.5 - Definizioni utilizzate nel manuale

1.6 - Servizio di Protocollo Informatico - Funzioni principali

1.7 - Principio di non discriminazione dei documenti elettronici

1.8 - Utilizzo della Firma digitale autorizzazioni e deleghe temporanee

1.9 - Trattamento dei dati personali, genetici, biometrici, dei dati realtivi alla salute e dei dati giudiziari

1.10 - Caselle di Posta Elettronica

1.11 - Aggiornamento indirizzi di posta certificata da IPA , INI-PEC e INAD

1.12 - Analisi e conferme in merito ad email di posta certificata richieste al SdP

1.13 - Gestione del labour turn over e formazione

2 - UNICITÀ DEL REGISTRO DI PROTOCOLLO INFORMATICO

2.1 - Altri registri di protocollo e sistemi informatici preesistenti

3 - CRITERI DI SICUREZZA

3.1 - Criteri adottati

3.2 - Specificità

3.3 - Formazione dei documenti - Aspetti di sicurezza

3.4 - Gestione dei documenti informatici - Aspetti di sicurezza

3.5 - Trasmissione e interscambio dei documenti informatici - Aspetti di sicurezza

3.6 - Accesso ai locali del Servizio di Protocollo - Aspetti di sicurezza

3.7 - Accesso ai documenti informatici del protocollo - Aspetti di sicurezza

3.8 - Gestione utenti interni della AOO - Aspetti di sicurezza

3.9 - Riesame delle problematiche di sicurezza adottate

4 - CRITERI DI CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE DEI DOCUMENTI

4.1 - Generalità

4.2 - Criteri di classificazione

4.3 - Criteri di fascicolazione

4.4 Gestione ed aggiornamento dei criteri di classificazione e di fascicolazione

5 - UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI

5.1 - Generalità

5.2 - Documento ricevuto

5.3 - Documento inviato

5.4 - Documento interno formale

5.5 - Documento interno informale

5.6 - Documento analogico

5.7 - Copia di un documento – casi previsti

5.8 - Formazione del documento

5.9 - Documento ricevuto – casi particolari

5.10 - Documento inviato – casi particolari

5.11 - Plichi chiusi ricevuti e contenenti particolari tipologie di documenti

5.12 - Corrispondenza elettronica ricevuta con il sistema di “AMHS - Message Handling”

5.13 - Corrispondenza elettronica inviata con il sistema di “AMHS - Message Handling”

5.14 - Corrispondenza dei documenti ai rispettivi procedimenti

6 - DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

6.1 - Generalità

6.2 - Flusso dei documenti in ingresso all' AOO

6.2.1 - Ricezione di documenti analogici a mezzo posta convenzionale

6.2.2 - Orari di protocollazione

6.2.3 - Gestione dei documenti

6.2.4 - Sottoscrizione dei documenti elettronici

6.2.5 - Documenti protocollati e documenti esclusi dalla protocollazione

6.2.6 - Procedure di gestione casi particolari

6.2.7 - Gestione del documento elettronico in ingresso

6.2.8 - Gestione del documento analogico in ingresso

6.2.9 - Rilascio della ricevuta attestante la ricezione di un documento analogico

6.3 - Flusso dei documenti in uscita dall'AOO

*6.3.1 - G*estione del documento elettr*onico in uscita*

6.3.2 - Gestione del documento analogico in uscita

6.4 - Assegnazione dei documenti ricevuti e procedure di classificazione

6.5 - Email certificate non consegnate

6.6 - Conservazione dei documenti nell'archivio corrente

6.7 - Trasmissione FAX

7 - ARCHIVI

7.1 - Archivio dell'AOO

7.2 - Archiviazione dei documenti informatici

7.3 - Archiviazione dei documenti analogici

8 - REGISTRAZIONI DI PROTOCOLLO

8.1 - Attribuzione del protocollo

8.2 - Registro informatico di protocollo

9 - IL REGISTRO DI EMERGENZA

9.1 - Apertura del registro di emergenza

9.2 - Chiusura del registro di emergenza e sincronizzazione del registro di protocollo

10 - APPROVAZIONE E AGGIORNAMENTO MANUALE, NORME FINALI

10.1 - Modalità di approvazione e aggiornamento del manuale

10.2 - Abrogazioni

10.3 - Pubblicità del presente manuale

10.4 - Operatività del presente manuale

1 - PRINCIPI GENERALI

1.1 - Premessa

Il presente manuale è redatto in conformità a quanto previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale emanate con Determinazione 407/2020 ed aggiornate con Determinazione 371/2021.

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

1.2 - Definizione dell'ambito di applicazione del manuale

Il presente manuale disciplina il funzionamento del sistema di protocollo informatico della Direzione degli Armamenti Navali che è organizzata come Area Organizzativa Omogenea nell'ambito del Segretariato Generale della Difesa / DNA.

L'insieme dei dati, conforme alle Regole Tecniche, associati dal software del protocollo informatico a ciascun invio o ricezione di documentazione, fa fede anche con rilievo giuridico dell'operazione effettuata.

1.3 - Norme principali di riferimento

- Regolamento (UE) n.910/2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
- Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445, testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa e ss.mm.ii.

- Legge 9 gennaio 2004, n. 4 e ss.mm.ii, disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici.
- Decreto Legislativo 7 marzo 2005, n. 82 e ss.mm.ii, Codice dell'Amministrazione Digitale.
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.
- AgID REM SERVICES - Criteri di adozione degli standard ETSI – Policy IT.
- AgID Circolare 60/2013 - Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni.
- Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi – Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le Regole tecniche di cui al DPCM 13.12.2013.
- AgID Istruzioni per la produzione e conservazione del registro giornaliero di protocollo v1.1 marzo 2016 e ss.mm.ii.
- AgID Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate 2019.
- AgID Linee Guida per la Modellizzazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design 2020
- AgID Determinazioni 407/2020 e 371/2021 - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.
- Normativa UE in materia di trattamento di dati personali:

- Regolamento (UE) n.679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (data di attuazione in Italia: 25/05/2018).
- Convenzione Consiglio UE 108/1981. Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.
- Direttiva (UE) 2022/2555 , relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).
- Direttiva (UE) 680/2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.
- Direttiva (UE) 681/2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.
- Direttiva (UE) 140/2009 relativa ad un quadro normativo comune per le reti ed i servizi di comunicazione elettronica.

- Normativa nazionale in materia di trattamento di dati personali:
  - Decreto Legislativo 196/2003, Codice in materia di protezione dei dati personali.
  - Decreto Legislativo 101/2018, disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

- Decreto Legislativo 65/2018, attuazione della Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
- Decreto Legislativo 138/2024, recepimento della Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la Direttiva (UE) 2016/1148.

- International Organization for Standardization – norme di riferimento
  - ISO/IEC 27017:2015 “Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services”.
  - ISO 27799:2016 “Health informatics — Information security management in health using ISO/IEC 27002”.
  - ISO 22316:2017 “Security and resilience — Organizational resilience — Principles and attributes”.
  - ISO/IEC 27003:2017 “Information technology — Security techniques — Information security management systems — Guidance”.
  - ISO 22316:2017 “Security and resilience — Organizational resilience — Principles and attributes”.
  - ISO 22320:2018 “Security and resilience — Emergency management — Guidelines for incident management”.
  - ISO 31000:2018 “Risk management — Guidelines”.
  - ISO 22301:2019 “Security and resilience — Business continuity management systems — Requirements”.

- ISO/IEC 27018:2019 “Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”.
- IEC 31010:2019 “Risk management — Risk assessment techniques”.
- ISO/TS 22317:2021 “Security and resilience — Business continuity management systems — Guidelines for business impact analysis”.
- ISO/IEC TS 27110:2021 “Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines”.
- ISO/IEC 27001:2022 “Information security, cybersecurity and privacy protection — Information security management systems — Requirements”
- ISO/IEC 27002:2022 "Information security, cybersecurity and privacy protection — Information security controls”.
- ISO/IEC 27005:2022 “Information security, cybersecurity and privacy protection — Guidance on managing information security risks”.
- ISO/IEC 27032:2023 “Cybersecurity — Guidelines for Internet security”.
- ISO/IEC 29134:2023 “Information technology — Security techniques — Guidelines for privacy impact assessment”.
- ISO/IEC 29100:2024 “Information technology — Security techniques — Privacy framework”.

1.4 - Acronimi utilizzati nel manuale

- **AOO** - Area Organizzativa Omogenea;
- **MdG** - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;
- **RSP** - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi

documentali e degli archivi;

• **SdP** - Servizio di protocollo informatico;

• **UU** - Ufficio Utente - un ufficio dell'AOO ovvero il soggetto, mittente o destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali;

• **IPA** - Indice delle Pubbliche Amministrazioni: è l'archivio ufficiale degli Enti pubblici e dei Gestori di pubblici servizi. Realizzato e gestito dall'Agenzia per l'Italia digitale, contiene informazioni dettagliate sugli Enti, sulle strutture organizzative, sulle competenze dei singoli uffici.

I contenuti dell'IPA sono strutturati in tre macro livelli:

- ✔ informazioni di sintesi sull'Ente: indirizzo postale, codice fiscale, logo, responsabile e riferimenti telematici (sito web istituzionale, indirizzi di posta elettronica);
- ✔ informazioni sulla struttura organizzativa e gerarchica e sui singoli uffici (Unità Organizzative - UO), corredate con informazioni di dettaglio;
- ✔ informazioni sugli uffici di protocollo (AOO).

Sono gli Enti stessi ad aggiornare con cadenza semestrale il sito dell'IPA.

Tutti i dati possono essere consultati tramite interfaccia web, in formato Open Data e, previa registrazione al portale, anche tramite interfaccia applicativa che utilizza il protocollo LDAP.

• **INI-PEC** - Indice Nazionale degli Indirizzi di Posta Elettronica Certificata istituito dal Ministero dello Sviluppo Economico. INI-PEC raccoglie tutti gli indirizzi di PEC delle Imprese e dei Professionisti presenti sul territorio italiano.

L'indice viene puntualmente aggiornato con i dati provenienti dal Registro Imprese e dagli Ordini e dai Collegi di appartenenza, nelle modalità stabilite dalla legge.

• **INAD** - Indice Nazionale dei Domicili Digitali. L’indice è rivolto particolarmente alle persone fisiche, ai professionisti che svolgono una professione non organizzata in ordini, albi o collegi ai sensi della legge n. 4/2013 e agli enti di diritto privato non tenuti all'iscrizione nell' INI-PEC.

- **ACL -** Lista di condizioni contenenti le restrizioni di accesso o permessi specifici che nell'ambito del presente manuale sono riferite alla struttura del protocollo informatico come di volta in volta dettagliato.

1.5 - Definizioni utilizzate nel manuale

- **Documento elettronico**: qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (Reg. eIDAS art. 3, n. 35). Agli effetti del presente manuale ci si riferisce a tale tipologia di documento anche con il termine di "**documento informatico**".
- **Documento analogico**: documento formato utilizzando una grandezza fisica che assume valori continui, come, ad es., l'inchiostro su carta, le immagini contenute in filmati e le magnetizzazioni su nastro.

  Nell'attività amministrativa, di norma il documento analogico è un documento formato su supporto cartaceo prodotto con strumenti analogici (es. documento scritto a mano o con supporto meccanografico) o con strumenti informatici (es. documento prodotto con un sistema di videoscrittura e stampato).
- **Copia informatica di un documento analogico**: documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.
- **Copia per immagine su supporto informatico di documento analogico**: documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto.
- **Copia informatica di un documento informatico**: documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari.

- **Copia analogica di un documento informatico**: documento in formato non elettronico di un documento informatico.

1.6 - Servizio di Protocollo Informatico - Funzioni principali

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

Il sistema di conservazione dei documenti informatici ha la funzione di garantire il mantenimento nel corso del tempo, dell'autenticità, integrità, leggibilità e reperibilità dei documenti digitali ivi conservati.

Al suddetto servizio è preposto un funzionario responsabile del servizio di protocollo informatico, della gestione dei flussi documentali e degli archivi (RSP), nominato con OdS dal Direttore della Direzione.

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

- predisporre il manuale di gestione del protocollo informatico con la descrizione dei criteri seguiti nella suddetta gestione e le modalità di revisione del medesimo e provvedere alla sua pubblicazione sul sito della Direzione;
- 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, per quanto di competenza, il rispetto delle disposizioni normative durante le operazioni di protocollo inclusa la chiusura giornaliera del registro giornaliero di protocollo;
- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;
- autorizzare, a cura del SdP o di temporaneo sostituto, le eventuali operazioni di annullamento della registrazione di protocollo;
- vigilare, per quanto di competenza, sull'osservanza delle disposizioni delle norme vigenti da parte del personale autorizzato e degli incaricati;

- curare, in caso di emergenza, l'apertura, l'uso e la chiusura di un registro di protocollo alternativo con gli strumenti e le funzionalità disponibili nel SdP.

1.7 - Principio di non discriminazione dei documenti elettronici

Il Regolamento eIDAS (art. 46) stabilisce la non discriminazione dei documenti elettronici rispetto ai documenti analogici.

1.8 - Utilizzo della Firma digitale autorizzazioni e deleghe temporanee

Tutti i dipendenti della Direzione sono provvisti di firma digitale.

L'uso di tale tipologia di firma è obbligatorio per tutti i soggetti che sono delegati a rappresentarla.

Il Direttore, il Capo Segreteria Particolare, i Vice Direttori, i Capi Reparto ed i Capi Ufficio sono preposti a rappresentare la Direzione nelle rispettive materie di competenza ed in quelle ad esse assimilabili in ambito gerarchico.

In caso di impossibilità a procedere del titolare ed in situazione di assenza di altro dipendente abilitato nell'area di competenza può essere nominato un sostituto con OdS a cura del Direttore della Direzione.

Nel caso di cui sopra e solo per comprovati motivi di necessità ed urgenza, l' RSP può autorizzare, a seguito di formale richiesta del titolare abilitato che specifichi detti motivi e, solo nel caso di impossibilità a delegare uno dei sostituti previsti per temporaneo impedimento ad operare dei medesimi, altro dipendente (limitatamente al ruolo di Capo Servizio o Sezione), indicato dal delegante, alla funzionalità di firma nel protocollo. Il delegato dovrà limitarsi, in tale caso, al solo espletamento della problematica che riveste il carattere di necessità ed urgenza affidatagli dal delegante.

1.9 - Trattamento dei dati personali, genetici, biometrici, dei dati relativi alla salute e dei dati giudiziari

Il protocollo della Direzione contiene esclusivamente dati riferentisi all'espletamento degli obblighi istituzionali della Direzione e per cui esiste un interesse legittimo.

La Direzione non trasferisce i dati personali detenuti in Paesi terzi.

Con particolare riferimento ai dati particolari e ai dati personali relativi a condanne penali e reati detenuti, il SdP assicura la corretta gestione delle autorizzazioni e deleghe, previste dal software di protocollo in uso, per garantire la liceità, la limitazione e la minimizzazione, l'integrità e la riservatezza del loro trattamento.

In caso il SdP rilevi o sia informato di elementi oggettivi inerenti una violazione dei dati personali (data breach) l' RSP provvede, nel più breve tempo possibile, a notificarlo all'Ufficio del Direttore della Direzione per i successivi adempimenti previsti dal Regolamento.

1.10 - Caselle di Posta Elettronica

L' AOO è dotata della seguente casella di posta elettronica certificata: navarm@postacert.difesa.it che ne costituisce l'indirizzo digitale previsto dall'art. 6 del Decreto Legislativo 7 marzo 2005, n. 82.

Tale casella di posta è accreditata presso l'Indice dei Domicili digitali della Pubblica Amministrazione e dei Gestori dei Pubblici Servizi (IPA).

E' attiva, inoltre, anche una casella di posta ordinaria: navarm@navarm.difesa.it .

Si ribadisce che le due email citate non sono assimilabili ad email personali; pertanto nessun dipendente dell'AOO o mittente esterno può legittimamente attendersi l'esclusione, dalla lettura dei messaggi ivi inviati, di utenti non dallo stesso esplicitamente designati.

Ciò è vero sia per l'invio della corrispondenza elettronica da parte dell' AOO, in cui nella fase di predisposizione e di approvazione/invio possono essere coinvolti più UU non necessariamente

corrispondenti a precise persone fisiche (possibilità di delega della funzione), sia in fase di ricevimento di corrispondenza da parte dell' AOO, nell'ambito della quale per la classificazione, la fascicolazione e l'inoltro della documentazione essa può essere letta da UU non coincidenti con quanto atteso dal ricevente.

Pertanto, pur essendo pienamente lecito l'utilizzo di tali canali anche per le comunicazioni riguardanti dati personali e particolari ai fini istituzionali (ad es. pratiche del personale), non è possibile attendersi limitazioni univoche di accesso a tali comunicazioni oltre le normali attenzioni previste dalla normativa su dati personali e particolari.

E' invece espressamente escluso l'uso di tali email per invio o ricezione di comunicazioni a carattere personale e non d'interesse per l' AOO.

1.11 - Aggiornamento indirizzi di posta certificata da IPA , INI-PEC ed INAD

L’aggiornamento degli indirizzi di posta certificata fruibili tramite il software di protocollo provenienti da IPA è automatico e nelle more dell’aggiornamento periodico vi provvede, in caso di necessità, il SdP.

L’aggiornamento degli indirizzi di posta certificata fruibili tramite il software di protocollo relativi all’indice INI-PEC e INAD è manuale. Il SdP provvede all’inserimento di indirizzi specifici in caso di necessità o su specifica segnalazione di un UU interno.

1.12 - Analisi e conferme in merito ad email di posta certificata richieste al SdP

Il software di protocollo dà evidenza delle ricevute di invio delle email certificate inviate dall’AOO così come delle email ricevute e dei relativi allegati.

Tuttavia qualora un UU interno abbia necessità di avere conferma dal SdP, a seguito di segnalazione / contestazione formale, dell’esistenza, nell’ambito del software di protocollo informatico, di specifiche

email certificate inviate o ricevute dall'AOO, nonché del loro corretto invio o ricezione, deve inviare la richiesta al RSP unitamente ai seguenti elementi eventualmente ottenibili dal corrispondente esterno:

- per le email certificate inviate dall'AOO una delle seguenti ricevute:

  la "ricevuta di avvenuta consegna completa" formata dal file "postacert.eml", contenente il messaggio originale, completo di testo ed eventuali allegati e il file "daticert.xml" che riproduce l'insieme di tutte le informazioni relative all'invio (mittente, gestore del mittente, destinatari, oggetto, data e ora dell'invio, codice identificativo del messaggio);

  la "ricevuta di avvenuta consegna breve" che include un estratto del messaggio originale e i dati di certificazione;

  la "ricevuta di avvenuta consegna sintetica" che fornisce i dati di certificazione;

- per le email certificate ricevute dall'AOO: la busta di trasporto con il file "postacert.eml", contenente il messaggio originale, completo di testo ed eventuali allegati, e il file "daticert.xml" che riproduce l'insieme di tutte le informazioni relative all'invio (mittente, gestore del mittente, destinatari, oggetto, data e ora dell'invio, codice identificativo del messaggio).

La richiesta verrà esaminata nel più breve tempo possibile e verrà fornita, qualora necessario, una risposta scritta in merito alla richiesta.

In assenza della ricevuta di avvenuta consegna per posta certificata inviata dall'AOO, per spazio esaurito nella casella del destinatario, non verrà fornita nessuna conferma dal SdP in merito alla notifica specifica non potendola ritenere completata.

1.13 - Gestione del labour turn over e formazione

L’SdP provvede alla formazione del nuovo personale della Direzione per quanto concerne il software del protocollo informatico. E’ prevista anche la redazione di sintetici manuali per la gestione, ad uso interno dell’AOO, per particolari tipologie di documenti richiedenti procedure informatiche specifiche (ad es. divisione, ad opera di sistemi documentali esterni, di file in più parti, gestione di documenti a crittografia simmetrica, gestione di documenti contenenti firme multiple ed estrapolazione delle diverse versioni firmate).

2 - UNICITÀ DEL REGISTRO DI PROTOCOLLO INFORMATICO

2.1 - Altri registri di protocollo e sistemi informatici preesistenti

Il registro di protocollo informatico gestito dal relativo servizio (SdP) è l’unico registro autorizzato dalla Direzione.

Per motivi di conservazione archivistica la Direzione continua a mantenere copia del registro di protocollo informatico precedente, basato su una diversa struttura e logica di funzionamento.

Tale registro non è comunque più accessibile alla consultazione da parte dei dipendenti della Direzione ed eventuali ricerche su tale registro sono demandate all’RSP.

3 - CRITERI DI SICUREZZA

3.1 - Criteri adottati

I criteri di sicurezza adottati garantiscono che:

- i documenti e le informazioni trattate dall'AOO siano disponibili, integri e correttamente custoditi;
- i dati particolari e i dati personali relativi a condanne penali e reati detenuti vengano in particolare custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive

misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

3.2 - Specificità

Considerata la particolare modalità di fruizione del servizio di gestione del protocollo della Direzione, alcune funzioni di sicurezza sono di competenza del Segretariato Generale della Difesa/DNA quale gestore del database server, dell'application server del protocollo e della casella di posta certificata e del Comando C4 Difesa dello Stato Maggiore della Difesa per quanto concerne la firma digitale.
L'AOO è responsabile della 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 alla rilevanza dei dati/documenti trattati.

3.3 - Formazione dei documenti - Aspetti di sicurezza

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

- l'identificabilità del soggetto che ha formato il documento e l'AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti tramite 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 possono soddisfare i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, XML e TIFF.

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

Per attribuire in modo certo la titolarità del documento e la sua integrità ci si serve della firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui alle Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate AgID 2019.

3.4 - Gestione dei documenti informatici - Aspetti di sicurezza

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, in condizioni di sicurezza, informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;

- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati particolari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

3.5 - Trasmissione e interscambio dei documenti informatici - Aspetti di sicurezza

I dipendenti dell'AOO non possono cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche. Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

3.6 - Accesso ai locali del Servizio di Protocollo - Aspetti di sicurezza

II controllo degli accessi fisici al SdP è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale autorizzato;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti devono esplicare la procedura di registrazione. Essi non possono entrare e trattenersi nelle aree protette se non accompagnati da personale del SdP autorizzato;
- ogni persona che accede alle risorse della sede in locali protetti è identificata.

3.7 - Accesso ai documenti informatici del protocollo - Aspetti di sicurezza

II controllo degli accessi software è assicurato utilizzando l'autenticazione tramite smart card e solo in subordine, per un periodo di tempo limitato e su autorizzazione del RSP, tramite username e password.
Si adotta quindi una profilazione preventiva che consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.
Queste, in sintesi, sono:

- consultazione, per visualizzare in modo selettivo, delle registrazioni di protocollo eseguite da altri;
- inserimento, per apporre gli estremi di protocollo ed effettuare una registrazione di protocollo ed associare i documenti;
- modifica di alcuni metadati di protocollo;
- annullamento di una registrazione di protocollo. Questa funzione è di competenza del RSP o comunque eseguita da personale del SdP di volta in volta dallo stesso autorizzato.

Il software di protocollo informatico inoltre consente/assicura :

- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una Access Control List (ACL) che consente di stabilire quali utenti o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).
Considerato che il SdP segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo profilo o agli uffici dipendenti.

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

3.8 - Gestione utenti interni della AOO - Aspetti di sicurezza

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

Gli account utente di protocollo creati non sono di norma cancellati ma, eventualmente, disabilitati.

3.9 - Riesame delle problematiche di sicurezza adottate

II riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti attinenti alla sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli stessi obiettivi o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni adottate o a seguito dei risultati delle attività di audit. In ogni caso, tale attività è svolta almeno con cadenza annuale.

4 - CRITERI DI CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE DEI DOCUMENTI

4.1 - Generalità

Così come è necessario dare certezza in merito all’esistenza di documenti ricevuti o inviati dall’AOO, è anche indispensabile garantirne la reperibilità tramite una ricerca articolata intendendo per tale una ricerca che includa la possibilità d’interrogazione del database di riferimento tramite elementi che esulano dalla mera circostanza del ricevimento o invio del documento ricercato.

Il sistema di classificazione ad albero adottato nell’ambito dell’AOO connette logicamente un insieme di metadati ai documenti archiviati sulla base delle esigenze organizzative della Direzione.

La primaria finalità di tale associazione è quella di raggruppare i documenti che presentano affinità di argomento o procedimento.

È stato inoltre predisposto dalla Direzione un portale web accessibile sulla intranet ministeriale, contenente tutte le regole di formazione del suddetto sistema.

Tale applicazione web prevede anche un canale di comunicazione fra i dipendenti della Direzione e l' SdP. Il Servizio provvede all'analisi e alla valutazione di ogni segnalazione o proposta avanzata per il tramite di questo canale.

4.2 - Criteri di classificazione

Il sistema di classificazione adottato nell'ambito dell'AOO è articolato in tre livelli gerarchici organizzati in modo da rappresentare una traslazione informatica dei criteri organizzativi e gestionali dell'intera struttura.

4.3 - Criteri di fascicolazione

Tutti i documenti classificati nel sistema di protocollo informatico sono poi inseriti in fascicoli ed eventualmente in sottofascicoli in dipendenza della materia trattata.

4.4 - Gestione ed aggiornamento dei criteri di classificazione e di fascicolazione

La gestione di tutti i livelli di classificazione è demandata all'RSP e per sua delega al SdP essendo necessario mantenere i criteri archivistici previsti per la conservazione dei fascicoli di protocollo.

I tre livelli di fascicolazione sono modificabili e/o integrabili su istanza motivata di un responsabile di Divisione, Ufficio o Reparto all'Ufficio del Direttore della struttura.

I due livelli di classificazione sono invece modificabili e/o integrabili su richiesta dei singoli UU al SdP per il tramite del portale dedicato.

Le richieste devono contenere, a pena di inammissibilità, i motivi per cui si ritiene necessario procedere ad una modifica e/o integrazione degli item di classificazione o fascicolazione esistenti e verranno accolte in modo da prevedere la modifica necessaria al più basso dei cinque livelli previsti.
Per le richieste relative ai due livelli di fascicolazione (fascicolo e sottofascicolo), esse devono anche comprendere gli UU interessati rispettivamente in lettura, scrittura e copia dei documenti, in modo da permettere al SdP di associare al nuovo item la corretta ACL.
Il primo livello di fascicolazione (fascicolo) presenta inoltre la possibilità di termine temporale di modificabilità dello stesso. Se non diversamente previsto e/o richiesto e qualora la tipologia dell'item lo rendesse possibile, all'item verrà associato il termine di scadenza coincidente con la fine dell'anno solare in corso.
Possono essere assegnati agli UU i seguenti permessi relativamente alle ACL dei fascicoli:
Consultazione fascicolo - Lettura documento contenente dati particolari - Modificazione metadati fascicolo - Chiusura fascicolo - Aggiunta documento a fascicolo - Copia documento in diverso fascicolo.
Sono riservati all'RSP e per sua delega al SdP i seguenti permessi relativamente alle ACL dei fascicoli: spostamento documenti fra fascicoli ed eliminazione di un documento da un fascicolo.

5 - UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI

5.1 - Generalità

Per quanto attiene agli aspetti operativi del processo di gestione documentale, il documento amministrativo è così classificabile:

- ricevuto;
- inviato;
- interno formale;

- interno informale.

Il documento amministrativo scambiato in termini tecnologici è così classificabile:

- informatico;
- analogico.

L'AOO forma originali informatici dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri (art. 46 Regolamento eIDAS e art. 40 del D.Lgs. n. 82/2005).

5.2 - Documento ricevuto

La modalità da preferirsi per l'invio di un documento all'AOO è l'invio di un originale informatico tramite posta elettronica certificata ed è altresì utile ricordare che alcune categorie di mittenti sono tenute a norma di legge all'uso di tale modalità di invio (cfr. anche documento ricevuto – casi particolari).

Ciò premesso, la corrispondenza in ingresso può essere ricevuta dalla AOO con diversi mezzi.

Un documento informatico può essere ricevuto:

- a mezzo posta elettronica convenzionale o certificata;
- su altro supporto idoneo (a titolo non esaustivo si indica il supporto ottico o una pen drive)

Un documento analogico può essere recapitato:

- a mezzo posta convenzionale o corriere;
- a mezzo posta raccomandata;
- a mezzo telegramma;
- con consegna diretta da parte dell'interessato se dipendente della Direzione o tramite persona delegata degli UU aperti al pubblico.

A fronte delle tipologie descritte esiste un'ulteriore modalità detta "ibrida" composta da un documento analogico (lettera di accompagnamento) e da un documento informatico che comportano diversi metodi

di acquisizione.

5.3 - Documento inviato

Il documento informatico, compresi gli eventuali allegati, è inviato, di norma, per mezzo della sola posta elettronica certificata se la dimensione della relativa email non supera quella prevista dal sistema di posta utilizzato e/o nel limite di destinatari ammesso da tale canale.

Nel caso di trasmissione analogica, con o senza eventuale supporto rimovibile per eventuali allegati, si procede alla creazione di una copia analogica di originale informatico (cfr. copia di un documento protocollato).

5.4 - Documento interno formale

Documento informatico di rilevanza amministrativa giuridico-probatoria che viene redatto tramite sistemi di video scrittura, firmato elettronicamente con firma digitale e, se necessario, con contemporanea apposizione di marca temporale (si consiglia la firma di un file PDF/A con firma PADES-BES e contemporanea apposizione di marca temporale). Il documento può poi essere inviato ad altro UU tramite il software di protocollo.

5.5 - Documento interno informale

Per questa tipologia di documento e solo qualora sia necessaria la sottoscrizione con firma digitale e la sua registrazione a protocollo, vale quanto illustrato nel paragrafo precedente.

Occorre tenere presente che il software di protocollo non è un document management system e non prevede quindi le gestioni proprie di questa categoria di software.

L’AOO adotta, nei limiti della propria autonomia, misure organizzative idonee a definire tipologie di tali documenti per cui si richiede la registrazione a protocollo.

Gli UU non sono comunque autorizzati a gestioni interne di domande o documenti da scambiare con l'AOO in alternativa all'utilizzo caselle di posta istituzionali del software di protocollo (cfr. 1.10).

5.6 - Documento analogico

L'indirizzo preposto alla ricezione della documentazione analogica inerente all'attività dell'AOO è il seguente:

Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti

Direzione degli Armamenti Navali

Via di Centocelle 301 - 00175 Roma

Tale canale di trasmissione deve considerarsi residuale rispetto al canale di trasmissione per PEC ed in subordine per PEI.

5.7 - Copia di un documento – casi previsti

- Copia informatica di un documento analogico protocollato: non utilizzata dal SdP.
- Copia per immagine su supporto informatico di documento analogico protocollato: è prodotta durante la fase di registrazione a protocollo del documento analogico dal SdP.
- Copia informatica di un documento informatico protocollato: liberamente creabile dall'UU di competenza, per esigenze interne o dal SdP per ricostruzione di documenti ricevuti suddivisi in più email.
- Copia analogica di un documento informatico protocollato: prevista nel caso di documento firmato elettronicamente in uscita, ma inviato in modalità analogica; la conformità al documento originale è attestata da dichiarazione dell'RSP.

5.8 - Formazione del documento

Il documento informatico formato ed inviato tramite il protocollo garantisce:

- la riferibilità al soggetto che ha formato il documento nell'ambito dell'AOO;
- la sottoscrizione, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- la leggibilità tramite software di ampia diffusione o comunque facilmente reperibili online;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse. Gli standard raccomandati sono: PDF, XML e TIFF, come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi;
- la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento firmato con firma digitale. Per l'attribuzione della datazione temporale dei documenti prodotti all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 ("Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici").

Il software del protocollo informatico consente:

- la disponibilità, la riservatezza e il mantenimento dell'integrità dei documenti e del registro di protocollo;
- la corretta registrazione di protocollo dei documenti in entrata ed in uscita;
- la ricerca di informazioni in merito a documenti connessi ad un dato documento attraverso diversi criteri di ricerca;

- il reperimento delle informazioni riguardanti i documenti registrati nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati personali, genetici, biometrici e dati relativi alla salute o dei dati giudiziari;
- la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

5.9 - Documento ricevuto – casi particolari

- Documento elettronico pervenuto erroneamente: il documento viene inviato al corretto destinatario se identificabile in modo certo dall'intestazione o dal corpo del documento; in subordine il documento viene rinviato al mittente dal RSP con l'indicazione di documento pervenuto erroneamente, se inviato per posta elettronica convenzionale, se inviato per posta elettronica certificata viene protocollato in uscita ed inviato.
- Documento analogico pervenuto erroneamente: il documento viene protocollato in uscita e rinviato in modalità analogica al mittente. Viene acclusa una comunicazione con il motivo della restituzione.
- Il mittente di un documento analogico appartiene ad una categoria che è tenuta, a norma della vigente normativa, a corrispondere con la PA servendosi dell'indirizzo digitale di quest'ultima tramite posta elettronica certificata:
  il documento analogico viene protocollato in uscita e rinviato al mittente unitamente ad una lettera indicante le modalità di corretto invio della stessa.
- L'AOO riceve un' email convenzionale unitamente ad un'email certificata dallo stesso mittente di contenuto identico e con gli stessi documenti allegati:
  viene accertata la duplicazione del contenuto tramite il calcolo dell'hash dei documenti inviati.
  E' quindi protocollato l'invio tramite email certificata ed annullato l'invio tramite email

convenzionale, restituendo contestualmente un' email di notifica al mittente dell'avvenuta cancellazione a cura dell'RSP.

- L'AOO riceve email certificate duplicate indirizzate a diversi UU interni:

  viene accertata la duplicazione del contenuto tramite il calcolo dell'hash dei documenti inviati, quindi tutte le email certificate successive alla prima vengono archiviate a cura dell'RSP, dopo aver protocollato il contenuto delle stesse in uscita, il mittente viene informato, tramite un'email certificata, del motivo dell'archiviazione (documento già pervenuto).
- L'AOO riceve tramite posta elettronica certificata contenuto classificabile come spam:

  l'email viene isolata dal SdP ed archiviata dal RSP, senza ulteriore trattazione (ex art. 40-bis D.Lgs. 82/2005 e ss.mm.ii)
- L'AOO riceve email inviata tramite indirizzo convenzionale o comunicazione analogica classificata come spam:

  tale email o comunicazione analogica viene isolata dal SdP ed eliminata senza essere protocollata a cura del RSP.
- L'AOO riceve un'email certificata o convenzionale con documenti crittografati con chiave simmetrica:

  essa viene normalmente gestita se dal testo in chiaro inviato unitamente al documento cifrato risulta identificabile o desumibile l'UU di competenza, altrimenti viene archiviata dall'RSP dopo essere stata protocollata in uscita e dopo aver inviato al mittente un' email certificata nella quale si chiede di fornire gli elementi necessari ad una corretta trattazione della comunicazione e di ripeterne l'invio.
- L'AOO riceve diverse email certificate o convenzionali con file suddivisi in molteplici invii:

se tali email sono inviate simultaneamente, come di norma avviene in tali casi, il SdP si occupa della ricostruzione dei documenti suddivisi e comunica all'UU l'arrivo di una comunicazione suddivisa.

5.10 - Documento inviato – casi particolari

Il documento elettronico prodotto dall'AOO è trasmesso di norma tramite email certificata ad eccezione dei seguenti casi:

- corrispondente privo di una qualsiasi casella di posta elettronica;
- documento primario a cui è associato un allegato analogico non dematerializzabile;
- documento primario a cui è associato un allegato in formato elettronico che, per caratteristiche proprie, non può essere inviato per via telematica, come ad esempio, un documento la cui dimensione sia eccessiva e non gestibile dai servizi di posta elettronica.

A tal proposito si precisa che la dimensione massima complessiva degli allegati in uscita, tramite PEC, deve essere di 100 MB; tale limite è da considerarsi cumulativo sul numero dei destinatari (ad esempio, con 10 destinatari la massima dimensione del messaggio è di 10 MB). Per quanto riguarda la PEI, la dimensione massima complessiva degli allegati in uscita deve essere di 30 MB.

Nei casi sopraelencati, la formazione e la sottoscrizione del documento primario avviene comunque secondo le modalità idonee alla produzione di un originale in formato elettronico. Solo la trasmissione, sia del documento primario firmato elettronicamente, che della documentazione eventualmente allegata, viene effettuata con le tecnologie postali analogiche.

Più nel dettaglio, nel primo dei casi segnalati, il software di protocollo provvede autonomamente a trasferire il documento in questione nella lista dei documenti da materializzare, che è l'elenco dove confluiscono i documenti che saranno successivamente spediti con i servizi postali tradizionali.

Negli altri due casi, invece, è l'operatore che, in fase di "predisposizione" del sistema, stabilisce, servendosi della dichiarazione di "allegato analogico", che il documento non deve essere trasmesso per posta elettronica, ma deve confluire nella già descritta lista dei documenti da materializzare (è necessario segnalare che, nei casi in cui vi sia un allegato analogico e il documento deve essere spedito a più destinatari, alcuni dei quali per conoscenza, e questi ultimi dispongano di un indirizzo di posta elettronica, il software di protocollo procede comunque alla trasmissione del documento elettronico primario (privo di allegati) limitatamente agli indirizzi per conoscenza.

Pertanto, nei casi appena descritti il sistema informatico completa le operazioni di firma elettronica, apposizione della marca temporale e protocollazione del documento senza procedere alla successiva trasmissione.

Possono accedere alla lista dei documenti da materializzare solo gli operatori abilitati a tale funzione che provvedono alla stampa del documento primario e degli eventuali allegati.

Sul documento così stampato sarà apposto, sul retro, la seguente dicitura:

Si attesta che il presente documento è copia analogica del documento informatico firmato digitalmente composto complessivamente da n. ___ pagine.

Roma, xx xx xxxx

timbro e FIRMA

A tale scopo, il SdP ha distribuito, a ciascuno UU della Direzione, i timbri con la sopra indicata dicitura.

Dopo l’apposizione della firma sotto tale attestazione, il documento primario e gli eventuali allegati vengono spediti all’indirizzo postale del corrispondente attraverso il tradizionale servizio postale, secondo le modalità descritte nel paragrafo inerente al flusso dei documenti analogici in uscita.

5.11 - Plichi chiusi ricevuti e contenenti particolari tipologie di documenti

Tutti i plichi chiusi indirizzati all’AOO vengono aperti, fatta eccezione per i casi in cui sugli stessi siano presenti diciture e/o scritte che consentano di ricondurle a specifiche fattispecie, quali ad esempio: fascicolo sanitario personale, procedure di gara e/o contratti coperti da segreto, documenti classificati, etc...

5.12 - Corrispondenza elettronica ricevuta con il sistema di “AMHS - Message Handling”

Tutta la messaggistica non classificata ricevuta attraverso l’apposita postazione AMHS - Message Handling sarà trasmessa al SdP per le normali attività di protocollo ed indirizzamento.

5.13 - Corrispondenza elettronica inviata con il sistema di “AMHS - Message Handling”

Gli eventuali messaggi in uscita relativi al “AMHS - Message Handling” vengono comunque inviati tramite protocollo informatico.

5.14 - Corrispondenza dei documenti ai rispettivi procedimenti

Il SdP non effettua verifiche sull’integrità, sufficienza e pertinenza dei documenti ricevuti e protocollati.

Tale compito spetta all’UU di competenza e, nel suo ambito, al responsabile del singolo procedimento amministrativo. In caso di documento con firma elettronica invalida o comunque non correttamente

apposta, il controllo di tale firma, e più in generale ogni controllo formale e sostanziale del documento, è di competenza del responsabile del procedimento amministrativo cui il documento si riferisce.
Il personale dell'AOO in caso di perplessità su firme elettroniche apposte su documenti protocollati, può comunque richiedere un parere tecnico, sul caso specifico, all'RSP.

6 - DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

6.1 - Generalità

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni e le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.
Il SdP non mantiene evidenza dei documenti lavorati al di fuori delle procedure descritte nel presente capitolo.
I flussi di seguito descritti riguardano i documenti:

- ricevuti dall' AOO dall'esterno;
- ricevuti dall' AOO dall'interno e destinati ad essere ritrasmessi nell'ambito dell' AOO stessa;
- inviati dall' AOO all'esterno.

Le comunicazioni informali trasmesse fra i diversi uffici dell'AOO o fra questi e l'esterno, con o senza documenti allegati, non implicano invece alcuna attività connessa al protocollo informatico.
Il flusso in ingresso viene gestito in modalità centralizzata dal SdP che provvede alla protocollazione dei documenti ed al loro successivo smistamento all' UU di competenza.
Il flusso documentale in uscita e quello interno all'AOO è gestito dai singoli UU, secondo le regole descritte nel presente manuale e tramite le funzionalità previste dal SdP.

6.2 - Flusso dei documenti in ingresso all'AOO

6.2.1 - Ricezione di documenti analogici a mezzo posta convenzionale

I documenti pervenuti a mezzo posta sono ritirati giornalmente da un addetto del SdP presso l’ufficio postale interno.

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

In caso venga in tale fase individuata corrispondenza indirizzata ad altra Amministrazione, essa viene restituita al servizio postale che provvede ad inoltrarla all'indirizzo corretto.

La corrispondenza relativa a bandi di gara di norma è inviata su portali dedicati con procedura informatica idonea a garantire gli aspetti di integrità, riservatezza e non modificabilità degli atti trasmessi e qualora non possibile su protocollo informatico con procedura informatica, di analoghi requisiti, predisposta dalla Direzione.

Qualora fosse necessario servirsi di procedura analogica, l’ Ufficio postale del COMAER appone sulla busta la data e l'ora di arrivo della medesima, la busta viene successivamente registrata a protocollo con la segnatura applicata sull'esterno del plico chiuso e consegnata all'Ufficio competente.

Se presente, il modulo A/R viene firmato e datato dal personale che effettua la scansione della sola busta chiusa per poi essere riconsegnato presso l’Ufficio Postale per la trasmissione dello stesso al mittente.

La corrispondenza personale, eventualmente ricevuta, non viene aperta, né protocollata, ma viene consegnata al destinatario che ne valuterà il contenuto e, nel caso dovesse riguardare l'AOO, provvederà a inoltrarla al SdP per la registrazione.

I dipendenti dell’AOO non possono comunque servirsi di tale modalità di ricezione per la propria corrispondenza privata.

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

Tranne nei casi sopra citati ed in altri assimilabili, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione. La corrispondenza in ingresso viene aperta il giorno lavorativo in cui è pervenuta e protocollata.

Il contenuto della busta sarà scansionato nella sua totalità, se il documento è nei formati previsti per la scansione e consegnato in formato elettronico all'UU competente alla sua trattazione, presumibilmente nella stessa giornata nella quale è stata ritirata dall'Ufficio Postale.

Se non fosse possibile procedere alla dematerializzazione della corrispondenza pervenuta, viene scansionata la sola lettera di trasmissione, ai fini dell'apposizione del protocollo e successivamente viene consegnata l'intera documentazione in formato cartaceo all' UU competente.

Per ciò che attiene, invece, alla documentazione classificata, il personale addetto al Servizio di protocollo informatico provvede all'apertura della busta e consegna dell'incartamento presso l'Ufficio Punto Controllo Nato (P.C.N.) per la successiva trattazione a cura del personale preposto, previa registrazione di tale passaggio.

6.2.2 - Orari di protocollazione

I documenti in ingresso, informatici o analogici, vengono protocollati dal lunedì al venerdì, con il seguente orario:

- lunedì - giovedì dalle ore 07:30 alle ore 16:00;
- venerdì dalle ore 07:30 alle ore 12:00.

Relativamente alla protocollazione dei documenti in uscita, il software di protocollo è sempre operativo, ad eccezione del periodo in cui viene effettuata la stampa delle registrazioni di protocollo del giorno.

Il sistema effettua tale operazione in modalità automatica, intorno alle ore 24 di ogni giorno.

Durante tale attività, della durata di pochi minuti, potrebbe non essere garantito l'accesso al sottosistema di protocollazione.

6.2.3 - Gestione dei documenti

L'AOO gestisce i propri documenti con mezzi informatici.

Al fine di uniformare le modalità gestionali, anche i documenti analogici in ingresso vengono dematerializzati e gestiti, all'interno dei flussi di lavoro, in modalità informatica mediante produzione, tramite il software di protocollo, di copie per immagini su supporto informatico dei documenti analogici stessi.

Le copie così prodotte, con apposta firma elettronica dall'addetto del SdP di volta in volta incaricato sono successivamente protocollate.

6.2.4 - Sottoscrizione dei documenti elettronici

Il Direttore di NAVARM, nell'esercizio delle proprie funzioni, delega i Dirigenti e/o i Funzionari alla firma di documentazione amministrativa e tecnica, secondo le attribuzioni relative alla posizione organica dagli stessi pro tempore ricoperta (cfr. 1.8).

L'abilitazione alla firma sul Protocollo Informatico viene tecnicamente abilitata dall' RSP tramite apposita configurazione sul profilo dell'interessato.

La firma digitale apposta su file convertiti in formato PDF/A è di tipo PADES.

Gli allegati che, per la loro natura o per il loro utilizzo non possono o non devono essere firmati, sono conservati nel loro formato originale mediante l'utilizzo di apposita funzionalità presente nella fase di predisposizione del documento.

6.2.5 - Documenti protocollati e documenti esclusi dalla protocollazione

Sono oggetto di protocollazione tutti gli atti amministrativi inerenti all'attività dell'AOO.

Sono oggetto di registrazione obbligatoria i documenti ricevuti o inviati dall'Amministrazione e tutti i documenti informatici.

Sono esclusi dalle registrazioni di protocollo i documenti elencati nell'art.53 c.5 D.P.R. 445/2000 e cioè:

- gazzette ufficiali;
- bollettini ufficiali e notiziari della pubblica amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiali statistici;
- atti preparatori interni;
- giornali;
- riviste;
- libri;
- materiali pubblicitari;
- inviti a manifestazioni;
- tutti i documenti già soggetti a registrazione particolare dell'Amministrazione, quali i documenti soggetti a classifica di sicurezza nazionale con classifica superiore al non classificato controllato.

6.2.6 - Procedure di gestione casi particolari

I documenti:

- contenenti dati personali, genetici, biometrici e dati relativi alla salute o dati giudiziari (cfr. 1.9);
- di carattere e di indirizzo politico che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
- dalla cui pubblicità possa comunque derivare pregiudizio a terzi o al buon andamento dell'attività

amministrativa;

vengono gestiti con le specifiche di seguito indicate.

Questi documenti sono visibili soltanto dal personale preventivamente autorizzato a trattare dati personali, genetici, biometrici e dati relativi alla salute o dati giudiziari, ai sensi della normativa vigente, ed è fatto obbligo, pertanto, a tali utenti, di selezionare, nella fase di predisposizione, l'apposito campo "dati particolari/giudiziari", affinché venga messa in evidenza la peculiarità dei documenti trattati. Con tale procedura i documenti saranno visibili all'interno del sistema solo dagli operatori abilitati a tale particolare trattazione facenti parte dello stesso "campo di visibilità" dell'utente che ha predisposto il documento.

- Vengono trattati con le stesse modalità sopra descritte anche quei documenti con la classifica "I.N.C.C." (informazioni non classificate controllate) e classifiche equivalenti.

6.2.7 - Gestione del documento elettronico in ingresso

Il presente paragrafo descrive le procedure di trattazione del documento elettronico ricevuto (cfr 5.2) e dei relativi casi particolari (cfr. 5.9).

Di norma, la ricezione di un documento elettronico è assicurata tramite la casella di posta elettronica di cui al par. 1.10.

Il SdP provvede alla registrazione del documento ricevuto, salvo quanto discusso per la trattazione dei casi particolari, dopo aver eseguito la verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo ed alla assegnazione all'UU di competenza.

Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso sarà restituito al mittente.

L'operazione di ricezione del documento informatico avviene con le modalità previste dalle regole tecniche e normative vigenti, con particolare riferimento: allo standard del formato del documento, alle

modalità di trasmissione, alle informazioni minime e complementari comunemente scambiate tra le AOO e associate al documento, alla verifica dell'autenticità, della provenienza e dell'integrità della comunicazione.

Si forniscono di seguito delle regole tecniche utili per assicurare la corretta comunicazione con l' AOO:

- il formato preferibilmente accettato per file allegati ai messaggi di posta elettronica, come documenti primari, è il PDF e PDF/A;
- sono comunemente accetti anche i formati: JPG, P7M, TXT, TIFF e quelli utilizzati dai software Office considerati standard o standard de facto;
- i file allegati al documento primario possono altresì essere inviati in formati diversi se autorizzati dal SdP;
- i file allegati possono essere compressi nei formati ZIP o RAR;
- i file allegati devono avere una denominazione non troppo estesa (preferibilmente 8 caratteri) e priva di caratteri speciali;
- l'invio di allegati non previsti può comportare la ritrasmissione al mittente del messaggio;
- la dimensione massima complessiva degli allegati in entrata, per le caselle di cui al par. 1.10 sono di 100 MB per la casella PEC e di 30 MB per la casella PEI; in caso di superamento di tali limiti il messaggio non sarà recapitato all'AOO dal sistema di posta; allegati di dimensione superiore potranno essere inviati su supporto informatico (CD - DVD – USB);
- le eventuali marche temporali devono essere contenute nella stessa email del file firmato elettronicamente;
- l'eventuale apposizione di firma elettronica non valida rende liberamente valutabile il documento ricevuto;

• ogni email deve essere relativa e contenere la documentazione di singolo argomento; pertanto un mittente che debba inviare più documenti afferenti a pratiche diverse dovrà inviare tante email per quanti sono i documenti da trasmettere;

• l'oggetto dell'email con cui viene inviato il documento non deve superare i 255 caratteri.

Se un documento informatico viene inviato ad una casella di posta elettronica ordinaria afferente un UU dell'AOO il titolare di tale casella deve invitare il mittente ad inviare nuovamente il documento alla casella postale dell'AOO (cfr. 1.10) ai fini della protocollazione del documento stesso.

I messaggi inviati sulla casella di posta elettronica certificata vengono inseriti in una coda di tipo FIFO.

Ogni operatore del SdP, in dipendenza delle abilitazioni a lui concesse, accede alla coda di messaggi.

Se la protocollazione di un messaggio non viene completata, quel messaggio sarà trattato dal primo operatore che, subito dopo, accederà alla stessa coda dei messaggi.

L'operatore, quindi, procede alla protocollazione del messaggio, provvedendo all'assegnazione dello stesso all'UU competente ovvero, nei casi dubbi o quando il messaggio è palesemente non di competenza dell'AOO, lo invia in un apposito elenco, gestito dal RSP.

I documenti che vengono sottoposti alla successiva gestione del RSP, esperite le dovute verifiche, possono essere protocollati direttamente da quest'ultimo.

L'email certificata ricevuta che rientrasse nella categoria del c.d. SPAM, generalmente email pubblicitaria o commerciale, se proveniente da indirizzo PEC viene protocollata; se proveniente da email non certificata non viene protocollata e non viene spedito alcun messaggio al mittente.

Nel caso di email non certificata è comunque facoltà dell' RSP eliminare l'email inviando di massima un messaggio al mittente.

A tale scopo il sistema mette a disposizione una selezione di messaggi predefiniti o la possibilità di definirne uno specifico.

Tutti gli utenti dell' AOO devono porre particolare attenzione ai messaggi di posta elettronica certificata presenti in posta non consegnata in cui si possono trovare risposte inviate tramite i comuni client di posta ai messaggi inviati dalla stessa AOO.

Nel caso in cui il documento principale della email in ingresso non sia correttamente firmato elettronicamente, l'operatore addetto alla protocollazione inserirà la seguente nota: "documento privo di firma elettronica", provvedendo allo smistamento all'UU di competenza. Tale documento sarà valutato dall'UU competente che provvederà ad informare il mittente di eventuali criticità.

6.2.8 – Gestione del documento analogico in ingresso

Il documento ricevuto su supporto analogico, dopo le operazioni di registrazione e segnatura, è acquisito in formato digitale (copia per immagine di documento analogico) attraverso un processo di scansione che avviene secondo le fasi di seguito indicate:

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

Il documento analogico, dopo l'operazione di riproduzione in formato immagine, viene quindi protocollato ed archiviato in base alla sua tipologia.

Metadati principali di protocollazione sono i seguenti:

- Mittente;
- Oggetto;
- Protocollo mittente;
- Data protocollo mittente;
- Eventuali note.

Al documento analogico principale possono essere associati allegati analogici i quali vengono inseriti nella fase di scansione del documento di riferimento utilizzando un apposito separatore idoneo a distinguerli dal documento primario.

Possono, altresì, essere associati al documento primario allegati su supporto elettronico o ottico, i quali vengono annessi al documento principale scansionato e protocollato ed inviati all'UU di competenza.

Tutti gli addetti del SdP sono abilitati all'apposizione della propria firma elettronica sui documenti scansionati.

Nella generalità dei casi tuttavia, l' originale del documento analogico ricevuto, non viene inviato agli UU, ma è custodito nell'archivio corrente dell'AOO presso l'Ufficio del SdP, ed inserito sequenzialmente in appositi raccoglitori distinti per arco temporale.

Ciascun documento analogico indispensabile agli UU ai fini della successiva trattazione e per il prosieguo dell'iter amministrativo, viene invece archiviato direttamente all'interno del rispettivo UU competente, previa firma attestante il ritiro dello stesso su di un apposito registro gestito dall'Ufficio del SdP.

6.2.9 - Rilascio della ricevuta attestante la ricezione di un documento analogico

Quando un documento analogico è consegnato direttamente dal mittente o da altra persona incaricata al SdP ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, il personale del SdP che lo riceve è autorizzato a:

- rilasciare gratuitamente fotocopia della prima pagina del documento;
- apporre gli estremi della segnatura se contestualmente alla ricezione avviene anche la protocollazione;
- apporre sulla copia così realizzata il timbro dell'Amministrazione, con data e ora di ricezione unitamente a firma dell'operatore.

6.3 - Flusso dei documenti in uscita dall' AOO

6.3.1 – Gestione del documento elettronico in uscita

La documentazione elettronica è trasmessa, salvo motivate eccezioni, all'indirizzo elettronico certificato corrispondente al destinatario.

Il personale del SdP, e più in generale qualunque impiegato della Direzione che curi la redazione o la trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici, non può duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche. Come normativamente previsto, tutta la documentazione amministrativa dell' AOO viene prodotta in originale in modalità elettronica.

Quando l'iter procedimentale è perfezionato, il dirigente competente provvede a firmare elettronicamente il documento sul quale verrà apposta una marca temporale, in automatico dal software di protocollo all'atto della firma.

Il software di protocollo sulla base delle informazioni inserite nella fase di predisposizione dello specifico documento, provvede ad inviare, per posta elettronica, il documento primario e tutti gli eventuali allegati presenti.

L'utilizzo della casella postale elettronica istituzionale, in luogo di quella di posta elettronica certificata, deve considerarsi residuale e viene selezionato dall'operatore che ha predisposto la pratica, può altresì essere modificato da tutti coloro i quali hanno titolo a farlo fino alla firma del documento stesso. È importante precisare che il software di default, è impostato per l'invio della documentazione sulla casella di posta elettronica certificata del destinatario.

Al fine di inviare correttamente un documento elettronico è necessario attenersi ad alcune regole relative alla preparazione del file che deve essere allegato in fase di predisposizione:

• utilizzare il modello nel formato RTF all'uopo predisposto e il cui facsimile è disponibile sulla rete intranet della Direzione (il sistema provvederà alla successiva conversione in formato PDF/A del documento all'atto della firma dello stesso);

• nella denominazione del file non si devono utilizzare caratteri speciali e/o lettere accentate o punti; si suggerisce, eventualmente, di utilizzare il carattere _ (underscore) al posto di tali caratteri;

• è altresì opportuno che il nome del file sia di lunghezza limitata.

È necessario segnalare che, qualora come allegato venga inserito un documento elettronico già firmato elettronicamente, l'operatore che sta effettuando la predisposizione debba usare l'apposita funzionalità per negare la firma del documento, al fine di evitare la successiva conversione in PDF/A del documento.

6.3.2 - Gestione del documento analogico in uscita

Come già segnalato in precedenza, nell'ambito dell'AOO vengono prodotti esclusivamente documenti originali informatici.

Tuttavia, come già ampiamente indicato nei paragrafi precedenti può essere necessario procedere alla trasmissione attraverso il servizio postale convenzionale di un particolare documento.

La procedura di preparazione di un tale documento da parte dell'operatore incaricato è già stata descritta precedentemente.

Se il documento deve poi essere trasmesso per posta ordinaria, viene portato, già imbustato e predisposto all'invio, presso il locale preposto al Servizio Postale che provvederà al successivo inoltro all'Ufficio Postale del sedime.

È fatto obbligo agli addetti di ogni Segreteria di Reparto, di compilare in maniera leggibile ed in tutta la sua interezza l'apposita modulistica richiesta a corredo di ciascuna tipologia di spedizione dal Servizio Postale.

Inoltre, al fine di evadere tempestivamente il flusso della corrispondenza in uscita, il documento da spedire deve essere consegnato al personale preposto, per consentirne in tempo utile lo smistamento presso l'Ufficio Postale.

6.4 - Assegnazione dei documenti ricevuti e procedure di classificazione

Gli addetti all'Ufficio di protocollo provvedono ad inviare il documento ai Capi degli UU interessati o personale delegato dagli stessi che provvedono alla successiva gestione interna all' UU:

- eseguono una verifica preliminare di congruità;
- in caso di errore restituiscono il documento al RSP con eventuale annotazione in merito alla competenza se conosciuta, che provvederà a riassegnare il documento all' UU competente;
- in caso di verifica positiva, eseguono l'operazione di presa in carico riassegnandola al proprio interno ad un UU;
- l'UU che gestisce la documentazione provvede alla classificazione del documento sulla base del titolario di classificazione in essere presso l'AOO.

L'assegnazione dei documenti pervenuti in originale informatico avviene, normalmente, entro la giornata di ricezione.

Per i documenti pervenuti in modalità analogica, deve essere tenuto in considerazione il tempo medio necessario per le attività di dematerializzazione, descritte nel paragrafo inerente alla gestione del flusso in ingresso della documentazione analogica.

Nel caso di pratiche afferenti materie trattate dalla Direzione, ma di competenza di altro Ente/Comando ed erroneamente indirizzate a NAVARM, sarà cura del UU competente di provvedere al relativo inoltro all'Ente di pertinenza.

Non è invece onere del personale del SdP controllare la completezza formale e sostanziale della documentazione pervenuta e soggetta alle operazioni di protocollazione. Tale verifica e le azioni conseguenti sono di competenza dell' UU interessato alla tematica.

6.5 – Email certificate non consegnate

Il software di protocollo evidenzia i messaggi che segnalano all'AOO mittente NAVARM un problema di ricezione del documento inviato alla casella postale del destinatario.

Questi messaggi sono automaticamente inseriti come ricevute allegate al documento che non ha raggiunto il destinatario; tale documento, pertanto, con le relative ricevute, viene ricollocato dal sistema sulla scrivania virtuale nella voce "posta non consegnata" del primo utente che ha predisposto il documento (tale messaggio è visibile anche da qualsiasi utente sulla cui scrivania è transitato il documento), per le opportune azioni del caso.

In questi casi, l'utente, dopo le necessarie verifiche, può:

- nuovamente inviare il documento alla casella postale iniziale;
- inviare il documento ad una casella postale diversa;
- provvedere alla materializzazione del documento per la successiva trasmissione per posta ordinaria.

È consigliabile, per quanto esposto, verificare con adeguata periodicità l'eventuale presenza di messaggi non recapitati nella casella "posta non consegnata".

In caso di modalità informali di invio delle risposte alle comunicazioni inviate dall'AOO si può verificare che tali risposte arrivino direttamente alla "posta non consegnata" anziché nel flusso in ingresso gestito dal SdP.

6.6 - Conservazione dei documenti nell'archivio corrente

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

- classificazione 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.

La creazione e la gestione dei fascicoli informatici è riservata al personale del SdP.

6.7 – Trasmissione FAX

Il SdP non prevede ricezione/invio via fax.

Ai sensi dell’art.47 c.2 lett.c del CAD è esclusa la comunicazione via fax tra PP.AA.

7 - ARCHIVI

7.1 - Archivio dell’AOO

Sulla base della normativa vigente, l’ AOO prevede un’organizzazione archivistica così articolata:

• archivio corrente: è costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o verso i quali sussista comunque un interesse, laddove non sia intervenuta la prescrizione in aderenza al Codice Civile; tali documenti, protocollati nel periodo corrente, sono immediatamente disponibili;

• archivio di deposito: è il complesso dei documenti relativo ad affari e a procedimenti amministrativi conclusi entro i 40 anni; detti documenti non risultano più necessari per il corrente svolgimento del procedimento amministrativo, anche se verso tali documenti può tuttavia sussistere un interesse sporadico;

• archivio storico: è costituito da documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l’effettuazione delle operazioni di scarto, alla conservazione perenne.

L’AOO produce esclusivamente documenti digitali per i quali è prevista un'archiviazione nell'ambito del software di protocollo su sistema di base di dati.

7.2 - Archiviazione dei documenti informatici

I documenti informatici sono archiviati su supporti di memorizzazione gestiti dalla Struttura che eroga il servizio in modo non modificabile e contestualmente alle operazioni di registrazione e segnatura di protocollo.

Ogni giorno viene anche prodotto il registro giornaliero delle registrazioni di protocollo, firmato con firma digitale in modalità manuale o automatica.

7.3 - Archiviazione dei documenti analogici

I documenti analogici preesistenti l'attuale sistema di protocollo non sono oggetto di modifiche di archiviazione, se non quelle connesse al normale decorso del tempo.

Per i documenti che attualmente continuano a pervenire in modalità analogica e per i quali non è previsto o non si decide il rinvio al mittente (vedasi documenti ricevuti - casi particolari), si procede alla generazione di copie per immagine su supporto informatico di documento analogico secondo la modalità prevista dal software di protocollo in uso a cura del SdP. Gli originali analogici sono custoditi nell’archivio corrente del Servizio di Protocollo Informatico ed inseriti, senza alcuna catalogazione, in appositi contenitori. Se i documenti analogici così duplicati sono necessari anche in originale analogico agli UU di competenza vengono ad essi consegnati, previa apposizione di firma su apposito registro conservato dal SdP o con procedura informatica equivalente.

8 - REGISTRAZIONI DI PROTOCOLLO

8.1 - Attribuzione del protocollo

Il SdP appone al documento protocollato un riferimento di protocollo, come previsto dalla normativa vigente.

Gli UU dell'AOO sono informati della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del protocollo nonché di segnalare la tipologia di documenti contenenti tali dati utilizzando le funzionalità del software di protocollo.

8.2 - Registro informatico di protocollo

Il SdP provvede, in fase di chiusura dell'attività di protocollo giornaliera e comunque entro il successivo giorno lavorativo, ad effettuare le seguenti operazioni:

- estrazione delle registrazioni giornaliere nel file del registro di protocollo;
- applicazione della firma digitale al file così realizzato;
- conservazione automatica del file firmato con le funzionalità previste dall'applicazione di protocollo.

9 - IL REGISTRO DI EMERGENZA

9.1 - Apertura del registro di emergenza

Ogni qualvolta, per cause tecniche, non è possibile utilizzare il software di protocollo in modalità realtime per periodi di tempo rilevanti, il RSP o, in sua assenza, un delegato del SdP autorizza un registro di emergenza per le operazioni di protocollo, per il periodo di tempo strettamente necessario.

Anche in situazioni di emergenza, è fatto divieto agli UU dell'AOO di creare registri di protocollo diversi da quello gestito dal SdP.

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

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, l'RSP o un delegato del SdP in sua assenza autorizzano l'uso del registro di emergenza con cadenza giornaliera.

9.2 - Chiusura del registro di emergenza e sincronizzazione del registro di protocollo

Venuti meno i motivi che hanno causato il ricorso al registro di emergenza, il RSP o in sua assenza un membro del SdP delegato chiudono il registro di emergenza apponendovi una dichiarazione con data ed ora della chiusura dello stesso.

I documenti ricevuti e protocollati in emergenza, vengono nuovamente protocollati usando la normale metodologia e riportando, anche in tale fase, il numero loro assegnato nella fase di protocollo di emergenza, mediante la funzionalità di annotazione del software di protocollo.

I documenti inviati in tali circostanze in modalità analogica, perché ritenuti indifferibili, sono invece protocollati con analoga procedura, ma non ritrasmessi, registrando il loro invio avvenuto come documenti analogici.

Per tenere traccia del protocollo di emergenza, anche in tal caso, si utilizzerà il metadato del protocollo mittente. La procedura si conclude protocollando anche il registro di emergenza come documento interno all'AOO.

10 - APPROVAZIONE E AGGIORNAMENTO MANUALE, NORME FINALI

10.1 - Modalità di approvazione e aggiornamento del manuale

L'Amministrazione adotta il presente "Manuale di gestione" su proposta dell’RSP.

Il presente manuale dovrà essere aggiornato a seguito di:

- cambiamenti della normativa d’interesse;
- introduzione di nuove e diverse metodologie sostitutive di quelle menzionate o ad esse complementari, adottate con il fine di migliorare quelle in uso o per la necessità di contemplare tipologie di trattazione dei documenti non precedentemente adottate;
- modifiche apportate negli allegati.

10.2 - Abrogazioni

Il presente manuale sostituisce ed abroga il precedente e tutti i regolamenti interni all'AOO nelle parti contrastanti con lo stesso.

10.3 - Pubblicità del presente manuale

II presente manuale è disponibile alla consultazione del pubblico che ne può prendere visione sul sito istituzionale dell'Amministrazione, nell'apposita area dedicata.

Esso è reso disponibile inoltre nell’area intranet dell’AOO.

10.4 - Operatività del presente manuale

II presente manuale entra in vigore dopo 15 gg dalla sua pubblicazione sul sito istituzionale della Direzione.