RAPPRESENTANZA MILITARE ITALIANA PRESSO IL COMANDO SUPREMO DELLE POTENZE ALLEATE IN EUROPA

M A N U A L E D I G E S T I O N E

DEL PROTOCOLLO INFORMATICO

Edizione 2024

ATTO DI APPROVAZIONE

Approvo il presente:

"MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DELLA RAPPRESENTANZA MILITARE ITALIANA PRESSO IL COMANDO SUPREMO DELLE POTENZE ALLEATE IN EUROPA. Edizione 2024",

che abroga e sostituisce il precedente.

IL RAPPRESENTANTE MILITARE ITALIANO
Gen. D. Paolo RICCÒ

Firmato Digitalmente da/Signed by:
PAOLO RICCO'

In Data/On Date:
venerdì 7 giugno 2024 09:45:56

PREMESSA

Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, prevedono l'adozione del "Manuale di gestione del protocollo informatico, dei documenti e dell'archivio" per tutte le amministrazioni di cui all'articolo 2, comma 2, del Decreto Legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale.

Il presente Manuale di Gestione, redatto secondo quanto previsto dalle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici", descrive il sistema di gestione anche ai fini della conservazione dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio, per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

In questo ambito, è previsto che ogni Amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo n.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 di questo Manuale di Gestione è quello di descrivere sia il sistema di gestione documentale, a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili per gli addetti al servizio e per i soggetti esterni che a diverso titolo interagiscono con l'Amministrazione. Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale sulla quale avviare il processo di ammodernamento e di trasparenza dell'attività dell'Amministrazione.

Il presente Manuale di Gestione è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni necessarie per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti, pertanto, si rivolge non solo agli operatori di protocollo, ma in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'Amministrazione ed in particolare, nel nostro caso, con questa Rappresentanza Militare Italiana presso S.H.A.P.E..

Eventuali commenti, suggerimenti e proposte di modifica al Manuale, possono essere inviate direttamente all'autore del presente documento, di seguito riportato:
ITALDELEGA "Rappresentanza Militare Italiana presso S.H.A.P.E." – Sezione Affari Generali.
Email: idshape.csezaagg@smd.difesa.it
Telefono: +39 06 46916 3312 - VoIp: 2063312

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

1	
2	
3	
4	
5	
6	
7	

SOMMARIO

ALLEGATI:

A. **"ELENCO DELLE PRINCIPALI ABBREVIAZIONI".**
B. **"ISTRUZIONI PER LA REDAZIONE DEL MANUALE DI AOO".**
C. **"SCHEMI DI FLUSSO IN ENTRATA ED USCITA DEI DOCUMENTI".**
D. **"REGOLE GENERALI DI SCRITTURA DEI DATI".**
E. **"MODELLO DI O.D.G./O.D.S. DI DELEGA DELLE FUNZIONI DI RDS/OPERATORE".**
F. **"IL TITOLARIO O PIANO DI CLASSIFICAZIONE".**

1. MODELLO ORGANIZZATIVO

Il presente documento definisce le regole ed i principi per la gestione della documentazione prodotta e archiviata negli enti dell'Area Tecnico-Operativa Interforze (T.O.I.) dipendenti dallo Stato Maggiore della Difesa, fornendo le istruzioni necessarie ad assicurare il corretto funzionamento dei servizi per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. L'Area T.O.I. è composta da una pluralità di Enti e Comandi articolati su più Aree Organizzative Omogenee (AOO), compresa Italdelega.

1.1. AREE ORGANIZZATIVE OMOGENEE

Ai sensi dell'art. 50 del Testo Unico, le AOO sono gli insiemi di "Uffici da considerare ai fini di una gestione unica e coordinata dei documenti". L'elenco delle AOO dell'Area T.O.I., pubblicato sul sito della Difesa, è suscettibile di modifiche in relazione all'esigenza di nuove AOO o alla loro riorganizzazione.

1.2. COORDINATORE DELLA GESTIONE DOCUMENTALE

Al fine di garantire criteri uniformi per la gestione dei documenti nelle diverse Unità Organizzativa (UO), questa Rappresentanza Militare ha individuato il Responsabile Del Servizio (RDS) nel Capo Sezione Affari Generali.

Il RDS assolve i compiti indicati nelle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici e, in particolare:

- definisce ed assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna tra le Unità Organizzative;
- predispone il Manuale di gestione ai fini della conservazione dei documenti informatici e istruzioni per il corretto funzionamento dei servizi per la tenuta del protocolli informatici, della gestione dei flussi documentali e degli archivi;
- è sostituito dal Vicario nei casi di vacanza, assenza o impedimento.

1.3. RESPONSABILE DEL SERVIZIO (RDS)

Per ogni AOO deve essere nominato un RDS preposto alla gestione documentale del protocollo informatico e gestione documentale, del Servizio di protocollo informatico e gestione documentale. Il RDS deve essere un dirigente o funzionario, Ufficiale con il grado minimo di Capitano (o equivalente) ovvero dipendente civile a partire dalla categoria C1.
Il RDS assicura il rispetto, nell'ambito dell'AOO, delle indicazioni contenute nel presente Manuale e definisce le scelte organizzative connesse alla gestione documentale e al protocollo informatico di sua competenza.
In particolare, il RDS:

- attribuisce il livello di autorizzazione per l'accesso alle funzioni del sistema di protocollo informatico e di gestione documentale;
- garantisce lo svolgimento delle operazioni di registrazione e di segnatura di protocollo, nel rispetto nel rispetto delle normative vigenti;
- si adopera, in caso di guasti o anomalie, affinché le funzionalità del sistema siano ripristinate nel più breve tempo possibile;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali;

- autorizza le operazioni di annullamento delle registrazioni di protocollo di cui all'articolo 54 del DPR 445/2000;
- predispone il Manuale di AOO, secondo il modello riportato in Allegato "B", riportando, altresì, le determinazioni assunte in materia di gestione documentale in relazione alle specifiche esigenze dell'AOO;
- autorizza l'apertura del registro di emergenza nella modalità *stand alone* dopo aver accertato l'indisponibilità del sistema e, dopo aver verificato il ripristino del suo corretto funzionamento, ne dispone la chiusura;
- per la rilevanza dei compiti assegnati e per la funzione da svolgere, anche verso l'esterno dell'AOO, la nomina del RDS è effettuata con Ordine del Giorno.

Nel caso di avvicendamento del RDS, il nuovo Responsabile deve prendere visione del Manuale di AOO, verificare le regole in esso contenute ed eventualmente modificarle, aggiornandolo. Le regole contenute nel Manuale di AOO si intenderanno valide fino alla pubblicazione della nuova versione.

1.4. VICARIO DEL RDS

Per i casi di vacanza, assenza, impedimento o comunque, nelle veci del RDS, interviene il "Vicario" appositamente individuato per tale funzione.

In caso di contemporanea assenza del RDS e del suo Vicario, anche per un solo giorno, sarà indispensabile nominare comunque, con atto formale, un dipendente dell'AOO che svolga, per il tempo strettamente necessario, il ruolo di RDS.

1.5. MANUALE DI GESTIONE

Il presente Manuale del protocollo informatico, dei flussi documentali e degli archivi della Rappresentanza contiene le regole per la gestione dei servizi di protocollo, l'uso dei titolari di classificazione e le regole per la costituzione e manutenzione dei fascicoli elettronici nell'ambito dell'Area di pertinenza. In particolare, il Manuale:

- definisce le modalità di relazione con l'utenza, con particolare riferimento alla ricezione dei documenti cartacei;
- descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, all'AOO individuando le responsabilità connesse alla relativa gestione;
- definisce le regole di registrazione, di smistamento e di assegnazione dei documenti ricevuti;
- indica le UO responsabili delle attività di registrazione di protocollo e i relativi orari di operatività;
- individua le tipologie di documenti esclusi dalla registrazione di protocollo o soggetti a registrazione particolare;
- riporta le modalità di utilizzo del registro di emergenza.

1.6. APPLICABILITÀ DEL MANUALE

I principi gestionali contenuti nel Manuale si applicano ai flussi documentali, in entrata, uscita ed interni alle UO di Italdelega SHAPE. Il Manuale è aggiornato a cura del RDS è pubblicato sul sito internet dell'AD, nelle pagine dello Stato Maggiore della Difesa.

1.7. MANUALI DI GESTIONE DELLE AOO.

Il RDS assicura il rispetto, nell'ambito di Italdelega, delle indicazioni contenute nel presente Manuale.
Il Manuale entra in vigore con Ordine del Giorno e viene aggiornato ogni qualvolta il RDS lo ritiene opportuno. Il RDS richiede tempestivamente la pubblicazione di ogni nuova versione del Manuale di AOO sul sito internet della Difesa, nella pagina dell'Ente.

1.8. SERVIZIO DI PROTOCOLLO INFORMATICO E GESTIONE DOCUMENTALE

Si tratta di una funzione svolta dalle Sezioni. L'UO responsabile delle attività di registrazione di protocollo ed i relativi orari di servizio devono essere indicati nel Manuale di AOO.

1.9. CARATTERISTICHE GESTIONALI

La gestione dei documenti informatici nelle AOO di Italdelega avviene secondo un modello di protocollazione:

- accentrata, per la posta in ingresso, nel *Registry* di Italdelega, in quanto tutta la corrispondenza indirizzata dove essere registrata in un unico punto dagli addetti dell'UO a livello di Sezione/Nucleo che assicura le funzionalità del Protocollo Informatico;
- distribuita, per i documenti informatici in uscita o interni, in quanto le Sezioni possono protocollare e trasmettere direttamente la documentazione prodotta.

In Allegato "C" sono riportati gli schemi di flusso in entrata ed uscita dei documenti informatici.

1.10. APPLICATIVO UTILIZZATO

L'intero processo di gestione dei documenti e del processo di protocollazione sono gestiti attraverso il sistema di protocollo informatico e gestione documentale ADHOC.
Tutte le informazioni di dettaglio inerenti alle funzionalità presenti nel sistema ADHOC sono reperibili in una raccolta *online* sulla maschera "cruscotto" dell'applicativo, nella voce "Bollettini" e nella voce "Guida".
Per le specifiche procedure di accesso ai vari menù e funzionalità, si rinvia alla consultazione della predetta documentazione.

1.11. IL SISTEMA DEI REGISTRI E LE TIPOLOGIE DOCUMENTALI

E' istituito il Registro Generale di Protocollo, per la registrazione delle comunicazioni ricevute, spedite ed interne alla AOO. Si possono utilizzare, inoltre i registri disponibili sul sistema ADHOC per la registrazione di particolari tipologie di documenti. I registri aggiuntivi sono attivati dal RDS e possono riguardare le registrazioni in ingresso (ad esempio le fatture) gli atti interni (Ordini del Giorno e decreti) o particolari procedimenti (le gare).
Ciascun registro è identificato da:

- un codice, utilizzato come prefisso nella segnatura di protocollo, di tre caratteri, a cui sarà automaticamente aggiunto l'anno nel quale si effettua la registrazione dei documenti (REG2024, per il Registro Generale del 2024);

- una descrizione che di norma è fissa, predefinita nel sistema e in alcuni casi è personalizzabile.

Di seguito si riportano alcuni dei registri attivabili con il sistema ADHOC, indentificati con il codice di 3 caratteri e la relativa descrizione:

- REG Generale (sempre attivo);
- APT Note/Appunti;
- COO Coordinamento;
- ODG Ordini del Giorno;
- ODS Ordini di Servizio;
- FAT Fatture;
- RFT Rifiuto Fatture;
- GEP Gestione Personale;
- RVA Richiesta variazioni;
- CDS Consiglio di Stato;
- GAR Gare;
- DE1 Decreti ed atti a rilevanza esterna (personalizzabile).

2. FORMAZIONE, REGISTRAZIONI E ARCHIVIAZIONE DEI DOCUMENTI

2.1. FORMAZIONE

In aderenza alla normativa vigente (art. 40 del [CAD]), Italdelega produce esclusivamente documenti originali informatici con l'uso della firma digitale. I titolari che hanno capacità di firma sono indicati dai Capi AOO/UO.
I documenti cartacei in ingresso vengono dematerializzati in modo che l'intero flusso documentale venga gestito in maniera elettronica.
Il documento deve trattare un unico argomento, indicato in maniera sintetica nello spazio riservato all'oggetto.
L'intera documentazione amministrativa, in pratica tutti i documenti informatici firmati digitalmente, viene gestita dal protocollo informatico nel formato PDF/A.
Gli allegati che, per la loro natura o per il loro utilizzo, non possono o non devono essere convertiti, sono conservati nel loro formato originale.
I documenti, analogici o informatici, vengono gestiti in relazione al loro formato, nell'ambito di Italdelega e suddivisi nel seguente modo:

- in ingresso;
- in uscita;
- interno.

2.2. FLUSSI DELLA DOCUMENTAZIONE

Per quanto attiene ai documenti informatici, Italdelega utilizza due canali principali:

- casella di Posta Elettronica Istituzionale (PEI);
- casella di Posta Elettronica Certificata (PEC che riceve esclusivamente messaggi inviati da altre caselle PEC);

La posta analogica viene inviata e ricevuta attraverso i seguenti canali:

- servizi postali ufficiali (Bolgetta diplomatica) ed altri operatori abilitati;
- a mezzo "corriere militare".

Le documentazioni pervenute attraverso canali differenti non assumono rilevanza ufficiale e il loro eventuale assoggettamento a protocollo deve essere valutato alla luce delle normative vigenti.
Le caselle di posta elettronica e l'indirizzo postale per la ricezione della corrispondenza cartacea sono resi pubblici con le modalità previste dalle normative vigenti.

2.3. PROTOCOLLAZIONE E REGISTRAZIONE

All'interno di Italdelega tutti i documenti devono essere oggetto di registrazione. In particolare, per i documenti ricevuti o inviati, la registrazione di protocollo prevista dall'art. 53 del DPR 445/2000 ha la funzione giuridica di garantire la trasparenza amministrativa in relazione alle operazioni di ricezione e di invio.
Tramite i registri di Protocollo Generale e gli altri registri istituiti con le finalità indicate nel presente Manuale, è possibile registrare ufficialmente l'esistenza di un documento all'interno della AOO e tenere traccia delle sue movimentazioni.

2.4. UNICITÀ DELLA REGISTRAZIONI

Le registrazioni di protocollo sono uniche, cosi come la numerazione progressiva delle stesse. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo. I numeri di protocollo individuano un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Il numero di protocollo è costituito da almeno sette cifre numeriche.

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

La documentazione non registrata presso la AOO è considerata giuridicamente inesistente presso l'Amministrazione. Non è consentita la protocollazione di un documento già protocollato.

In sintesi, i registri quali atti pubblici originari che fanno fede della formazione, tempestività e dell'eventuale ricevimento o spedizione dei documenti, indipendentemente dalla regolarità degli stessi, sono idonei a produrre effetti giuridici.

2.5. DATI DELLA REGISTRAZIONE DI PROTOCOLLO

Il sistema, per ciascuna registrazione di protocollo prevede l'inserimento dei dati previsti all'art. 53 [DPR] con le regole ivi descritte. In particolare:

- il numero progressivo viene generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione è assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente per i documenti ricevuti o, in alternativa, il/i destinatario/i per i documenti spediti, sono registrati in forma non modificabile e reperiti nella tabella dei mittenti e destinatari del sistema informatico;
- l'oggetto del documento è registrato in forma non modificabile;
- la data e il protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico calcolata con l'algoritmo SHA-256.

Nella redazione dei campi "oggetto" e in generale, ogni qualvolta sia necessario digitare una descrizione nel sistema informatico, è necessario riferirsi a quanto riportato in Allegato "D". Nel caso in cui si tratti di un documento informatico proveniente da una P.A., dotato di file "segnatura.xml", i relativi dati saranno utilizzati a completamento automatico delle informazioni afferenti alla registrazione di protocollo.

2.6. SEGNATURA DI PROTOCOLLO DEI DOCUMENTI

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

Sui documenti in ingresso, se presente, vengono utilizzati dati contenuti nel file "segnatura.xml", purché conforme alle indicazioni della [CIRC].

Se è attivata la produzione e la firma automatica del registro giornaliero di protocollo, la segnatura di protocollo viene anche apposta nella porzione in alto a sinistra della prima pagina del documento primario. Tale segnatura viene anche firmata in modalità automatica dal RDS. Il file "segnatura.xml" viene allegato a tutti i documenti in uscita per posta elettronica.
Il formato della segnatura di protocollo delle AOO, conformemente alla normativa, prevede i seguenti dati che, a titolo di esempio, sono stati riferiti alla AOO di SMD:

- Codice dell'Amministrazione: **M_D**;
- Codice dell'AOO: **A46D85F**;
- Codice del registro: **REG**;
- Numero di protocollo: **1234567**;
- Data di registrazione: **gg-mm-aaaa**.

La segnatura di protocollo risulterà, pertanto: **M_D A46D85F REG2023 1234567 02-01-2023**.

2.7. DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE

Il sistema documentale utilizzato è abilitato alla trattazione dei documenti "NON CLASSIFICATI". La posta classificata erroneamente pervenuta al protocollo deve essere posta all'attenzione dell'Ufficiale alla Sicurezza di Italdelega.
Inoltre, sono esclusi dalla registrazione di protocollo:

- Gazzette Ufficiali;
- bollettini ufficiali P.A.;
- notiziari P.A.;
- note di ricezione circolari;
- note di ricezione altre disposizioni;
- materiali statistici;
- giornali, riviste e libri;
- materiali pubblicitari;
- inviti a manifestazioni che non attivino procedimenti amministrativi;
- documenti classificati;
- documenti già soggetti a registrazione particolare dell'AD;
- fogli di viaggio;
- note caratteristiche;
- registro delle presenze;
- modelli 730;
- posta classificabile come spam.

2.8. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

Non è possibile modificare anche un solo campo tra quelli obbligatori nella registrazione di un protocollo. Per correggere eventuali errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, è necessario annullare l'intera registrazione ed inserirne una nuova.
Solo il RDS è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo. Il registro elettronico, mediante la funzione "visualizza gli annullati", riporta i motivi dell'annullamento. L'annullamento di una registrazione di protocollo può

avvenire anche su richiesta delle UO, specificando, in una apposita nota, i motivi, ma non può riguardare i contenuti trattati nel documento. In tali casi è l'UO assegnataria, competente per la materia, che deve provvedere ad informare il mittente, con apposite comunicazione PEI/PEC, sulla base di quanto ricevuto. Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data e l'ora dell'annullamento.
È sempre possibile visualizzare, per gli utenti abilitati, i documenti annullati e le relative motivazioni di annullamento. L'annullamento di una registrazione di protocollo comporta l'invio automatico, da parte del sistema ADHOC, di un messaggio al mittente con la motivazione che è stata inserita nella fase di annullamento (ad es: esigenza della firma elettronica, della copia di un documento d'identità o quanto necessario per la corretta registrazione a protocollo).

2.9. PRIVACY E TUTELA DEI DATI PERSONALI

La trattazione dei documenti contenenti dati personali, sensibili e giudiziari deve avvenire nel rispetto della legge. Per i documenti contenenti dati personali o dati sensibili (cioè quelli idonei a rivelare: l'origine razziale ed etnica, le convinzioni religiose, filosofiche od altro, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale) e dati giudiziari, sono previste particolari forme di riservatezza e di accesso controllato, mediante la selezione di un filtro elettronico. I dati in questione devono essere individuati come tali nel sistema di protocollo, selezionando l'apposita casella di spunta, sin dal momento della loro protocollazione in ingresso o in uscita.
Qualora un documento contenente dati sensibili e personali non venga individuato al momento della protocollazione è compito di chiunque ne riconosca le caratteristiche provvedere ad integrare la registrazione di protocollo attribuendo al documento la spunta prevista.
In generale, è opportuno che venga posta particolare attenzione, a partire dal momento della protocollazione, alla redazione dell'oggetto del documento per escludere la possibilità che da esso possano desumersi dati sensibili e personali (anonimizzazione).

2.10. PRODUZIONE DEI REGISTRI GIORNALIERI

Il sistema provvede alla generazione delle registrazioni di protocollo della giornata. Durante tale attività, della durata di pochi minuti, non è possibile protocollare atti né in uscita né in entrata.
I registri particolari entrano nella gestione quotidiana al pari del Registro Generale e, dopo aver staccato il primo numero di protocollo, anche tale registri vengono firmati ogni giorno per consentire successive protocollazioni.
La stampa delle registrazioni giornaliere viene firmata digitalmente in modalità automatica a cura del RDS. La stampa viene archiviata all'interno del sistema ed è sempre possibile effettuarne copie cartacee o digitali.

3. LA GESTIONE DEI DOCUMENTI INFORMATICI

3.1. SPECIFICHE DEI DOCUMENTI INFORMATICI IN INGRESSO

Le AOO dell'Area T.O.I. sono predisposte alla ricezione e gestione di documenti informatici tramite una casella PEI ed una casella PEC, pubblicate anche sulle pagine del protocollo informatico della AD.

Sono accettati i documenti informatici conformi alle seguenti regole:

- il formato preferibile per file allegati ai messaggi di posta elettronica, come documenti primari, sono il PDF ed il PDF/A;
- sono accettati anche i formati JPG, P7M, TXT, TIFF, TIF, XML;
- i file allegati al documento primario, oltre ai predetti formati, possono essere in formato ZIP o nei formati concordati con l'U.O. interessata;
- l'invio di allegati non previsti comporta la ritrasmissione al mittente del messaggio;
- le marche temporali apposte alle firme digitali devono essere in formato *embedded* e non *detached*;
- l'apposizione di firma digitale non valida rende inutilizzabile il file trasmesso;
- ad ogni trasmissione deve essere associata la documentazione relativa ad un unico argomento quindi il mittente che deve inviare cinque diverse pratiche, dovrà effettuare cinque diversi invii;
- la casella postale del mittente deve essere riferita alla persona giuridica (ad esempio, la ditta ROSSI SPA dovrà inviare la propria documentazione dalla casella postale rossispa@xxxxx.it e non dalla casella postale mario.rossi@rossispa.xxxxx.it);
- il nome dei file allegati deve essere di lunghezza moderata, non contenere spazi, lettere accentate, caratteri speciali, virgolette e apici. Si suggerisce di utilizzare il carattere "_" (*underscore*) al posto dei predetti caratteri, (ad esempio "richiesta_di_risarcimento.pdf" o "foto_di_citta.jpg"). Da evitare nomi come "1° documento.pdf" oppure "si.trasmette.domanda.pdf".

Se un documento informatico viene inviato ad una casella di posta elettronica ordinaria personale o funzionale, il titolare di tale casella deve inviare un messaggio al mittente segnalando la necessità di inviare nuovamente il documento alla corretta casella postale PEI/PEC dell'AOO.

3.2. PROCEDURE PER IL PROTOCOLLO DEI DOCUMENTI INFORMATICI IN INGRESSO

I messaggi giunti sulle caselle di posta vengono inseriti in un'apposita coda alla quale accedono gli addetti al protocollo.

Gli addetti protocollano il messaggio, procedendo alla successiva assegnazione all'UO competente ovvero, nei casi dubbi, invia il messaggio ad un apposito elenco, denominato "lista RDS".

Se la protocollazione di un messaggio non viene completata, il messaggio viene nuovamente presentato nella coda dei messaggi.

I documenti inseriti nella "lista RDS" vengono gestiti dal RDS e possono essere protocollati, rispediti al mittente (solo per la PEI) o gestiti dal personale incaricato, secondo le deleghe ed i profili di accesso assegnati dal RDS.

Gli addetti al protocollo inviano anche i messaggi erroneamente pervenuti all'AOO alla predetta "lista RDS".
Se il RDS accerta un errore di spedizione provvede affinché venga inviato al mittente una comunicazione tramite un'apposita lettera o una notifica di eccezione.
I documenti in ingresso sono assegnati giornalmente, tramite le UO, ai Responsabili del Procedimento Amministrativo (RPA) e/o ai sostituti da essi incaricati, che provvedono alla successiva gestione interna. Gli utenti, tramite la funzionalità "Gestione delle deleghe", possono stabilire l'utente che subentra nella gestione della corrispondenza durante il loro periodo di assenza.
Il controllo della completezza formale e sostanziale della documentazione pervenuta è di competenza del personale dell'UO che tratta la specifica tematica. Qualora sia necessario acquisire ulteriori documenti, l'UO provvede direttamente a richiederli al mittente.
Le e-mail considerate spam non vengono protocollate e non viene spedito nessun messaggio al mittente.

3.3. DOCUMENTI INFORMATICI PROVENIENTI DA ALTRE PUBBLICHE AMMINISTRAZIONI

La documentazione proveniente da altre pubbliche amministrazioni sarà oggetto di protocollazione e successiva gestione all'interno dell'AOO, nel rispetto dell'art. 47 [CAD]. Pertanto, è necessario che la stessa rientri in almeno una delle sottoelencate casistiche:

- sia firmata digitalmente;
- risponda alle regole dell'interoperabilità promulgate dall'AgID;
- la casella postale mittente sia certificata.

Il *Registry* si riserva di protocollare o non protocollare gli atti che non rispondono ad almeno uno dei requisiti di cui sopra, in relazione alla possibilità di determinare la provenienza del documento.

3.4. DOCUMENTI INFORMATICI PROVENIENTI DA AZIENDE E LIBERI PROFESSIONISTI

Le aziende devono inviare le proprie comunicazioni utilizzando la casella di posta elettronica certificata (idshape@postacert.difesa.it), secondo le disposizioni del DPCM 21 marzo 2011, utilizzando come canale preferenziale quella registrata nell'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata istituito dal Ministero dello Sviluppo Economico (INI-PEC). Anche i liberi professionisti dovranno utilizzare, preferibilmente, il canale di posta elettronica certificata registrato nell'INI-PEC.
In entrambi i casi è opportuna l'apposizione della firma digitale, da parte del rappresentante legale, sui documenti trasmessi.
È necessario che risulti possibile l'accertamento della provenienza del documento, ai sensi dell'art. 45 del [CAD].

3.5. DOCUMENTI INFORMATICI PROVENIENTI DA PRIVATI CITTADINI

I privati cittadini, in funzione della tipologia di casella disponibile, possono utilizzare entrambe le caselle di posta elettronica dell'AOO. Non è possibile

inviare sulla casella PEC una e-mail normale. Per la protocollazione è necessario attenersi alle disposizioni dell'art. 45 del [CAD], che prevede, in ogni caso, l'accertamento della provenienza.
A tal fine, è necessario inviare i documenti avendo cura di apporre la firma digitale ovvero di allegare scansione del proprio documento di identità in corso di validità o, comunque, di seguire quanto prescritto dall'art. 38 del DPR 445/2000 in combinato disposto con l'art. 65 del [CAD].

3.6. MESSAGGI DI NOTIFICA DI ECCEZIONE

Il sistema prevede sette casi preimpostati di restituzione al mittente dei documenti pervenuti tramite PEI:

- il messaggio è corrotto o uno dei documenti non leggibile;
- dati non congruenti nella segnatura informatica;
- segnatura non conforme alla circolare AgID n. 60 del 23.01.2013;
- mancata sottoscrizione del documento primario;
- destinatario errato;
- verifica di integrità dei documenti negativa;
- il documento o gli allegati dichiarati all'interno del file "segnatura.xml" non corrispondono a quanto ricevuto.

Oltre ai casi suindicati è possibile inviare un messaggio non preimpostato, riportando i motivi della restituzione.

3.7. SPECIFICHE DEI DOCUMENTI INFORMATICI IN USCITA

A tutti i documenti trasmessi viene allegato il file "segnatura.xml", contenente le informazioni previste dalla [CIRC].
Il corretto invio dei documenti richiede l'osservanza delle seguenti regole:

- utilizzo di formati previsti nell'AD (PDF/ODT/DOCX/RTF);
- la denominazione non deve contenere caratteri speciali (*,',^, ecc.);
- la denominazione non deve essere usato il carattere "." (punto).

In caso di inserimento, come allegato, di un documento già firmato che non deve essere modificato, è necessario che nella predisposizione venga selezionata la voce "NO FIRMA". Per quanto riguarda le dimensioni complessive dei file, si evidenzia che la posta elettronica certificata può trasmettere fino a 100 MB.
Tutta la documentazione amministrativa dell'AOO viene prodotta in originale in modalità informatica con l'apposizione della firma digitale e della marca temporale.

3.8. UTILIZZO CASELLA PEC O PEI IN USCITA

Il sistema informatico, sulla base delle informazioni inserite, provvede ad inviare, per posta elettronica, il documento primario e gli allegati a tutti i destinatari inseriti.
L'utilizzo della casella PEI, piuttosto che della PEC, può essere impostato durante la predisposizione e può essere modificato da tutti coloro che visionano il documento, fino alla firma dello stesso.
Nei casi previsti dalla legge o qualora si renda necessario disporre di una ricevuta di ricezione della corrispondenza inviata, viene utilizzata la casella di posta elettronica certificata (PEC). Parimenti si utilizzerà la casella di PEC ogni qualvolta che il corrispondente richieda esplicitamente l'impiego di tale

strumento. Negli altri casi è possibile utilizzare anche la casella PEI. In particolare, è necessario utilizzare:

- con le altre PA, la casella di posta PEI o PEC, in funzione delle specifiche esigenze della pratica in trattazione (se disponibile PEC – IPA);
- con le imprese ed i professionisti la PEC (preferibilmente INI-PEC);
- con i cittadini, il canale indicato dagli stessi nelle istanze presentate, significando che, l'assolvimento di eventuali "obblighi di comunicazione", richiede l'utilizzo dei canali previsti dalla normativa vigente.

3.9. RICEVUTE DEI DOCUMENTI INFORMATICI

Il sistema gestisce in automatico:

- le ricevute generate dal sistema di PEC;
- le ricevute previste dalla [CIRC] per i documenti dotati di file "segnatura.xml" delle P.A.;
- i messaggi di "eccezione" che segnalano un problema di ricezione nella casella postale del destinatario (ad esempio, destinatario sconosciuto, casella postale del destinatario piena, ecc.).

La citata messaggistica, viene automaticamente inserita in allegato al documento di origine ed è consultabile con le normali funzioni di consultazione. In caso di "posta non consegnata" il documento viene evidenziato sulla scrivania virtuale dell'utente che lo ha predisposto. Dopo le verifiche del caso, è possibile:

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

Almeno una volta al giorno è necessario verificare la presenza di eventuali messaggi di "posta non consegnata".

In alcuni casi, la procedura automatica non riesce a gestire alcune tipologie di ricevute, con particolare riferimento alle notifiche delle "eccezioni". In tal caso, il messaggio deve essere acquisito a protocollo ed inviato all'UO interessata.

3.10. DOCUMENTO INTERNO

Per documenti interni si intendono quelli scambiati tra le diverse articolazioni (UO) afferenti alla medesima AOO.

Se tra gli indirizzi per competenza o per conoscenza viene inserita una UO interna all'AOO, il sistema informatico provvede ad inviare il documento sulla scrivania virtuale dell'UO destinataria.

Rimangono invariate le susseguenti attività gestionali, compresa l'eventuale necessità di ricorrere alla materializzazione del documento.

4. LA GESTIONE DEI DOCUMENTI ANALOGICI

4.1. DOCUMENTO ANALOGICO

Per documento analogico si intende la rappresentazione non informatica di atti e dati, giuridicamente rilevanti. Di norma, nell'attività amministrativa il documento analogico è un documento stampato su carta, prodotto con strumenti informatici.

I documenti analogici devono pervenire in originale o in copia autentica attraverso il servizio postale o consegnati direttamente agli indirizzi preposti alla ricezione della corrispondenza analogica di ciascuna AOO riportati nel presente documento e pubblicati sul sito internet della Difesa. La documentazione così pervenuta sarà in ogni caso soggetta a processo di scansione, ai sensi dell'art. 23 *ter* comma 3 del [CAD], allo scopo di effettuarne, nel limite di quanto possibile rispetto alla natura e consistenza degli allegati, una gestione digitalizzata.

4.2. TIPOLOGIA DI SPEDIZIONI

Il servizio postale deve essere utilizzato nei casi di necessità e per esigenze d'ufficio, rispettando i criteri di economia e speditezza. La principale tipologia di spedizione attualmente prevista è la raccomandata o pacco ordinario e prevede la ricevuta dell'avvenuta spedizione e la verificare dello stato di lavorazione (fino a 30 Kg).

Il servizio di "corrieri militari" invece, viene assicurato secondo le seguenti modalità:

- senza tracciatura;
- con tracciabilità, qualora sia necessaria la prova dell'invio.

4.3. RITIRO DELLA CORRISPONDENZA

Il personale preposto deve provvedere, giornalmente, alla consegna della posta analogica da spedire ed al ritiro di quella indirizzata all'AOO o ad una sua UO al servizio postale di riferimento. Le modalità di consegna e ritiro devono essere riportate nel Manuale di AOO.

Il militare incaricato deve verificare che su tutti i documenti prelevati risulti l'indirizzo dell'AOO o di una delle sue UO.

La corrispondenza che risulti indirizzata ad altra AOO, deve essere restituita con apposto il timbro / dicitura "NON INDIRIZZATA ALL'AOO".

In caso di parziale o totale lacerazione del plico si riporta, sull'involucro, la dicitura "GIUNTO LACERO" con timbro e firma dell'incaricato.

4.4. CORRISPONDENZA CHE NON DEVE ESSERE APERTA

Il personale preposto non è autorizzato all'apertura di buste, plichi o pacchi che:

- riportano una delle seguenti diciture:
  - Grado Nome Cognome;
  - ESCUSIVO PER IL TITOLARE;
  - ESCLUSIVO PER (Grado, Nome, Cognome);
  - PERSONALE PER (Grado, Nome, Cognome);
  - Al Capo del Reparto o dell'Ufficio;
- abbiano come destinatario gli organi di sicurezza;

- evidenziano "fascette di sicurezza" o diciture "a mezzo di corriere abilitato" anche se prive dell'indicazione della classifica di segretezza del documento contenuto.

Tale corrispondenza viene consegnata direttamente alle UO. Sarà cura dei destinatari provvedere alla riconsegna di quanto ricevuto, per l'eventuale registrazione a protocollo.

Si precisa che, per motivi di sicurezza, plichi e pacchi, a "titolo personale" non possono essere ricevuti tramite i canali della corrispondenza di servizio.

4.5. EVENTUALI PLICHI CON DOCUMENTI CLASSIFICATI

Il protocollo informatico non è abilitato alla gestione della documentazione classificata. Nel caso in cui, successivamente all'apertura di un plico ordinario o di una "raccomandata/assicurata", si rinvenga una seconda busta o un documento riportante una "classifica di segretezza":

- si richiude il plico con i sistemi normalmente in uso (nastro adesivo, punti metallici, spago, ecc.) apponendo il timbro previsto;
- si informano i diretti superiori e gli organi di sicurezza.

4.6. REGISTRAZIONI DELLE CONSEGNE DELLA POSTA

Di norma, il ritiro della posta ordinaria non prevede registrazioni di dettaglio, ad eccezione delle eventuali "distinte di consegna", da custodire per almeno un anno. Per quella tracciata, raccomandate, assicurate, pacchi e atti giudiziari è necessaria la registrazione dei vari passaggi, con particolare riferimento alla documentazione che viene:

- restituita perché non diretta all'AOO;
- consegnata ai destinatari, senza apertura della busta e registrazione di protocollo.

Ciascuna AOO, sulla base delle dimensioni dei flussi di corrispondenza analogica, adatta le registrazioni e le ricevute alle proprie esigenze.

4.7. CONTROLLI ALL'APERTURA DEI PLICHI PROVENIENTI DAI SERVIZI POSTALI

Il personale preposto adotta opportune modalità organizzative atte a prevenire e limitare eventuali rischi e pericoli di contaminazione per i plichi provenienti dal servizio postale.

In caso di corrispondenza sospetta, deve essere avvertito con immediatezza il diretto superiore ed la *Military POLICE* di Shape.

4.8. PERSONALE ABILITATO ALLE ATTESTAZIONI DI CONFORMITÀ DELLE COPIE INFORMATICHE

La scansione ed il protocollo con il sistema ADHOC consente la dematerializzazione della documentazione analogica in ingresso. L'intero flusso documentale viene gestito in maniera elettronica, con un processo di validazione ai sensi dell'art. 23 ter comma 3 del [CAD]. L'elenco del personale delegato a tale attività viene individuato con apposito ordine di servizio, secondo il modello in Allegato "E".

4.9. PROCEDURE PER LA REGISTRAZIONE

I documenti sono scansionati massivamente, a cura di addetti abilitati alla funzione e, di seguito, valorizzati attraverso l'inserimento dei dati essenziali per la protocollazione:

- Codice Amministrazione mittente, se presente;
- Codice AOO mittente, se presente;
- Mittente;
- Oggetto;
- Protocollo mittente;
- Data protocollo mittente.

Gli allegati cartacei, vengono inseriti nella fase di scansione massiva del documento di riferimento in formato analogico ovvero allegati informatici possono essere gestiti nel processo di dematerializzazione con un opportuno separatore idoneo a distinguerli dal documento primario di appartenenza.

Gli allegati digitali sono accettati, se forniti, su supporto ottico (CD ovvero DVD) ovvero su memoria con connessione USB.

Non possono essere accettati allegati informatici su supporti diversi da quelli indicati. In ogni caso i supporti informatici non vengono riconsegnati al mittente ma rimangono associati al documento cartaceo originario. Il contenuto del supporto, qualora la dimensione non sia eccessiva, può essere associato al documento primario di appartenenza, subito dopo il processo di scansione di quest'ultimo. Il processo di acquisizione termina con l'apposizione della firma digitale e la marca temporale, sul file ottenuto dal processo di scansione massiva e con l'invio alla UO destinataria.

Il documento analogico originale e gli eventuali allegati vengono custoditi presso l'AOO/UO ai soli fini di eventuali verifiche. Le operazioni di dematerializzazione avvengono di norma entro il giorno successivo alla ricezione del documento.

4.10. DOCUMENTO IN USCITA

La procedura standard prevede l'invio automatico dei documenti all'indirizzo email del/dei destinatario/i interessati. Tuttavia, è possibile inviare la documentazione nella "Lista dei documenti da materializzare" e procedere alla stampa, nei seguenti casi:

- documento che non deve essere trasmesso per posta elettronica;
- destinatario senza casella di posta elettronica;
- documento primario a cui è associato un allegato, analogico non dematerializzatile, o informatico che non può essere inviato per posta elettronica in quanto ad esempio, risulta di dimensioni eccessive.

I documenti confluiti nella lista dei documenti da materializzare devono essere stampati dagli operatori abilitati con l'apposizione del glifo timbro digitale sul primario. Il destinatario può verificare l'origine del documenti seguendo le indicazioni contenute nella pagina di supporto al Glifo della sezione protocollo informatico del sito www.difesa.it.

4.11. PREDISPOSIZIONI DEI PLICHI

Italdelega predispone la corrispondenza analogica da spedire, tramite il servizio postale o con i corrieri militari, con buste di dimensioni ridotte e, per l'inoltro di stampe e pacchi, con i mezzi più idonei (*cellofan*, carta resistente,

etc.). Per la corrispondenza "assicurata" è necessario utilizzare buste resistenti ed accertarsi che il plico non sia lacero. I plichi ed i pacchi devono essere ben chiusi con nastro adesivo, spago, etc..
La posta da spedire deve essere predisposta, utilizzando la modulistica prevista significando che, in aderenza alla vigente normativa in materia di trasparenza amministrativa, è fatto obbligo di compilare in maniera leggibile ed in tutta la sua interezza la modulistica a corredo di ciascuna tipologia di spedizione.
Inoltre, al fine di evadere tempestivamente il flusso della corrispondenza in uscita, essa deve essere consegnata al personale preposto per consentirne in tempo utile la consegna al servizio postale o ai corrieri.

4.12. FAX

In considerazione del divieto di utilizzo di fax tra le Pubbliche Amministrazioni e dell'obbligo di comunicare con le imprese esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione ovvero per via telematica, non sono più disponibili apparati fax.
L'eventuale trasmissione/ricezione di documentazione attraverso tale strumento da parte di privati cittadini può, eventualmente essere effettuata verso l'UO di competenza, solo se queste ultime ne sono in possesso.
Il mittente che invia il fax:

- non deve farlo pervenire con altri strumenti, come da "art. 45 del [CAD]";
- deve corredare il documento spedito, dalla fotocopia del documento di identità del mittente.

4.13. DOCUMENTO NON FIRMATO

I documenti cartacei privi di mittente, qualora configurabili quali esposti anonimi, sono trattati nell'ambito delle AOO procedendo alla scansione solo della busta ed all'apposizione del protocollo e della data sulla stessa e sul primo foglio (con apposito timbro o a mano).

5. SISTEMA CLASSIFICAZIONE, FASCICOLAZIONE E ARCHIVIO

5.1. TITOLARIO

Si definiscono nel Manuale di AOO la gestione degli archivi sulla base dei riferimenti normativi e metodologici in vigore. In particolare, il "Titolario di archivio" deve:

- discendere dal modello funzionale che caratterizza le attività svolte;
- svilupparsi su funzioni, sotto funzioni e attività;
- prevedere non più di 3 livelli.

La sua struttura deve presentare caratteri di generalità e di completezza necessari per soddisfare le esigenze di classificazione delle UO.

L'aggiornamento del Titolario compete esclusivamente al vertice dell'AOO, su proposta del RDS. Ciascuna UO può chiedere integrazioni, varianti e aggiunte al Titolario sulla base delle proprie necessità. Dopo ogni modifica il RDS provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

È possibile, registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.

Il Titolario non è retroattivo, significando che le sue variazioni non possono applicarsi ai documenti classificati in precedenza.

In Allegato "F" sono stati riportati utili approfondimenti sullo specifico argomento.

5.2. CLASSIFICAZIONE DEI DOCUMENTI

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

Tutti i documenti ricevuti e prodotti delle UO dell'AOO, indipendentemente dal supporto sul quale sono formati, sono classificati in base Titolario.

Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse), il fascicolo di appartenenza e, eventualmente, il sottofascicolo nonché l'UO di competenza.

5.3. FASCICOLAZIONE DEI DOCUMENTI

Lo strumento di base per gestire la classificazione è il "fascicolo".

Il sistema prevede che i primi tre livelli del Titolario (titolo, classe e sottoclasse) vengano precaricati e gestiti in modalità accentrata dal RDS.

I fascicoli ed i sottofascicoli sono invece gestiti direttamente dagli interessati ai relativi procedimenti.

In particolare, per poter classificare un documento è necessario inserirlo in un fascicolo oppure in un sottofascicolo.

Per quanto riguarda la descrizione occorre attenersi alle regole generali di scrittura dei dati, indicate nell'Allegato "D". Inoltre, è opportuno evidenziare che non possono essere creati fascicoli con denominazione generica come ad es. "Varie" e che il sistema mantiene traccia della data di creazione del fascicolo e degli autori.

5.4. DEPOSITO/ARCHIVIO DELL'AOO

Italdelega produce esclusivamente originali informatici e, inoltre, tutti gli atti cartacei pervenuti vengono dematerializzati rendendoli validi a tutti gli effetti di legge.
Pertanto, l'universalità dei documenti originali afferenti all'AOO, a partire dalla data di avvio del servizio, sono archiviati all'interno del sistema informatico, che ne consente la gestione e l'accesso, secondo le norme di legge previste.
Tuttavia esiste un consistente numero di atti cartacei che, fino alla loro dematerializzazione, devono essere gestiti con il sistema di custodia da parte delle UO.

5.5. ARCHIVIAZIONE DEI DOCUMENTI INFORMATICI

I documenti informatici sono archiviati su supporti di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo, sui supporti di memoria del sistema ADHOC.
Il sistema è conforme alle norme vigenti, ciascun documento è dotato di firma digitale, di marca temporale, di *hash* in formato SHA-256 e delle informazioni di registrazione ad esso associate.
Ogni giorno viene anche prodotto, il registro giornaliero delle registrazioni di protocollo, firmato digitalmente in modalità automatica.

5.6. ARCHIVIAZIONE/CUSTODIA DEI DOCUMENTI ANALOGICI

Per quanto attiene l'organizzazione degli archivi cartacei si precisa quanto segue:

- l'archivio attivo custodirà tutte le cartelle dell'anno corrente e quelle dei precedenti 10 anni, già suddivise in ordine cronologico. Allo scadere del 10° anno, saranno valutati i documenti da scartare secondo modalità stabilite da una commissione ad *hoc*, mentre i documenti non scartati saranno conservati nell'archivio di deposito;
- l'archivio di deposito conterrà tutti i documenti per una durata pari a 50 anni. Alla scadenza del 50° anno una commissione, composta anche da un rappresentante del Ministero dei Beni Culturali e del Ministero dell'Interno, stabilirà quali documenti siano testimonianza di valore di civiltà e quindi da depositare nell'archivio storico;
- l'archivio storico custodirà i documenti ritenuti di valenza storica.

I documenti cartacei sono tenuti in cartelline da carteggio, indicando il giorno in cui la documentazione viene trattata e custodite presso le UO a cura delle Segreterie. Le UO comunicano al RDS il personale responsabile di tali archiviazioni.

5.7. CONSERVAZIONE

La conservazione è disciplinata dal Manuale di Conservazione della Difesa che illustra nel dettaglio l'organizzazione del processo, i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività.

6. SICUREZZA ED ABILITAZIONI DI ACCESSO

6.1. PIANO DI SICUREZZA

La sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici archiviati sono garantiti dal sistema ADHOC, gestito presso il Centro di Elaborazione Dati Unificato dell'Area Tecnico Amministrativa, che ne cura anche i processi di backup.
Il Piano della Sicurezza informatica relativo ai collegamenti, alle modalità di trasmissione ed interscambio dei documenti, in quanto parte del più ampio Piano di Sicurezza Informatica dell'AD, viene predisposto ed aggiornato dagli enti preposti.
Di seguito, pertanto, saranno riportate le misure di controllo per garantire l'impiego dei servizi del sistema ADHOC.
I vari processi sono caratterizzati da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).
Gli utenti del sistema documentale, in base alle rispettive competenze, hanno autorizzazioni di accesso differenziate per le tipologie di operazioni stabilite dall'ufficio di appartenenza.

6.2. ACCESSO AL SISTEMA

L'accesso al sistema avviene tramite CMD nel seguente modo:
- si inserisce la propria CMD all'interno del lettore di Smart card collegato al computer;
- si digita nell'apposito campo il proprio pin carta.

In caso di indisponibilità della CMD è possibile accedere al sistema per un limitato periodo di tempo tramite apposite credenziali. L'attivazione della deroga, considerata la sua rilevanza ai fini della sicurezza, deve essere autorizzata dall'RDS o dal personale da costui delegato.
Il RDS, avvalendosi di una utenza privilegiata (amministratore di sistema), assegna agli utenti diversi livelli di autorizzazione. Tali utenti una volta identificati, sono suddivisi secondo diversi profili di accesso in base alle rispettive competenze. E' possibile assegnare più ruoli utilizzando la stessa password di accesso.

6.3. PROFILI D'ACCESSO

La strutturazione degli accessi prevede una realizzazione di una serie di profili sulla base della struttura ordinativa e delle rispettive competenze.
Le principali profilazioni riguardano le funzioni di:
- amministratore di sistema, il quale può accedere ai profili di configurazione di base del sistema (in genere è rilasciata ad un numero limitato di utenti);
- protocollazione in ingresso, che rappresenta la funzione destinata agli operatori di protocollo in ingresso dei documenti informatici e cartacei;
- materializzazione dei documenti che è l'elenco all'interno del quale confluiscono i documenti che per le proprie caratteristiche, non possono essere inviati per posta elettronica. In linea generale è consigliabile avere un utente con questo profilo in ciascuna UO. I documenti che sono presenti nella succitata lista verranno eliminati dagli amministratori del sistema dopo 60 giorni;

- accesso alla tabella dei mittenti e destinatari, che funge da punto di snodo fondamentale per la gestione della corrispondenza. L'accesso a tale tabella deve garantire uniformità e coerenza ai dati immessi;
- abilitazione alla firma digitale degli atti, che è in genere legata alla funzione di firma di documenti verso l'esterno;
- predisposizione di documento che consente di preparare gli atti per il flusso in uscita;
- consultazione, per la quale in linea generale, tutti gli utenti dovrebbero essere abilitati e il quale accesso è comunque legato al cono d'ombra di visibilità, determinato dalla propria posizione nell'albero gerarchico dell'AOO. In particolare, le informazioni legate al registro di protocollo sono visibili a tutti gli utenti mentre i documenti, in quanto tali, sono visibili solo a chi appartiene al relativo cono d'ombra. Va ricordata, a questo proposito, l'ulteriore profilazione, inerente alla possibilità di accedere ai documenti che contengono dati sensibili;
- accesso alla scrivania, che deve essere abilitata a tutti gli utenti, poiché permette lo scambio della corrispondenza e le attività gestionali dei documenti in ingresso/uscita;
- abilitazioni di accesso ai fascicoli, con la quale si consente l'apertura dei fascicoli, nonché l'assegnazione delle specifiche abilitazioni tramite la creazione o associazione dei relativi *template*;
- trasmissione degli atti, attivata solo per gli utenti con poteri di firma stabiliti in ambito UO.

I profili ora delineati non vanno considerati esaustivi delle molteplici possibilità fornite dal sistema ADHOC e, inoltre, è possibile anche creare profili ex-novo che contengano un misto di quelli elencati. L'assegnazione dei profili ed il loro aggiornamento sono stabiliti dal RDS sulla base delle effettive esigenze, formalizzate con apposite richieste dai responsabili delle diverse UO.

Allo scopo di agevolare l'assolvimento dei compiti connessi alla protocollazione e gestione documentale può essere necessario individuare, all'interno dell'AOO, una o più figure definendo il contesto organizzativo (UO) e la tipologia delle attività che le stesse potranno esercitare, la cui nomina deve essere effettuata con atto formale dell'Ente di appartenenza (Ordine di servizio, Decreto, Ordine del Giorno, Atto Dispositivo, ecc. secondo il modello in Allegato "E"). Tali figure, pur non avendo una dipendenza organica diretta dall'RDS, svolgeranno alcune funzioni, definite con apposite normative interne, per garantire il buon andamento della gestione documentale nelle strutture più articolate e complesse. L'RDS dovrà, comunque, esercitare la vigilanza sull'osservanza delle disposizioni in questione, rimanendone responsabile.

7. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

7.1. ATTIVAZIONE

Ogni qualvolta, per motivi accidentali o programmati, non fosse possibile utilizzare il sistema informatico per un periodo di tempo significativo, il RDS deve emettere una dichiarazione, da acquisire agli atti, indicando, con esattezza, la data e l'ora di inizio del non funzionamento e il relativo motivo.
In caso di utilizzo di appositi software, la protocollazione deve avvenire solo presso specifiche postazioni di lavoro sulle quali è stato preventivamente installato, consentendo quindi alla AOO di proseguire le attività di protocollazione.
L'elenco delle postazioni presso le quali sono installati i Registri di emergenza deve essere portato a conoscenza del personale dell'AOO e deve essere dichiarato all'interno del Manuale di AOO.
Il RDS/Vicario assicura che presso ciascuna postazione di emergenza siano sempre disponibili le versioni aggiornate delle indicazioni agli utenti per operare in emergenza.

7.2. SVOLGIMENTO DELLE ATTIVITÀ

Durante il periodo di non funzionamento del sistema informatico NON sarà possibile protocollare documenti informatici in ingresso, in quanto tale attività è strettamente correlata alle funzionalità del sistema stesso.
In presenza di un documento analogico in arrivo da protocollare immediatamente, si procederà al suo inserimento nel registro di emergenza, provvedendo alla consegna del medesimo all'UO di competenza.
Per quanto riguarda la documentazione in uscita, essendo possibile solo con l'apposizione della firma digitale e la disponibilità della posta elettronica, la funzione di registrazione a protocollo non sarà possibile. In caso di urgenza, l'UO dovrà procedere con metodologie alternative e consegnare il documento all'RDS, per la protocollazione di emergenza e la successiva trasmissione tramite canali analogici.
Appare evidente che non è conveniente procedere con tali modalità ed è opportuno ridurre al minimo indispensabile l'accesso a tali funzioni. Si sottolinea che in caso di blocco del sistema, viene inibito anche l'accesso all'archivio informatico e alle funzioni di ricerca in generale.

7.3. RIATTIVAZIONE DEL SISTEMA INFORMATICO

Alla ripresa del normale funzionamento del sistema ADHOC, il RDS produce una ulteriore dichiarazione, con l'esatta indicazione della data e dell'ora della ripresa del servizio.
Tutte le dichiarazione del RDS di attivazione e chiusura del registro di emergenza sono conservate a cura dello stesso.
Dopo la riattivazione sia i documenti in ingresso, sia i documenti in uscita protocollati in emergenza, dovranno essere inseriti nel sistema ADHOC con le procedure previste.
In particolare, nell'oggetto si dovrà riportare il numero del registro di emergenza (RE xxxxxx gg-mm-aaaa) per consentire la ricerca del numero di registrazione di emergenza tramite il campo "oggetto".

8. CARATTERISTICHE SPECIFICHE DELL'AOO DI ITALDELEGA

8.1. PREMESSA

Italdelega si è dotata di un Manuale per la gestione documentale (di seguito denominato Manuale) in cui sono definiti i principi generali e le regole, comuni a tutte le Unità Organizzative (UO) che dipendono da Italdelega.
Inoltre, il presente documento raccoglie le scelte organizzative e le disposizioni relative alla gestione dei flussi documentale valide per l'Area Organizzativa Omogenea di Italdelega.

8.2. UNITÀ ORGANIZZATIVE RESPONSABILI DEI DOCUMENTI

L'AOO di Italdelega (codice AOO: A46D85F) comprende le seguenti Unità Organizzative (UO) interne, responsabili per l'organizzazione e la tenuta dei documenti gestiti:

- (UO) SEZIONE SEGRETERIA;
- (UO) SEZIONE AMMINISTRAZIONE;
- (UO) SEZIONE ASSISTENZA SPIRITUALE;
- (UO) UFFICIO RAPPRESENTANZA MILITARE ITALIANA;
  - (UO) SEZIONE PERSONALE;
  - (UO) SEZIONE OPERAZIONI E ADDESTRAMENTO;
  - (UO) SEZIONE AFFARI GENERALI;
  - (UO) SEZIONE SANITARIA.

8.3. CASELLE DI POSTA ELETTRONICA ED INDIRIZZI POSTALI.

Italdelega SHAPE riceve la documentazione ai seguenti indirizzi, pubblicati anche sul sito internet della AD:

- indirizzo di Posta Elettronica Certificata (PEC): idshape@postacert.difesa.it;
- Riceve esclusivamente messaggi inviati da altre caselle di PEC;
- indirizzo di posta elettronica ordinaria istituzionale: idshape@smd.difesa.it;
- indirizzo postale:
  - indirizzo in Belgio : *Avenue de Londres* BLDG 101 B7010 SHAPE;
  - indirizzo in Italia : Via XX Settembre 123/a 00187 ROMA.

8.4. UNITA' ORGANIZZATIVA RESPONSABILE ED ORARI.

L'unità organizzativa responsabile del protocollo informatico in ingresso e della gestione documentale nell'AOO di Italdelega è l'Ufficio Protocollo, che assicura la protocollazione in ricezione di tutta la corrispondenza ricevuta entro le ore:

- 17:00, dal lunedì al giovedì;
- 15:00, il venerdì.

La corrispondenza pervenuta all'AOO oltre gli orari sopra indicati sarà oggetto di protocollazione il primo giorno lavorativo utile successivo alla ricezione.

8.5. SERVIZIO DI SCAMBIO POSTA

Il personale della Segreteria addetto al protocollo è disponibile per le attività di ritiro e/o consegna della corrispondenza analogica nei seguenti orari:

- lunedì/giovedì - dalle ore 09:00 alle 17:00 (ritiro e consegna).
- venerdì - dalle ore 09:00 alle 15:00 (ritiro e consegna).

Il responsabile assicura la ricezione e la consegna della posta in arrivo, con particolare riferimento agli "allegati analogici" dei documenti informatici.
La posta proveniente dal servizio postale e dai corrieri abilitati viene prelevata giornalmente presso il *Registry* di SHAPE mentre, ad ogni favorevole occasione, presso la Rappresentanza Italiana presso il Consiglio Atlantico (RICA) di Bruxelles.

8.6. TITOLARIO

Il "Titolario di archivio dello Stato Maggiore della Difesa, – SMD I 006 – Edizione 2013", come riferimento è pubblicato sul sito internet dell'AD

8.7. POSTAZIONE INFORMATICA DEL REGISTRO DI EMERGENZA

La protocollazione in entrata e in uscita, in caso di indisponibilità del sistema documentale proseguirà, in modalità di emergenza, come indicato nel presente Manuale.

ALLEGATI

ELENCO DELLE PRINCIPALI ABBREVIAZIONI

- AD: Amministrazione Difesa;
- ADHOC: Applicativo per il protocollo informatico e la gestione documentale in uso presso lo Stato Maggiore della Difesa;
- AgID: Agenzia per l'Italia digitale;
- AOO: Area organizzativa omogenea;
- [CAD]: Decreto Legislativo 7 marzo 2005 n. 82;
- CGD: Coordinatore della gestione documentale dell'area tecnico operativa interforze;
- [CODBCP]: Decreto Legislativo 22 gennaio 2004 n. 41;
- [CODPRI]: Decreto Legislativo 30 giugno 2003 n. 196;
- [DIR]: Direttiva SMD-I-004;
- DPR: Decreto del Presidente della Repubblica;
- [DPR]: DPR 28 dicembre 2000 n. 445;
- D.Lgs: Decreto Legislativo;
- [GDPR]: Regolamento UE n. 2016/679;
- INCC: Informazioni non Classificate controllate IPA Indice delle Pubbliche Amministrazioni;
- l.: Legge;
- P.A.: Pubblica Amministrazione;
- PDF/A: Standard internazionale (ISO19005), sottoinsieme dello standard PDF, appositamente pensato per l'archiviazione nel lungo periodo di documenti elettronici
- PEC: Posta elettronica certificata;
- PEI: Posta elettronica istituzionale;
- PI: Protocollo informatico;
- RDS: Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi;
- RPA: Responsabile del procedimento amministrativo;
- UO: Unità Organizzativa.

ALLEGATO "B"

ISTRUZIONI PER LA REDAZIONE DEL MANUALE DI AOO

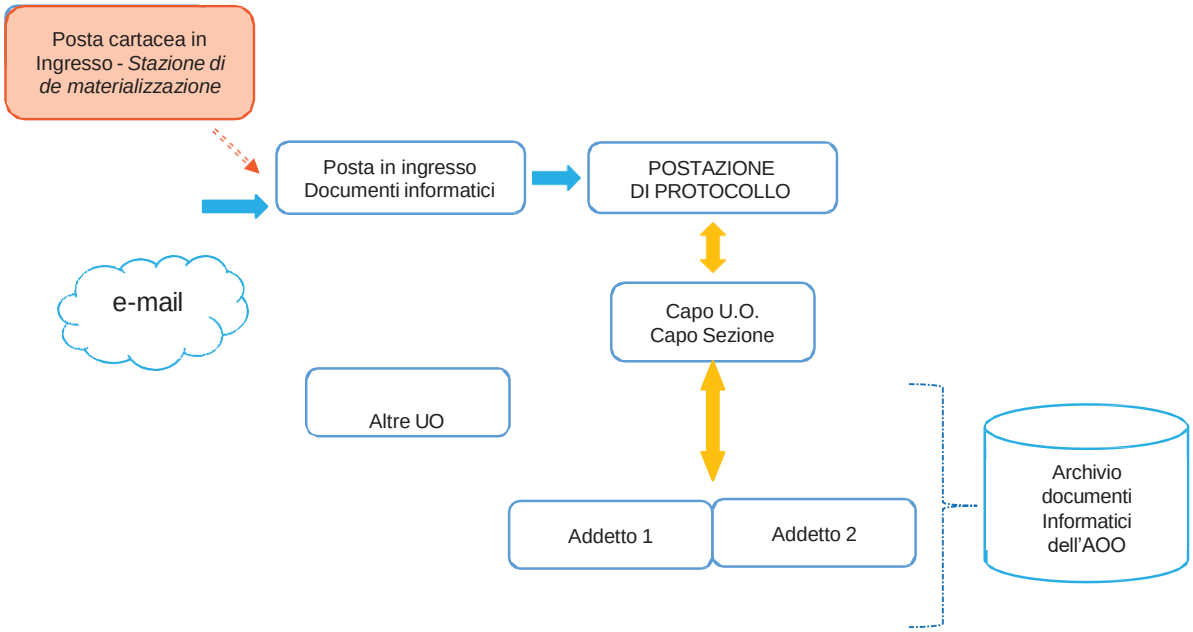
La Rappresentanza Militare Italiana (Italdelega) è dotata di un Manuale per la gestione documentale in cui sono definiti i principi generali e le regole, comuni a tutte le AOO di Comandi ed Enti che dipendono dallo Stato Maggiore della Difesa.

Vengono riportate le caratteristiche dell'AOO, le principali scelte organizzative e le specifiche disposizioni relative alla gestione del protocollo informatico e dei flussi documentali. In particolare vengono precisati:

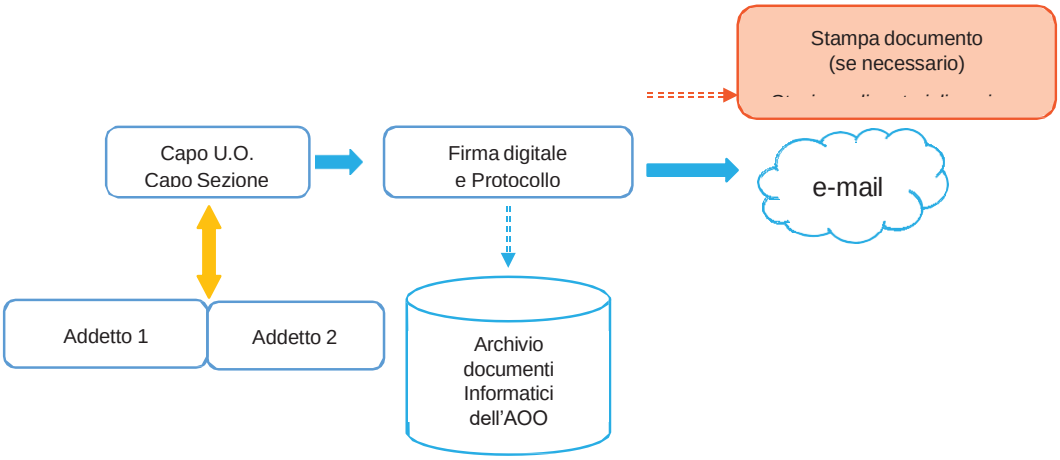
- UO responsabili dei documenti;
- Caselle di posta elettronica ed indirizzi postali;
- UO responsabile della gestione del protocollo e del sistema documentale e i relativi orari;
- Servizio di scambio posta;
- Titolario;
- Postazione informatica del registro di emergenza.

Le scelte organizzative e le disposizioni particolari, valide esclusivamente per l'AOO o relative a specifiche esigenze, possono essere inserite opportunamente nel documento, aggiungendo, nel paragrafo 8, le modifiche apportate.

SCHEMI DI FLUSSO IN ENTRATA ED USCITA DEI DOCUMENTI



Flusso in ingresso



Flusso in uscita

ALLEGATO "D"

REGOLE GENERALI DI SCRITTURA DEI DATI

In tutti i sistemi informatici è di particolare importanza la qualità delle informazioni che vengono inserite al suo interno. Ancora di più rileva tale importanza in un sistema diffuso e invasivo come quello di PI e gestione documentale.
È facilmente intuibile, infatti, come, in assenza di regole comuni e coerenti, non sarà possibile ottenere tutti i benefici attesi dal sistema, in quanto, semplicemente, i documenti potrebbero essere difficilmente rintracciabili o, nei casi peggiori, non rintracciabili!
Vengono di seguito riportate poche regole, cui tutti gli utenti del sistema devono attenersi, nella redazione dei campi "Oggetto", dei nomi dei fascicoli e, in generale, ogni qualvolta sia necessario digitare una qualunque descrizione.

Nomi di persona	Prima il Cognome e poi il Nome, in maiuscolo solo la prima lettera. Esempio: Rossi Mario
Titoli di cortesia, nobiliari ecc.	Sempre omessi
Nomi di città	In lingua, italiana, se disponibile
Nomi di stati	In lingua italiana
Nomi di ditte	Lettera maiuscola solo nella prima lettera L'eventuale forma societaria in minuscolo, senza punti di separazione. Esempio: Acme srl
Enti/associazioni	Lettera maiuscola solo per l'iniziale della denominazione
Ministeri	Scritti per esteso Esempio: Ministero della Difesa
Enti di secondo livello	Esempio: Stato Maggiore Difesa V Reparto e NON V Reparto SMD
Sigle di enti	Senza punti: Esempio: ISTAT
Università	Esempio: Università degli studi di Roma
Virgolette/apici	Utilizzare, digitandolo dalla tastiera (no copia/incolla da Word) il relativo carattere
Caratteri speciali	Non si devono utilizzare (Es.: *,',^ ecc...)
Date	Formato numerico, separatore trattino. Esempio: 01-01-2012

ALLEGATO "E"

MODELLO DI O.D.G./O.D.S. DI DELEGA DELLE FUNZIONI DI RDS/OPERATORE

ORDINE DEL GIORNO/SERVIZIO

OGGETTO: Attestazioni di conformità agli originali analogici delle copie su supporto informatico mediante l'utilizzo della firma digitale.

PREMESSO CHE:

è necessario assicurare la dematerializzazione dei documenti cartacei pervenuti presso la sede di_____, tramite i servizi postali o corrieri abilitati e che alle predette attività deve provvedere il personale in forza al:

-Sezione, Nucleo

VISTO: il D.P.R. n. 445 del 28/12/2000, "Testo Unico delle Disposizioni Legislative e regolamentari in materia di documentazione amministrativa", circa la gestione dei flussi documentali e dei procedimenti amministrativi delle P.A.;

VISTO: l'articolo 23 ter, comma 3, del [CAD] di cui al D.Lgs. n. 82 del 7/3/2005 e successive modificazioni e integrazioni, circa le copie su supporto informatico di documenti analogici ed il valore giuridico della conformità all'originale delle copie informatiche realizzate dai delegati;

il seguente personale:

Grado, Cognome e Nome

è delegato alle attestazioni di conformità all'originale analogico della copia su supporto informatico
mediante l'utilizzo della firma digitale.

Firma

_____