REGGIMENTO LOGISTICO
“FOLGORE”

MANUALE DI GESTIONE
dell’Area Organizzativa

(Codice identificativo interno: M_D E25800)
(Codice identificativo univoco: AE57B7E)

PAGINA NON SCRITTA

REGGIMENTO LOGISTICO “FOLGORE”

ATTO DI APPROVAZIONE

Approvo il presente “Manuale di Gestione dell’Area Organizzativa – M_D E25800”.

Esso è stato redatto in conformità delle nuove Linee Guida sulla formazione, gestione e conservazione del documento informatico dell’Agenzia per l’Italia Digitale (ai sensi dell’articolo 71 del Codice dell’Amministrazione Digitale [CAD] di cui al Decreto Legislativo 07 marzo 2005, n.82) che hanno aggiornato le regole tecniche sulla formazione, protocollazione, gestione e conservazione dei documenti informatici precedentemente regolate nel Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 e nel Decreto del Presidente del Consiglio dei Ministri del 14 novembre 2014.

Pisa,

IL COMANDANTE
Col. tramat. (par.) RN Guido BULSEI

Firmato Digitalmente da/Signed by:
GUIDO BULSEI
Comandante
In Data/On Date:
giovedì 25 agosto 2022 10:19:01

PAGINA NON SCRITTA

SOMMARIO

ELENCO DEGLI ALLEGATI

ACRONIMI

All'interno del manuale di gestione, per rendere più snello il testo, saranno utilizzati degli acronimi che vengono riportati di seguito, con il relativo significato:

AD	**A**mministrazione **D**ifesa
AgID	**Ag**enzia per l'**I**talia **D**igitale
AOO	**A**rea **O**rganizzativa **O**mogenea
AOO-M_D E25800	AOO del Reggimento Logistico "FOLGORE"
CAD	**C**odice **A**mministrazione **D**igitale
LLGG	**L**inee **G**uida sulla formazione, gestione e conservazione dei documenti informatrici emanate dall'AgID
CODPR	**Cod**ice di **Pr**otezione dei dati personali
DIR	**Dir**ettiva
D.Lgs.	**D**ecreto **L**egislativo
DPCM	**D**ecreto della **P**residenza del **C**onsiglio dei **M**inistri
DPR	**D**ecreto del **P**residente della **R**epubblica
eIDAS	**e**lectronic **I**dentification**, A**uthentcation**, S**ignature
GDPR	**R**egolameno **G**enerale per la **P**rotezione dei **D**ati
IPA	**I**ndice delle **P**ubbliche **A**mministrazioni
MdG	**M**anuale **d**i **G**estione del protocollo informatico
NdP	**N**ucleo per la tenuta **d**el **P**rotocollo informatico
PA	**P**ubblica **A**mministrazione
PEC	**P**osta **E**lettronica **C**ertificata
PEI	**P**osta **E**lettronica **I**stituzionale
PI	**P**rotocollo **I**nformatico
RDS	**R**esponsabile **d**el **S**ervizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi
RPA	**R**esponsabile del **P**rocedimento **A**mministrativo
UE	**U**nione **E**uropea
UO	**U**nità **O**rganizzativa

RIFERIMENTI NORMATIVI

Di seguito sono riportati i riferimenti normativi di maggior rilevanza costituenti argomento di questo Manuale con le relative abbreviazioni indicate a fianco di ciascuno di essi. Tali norme sono da intendersi comprensive delle aggiunte, varianti e correzioni nel frattempo intervenute sul provvedimento stesso.
La normativa inerente al Protocollo Informatico (PI) è piuttosto vasta: vengono qui riportati solo gli atti principali, rimandando ad eventuali richiami all'interno del Manuale per norme di maggior dettaglio.

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. (DPR)
Testo unico delle disposizioni legislative e regolamenti in materia di documentazione amministrativa. Con il DPR n. 445 si effettua una razionalizzazione e semplificazione della normativa inerente al PI. Viene, pertanto, abrogato con l'art 77 il DPR 428/98, facendo salvi gli atti di legge emessi successivamente alla sua entrata in vigore (art 78 DPR n. 445). La normativa inerente al PI viene semplificata e raggruppata negli articoli dal 50 al 70 del presente DPR.
Il DPR è il documento di riferimento principale per il PI.

Decreto Legislativo 30 giugno 2003, n. 196. (CODPR) e Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR)
"Codice in materia di protezione dei dati personali" (CODPR) testo unico che disciplina e garantisce il trattamento dei dati personali.
"Regolamento generale sulla protezione dei dati" (GDPR) ha lo scopo di armonizzare la regolamentazione in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati all'interno dell'Unione Europea.

Direttiva SMD-I-004 (DIR)
Il protocollo informatico nella Difesa.

Decreto del Presidente della Repubblica 11 febbraio 2005, n.68
Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata.

Decreto Legislativo 7 marzo 2005, n. 82 (CAD)
Codice dell'Amministrazione Digitale.

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013. (DPCM 2013)
Regole tecniche per il protocollo informatico e regole tecniche per la conservazione dei documenti informatici(ai sensi dell'art. 71, del CAD di cui al decreto legislativo n.82 del 2005).

Decreto del Presidente del Consiglio dei Ministri 14 novembre 2014. (DPCM 2014)
Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei dei documenti informatici delle amministrazioni (ai sensi dell'art. 71, del CAD di cui al decreto legislativo n.82 del 2005).

Linee Guida (LLGG) sulla formazione, gestione e conservazione dei documenti informatrici emanate dall'Agenzia per l'Italia Digitale (ai sensi dell'art. 71, del CAD di cui al decreto legislativo n.82 del 2005) in esecuzione dal 01 gennaio 2022.

Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

1. PRINCIPI GENERALI

1.1. PREMESSA

Il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 ed il Decreto del Presidente del Consiglio dei Ministri 14 novembre 2014 (ai sensi dell'articolo 71, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n.82 del 2005), prevedono, ai sensi dell'art. 3, che le pubbliche amministrazioni di cui all'art. 2 comma 2 del Codice (CAD) provvedano ad individuare 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 e che sia adottato il manuale di gestione di cui all'art. 5.
I citati DPCM sono stati aggiornati dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatrici emanate dall'AgID ed in esecuzione dal 01 gennaio 2022.

1.2. AMBITO DI APPLICAZIONE

Il presente Manuale di Gestione (di seguito MdG) è rivolto al personale interno all'Area Organizzativa Omogenea (di seguito AOO), relativa al Reggimento Logistico "Folgore", e ai soggetti esterni che hanno la necessità di interagire con essa, e descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi del Reggimento Logistico "Folgore".
Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti e alle informazioni e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno dell'amministrazione, anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa. In particolare essa si fonda sulla compenetrazione dei seguenti principi archivistici:

- la produzione della segnatura di protocollo, cioè l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, dei metadati riguardanti il documento stesso funzionali alla ricezione o spedizione delle pubbliche amministrazioni;
- la registrazione di protocollo del documento, cioè l'attività di memorizzazione dei dati necessari a conservare le informazioni per ogni documento ricevuto o spedito dalle pubbliche amministrazioni;
- la classificazione del documento, che lo dota della collocazione logico-funzionale nell'Archivio;
- la fascicolazione del documento protocollato che attesta la sua effettiva gestione nell'ambito di un procedimento amministrativo o di un'attività.

Si ritiene utile ricordare come il registro di protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

1.3. DEFINIZIONI E NORME DI RIFERIMENTO

Ai fini del presente manuale si intende per:

- *Amministrazione*, il Reggimento Logistico "Folgore";
- *Archiviazione elettronica*, il processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione;
- *Archiviazione ottica*, operazione che genera, su supporto di memorizzazione una registrazione contenente la versione iniziale di una istanza di un documento informatico;
- *Archivio*, la raccolta ordinata degli atti spediti, inviati o comunque formati dall'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'AOO sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono (cd. *Vincolo archivistico)*. Essi sono ordinati e archiviati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo,

legale o storico. Pur considerando che l'archivio è unico per ogni AOO dell'Amministrazione Difesa, per motivi tecnico-organizzativi e di responsabilità, viene suddiviso in tre sezioni: corrente, di deposito e storica;

- *Archivio corrente*, la raccolta degli atti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista ancora un interesse;
- *Archivio di deposito*, l'insieme degli atti relativi ad affari e a procedimenti amministrativi conclusi. Detti atti non risultano più necessari per il corrente svolgimento di procedimenti amministrativi; verso tali documenti può, tuttavia, sussistere un interesse sporadico;
- *Archivio storico*, l'insieme degli atti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati alla conservazione perenne presso l'archivio storico di F.A., previo operazioni di scarto effettuate da apposita commissione;
- *Area Organizzativa Omogenea (AOO)*, un insieme di unità organizzative (UO) facenti capo alla stessa Amministrazione che usufruiscono, in modo omogeneo e coordinato, dei servizi informatici per la gestione dei flussi documentali e, in particolare, del servizio di protocollazione (art. 50 comma 4 del DPR). Per ciascun tipo di provvedimento relativo ad atti di propria competenza, è individuata l'UO responsabile dell'istruttoria e di ogni altro adempimento procedimentale per l'adozione del provvedimento finale. A tal fine deve essere utilizzato solo ed esclusivamente un unico registro di protocollazione degli atti;
- *Busta di trasporto*, il documento informatico che contiene il messaggio di posta elettronica certificata;
- *Classificazione*, l'attribuzione a ciascun documento di un indice (di classificazione) inserito in una struttura di voci (piano di classificazione), e l'associazione dello stesso ad una definita unità archivistica generalmente identificata come fascicolo;
- *Codice*, il decreto legislativo 7 marzo 2005 n.82 – Codice dell'A.D.;
- *Dati anonimi*, dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile: art. 4, comma 1, lett. n) del CODPR;
- *Dati giudiziari*, i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1 del DPR 14 novembre 2002 n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale: art.4, comma 1, lett. e) del CODPR;
- *Dati personali*, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale: art. 4, comma 1, lett. b) del CODPR;
- *Dati sensibili*, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale: art. 4, comma 1, lett. d) del CODPR;
- *Documento amministrativo*, ogni rappresentazione, comunque formata, dei contenuti di atti, anche interni, delle pubbliche amministrazioni, o, comunque, utilizzati ai fini dell'attività pratica dell'Amministrazione;
- *Documento analogico*, la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;
- *Documento informatico*, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti "art.1, lett. p)–bis del CAD";
- *Fascicolazione*, l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi;

- *Fascicolo*, insieme minimo di documenti, composto dall'ordinata riunione di carte relativa ad uno stesso affare o procedimento amministrativo;
- *Fascicolo/pratica archiviato*, il fascicolo che ha completato il suo ciclo all'interno della trattazione dell'affare e viene trasferito dall'ufficio utente all'Archivio Deposito;
- *Fascicolo/pratica chiuso*, il fascicolo che ha completato il suo ciclo all'interno della trattazione dell'affare, ma è conservato all'interno dell'ufficio utente di competenza;
- *Firma digitale*, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica ed una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
- *Firma elettronica*, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
- *Firma elettronica qualificata*, la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale per la creazione della firma elettronica;
- *Fruibilità di un dato*, la possibilità di utilizzare un dato anche trasformandolo nei sistemi informativi automatizzati di un'altra amministrazione;
- *Gestione informatica dei documenti*, l'insieme delle attività finalizzate alla registrazione e segnatura di un protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione dell'archivio adottato, effettuate mediante sistemi informatici;
- *Glifo*, contrassegno generato elettronicamente mediante una sequenza grafica idonea a rappresentare univocamente un documento amministrativo informatico o un suo estratto o copia o duplicato o i suoi dati identificativi;
- *Impronta di un documento informatico*, la sequenza di simboli binari in grado di identificarne univocamente il contenuto;
- *Linee Guida sulla formazione, gestione e conservazione dei documenti informatrici,* emanate dall'Agenzia per l'Italia Digitale*,* in esecuzione dal 01 gennaio 2022, sostituiscono le regole tecniche del DPCM 3 dicembre 2013 e del DPC del 14 novembre 2014;
- *Log dei messaggi*, il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuta dal gestore;
- *Manuale di Gestione*, il documento, previsto dall'art. 5 del [DPCM] che descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del PI. In particolare, il Manuale contiene l'insieme delle regole, certificate dall'AOO, per un corretto ed efficace funzionamento del sistema di protocollo, dei procedimenti amministrativi informatici e del sistema documentale, costituendo, pertanto, la "carta dei servizi" dell'AOO stessa nella quale gli interessati trovano descritte le modalità di gestione del protocollo nei suoi diversi aspetti;
- *Messaggio di posta elettronica certificata*, un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati;
- *Nucleo protocollo*, Nucleo per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art.61, comma 1, del testo unico;

- *Password*, è associata ad uno specifico username e serve ad ottenere una identificazione univoca da parte del sistema a cui l'utente chiede l'accesso. La coppia username/password fornisce le credenziali di accesso. È una forma comune di autenticazione e per questo motivo la password è personale e segreta, non cedibile e deve rispettare le norme elementari di sicurezza;
- *Piano di conservazione degli archivi*, il piano contenente i criteri di organizzazione dell'archivio, di selezione periodica e conservazione permanente di documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali in conformità a quanto disposto dall'art.68, comma 1, del DPR 28 dicembre 2000, n.445;
- *Posta elettronica*, un sistema elettronico di trasmissione dei documenti informatici;
- *Posta Elettronica Certificata (PEC)*, ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'avvenuta ricezione del messaggio e al destinatario la garanzia dell'identità del mittente. La PEC istituzionale è strettamente connessa all'IPA, ove sono pubblicati gli indirizzi di posta certificata associati all'AOO e alle funzioni organizzative previste dalle Pubbliche Amministrazioni;
- *Posta Elettronica Istituzionale (PEI),* la email istituita da ciascuna AOO attraverso la quale possono essere ricevuti i messaggi da protocollare;
- *Regole tecniche*, il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013. Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n.82 del 2005;
- *Responsabile del Procedimento amministrativo (RPA)*, il dipendente della PA cui è affidata la gestione del procedimento amministrativo. È il Dirigente dell'unità organizzativa interessata che assegna a sé, oppure a un altro dipendente dell'unità, il ruolo di responsabile del procedimento;
- *Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (RDS)*, la figura prevista dall'art.61 del DPR, i cui compiti, elencati nel citato DPR art.61 e nel DCPM art.4, non sono meramente burocratici come quelli del classico Capo Ufficio Posta o figure simili, da sempre presenti nell'Amministrazione Difesa, ma hanno, principalmente, una valenza di tipo legale: il RDS garantisce il corretto funzionamento (a norma di legge) del sistema di PI dell'AOO, anche nei confronti di soggetti terzi e altre Pubbliche Amministrazioni;
- *Riferimento temporale*, l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata;
- *Segnatura di protocollo*, l'apposizione o associazione, all'originale del documento, in forma permanente e non modificabile, dei metadati riguardanti il documento stesso;
- *Sigillo elettronico,* dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi;
- *Testo Unico*, il Decreto del Presidente della Repubblica 28 dicembre 2000 n.445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- *Titolario d'archivio*, lo schema generale di voci logiche rispondenti alle esigenze funzionali e articolate in modo gerarchico, al fine di identificare, partendo dal generale al particolare, l'unità di aggregazione di base dei documenti all'interno dell'archivio.
- *Unità organizzativa (UO)*, uno dei sottoinsiemi dell'Area Organizzativa Omogenea rappresentato da un complesso di risorse umane e strumentali cui sono affidate competenze omogenee. Più semplicemente l'UO è un Ufficio dell'Area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico;
- *Utente di posta elettronica certificata*, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi ente, associazione e organismo, nonché eventuali unità

organizzative interne ove presenti, che sia mittente o destinatario di posta elettronica certificata;
- *Vicario,* sostituisce il RDS nel caso di una sua assenza o impedimento;
- *@D[h]OC,* sistema software di gestione del protocollo informatico.

1.4. AREA ORGANIZZATIVA OMOGENEA

Ai fini della gestione dei documenti del Reggimento Logistico "Folgore" è istituita l'Area Organizzativa Omogenea (di seguito AOO) codice identificativo interno:

M_D E25800

Laddove:
- **"M_D"**, è il Codice identificativo dell'Amministrazione Difesa (Codice IPA);
- **"E"**, rappresenta il primo carattere del Codice Interno indicante l'appartenenza dell' AOO all'Esercito;
- **"25800"**, è la seconda parte del Codice Interno dell'AOO, che nel caso specifico è riferito al Codice SISME del Reggimento Logistico "Folgore".

Oltre al Codice Interno, all'AOO è stato assegnato, in aderenza alle LLGG dell'Agenzia per l'Italia Digitale, il Codice Univoco "**AE57B7E".**

All'interno della Area Organizzativa Omogenea del Reggimento Logistico "Folgore" (di seguito AOO) il sistema di protocollazione è unico e centralizzato per la corrispondenza in entrata, mentre è decentralizzato, per la corrispondenza in uscita, attraverso le Unità Organizzative (UO).

1.5. UNITÀ ORGANIZZATIVE

Nell'ambito dell'AOO, in aderenza alla definizione formulata dal "Testo Unico" e con riferimento alle finalità ed ai compiti delle sue componenti ordinative, sono state individuate le Unità Organizzative (UO) riportate nell'allegato "A".

Ciascuna UO è retta da un Dirigente/Funzionario responsabile per le funzioni di competenza. Inoltre, esistono una serie di articolazioni (Nuclei o strutture similari) a loro volta dipendenti dalle rispettive UO per le quali non si ritiene necessaria una dettagliata elencazione, ma di cui è necessario attestarne l'esistenza al fine di renderne coerente la menzione nel corso della descrizione dei processi interni all'AOO.

1.6. NUCLEO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, LA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Nell'AOO è istituito il Nucleo per la tenuta del protocollo informatico la gestione dei flussi documentali e degli archivi.

Alla guida del suddetto NdP è posto il Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RDS). Egli è funzionalmente individuato nell'ambito dell'Ufficio Maggiorità e Personale e si identifica con il Capo Ufficio Maggiorità e Personale.

Nei casi di vacanza, assenza o impedimento del RDS, la direzione del servizio è affidata al Vicario. In allegato "B" è riportato l'elenco del personale incaricato dell'erogazione e gestione del servizio.

È compito del RDS:
- predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere ad inviare il Manuale al Referente del protocollo per la Difesa per la successiva pubblicazione sul istituzionale del Ministero della Difesa;
- presiedere alle attività del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi alle dipendenze della stessa AOO;
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico;
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;

- attribuire il livello di autorizzazioni per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e modifica delle informazioni;
- garantire la regolarità delle operazioni di registrazione e segnatura del protocollo;
- garantire la corretta produzione e la conservazione dei registri giornalieri di protocollo;
- curare che le funzionalità del sistema, in caso di guasti o anomalie, possano essere ripristinate entro le 24 ore dal blocco delle attività e, comunque, nel più breve tempo possibile; autorizzando eventualmente lo svolgimento di registrazione di protocollo tramite il Registro di emergenza;
- autorizzare le operazioni di annullamento di un protocollo;
- vigilare sull'osservanza delle disposizioni da parte del personale autorizzato e incaricato.

Il sistema software utilizzato per la gestione del protocollo informatico (PI) è denominato "@D[h]OC".

1.7. CONSERVAZIONE REGISTRI GIORNALIERI DI PROTOCOLLO

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto dei registri giornalieri di protocollo, entro la giornata lavorativa successiva, viene inviato al sistema di conservazione attraverso un contenitore denominato *Pacchetto di Versamento*. Il sistema di conservazione effettua i controlli previsti dalla normativa e mette a disposizione del mittente un *Rapporto di Versamento* che contiene l'esito della trasmissione. Una volta che il contenuto del Pacchetto di Versamento ha superato i controlli previsti, i singoli documenti vengono inseriti in uno o più *Pacchetti di Archiviazione*, i contenitori che conservano i documenti inviati. Il mittente può accedere al *Rapporto di Archiviazione*, che identifica in modo univoco il Pacchetto di Archiviazione che contiene i documenti inviati in conservazione, attraverso tale informazione, è possibile richiedere, quando necessario, all'erogatore del servizio di conservazione, il documento in conservazione, che viene inviato al richiedente attraverso un *Pacchetto di Distribuzione*.
Il servizio, su indicazione del Responsabile della Conservazione della Difesa, viene erogato presso il Centro di Dematerializzazione e Conservazione Unico della Difesa, rinviando per tutti i dettagli più tecnici ed operativi al Manuale della Conservazione del Ministero della Difesa e al Manuale della Conservazione del già citato Centro.

1.8. RECAPITO DEI DOCUMENTI

L'AOO per l'invio della corrispondenza in forma telematica utilizza le seguenti caselle di posta elettronica:

- posta elettronica istituzionale (PEI): rgtlfolgore@esercito.difesa.it.
- posta elettronica certificata (PEC): rgtlfolgore@postacert.difesa.it.

In alternativa, l'indirizzo postale per la documentazione analogica diretta all'AOO è:

Reggimento Logistico "Folgore"
Via Aurelia Nord, 2 – 56122 PISA

La corrispondenza diversamente indirizzata, o diretta a entità non appartenenti all'AOO, non sarà accettata.
La documentazione inviata da una casella di posta elettronica ordinaria alla PEC dell'AOO non sarà recapitata, ed i mittenti riceveranno un messaggio con la seguente dicitura:
"non è stato possibile recapitare la sua mail alla PEC *rgtlfolgore@postacert.difesa.it* in quanto quest'ultima è configurata per ricevere esclusivamente da un casella PEC. Per comunicare con l'Ente tramite la sua casella di posta elettronica ordinaria può inviare il messaggio alla casella PEI di quest'ultimo ovvero ritrasmettere il messaggio utilizzando una casella PEC".

1.9. TUTELA DEI DATI PERSONALI

La documentazione contenente dati personali comuni, sensibili e/o giudiziari è gestita in conformità al Regolamento Generale per la Protezione dei Dati (UE) 679/2016 (GDPR) e del D.Lgs. 196/2003 Codice di protezione dei dati personali (CODPR), la loro trattazione e visione è consentita esclusivamente agli utenti abilitati.

In particolare, nella predisposizione o nella protocollazione di tali documenti gli utilizzatori del sistema sono obbligati a cliccare sull'apposito campo dati sensibili. Così facendo i documenti saranno visibili nel sistema solo agli utenti parimenti abilitati a tale trattazione.

1.10. ELIMINAZIONE PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

In coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'amministrazione sono registrati all'interno dei registri di protocollo informatico. Pertanto tutti i registri di protocollo cartacei sono stati aboliti ed eliminati.

1.11. ENTRATA IN VIGORE DEL MANUALE

Le regole indicate nel presente manuale saranno applicate a decorrere dalla sua pubblicazione sul sito istituzionale del Ministero della Difesa.

2. PIANO DI SICUREZZA

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

2.1. OBIETTIVI DEL PIANO DI SICUREZZA

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'AOO siano resi integri e disponibili, limitatamente al personale dell'AOO stessa;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2.2. GENERALITÀ

Al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti sono state adottate le misure tecniche e organizzative di seguito specificate:

- protezione periferica della rete Intranet dell'AOO;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, delle seguenti credenziali di accesso:
  - accesso tramite carta multiservizi della Difesa (CMD) attraverso i codici carta in possesso all'utente;
  - accesso tramite identificazione dell'utente da parte del sistema (user name) e autenticazione riservata (password);
- cambio delle password con frequenza almeno bimestrale durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi.
- Archiviazione ed invio in conservazione giornaliera, in modo non modificabile, dei registri di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata.

I dati personali registrati dalla logica del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

2.3. 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 mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo.

2.4. GESTIONE DEI DOCUMENTI INFORMATICI

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

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

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e dei registri di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- non permette la ricezione di comunicazioni da una casella di posta elettronica ordinaria ad una casella di posta elettronica certificata (PEC) dell'Amministrazione Difesa;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

2.5. COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce a quella in essere per tutte le attività svolte presso il sistema informatico dell'AOO e la cui responsabilità risale all'Ufficiale alla sicurezza CIS (Comunication and Information Systems) del Reggimento Logistico "Folgore".

3. FORMAZIONE, TRASMISSIONE, SOTTOSCRIZIONE E ARCHIVIAZIONE DEI DOCUMENTI INFORMATICI.

3.1. GENERALITÀ

Per la gestione dei documenti informatici, l'AOO dispone principalmente di due caselle di posta elettronica, una di tipo istituzionale (PEI) e l'altra di tipo certificata (PEC):

- posta elettronica istituzionale (PEI): rgtlfolgore@esercito.difesa.it;
- posta elettronica certificata (PEC): rgtlfolgore@postacert.difesa.it.

Inoltre ogni UO al suo interno dispone di ulteriori caselle di posta ordinaria per lo scambio di comunicazioni e documenti informatici che non devono essere protocollati.

3.2. REGOLE TECNICO-OPERATIVE DELLA COMUNICAZIONE

La trattazione di documentazione amministrativa attraverso le caselle di posta elettronica comporta la necessità di adeguarsi a determinati standard per consentire l'interoperabilità dei sistemi oltre che per rispondere al dettato normativo vigente. In particolare dovranno essere osservate le seguenti regole:

- devono essere inviate con il medesimo mezzo trasmissivo disponibile presso il destinatario. La posta elettronica certificata non garantisce la ricezione di messaggi inviati tramite posta ordinaria;
- l'oggetto deve essere riportato nell'omonimo campo del messaggio e non deve riportare caratteri speciali quali [, /, °, ^, virgolette, apici ecc..;
- i nomi dei file allegati devono essere privi di caratteri speciali, accenti e interpunzioni. In alternativa a tali caratteri si suggerisce di utilizzare il carattere _ (underscore). Esempi di file validi: richiesta_di_riscatto.pdf, foto_esercitazione.jpg, variazione_dell_utenza.pdf; mentre, non vanno bene nomi come: è il 1° documento.pdf, oppure, si.trasmette.domanda.pdf, o ancora, questa è la mia domanda per entrare a far parte dell'esercito.pdf;
- i documenti primarivengono normalmente prodotti nel formato PDF/A;
- i formati relativi agli allegati al messaggio sono suddivisi nelle seguenti categorie:
  - documenti impaginati (.pdf .docx, .doc, .odt, .rtf, .txt);
  - ipertesti (XML, HTML);
  - dati strutturati (SQL, CSV, .accdb, .mdb, .odb, JSON, JWT);
  - posta elettronica (.eml, .mbox);
  - fogli di calcolo (.xlsx, .xls, .ods);
  - presentazioni multimediali (.pptx, .ppt, .odp);
  - immagini raster (.jpg, .jpeg, .png, .gif, .tif, .tiff,);
  - immagini vettoriali (.svg, odg, .wmf, .emf);
  - modelli digitali (non presenti nella direttiva SMD-I-002, standardizzazione dei formati dei documenti elettronici della difesa);
  - caratteri tipografici (non presenti nella direttiva SMD-I-002, standardizzazione dei formati dei documenti elettronici della difesa);
  - suono (.wav, .mp3, .flac, .aiff, .ogg, .oga);
  - video (formati video MPEG-1, MPEG-2, MPEG-4, .wmv, .webm, .avi, .ov, .qt, .ogv, .ogg, .mk4, .3gp, .3g2);
  - sottotitoli (non presenti nella direttiva SMD-I-002, standardizzazione dei formati dei documenti elettronici della difesa);
  - contenitori multimediali (non presenti nella direttiva SMD-I-002, standardizzazione dei formati dei documenti elettronici della difesa);
  - archivi compressi (.zip, .tar, .gz);
  - applicazioni e codici sorgente (non presenti nella direttiva SMD-I-002, standardizzazione dei formati dei documenti elettronici della difesa);
  - applicazioni crittografiche (.p7m, PADES-.pdf)
- se di numero elevato, i file allegati al documento primario, rispettando i formati anzidetti, vengono compressi prevalentemente nel formato ZIP;
- l'invio difforme da quanto anzidetto comporta la restituzione al mittente del messaggio;
- l'eventuale necessità di inviare documenti in formati difformi da quelli sopra elencati potrà essere rappresentata al RDS, tramite l'UO cui è diretta la comunicazione;

- la massima dimensione complessiva dei documenti è di 30 Mb (PEI) – 100 Mb (PEC) suddivisi per il numero di destinatari. Superato tale limite, il sistema di posta elettronica non recapiterà il messaggio;
- la presenza della firma digitale non valida rende nullo il documento che sarà così restituito;
- in un singolo messaggio di posta elettronica deve essere associata la documentazione riguardante un unico argomento (pertanto se un mittente deve inviare cinque documenti afferenti cinque pratiche, dovrà inviare cinque mail);
- le marche temporali apposte insieme alla firma digitale devono essere in formato embedded e non detached (il file firmato e la firma devono essere contenuti in un'unica busta di file);
- la casella postale del mittente, in caso di persona giuridica, deve essere riferita a tale soggetto (a esempio, la ditta VERDI srl dovrà inviare la propria documentazione dalla casella postale aziendale verdisrl@xxxxx.it e non dalla casella postale personale carlo.verdi@verdisrl.xxxx.it).

3.3. FORMAZIONE DEI DOCUMENTI - ASPETTI OPERATIVI.

In aderenza alla normativa vigente (art. 40 del CAD) e alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatrici (LLGG), emanate dall'Agenzia per l'Italia Digitale, l'AOO produce gli originali dei propri documenti con mezzi informatici e procede alla dematerializzazione dei documenti cartacei in ingresso per consentire la gestione elettronica dell'intero flusso documentale. La documentazione dematerializzata in ingresso viene firmata digitalmente dal personale del Nucleo di Protocollo a ciò delegato. Fermo restando quanto previsto dalla norma, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità. Sul documento informatico è apposta oltre alla firma digitale del personale che ha dematerializzato il documento cartaceo anche l'attestazione di conformità con la dicitura "il presente documento è copia informatica conforme al documento amministrativo analogico da cui è tratta previo raffronto (art. 23 ter/3 D.lgs 82/2005 e par. 2.2 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici)".

Altri aspetti fondamentali di un documento sono:

- trattazione di un unico argomento indicato in maniera sintetica nello spazio riservato all'oggetto;
- riferimento ad un solo numero di registrazione di protocollo;
- possibilità di far riferimento a più fascicoli;
- consentire l'identificazione dell'amministrazione mittente.

3.4. SOTTOSCRIZIONE DEI DOCUMENTI INFORMATICI

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.

I documenti informatici prodotti dall'amministrazione, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità.

In particolare, tutta la documentazione confluente all'interno del sistema di protocollo informatico è convertita nel formato PDF/A. Gli allegati che per la loro natura o per il loro utilizzo non possono o non devono essere convertiti in tale formato, saranno mantenuti come in origine senza la firma digitale.

La sottoscrizione digitale dei documenti predisposti in uscita avviene in seno alla funzionalità di trasmissione che, mediante automatismi, consente la loro protocollazione e l'invio telematico verso destinatari in possesso di e-mail.

In aderenza al Regolamento Europeo Eidas (electronic Identification, Authentcation, Signature) al documento informatico in uscita deve essere apposto il sigillo elettronico cioè la firma del file segnatura .xml che garantisce l'origine e l'integrità del documento stesso.

3.5. REQUISITI DEGLI STRUMENTI INFORMATICI DI SCAMBIO

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

- l'integrità del messaggio;

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

3.6. RUBRICA

Per poter inviare/ricevere documenti da e verso l'AOO tramite il sistema software di gestione del PI, denominato @D[h]OC, è necessario inserire gli indirizzi dei corrispondenti nella "rubrica". A ciascun indirizzo deve essere associata una precisa tipologia tra le seguenti:

- Pubblica Amministrazione Italiana (IPA), indirizzi prelevati direttamente dall'Indice dei domicili digitali delle Pubbliche Amministrazioni (IPA);
- Persona Fisica, indirizzi apparteneti a persone fisiche ;
- Persona Giuridica, indirizzi appartenenti a persone giuridiche (varie tipologie di società);
- Amministrazione Estera, indirizzi appartenenti a Pubbliche Amministrazioni Estere.

Inoltre è stata introdotta la categoria "Pubblica Amministrazione (NON IPA)", per venire incontro a talune esigenze di comunicazione di Enti che non sono Aree Organizzative Omogenee, ancorchè non presente nelle LLGG.

L'indirizzo a cui non viene abbinata alcuna tipologia di quelle sopra descritte è considerato "Non Definito" e non può essere utilizzato per inviare/ricevere documenti da e verso l'AOO.

3.7. FIRMA DIGITALE

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo è la firma digitale utilizzata per inviare/ricevere documenti da e verso l'AOO e per sottoscrivere documenti, o qualsiasi altro "file" digitale con valenza giuridico-probatoria.

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'amministrazione fornisce la firma digitale ai soggetti delegati a rappresentare l'Amministrazione e identificati con il Comandante dell'Ente, i Dirigenti titolari delle UO o i Funzionari da questi delegati ed il personale del Nucleo di Protocollazione (NdP).

Un documento sottoscritto con firma digitale, formato secondo le prescrizioni del CAD:

- è equiparato alla scrittura privata e la firma si presume riconducibile al titolare, salvo prova contraria;
- fa piena prova ai sensi dell'art. 2702 del Codice Civile (fino a querela di falso della provenienza delle dichiarazioni da parte di chi ha sottoscritto il documento);
- soddisfa il requisito legale della forma scritta (art. 21 del CAD).

3.8. SIGILLO ELETTRONICO

Il sigillo elettronico, introdotto nel nostro ordinamento con l'emanazione del Regolamento Europeo Eidas (electronic Identification, Authentcation, Signature) che regolamenta l'uso delle firme elettroniche nella Comunità Europea, è equivalente a una firma elettronica qualificata con la differenza che non afferisce a d una persona fisica , bensì ad una persona giuridica e garantisce l'origine e l'integrità dei documenti informatici a cui è apposto.

3.9. USO DELLA POSTA ELETTRONICA CERTIFICATA

Per poter disporre di una conferma di avvenuta ricezione della corrispondenza, il veicolo privilegiato per le comunicazioni è la casella di PEC, sempreché anche il corrispondente disponga di una casella di PEC.

L'utilizzo della casella di PEI avverrà solo in mancanza di funzionamento della casella di PEC.

Si ribadisce che le comunicazioni inviate alla casella PEC da caselle di posta elettronica ordinaria non saranno accettate ed i mittenti riceveranno il messaggio di mancato recapito.

3.10. ARCHIVIAZIONE DEL DOCUMENTO INFORMATICO

I documenti informatici sono archiviati nel rispetto dell'art. 44 del CAD.

4. LA GESTIONE DEI DOCUMENTI – ASPETTI FUNZIONALI

4.1. GENERALITÀ

I documenti, sia analogici che informatici, vengono gestiti in relazione al loro formato, in ambito AOO, nel seguente modo:

- in entrata;
- in uscita;
- interno.

La gestione documentale, in generale, si basa sui principi di:

- centralità per quanto concerne la posta in ingresso, la totale corrispondenza indirizzata al Reggimento Logistico "Folgore" viene registrata in un unico punto il Nucleo di Protocollo (NdP);
- delega alle UO che hanno facoltà di trasmettere direttamente i documenti sia informatici sia analogici all'esterno dell'AOO.

Per poter produrre un documento in uscita sono previsti i seguenti passaggi:

- Formazione del documento principale ed eventuali allegati;
- Calcolo dell'impronta del documento principale e degli eventuali allegati;
- Generazione del numero di protocollo da assegnare al messaggio di protocollo;
- Formazione della segnatura di protocollo che deve rispettare l'XML, schema indicato nelle LLGG, utilizzando le impronte del documento principale e degli eventuali allegati, create nei passaggi precedenti.
- Apposizione di un sigillo elettronico qualificato alla segnatura di protocollo per garantire l'integrità autenticità.

In base al tipo di registro di protocollo utilizzato nella fase di predisposizione di un documento informatico in uscita si può avere le seguenti tipologie documentali:

- Generale (utilizzato generalmente per la maggior parte dei documenti informatici);
- Nota /Appunto;
- Coordinamento;
- Variazioni Matricolari;
- Ordini del Giorno;
- Ordini di Servizio;
- Gestione Personale;
- Deposito Telematico;
- Decreti;
- Fatture e Rifiuto Fatture;
- Gare.

I documenti in ingresso alla AOO sono assegnati direttamente ai Dirigenti titolari delle UO interessate (Responsabili del Procedimento Amministrativo) che provvedono alla successiva gestione interna.

Inoltre, il controllo della completezza formale e sostanziale della documentazione pervenuta e soggetta alle operazione di registrazione, spetta al personale dell'UO interessata alla tematica che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente, specificando le eventuali problematiche del caso.

Per i dettagli tecnici ed operativi relativi alla gestione dei documenti si rimanda alla lettura dei manuali e alla visione dei video presenti nel sistema di gestione documentale del P.I., denominato @D[h]OC, alla voce "Guida". Inoltre nel sistema @D[h]OC sono consultabili, nell'apposita sezione del cruscotto, i bollettini periodici con cui vengono descritte nuove funzionalità.

4.2. ORARIO DI EROGAZIONE DEL SERVIZIO

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

- lunedì – giovedì dalle ore 08:00 alle ore 16:30;
- venerdì dalle ore 08:00 alle ore 12:00.

Per i documenti in uscita, il servizio di protocollazione sarà fruibile dalle 08:00 alle 23:59 di ciascun giorno lavorativo. Questo poiché il cambio data richiede la chiusura dei registri di protocollo giornalieri che può avvenire in automatico tramite abilitazione al sistema da parte del RDS o manualmente dallo stesso entro le ore 08:00 del giorno lavorativo successivo.

4.3. DOCUMENTI PROTOCOLLATI E DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE

Il sistema informatico del protocollo è progettato al fine della trattazione esclusivamente/unicamente dei documenti *non classificati* fino a livello "NON CLASSIFICATO CONTROLLATO" (mediante la funzione del sistema *dati sensibili*). La posta classificata erroneamente pervenuta al NdP sarà consegnata al Punto Controllo NATO-UE/S del Comando.

Inoltre, a mente dell'art. 53 comma 5 del DPR, sono esclusi dalla registrazione di protocollo:

- le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione;
- le note di ricezione delle circolari e altre disposizioni;
- i materiali statistici, i giornali, le riviste e i libri;
- i materiali pubblicitari, gli inviti a manifestazioni;
- documenti già soggetti a registrazione particolare dell'Amministrazione;
- fogli di viaggio;
- documentazione caratteristica;
- registro delle presenze;
- modelli 730;
- licenze, permessi;
- esposti anonimi;
- informazioni elettroniche superiori ai 30/100 mega di dimensione oltre la quale il sistema non registra.

Relativamente ai documenti "sensibili" sono previste particolari forme di riservatezza e di accesso controllato mediante l'attivazione, da parte del personale del servizio di protocollo, di un filtro elettronico. L'UO competente per la trattazione può comunque, anche in un secondo momento, attivare le suddette limitazioni all'accesso.

4.4. DOCUMENTO INFORMATICO

L'AOO è predisposta alla ricezione e alla gestione di documenti informatici sulle caselle di posta elettronica certificata (PEC) e di posta elettronica istituzionale (PEI).

Se un documento informatico viene inviato ad una casella di posta elettronica afferente ad una UO, il titolare di tale casella deve inviare un messaggio al mittente segnalando la necessità di inviare nuovamente il documento alle caselle di PEI o PEC dell'AOO.

Se un documento informatico viene inviato da una casella di posta elettronica ordinaria alla PEC dell'AOO non sarà recapitato e di conseguenza non verrà protocollato

4.5. DOCUMENTO INFORMATICO IN ENTRATA SU POSTA ELETTRONICA ISTITUZIONALE

I messaggi pervenuti sulle caselle di Posta Elettronica Istituzionale (PEI) vengono presentati ai vari operatori di protocollo in ordine al loro arrivo. Se la protocollazione non viene completata, il relativo messaggio da registrare sarà presentato al primo operatore che, subito dopo, accederà alla stessa coda dei messaggi.

I messaggi possono essere protocollati e contestualmente assegnati all'UO competente, ovvero, essere inviati in un apposito elenco gestito dal RDS qualora siano rilevate anomalie.

Il RDS, a sua volta, potrà protocollare i messaggi a lui presentati, ovvero rispedirli al mittente segnalando le eventuali anomalie riscontrate, ovvero, nei casi previsti, cancellarli senza farli entrare all'interno del sistema documentale.

In particolare, il sistema prevede sette casi pre-impostati di messaggio che l'RDS invierà al mittente:

- il messaggio è corrotto o uno dei documenti non è leggibile;
- dati non congruenti nella segnatura informatica;
- segnatura non conforme alle LLGG;
- 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.

Ai sensi della normativa vigente è possibile protocollare un messaggio di posta elettronica ordinaria solo se firmato digitalmente.

Nel rispetto dell'art. 38 del DPR vengono comunque accettati e protocollati documenti informatici privi di firma digitale ai quali sia allegata una scansione del documento di identità del mittente. Tali documenti potranno comunque non essere accettati per la successiva trattazione dall'UO competente se viene riscontrata qualche irregolarità. Di tale evento sarà informato il mittente attraverso apposito messaggio preparato dall'UO assegnataria per competenza.
Nel caso in cui il mittente sia una PA, in assenza della firma digitale, è sufficiente che sia presente in allegato il file segnatura .xml, informazioni previste dalle LLGG.
In quest'ultimo caso, ove richiesto dal mittente, sarà trasmesso:

- messaggio di conferma di protocollazione, che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto;
- messaggio di notifica di eccezione, che notifica la rilevazione di un'anomalia in un messaggio ricevuto;
- messaggio di annullamento di protocollazione, che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza.

Il sistema gestisce in automatico, senza inserirli nelle rispettive code, i messaggi che segnalano un problema di ricezione nella casella postale ordinaria del destinatario (ad esempio, destinatario sconosciuto, casella postale del destinatario piena). Questi messaggi sono automaticamente inseriti quali allegati del documento che ha generato il messaggio stesso e il documento interessato viene ricollocato sulla scrivania virtuale *(posta non consegnata)* inerente ai documenti in ingresso del primo utente che ha predisposto il documento, per le opportune azioni del caso.
In particolare, l'addetto, dopo le necessarie verifiche può:

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

Almeno una volta al giorno viene verificata la presenza di messaggi.
Nel caso in cui un documento non rispondente ai requisiti succitati fosse registrato e assegnato all'Unità Organizzativa sarà cura di quest'ultima informare l'RDS per le azioni che ogni caso di errore richiede.
Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida" e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.6. DOCUMENTO INFORMATICO IN ENTRATA SU POSTA ELETTRONICA CERTIFICATA

La trattazione dei messaggi pervenuti sulle caselle di Posta Elettronica Certificata (PEC) segue le stesse regole indicate al precedente paragrafo con l'eccezione della differente coda di arrivo dei messaggi rispetto alla PEI e l'impossibilità dell'RDS di rispedirli al mittente. Inoltre non possono essere ricevuti messaggi provenienti da caselle di posta eletronica non certificata.

4.7. MESSAGGI IN ARRIVO SULLA POSTAZIONE E-MESSAGE

I messaggi telegrafici indirizzati al Reggimento Logistico "Folgore" sono <u>tutti</u> ricevuti sulla postazione "E–Message" dedicata del NdP.
Gli operatori di protocollo informatico provvederanno a:

- esportare il messaggio ricevuto in formato PDF (Portable Document Format);
- eseguire l'acquisizione nel sistema di PI del file .pdf così ottenuto;
- protocollare il messaggio;
- inoltrare il messaggio alle UO destinatarie in indirizzo.

4.8. DOCUMENTO INFORMATICO IN USCITA

Come già segnalato in precedenza tutta la documentazione amministrativa dell'AOO è originata e/o gestita in forma elettronica.
A seguito della formazione degli atti, i Dirigenti titolari delle UO o i funzionari da questi delegati provvedono al loro perfezionamento, attraverso le funzioni del sistema di PI, firmando digitalmente e apponendo la marca temporale al documento di interesse.

Il sistema, sulla base delle informazioni inserite durante la predisposizione, invia ai destinatari, per posta elettronica, il documento primario e tutti gli eventuali allegati.
Gli operatori delle UO, nella fase di predisposizione del documento informatico in uscita, devono inserire nel sistema "@D[h]OC" i seguenti dati/file:

- *Oggetto*, che non deve contenere caratteri speciali, interpunzioni e/o lettere accentate (esempi di caratteri da non usare: /'°,.^);
- *Classificazione*, selezionando i tre livelli del titolario d'archivio (Titolo, Classe e Sottoclasse), il fascicolo e/o il sottofascicolo.
- *Destinatari*, possono essere esterni e/o interni all'AOO, per i destinatari esterni si può prevedere l'utilizzo esclusivo della casella postale elettronica PEC che può essere modificato fino alla firma del documento stesso da tutti gli utenti che in successione ricevono il documento per il suo perfezionamento (Capo Nucleo, Capo Ufficio, ecc.);
- *Documenti*, inserimento del file da inviare come documento primario tramite la funzione "Sfoglia" e inserimento degli eventuali suoi file allegati tramite le funzioni "Allega da Protocollo" o "Allega da Testo (la preparazione del documento primario e degli eventuali allegati avviene al di fuori del sistema e prima di accedere alla predisposizione);

Inoltre possono essere utilizzate le seguenti funzioni del sistema "@D[h]OC":

- *Modifica UO Mittente*, per modificare l'UO di appartenenza dell'utente che sta predisponendo il documento;
- *Tipologia documentale*, per selezionare un registro di protocollo diverso da quello "generale"
- *Dati Sensibili*, per l'invio di documentazione contenente dati sensibili, limitandone la visibilità all'interno delle UO;
- *Priorità*, per evidenziare il livello di precedenza d'invio della documentazione;
- *Allegati Differenziati*, per l'invio di allegati differenziati ai vari destinatari. Per tale funzione non devono essere indicati sulla lettera di trasmissione i destinatari previsti ma la più generica dicitura "vedasi indirizzi in allegato" (gli indirizzi saranno successivamente generati automaticamente dal sistema);
- *Ruolo Firma*, per selezionare il dirigente/funzionario delegato che dovrà firmare digitalmente il documento informatico;
- *Note* da inserire per eventuali informazioni utili a tutti gli utenti che in successione ricevono il documento per il suo perfezionamento (Capo Nucleo, Capo Ufficio, ecc.);
- *Riferimenti/Seguiti e File Accessori*, per inserire documentazione contenete informazioni utili a tutti gli utenti che in successione ricevono il documento per il suo perfezionamento (Capo Nucleo, Capo Ufficio, ecc.), tale documentazione non verrà firmata, protocollata e inviata;

Al fine di inviare correttamente un documento informatico è necessario adottare i seguenti accorgimenti per i file che compongono la pratica stessa:

- utilizzare preferibilmente file con estensione PDF;
- nella denominazione dei file non si devono utilizzare caratteri speciali, interpunzioni e/o lettere accentate (esempi di caratteri da non usare: /'°,.^);
- i nomi dei file non devono superare i venti caratteri.

Qualora come allegato, venga inserito un documento informatico che non deve essere firmato digitalmente, l'operatore che sta effettuando la predisposizione deve spuntare la voce "No Firma", per evitare la successiva conversione in PDF/A del documento e l'apposizione della firma digitale.
Tutti i documenti trasmessi sono corredati del file segnatura.xml, contenente metadati ed informazioni previste dalle LLGG.
Potrebbe verificarsi, per motivi connessi ai sistemi di gestione della posta elettronica, che il documento firmato digitalmente e trasmesso dal sistema di PI non venga recapitato al/ai destinatari, in questo caso tale documento verrà visualizzato dagli utenti che lo hanno trattato come "posta non consegnata" e gli stessi potranno successivamente provvederne la ritrasmissione. Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.9. MESSAGGI IN PARTENZA SULLA POSTAZIONE E-MESSAGE

Le UO devono, mediante le funzioni del sistema di protocollo informatico:

- approntare il testo del messaggio in formato digitale, tenendo conto che il messaggio può essere approntato mediante il sistema E-Message e poi esportato in formato PDF, anziché essere stampato;
- inoltrare il messaggio fino al livello Responsabile della UO per la visione e l'approvazione (non deve essere utilizzata la funzione *Dati analogici*);
- approvare i documenti, mediante apposizione della firma digitale da parte del Responsabile della UO, contestualmente alla quale viene effettuata la registrazione di protocollo;
- inoltrare il documento a tutti gli indirizzi indicati in sede di predisposizione.

Successivamente, le stesse UO dovranno:

- inserire nel testo del messaggio prodotto con il sistema "E-Message" il numero di protocollo attribuito dal sistema di protocollo informatico;
- inviare il messaggio anche, laddove ritenuto necessario, tramite la postazione "E-Message" della UO.

I destinatari del messaggio, tra cui quelli eventualmente appartenenti alle UO stesse, riceveranno per posta elettronica il file prodotto dal sistema di PI che, firmato digitalmente, è di per sé idoneo alla trattazione e all'archiviazione.

Nel caso in cui fra i destinatari compaia una lista AIG (Address Indicator Group) e l'inserimento di tutti gli indirizzi nella rubrica del sistema, o la loro selezione, risulti troppo laboriosa si può provvedere a registrare il codice identificativo dell'AIG (es.: AIG 2395) nella tabella degli indirizzi, senza associare ad esso altri dati (indirizzi postale, e- mail, ecc.).

4.10. DOCUMENTO INFORMATICO INTERNO

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

In tutti quei casi nei quali tra gli indirizzi per competenza o per conoscenza di un documento vi sia una UO interna all'AOO, tale informazione viene esplicitamente dichiarata all'interno del sistema informatico che provvederà ad inviare, automaticamente, quel documento sulla scrivania virtuale del dirigente competente dell'UO destinataria.

Rimangono invariate le susseguenti attività gestionali compresa la eventuale necessità di dover ricorrere all'eventuale materializzazione del documento, nei casi previsti per tale procedura.

4.11. DOCUMENTO ANALOGICO

Non sarà accettata la corrispondenza diretta ad articolazioni estranee all'AOO o con indirizzo diverso dal seguente:

Reggimento Logistico "Folgore"
Via Aurelia Nord, 2 – 56122 PISA

4.12. DOCUMENTO ANALOGICO IN ENTRATA

La corrispondenza analogica in entrata può essere acquisita dalla AOO con diversi mezzi e modalità. In particolare è previsto il ritiro della corrispondenza in entrata da parte del personale del Nucleo Posta del Comando all'agenzia delle Poste Italiane come per il ritiro dei plichi dai corrieri civili/militari che verrà effettuato, previo comunicazione del personale di servizio, all'ingresso della Caserma.

I plichi postali sono sottoposti a verifica di sicurezza mediante apposite apparecchiature elettroniche presso i locali del Nucleo Posta del Comando. Per quanto attiene alla corrispondenza soggetta a protocollazione che dovesse giungere direttamente alle UO, essa sarà consegnata al Nucleo Posta preferibilmente nella stessa giornata di ricezione, altrimenti dovrà riportare in calce la data e l'ora in cui è stata consegnata per la protocollazione, seguita dalla sigla dell'UO.

La corrispondenza di tipo cartaceo che viene trattata dal Nucleo Posta è del tipo posta raccomandata, assicurata e ordinaria, escluso quella indirizzata al Punto Controllo NATO-UE/S.

4.12.1. POSTA RACCOMANDATA E ASSICURATA

Il personale del Nucleo Posta ritira le raccomandate e le assicurate destinate all'AOO, identificando i plichi e firmando per ricevuta le relative distinte di dettaglio.

Le raccomandate, le assicurate ed i plichi indirizzati nominativamente al personale appartenente all'AOO dovranno essere ritirati esclusivamente dai destinatari stessi.

4.12.2. POSTA ORDINARIA

La gestione della corrispondenza ordinaria segue le stesse modalità gestionali delle raccomandate e delle assicurate, con l'eccezione che essa non è accompagnata da distinte di dettaglio, ed è trattata dopo la protocollazione delle citate raccomandate e assicurate.

4.12.3. REGISTRAZIONE DEI DOCUMENTI ANALOGICI IN ENTRATA

L'attività di protocollazione si suddivide in quattro fasi consecutive di lavorazione:

- apposizione manuale, sul documento in trattazione, di:
  - codici identificativi delle UO (per competenza e per conoscenza);
  - riferimento alla presenza di allegati non scansionabili/caricabili nel sistema o di marche da bollo (rispettive diciture riportate sul documento: Analogico, Marca);
- scansione massiva dei documenti a cura di uno degli operatori del NdP;
- inserimento nel sistema informatico dei dati essenziali del documento in trattazione:
  - oggetto del documento;
  - denominazione del mittente;
  - segnatura di protocollo mittente;
  - selezione delle UO cui è assegnato il documento;
  - eventuale indicazione di Dato Sensibile secondo le disposizioni del CODPR;
  - eventuale indicazione di *Allegato Analogico,* se presente. In questa fase, l'operatore è tenuto ad effettuare un controllo scrupoloso sulla buona qualità della scansione e sulla corrispondenza esatta tra il documento analogico e la relativa copia per immagine che si accinge a convalidare;
- apposizione della firma digitale sui documenti così elaborati da parte del medesimo operatore responsabile dell'inserimento dei dati di cui al precedente alinea. Tale operazione attesta la conformità della copia per immagine al documento cartaceo originale e consente la contestuale protocollazione e assegnazione dei documenti stessi.

  Ogni documento cartaceo potrà essere accompagnato da allegati informatici memorizzati su CD, DVD e supporti con connessione USB. Tali allegati devono rispondere alle medesime regole di comunicazione indicate al precedente capitolo.

  Quando possibili, anche gli allegati informatici saranno importati nel sistema e associati al documento primario di appartenenza, subito dopo il processo di scansione di quest'ultimo.

  I supporti fisici degli allegati informatici non saranno restituiti al mittente poiché parte integrante dei rispettivi documenti cartacei. Inoltre, non saranno accettate tipologie di supporto fisico diverse da quelle menzionate.

  Il documento analogico originale, dopo essere stato registrato, sarà consegnato al personale delle UO interessate, previo firma digitale effettuata con la funzione *Ritiro Originali Cartacei* e custodito nell'archivio istituito dalle stesse U.O. che ne saranno responsabili della corretta conservazione.

  Compatibilmente con il carico di lavoro, tutto il processo di protocollazione avviene di norma entro il giorno di ricezione del documento.

  Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.13. DOCUMENTO ANALOGICO IN USCITA

Come previsto dall'art. 40 del CAD, nell'ambito dell'AOO, vengono prodotti esclusivamente documenti originali informatici, quindi non avrebbe senso parlare di flusso in uscita di documenti analogici.

Tuttavia, nelle circostanze di seguito descritte, la formazione e la sottoscrizione del documento avviene secondo modalità idonee alla produzione di un originale informatico, mentre la trasmissione del documento, completo di allegati, viene effettuata in forma analogica:

- il destinatario è privo di una qualsiasi casella di posta elettronica;
- il documento primario è corredato di allegato analogico non digitalizzabile;
- il documento primario ha un allegato informatico di dimensione eccessiva o non gestibile dai servizi di posta elettronica.

Le procedure di preparazione dell'atto da parte dell'operatore incaricato sono state già descritte nel citato paragrafo inerente al flusso in uscita del documento informatico con la differenza che deve essere utilizzata la funzione che riporta al sistema la presenza di *Dati Analogici* .

Per consentirne la stampa e la spedizione con i servizi postali tradizionali, i documenti rientranti in tali eccezioni confluiscono in un elenco denominato *lista dei documenti da materializzare*, per tali documenti è necessario che sia abilitata dall'RDS la funzione di apposizione automatica del *glifo*.
Il documento, completo di allegati, sarà inviato in forma analogica ai destinatari esterni per competenza attraverso il servizio postale, regolamentato nel capitolo successivo.
La lista dei documenti da materializzare è accessibile solo agli utenti abilitati che provvedono alla stampa del documento primario e degli eventuali allegati (in caso di allegati digitali provvedono al download in locale e successivo riversamento su adeguato supporto informatico) e assemblano l'intero documento per la spedizione analogica.
Qualora non sia possibile stampare il documento con il *glifo*, occorre apporre sul retro l'attestazione di corrispondenza all'originale informatico. Tale dichiarazione deve essere redatta con la seguente dicitura:

Si attesta che il presente documento è copia del documento informatico originale firmato digitalmente, composto complessivamente da _____ fogli.

Bologna, GG-MM-AAAA

IL <carica rivestita dal funzionario>
(<grado/qualifica Nominativo>)

L'attestazione dovrà essere sottoscritta da uno dei seguenti funzionari, aventi causa nella formazione dell'atto:
- Dirigente titolare dell'UO;
- Capo del Nucleo che ha predisposto l'atto.

Dopo la firma di tale attestazione il documento primario e gli eventuali allegati vengono spediti all'indirizzo postale del corrispondente, secondo le usuali procedure analogiche.
Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.14. DOCUMENTO ANALOGICO INTERNO

Il sistema non prevede l'origine di documenti analogici, l'eventuale documentazione cartacea segue le regole già descritte nel sottopara inerente al documento analogico in uscita.

4.15. FAX

Il fax, come disposto dell'art. 47 comma 2 lettera C, è vietato tra le Pubbliche Amministrazioni e con le Aziende è obbligatoria la comunicazione via PEC. Pertanto il fax può essere utilizzato solo con i privati cittadini seguendo le indicazioni dell'art. 38 del DPR 445/2000 e dell'art. 45 del CAD.

4.16. DOCUMENTI DI AUTORI IGNOTI O NON FIRMATI (ANONIMI)

I documenti non firmati, o i cui autori non sono individuabili, saranno protocollati indicando nel campo mittente la seguente dicitura: autore ignoto.
Essi saranno assegnati al RDS il quale, dopo averne vagliato il contenuto, potrà inoltrarli a una specifica UO per la trattazione.

4.17. DOCUMENTI ESCLUSIVI PER IL TITOLARE O INDIRIZZATI ALLE PERSONE

La corrispondenza analogica indirizzata direttamente al personale del Reggimento Logistico "FOLGORE", non viene aperta dal personale del Nucleo Posta, ma viene consegnata direttamente all'interessato.
Per le raccomandate e assicurate, valgono le indicazioni riportate al punto 5.12.1.
A riguardo si evidenzia che la posta privata indirizzata al personale deve giungere presso l'AOO solo ed esclusivamente per motivi straordinari.
A discrezione delle autorità e/o del personale cui è diretta, la corrispondenza a carattere istituzionale, argomento del presente paragrafo, potrà essere consegnata per la protocollazione al NdP. In tal caso, essa dovrà riportare tale volontà con una dichiarazione sottoscritta e apposta in calce al documento (ad esempio "protocollare"), seguita dal timbro dell'UO e dalla data.

Inoltre, i plichi presentati all'ingresso del Reggimento Logistico "Folgore" (sede dell'AOO), indirizzati nominativamente al personale dell'ente, dovranno essere ritirati all'ingresso dai diretti interessati o da loro delegati che saranno contattati dal personale ivi in servizio.

4.18. APPUNTI E NOTE

Nelle more del rilascio dello specifico modulo del sistema "@D[h]OC", deputato alla gestione degli Appunti e/o Note (da questo momento chiameremo, per semplicità, con la parola Appunti), la documentazione può essere predisposta mediante l'utilizzo di una procedura che permette di gestire il carteggio loro associato (allegati, lettere alla firma, ecc.) limitando la produzione di documentazione cartacea.

Per poter utilizzare questa tipologia documentale è necessario che il RDS abbia attivato il relativo registro di protocollo (*Note /Appunti*) con la funzione del sistema *Impostazione Registri*.

Per produrre un Appunto nella funzione di predisposizione deve essere prioritariamente selezionato lo specifico registro della tipologia documentale che viene identificato con la voce Nota/Appunto (se la voce non è presente nell'elenco a discesa significa che tale registro non è stato attivato dall'RDS), a selezione avvenuta la videata della predisposizione sarà modificata per adeguarsi alla scelta effettuata.

Le varianti di maggior rilievo rispetto alla predisposizione di un documento nel Registro Generale sono:

- la possibilità di indicare se l'Appunto in predisposizione sia necessario il coordinamento;
- l'obbligatorietà dell'indicazione del Ruolo Firma per l'Appunto che si sta predisponendo;
- l'impossibilità di inserire destinatari esterni.

L'Appunto è tipicamente composto da quattro elementi:

- l'Appunto in quanto tale;
- gli allegati dell'Appunto;
- le eventuali lettere che saranno fatte partire qualora l'appunto venisse approvato, a firma uguale o diversa dal firmatario dell'Appunto;
- Le note di coordinamento.

Nell'ambito della gestione dell'Appunto nel sistema è possibile inserire *Note* e *File Accessori,* con le stesse modalità dei documenti del Registro Generale. Va tenuto presente che tali dati seguono le regole generali di funzionamento, pertanto, ad esempio, le *Note* inserite per un Appunto non saranno visibili a chi riceverà quell'Appunto per esprimere un parere di coordinamento e i *File Accessori* verranno cancellati quando l'Appunto verrà protocollato o eliminato.

La predisposizione dell'Appunto, degli eventuali allegati e delle lettere che saranno fatte partire nel caso in cui l'Appunto venga approvato, avviene al di fuori del sistema e prima di accedere alla funzione di predisposizione, in modo non diverso da quanto avviene per i documenti predisposti normalmente.

Per la predisposizione di un appunto è obbligatorio indicare:

- l'oggetto;
- gli allegati dell'Appunto;
- le eventuali lettere che saranno fatte partire qualora l'Appunto venisse approvato, a firma uguale o diversa rispetto al firmatario dell'Appunto;
- le note di coordinamento;
- l'eventuale flusso di vertice.

Per la predisposizione di un appunto sarà quindi necessario inserire le seguenti informazioni:

- *UO Mittente* (è l'Unità Organizzativa da cui scaturisce l'Appunto. Il dato viene già precompilato dal sistema che riconosce l'U.O. di appartenenza dell'utente che sta operando. Può essere utile modificare l'U.O. mittente solo quando si rende necessario modificare il cono di visibilità dell'Appunto nelle successive fasi di consultazione;
- *Oggetto,* costituito da un massimo di 250 caratteri;
- *Tipologia Documentale*, selezionando la voce *Nota/Appunto*;
- *Ruolo Firma*, il dirigente/funzionario delegato che dovrà firmare digitalmente l'Appunto;
- *Classificazione*;
- *Documenti* (l'Appunto e gli eventuali allegati).

Inoltre possono essere inserite le seguenti informazioni:

- *Dati sensibili*;
- *Priorità (normale, urgente e urgentissimo)*;

- *Nota/Appunto di Vertice;*
- *Note*;
- *File Accessori*;
- *Riferimenti/Seguiti.*

Nella fase di predisposizione essendo l'Appunto un atto che rimane all'interno dell'AOO non è possibile inserire i *Destinatari esterni*.
Una volta inseriti tutti i dati necessari (sia obbligatori che facoltativi), per completare la predisposizione dell'Appunto utilizzando la funzione del sistema *Salva Sulla Scrivania* si può scegliere se annullarlo con la funzione *Annulla,* inviarlo alla scrivania dell'utente superiore (che potrà avviare il processo di approvazione) con la funzione *Salva Doc. Predisposti* o utilizzare la funzione *Aggiungi Lettera* che consente di associare all'Appunto una o più lettere che saranno fatte partire quando l'Appunto sarà approvato le lettere associate all'Appunto possono essere predisposte con la stesso firmatario dell'Appunto o con firmatario diverso, in ogni caso l'indicazione del ruolo firma è obbligatoria.
Accedendo all'elenco dei documenti predisposti in partenza e selezionando l'appunto di interesse si può modificarlo ulteriormente con la funzione *Modifica,* in questo caso riapparirà la videata di predisposizione dedicata agli appunti. Nella scrivania predisposti in partenza selezionando una lettera associata all'appunto viene presentata la videata di modifica predisposizione di una classica lettera (l'unica differenza consiste nella tipologia documentale che per una lettera non associata ad un Appunto è "Generale", mentre per le lettere associate ad Appunti viene mostrata l'indicazione lettera).
Nel caso si dovesse gestire nella scrivania predisposti in partenza un numero elevato di appunti, le lettere associate possono essere nascoste.
Terminata la fase di predisposizione l'Appunto viene inoltrato agli utenti per la successiva fase di approvazione. L'utente che riceve l'Appunto, sulla scrivania predisposti in partenza, potrà apportare le modifiche ritenute opportune e aggiungere eventuali decretazioni prima di inoltrarlo a sua volta ad altri utenti, proseguendo il giro di approvazione, o all'Autorità preposta alla sua approvazione finale. L'Autorità che ricevere l'Appunto potrà fornire specifiche indicazioni mediante decretazioni, oppure modificare/cancellare direttamente le lettere associate o firmarlo digitalmente.
Particolare attenzione meritano le lettere associate all'Appunto, queste saranno fatte partire subito dopo la firma dell'Appunto (se la firma è la stessa dell'Appunto) oppure saranno inviate sulla scrivania di chi le dovrà firmare. Qual'ora l'opinione dell'Autorità preposta all'approvazione dell'appunto sia, in merito alle lettere associate, di evitarne la partenza, sarà necessario eliminarle, utilizzando l'apposita funzione del menù di contesto; se, invece il relativo contenuto delle lettere associate non è di gradimento, queste andranno modificate prima di firmare l'Appunto, o apportando in modo diretto le modifiche necessarie oppure inviando l'Appunto ad un utente che provvederà ad eseguire le disposizioni fornite in relazione alle lettere da modificare, ritrasmettendo poi il tutto all'Autorità preposta alla firma.
Le lettere discendenti da un Appunto sono protocollate nel Registro Generale.
La gestione della tipologia documentale "nota/appunto" comprende la versione denominata nota/appunto di vertice. Gli appunti di vertice sono caratterizzati dal fatto di poter prevedere un flusso di vertice predeterminato che automatizza l'iter procedurale. Ciascun utente presente nel flusso stabilito, potrà approvare l'Appunto (in tal caso l'appunto sarà smistato automaticamente al livello successivo), oppure non approvare l'Appunto (in tal caso l'Appunto tornerà automaticamente all'utente precedente). Quando l'Appunto giunge sulla scrivania del ruolo apicale del flusso di vertice, avviene la formale approvazione della nota/appunto e a questo punto il documento inizierà a ritroso il suo flusso in discesa per tutti gli utenti che lo hanno precedentemente approvato, al fine di avere contezza delle decisioni di vertice. Nel flusso in "discesa" non sono possibili ulteriori interazioni con l'Appunto (non è possibile apportare modifiche), gli utenti del flusso di vertice che ricevono l'Appunto non visualizzeranno i pulsanti "APPROVA/NON APPROVA" ma al loro posto vi sarà solo il pulsante VISTO. Quando l'appunto tornerà sulla scrivania dell'utente che aveva innescato il flusso di vertice, tale utente avrà l'onere di firmare digitalmente l'Appunto e contestuale protocollazione dello stesso nel registro particolare "Note Appunti" oltre alla protocollazione delle lettere allegate nel "Registro Generale" (nel caso il firmatario delle lettere sia diverso dal firmatario dell'appunto, saranno smistate sulla scrivania del ruolo a ciò preposto).
Il flusso di vertice deve essere utilizzato solo dagli utenti apicali della propria organizzazione.

Per poter utilizzare il flusso di vertice delle Note/Appunti, è preliminarmente necessario pianificare e creare i flussi di approvazione da parte del vertice, attività in capo al Responsabile del Servizio.
Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.19. COORDINAMENTO

Il coordinamento di un appunto è una tipologia documentale a sé stante, anche se è direttamente correlato agli appunti e può essere presente solo a fronte di un appunto.
Per poter utilizzare questa tipologia documentale è necessario che il RDS abbia attivato il relativo registro di protocollo (*Coordinamento*) con la funzione del sistema *Impostazione Registri*.
Sono possibili due tipi di coordinamento:

- coordinamento sequenziale, prevede che l'utente che sta predisponendo un appunto per il quale sono necessari uno o più pareri di coordinamento da fornire secondo un ordine definito, individui le Unità organizzative di cui è necessario acquisire il parere, accertandosi che l'ordine con cui vengono segnalate al sistema sia quello desiderato per l'emissione dei pareri. Quando l'Autorità preposta alla firma dell'appunto lo riterrà, potrà avviare l'iter della richiesta di parere di coordinamento e a questo punto il sistema invierà l'appunto, completo di allegati e lettere, sulla scrivania Predisposti Partenza del primo utente della lista di coloro che devono fornire il parere di coordinamento. Quando tale utente fornirà il proprio parere, il sistema smisterà l'appunto, comprensivo del parere di coordinamento, al secondo utente della lista a suo tempo preparata; e così via fino all'ultimo utente della lista. Quando emessi tutti i pareri di coordinamento, sarà opportunamente segnalato sulla scrivania dell'Autorità preposta alla firma dell'appunto, per le attività conseguenti. Durante l'iter di espressione dei pareri di coordinamento richiesti, l'Autorità che ha avviato la richiesta dei pareri di coordinamento può richiamare, se ritenuto, l'appunto sulla propria scrivania Predisposti Partenza, interrompendo così la catena di richiesta dei pareri di coordinamento;
- coordinamento di tipo parallelo, durante la fase di predisposizione vengono individuate tutte le U.O. dalle quali ci si attende un parere di coordinamento. L'ordine di inserimento non sarà rilevante. Quando l'Autorità preposta alla firma dell'appunto lo riterrà, potrà avviare l'iter della richiesta di parere di coordinamento quindi il sistema invierà l'appunto, completo di eventuali allegati e lettere, sulla scrivania Predisposti Partenza contemporaneamente a tutti gli utenti della lista di coloro che devono fornire il parere di coordinamento. A mano a mano che i pareri saranno emessi il sistema ne terrà traccia e quando tutti i pareri saranno forniti l'appunto sarà opportunamente segnalato nella scrivania Predisposti Partenza dell'Autorità per le attività conseguenti. Anche in questo caso l'Autorità che ha avviato la richiesta dei pareri di coordinamento può richiamare, quando ritenuto, l'appunto sulla propria scrivania Predisposti Partenza, interrompendo così la richiesta di parere di coordinamento

Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.20. VARIAZIONI MATRICOLARI

Nel presente paragrafo verrà trattata la gestione delle variazioni matricolari.
Per poter gestire le richieste di variazione matricolare è necessario che sia attivato dall'RDS il relativo registro di protocollo (*Variazioni Matricolari*) con la funzione del sistema *Impostazione Registri*.
Il flusso dell'informazione può essere distinto in tre fasi:

- <u>Preparazione della richiesta di variazione matricolare</u>
  In questa fase la funzione dell'applicativo Matricola è di competenza del Nucleo Matricola dell'AOO.
  L'interazione automatica con l'istanza @D[h]OC dell'AOO viene utilizzata per:
  - consultazione e recupero dei documenti a riferimento;
  - predisposizione del documento nativo;

- monitoraggio dello stato della predisposizione;
- firma da parte del Comandante dell'AOO;
- registrazione del documento in uscita;
- archiviazione del documento nel sottofascicolo Documenti e Riferimenti dell'amministrato.

L'interazione automatica con l'istanza @D[h]OC dell'AOO di scopo Matricola Esercito viene visualizzata per:

- registrazione del documento in ingresso;
- archiviazione del documento nel sottofascicolo Documenti e Riferimenti dell'amministrato.

- Registrazione della variazione matricolare
  In questa fase la funzione dell'applicativo Matricola è di competenza del CUSE.
- Controllo e verifica a cura della DGPM
  In questa fase la funzione dell'appellativo è di competenza del PERSOMIL.

Il fascicolo matricolare dei dipendenti di questa AOO, in caso di trasferimento ad altra AOO, verrà migrato a quest'ultima accedendo alla specifica funzione del sistema di protocollo @D[h]OC. L'AOO ricevente una volta accettato il trasferimento del fascicolo matricolare a lei inviato avrà accesso a tutto il contenuto dello stesso. Il fascicolo una volta trasferito non sarà più visibile e quindi accessibile, ma i documenti in esso contenuti saranno comunque consultabili con la funzione del sistema di protocollo @D[h]OC "Consultazione". Si precisa che i documenti contenuti nel fascicolo trasferito mantengono il numero di protocollo dell'AOO che li ha generati

Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.21. ORDINI DEL GIORNO

Questa tipologia documentale consente la gestione degli Ordini del Giorno che vengono emessi dall'Ente.

Le creazione degli Ordini del Giorno è similare a quella dei documenti informatici in uscita con le differenze che nella fase di predisposizione del sistema @D[h]OC, con la funzione *Tipologia Documentale*, va inserita la voce *Ordini del Giorno* e che non è possibile inserire destinatari esterni.

Per poter utilizzare questa tipologia documentale è necessario che il RDS abbia attivato il relativo registro di protocollo (*Ordini del Giorno*) con la funzione del sistema *Impostazione Registri*.

Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.22. ORDINI DI SERVIZIO

Questa tipologia documentale consente la gestione degli Ordini di Servizio.

Le modalità operative di utilizzo degli Ordini del Giorno sono le stesse già descritte per gli Ordini del Giorno, ovviamente per poter utilizzare questa tipologia documentale è necessario che il RDS abbia attivato il relativo registro di protocollo (*Ordini del Servizio*) con la funzione del sistema *Impostazione Registri*.

Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I. "@D[h]OC" presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.23. GESTIONE PERSONALE

Questa tipologia documentale consente la gestione dei documenti necessari per la gestione del personale (quali, ad esempio, richieste di permessi, straordinari, ferie, e più in generale, tutta la documentazione afferente la gestione della quotidianità di un dipendente).

Le modalità operative di utilizzo sono le stesse già descritte nei paragrafi precedenti con la differenza che l'UO destinataria può essere la stessa dell'UO mittente. Per poter utilizzare questa tipologia documentale è necessario che il RDS abbia attivato il relativo registro di protocollo (*Gestione Personale*) con la funzione del sistema *Impostazione Registri*.

Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

4.24. DEPOSITO TELEMATICO

Questa tipologia documentale consente la gestione del deposito telematico di atti del processo amministrativo telematico. Attraverso questa tipologia documentale è possibile soddisfare esigenze derivanti dalle regole di trasmissione dei moduli di deposito del processo amministrativo telematico (PAT). In analogia alle altre tipologie documentali, per questa specifica esigenza il destinatario del documento richiede forme e modi di trasmissione difformi da quanto prevede la normativa nazionale sulla corrispondenza tra Pubbliche Amministrazioni. La differenza di maggior rilievo rispetto alle modalità operative delle precedenti tipologie documentali consiste nell'impossibilità di indicare destinatari interni e alcune varianti relative alla gestione dei destinatari esterni e ai documenti.
Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

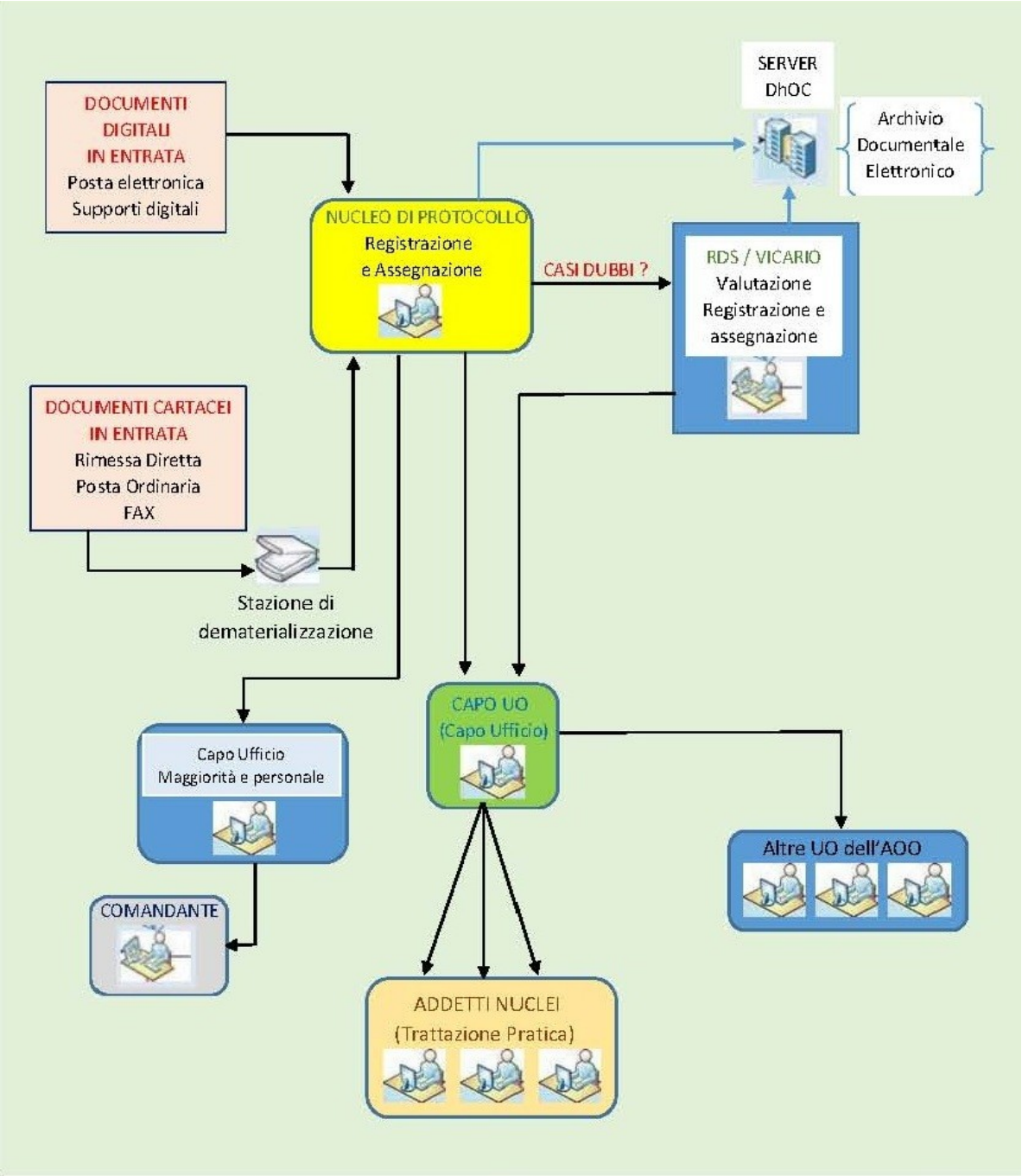
4.25. DECRETI

Questa tipologia documentale consente la gestione di decreti e, più in generale, atti dispositivi che, a vario titolo, devono essere prodotti dall'AOO (per esempio decreti di dipendenza da causa di servizio determinazioni a contrarre, ecc.). Possono essere identificate tre diverse tipologie la cui descrizione è personalizzabile a cura del RDS con la funzione del sistema @D[h]OC *Modifica* nel riquadro Descrizione di ciascuna di esse.
Le modalità operative di utilizzo sono le stesse già descritte nei paragrafi precedenti ed è necessario che il RDS abbia attivato i relativo registi di protocollo (siglati *DE1*,*DE2* e *DE3*) con la funzione del sistema *Impostazione Registri*
Per i dettagli tecnici ed operativi si rimanda alla lettura del "manuale protocollo" del sistema di gestione documentale del P.I., denominato @D[h]OC, presente alla voce "Guida"e alla consultazione dei bollettini periodici con cui vengono descritte nuove funzionalità.

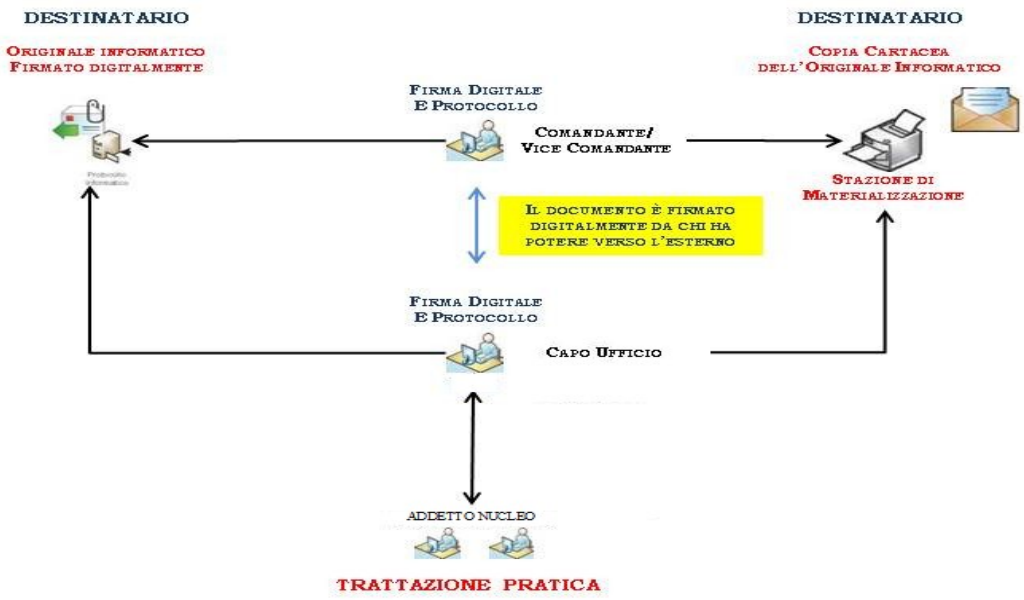
4.26. FATTURE E RIFIUTO FATTURE

Non ci soffermiamo sulla descrizione di queste tipologie documentali in quanto non di competenza amministrativa di questa AOO.

4.27. SCHEMA FLUSSO IN INGRESSO



4.28. SCHEMA FLUSSO IN USCITA



5. MODALITÀ DI PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

5.1. PREMESSA

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

5.2. UNICITÀ DELLA REGISTRAZIONE DEL PROTOCOLLO INFORMATICO

Nell'ambito della AOO, i registri di protocollo, menzionati al paragrafo successivo, hanno una numerazione delle registrazioni di protocollo progressiva. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo. La segnatura di protocollo individua un unico documento e, di conseguenza, ognuno di essi reca un solo numero di protocollo, costituito da 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 l'AOO è considerata giuridicamente inesistente presso l'Amministrazione e non può essere archiviato. Non è consentita la protocollazione di un documento già protocollato.

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

5.3. REGISTRI GIORNALIERI DI PROTOCOLLO

I registri giornalieri di protocollo disponibili nel sistema @D[h]OC sono i seguenti:

- Registro Generale (identificato con la sigla REG);
- Nota /Appunto (identificato con la sigla APT);
- Coordinamento (identificato con la sigla COO);
- Ordini del Giorno (identificato con la sigla ODG);
- Ordini di Servizio (identificato con la sigla ODS);
- Richiesta Variazioni Matricolari (identificato con la sigla RVA);
- Fatture (identificato con la sigla FAT);
- Rifiuto Fatture (identificato con la sigla RFT);
- Gestione Personale (identificato con la sigla GEP);
- Deposito Telematico (identificato con la sigla DTE);
- Decreti disponibili in tre tipologie (identificati con le sigle DE1, DE2, e DE3).

I registri attualmente utilizzati presso l'AOO- M_D E25800 sono i seguenti:

- Registro Generale (REG);
- Richiesta Variazioni (RVA);
- Ordini del Giorno (ODG).

Ogni giorno, entro le ore 08:00, il RDS provvede alla generazione, ed alla firma digitale, della stampa delle registrazioni di protocollo relative al giorno precedente.

5.4. 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:

- numero di protocollo del documento, generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile e reperiti nella tabella dei corrispondenti del sistema informatico;

- oggetto del documento registrato in forma non modificabile; gli addetti devono seguire le regole generali di codifica delle informazioni contenute nell'apposito paragrafo;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico calcolata con l'algoritmo SHA-256.

Va tenuto presente che, in caso si tratti di 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. Tali dati non saranno, per altro, modificabili dall'operatore.

Anche il campo oggetto per i messaggi provenienti per posta elettronica non sarà modificabile, poiché estratto direttamente dall'oggetto della mail pervenuta all'AOO.

5.5. SEGNATURA DI PROTOCOLLO DEI DOCUMENTI

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo mediante 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 vengono utilizzati dati contenuti nel file segnatura xml, purché conforme alle indicazioni delle LLGG.

Sui documenti in uscita la segnatura di protocollo viene indicata .

Al fine di garantire la validità del documento informatico così prodotto, la segnatura apposta sul documento viene firmata, in modalità automatica. Il file segnatura.xml viene allegato a tutti i documenti in uscita per posta elettronica e può essere utilizzato dalle Amministrazioni cui è stato inviato il documento per automatizzarne la registrazione di protocollo.

Il formato della segnatura di protocollo dell'AOO, conformemente alla normativa, prevede i seguenti dati:

- Codice dell'Amministrazione: M_D;
- Codice dell'AOO: E25800;
- Codice del Registro: REG oppure RVA oppure ODG;
- Anno di riferimento del Registro: 2020;
- Numero di protocollo: <progressivo di 7 cifre>;
- Data di registrazione: gg-mm-aaaa;

Esempi di segnatura di protocollo:

M_ D E25800 REG2020 0000001 01-01-2020;
M_ D E25800 RVA2020 0000001 01-01-2020;
M_ D E25800 ODG2020 0000001 01-01-2020

5.6. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

La necessità di modificare - anche un solo campo *tra quelli obbligatori della registrazione di protocollo, registrati in forma non modificabile* - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo. È altresì possibile annullare una registrazione di protocollo per un documento erroneamente fatto entrare nel patrimonio documentale dell'AOO. Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora dell'annullamento e rilasciata dall' RDS. Solo l'RDS è autorizzato ad annullare, ovvero a dare disposizioni di annullamento, le 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, specificando la nota ed il nominativo dell'interessato che ha indicato l'operazione, adeguatamente motivata, indirizzata al RDS. Si tenga presente che l'annullamento di un documento già trasmesso potrà essere effettuato solo a seguito di formale comunicazione al destinatario. Tale comunicazione sarà, dunque, citata nella nota di annullamento diretta al RDS.

5.7. DESCRIZIONE FUNZIONALE E OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO

Tutte le informazioni di dettaglio inerenti alle funzionalità presenti nel sistema informatico di PI e gestione documentale sono reperibili nel manuale utente del sistema stesso.

5.8. TITOLARIO

Sulla base dei riferimenti normativi e metodologici sopra esposti, è in uso il piano di classificazione dei documenti denominato "Titolario d'archivio".

Il Titolario adottato nell'ambito dell'AOO-M_D E25800 ricalca il "Titolario di archivio dell'Esercito Italiano"[1], che ha avuto il pregio di uniformare la classificazione delle AOO costituite in seno all'Amministrazione dell'Esercito Italiano. Esso si suddivide in tre livelli funzionali, in particolare:

- il 1° livello del Titolario **(titolo)** individua 12 voci funzionali, corrisponde ad aggregazioni di funzioni e si indica con il numero arabo;
- il 2° **(classe),** 3° **(sottoclasse)** livello del Titolario corrispondono alle successive articolazioni, mediante l'associazione alle suddette funzioni di 1° livello, delle rispettive sotto-funzioni e/o attività e/o materie di pertinenza, individuate mediante una preventiva analisi di studio del modello di Ente militare di riferimento. Si individuano anch'essi con il numero arabo.

Tutti i documenti ricevuti e prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al Titolario d'archivio. A titolo di esempio vengono riportate in tabella due voci di classificazione:

- 3.5.0 (Programmazione - Gestione del parco quadrupedi - Gestione del parco quadrupedi);
- 7.5.5.3 (Gestione risorse logistiche - Mantenimento mezzi e materiali - Lavorazioni esterne Preventivi).

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

---

[1]Approvato in 1[A] Edizione dal Sottocapo di SM dell'Esercito nel mese di giugno 2004, e in 2[A] Edizione il 13 gen. 2006 dal Capo Reparto Affari Generali dello Stato Maggiore dell'Esercito.

5.9. CLASSIFICAZIONE DEI DOCUMENTI

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.

Essa è eseguita 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 al sopra citato Titolario.

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

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

5.10. FASCICOLAZIONE DEI DOCUMENTI

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

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

I fascicoli e i sottofascicoli sono invece gestiti direttamente dagli interessati ai relativi provvedimenti. In particolare, per poter classificare un documento è necessario inserirlo in uno o più fascicoli oppure in sottofascicolo.

Il sistema consente la creazione di fascicoli e sottofascicoli.

Per tale attività gli addetti dovranno attenersi alle seguenti regole:

- il codice del fascicolo o del sottofascicolo deve essere numerico;
- la numerazione deve essere distanziata di 100 numeri, per consentire di poter intervenire in un tempo successivo senza sconvolgere l'impianto della fascicolazione. Avremo quindi il codice fascicolo 100, 200, 300 e così via; qualora la numerazione dei fascicoli renda più opportuno l'inserimento di un codice tra altri due fascicoli si procederà di 10 unità (esempio, tra il codice 100 e 200 si inserirà prima il codice 110, poi il 120 e così via).

Per quanto attiene alla descrizione occorre attenersi alle regole generali di scrittura dei dati, indicate nell'apposito paragrafo, inoltre appare opportuno evidenziare che non possono essere creati fascicoli con denominazione generica come ad es. "Varie".
Il sistema mantiene traccia della data di creazione del fascicolo.
E' possibile registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.
I fascicoli relativi a documentazione del personale in forza all'AOO, con apposita funzione del sistema di protocollo informatico @DhOC, possono essere trasferiti ad altra AOO (funzione utilizzabile in caso di trasferimento del personale).

6. ARCHIVIAZIONE DEI DOCUMENTI

6.1. DEPOSITO/ARCHIVIO DELL'AOO-M_D E25800

Sulla base della normativa vigente, per la custodia della documentazione registrata a protocollo, l'AOO-M_D E25800 prevede una organizzazione archivistica così articolata:

- archivio/custodia corrente - documenti archiviati nel corrente anno fino al precedente 2° anno;
- archivio di deposito - documenti archiviati oltre i 2 anni precedenti;
- archivio storico - documenti ritenuti di valenza storica, relativi ad atti esauriti da oltre 40 anni, quindi in considerazione che gli stessi potranno ritenersi esauriti al compimento del 10° anno (in base all'art. 2946 del codice civile), i documenti che andranno versati all'Ufficio Storico avranno di conseguenza un'esistenza di 50 anni.

L'AOO-M_D E25800 produce esclusivamente originali informatici e, inoltre, tutti gli atti cartacei pervenuti vengono dematerializzati e convalidati.
Pertanto, l'universalità dei documenti originali afferenti all'AOO-M_D E25800, a partire dalla data di avvio del servizio, sono archiviati all'interno del sistema informatico, che ne consente la gestione, ne garantisce l'accesso e provvede ad ottemperare alle norme di legge previste.
Tuttavia, esiste un consistente numero di atti cartacei prodotti precedentemente all'avvio del sistema @D[h]OC che continueranno ad essere gestiti da parte delle U.O.

6.2. 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 della struttura informatica del CSIE, che gestisce anche l'applicativo di protocollazione all'AOO-M_D E25800.
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 vengono anche, prodotti, i registri giornalieri delle registrazioni di protocollo, firmati digitalmente dal RDS.
Tutti i documenti sono inoltre fascicolati.
Le regole generali di archiviazioni sono disponibili nel paragrafo inerente alla classificazione.

6.3. ARCHIVIAZIONE/CUSTODIA DEI DOCUMENTI ANALOGICI

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

- archivio corrente:
  - saranno custoditi tutte le cartelle dell'anno corrente fino al precedente 2° anno, già suddivisi in ordine cronologico fino ad arrivare al 2° anno;
  - allo scadere del 2° anno verrà fatta un a valutazione dei documenti da scartare secondo modalità stabilite da ciascuna UO interessata. I documenti non scartati saranno conservati nell'archivio di deposito.
- archivio di deposito: verranno custoditi tutti i documenti fino al 50° anno. Alla scadenza un'apposita commissione stabilirà quali documenti siano testimonianza di valore di civiltà e quindi da inviare all'archivio storico.

Infine si evidenzia che nell'ambito delle UO dovranno essere stabiliti i responsabili all'archiviazione documentale attiva e segnalati all'RDS dal quale dipenderanno funzionalmente.

6.4. RITIRO E CONSULTAZIONE DEI DOCUMENTI ANALOGICI

I documenti analogici sono custoditi in relazione alla loro assegnazione presso gli archivi istituiti da ciascuna UO dell'AOO-M_D E25800. Qualora si presentasse l'esigenza di consultare tali documenti, il personale esterno alla UO di competenza dovrà compilare apposita richiesta.
Al termine della consultazione, i documenti dovranno essere riconsegnati al citato archivio.

7. ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

7.1. GENERALITÀ

Il controllo degli accessi è il processo volto a garantire che l'impiego dei servizi del sistema informatico di protocollo avvenga esclusivamente secondo modalità prestabilite.
Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).
Gli utenti del servizio di protocollo, in base alle rispettive competenze, hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza.
Le credenziali di accesso al sistema (user e password) sono del tutto personali e il loro uso ricade sotto la responsabilità di ciascun utente cui sono assegnate.

7.2. ACCESSO AL SISTEMA

L'accesso al sistema deve avvenire prioritariamente con l'utilizzo della tessera magnetica personale (CMD). L'RDS su richiesta motivata dell'utente abiliterà lo stesso all'accesso al sistema con una credenziale a lui assegnata composta da:

- RUOLO: stringa pubblica che l'utente usa per connettersi al sistema informatico;
- PROFILO: autorizzazioni concesse al ruolo per svolgere specifiche operazioni;
- USERID: identifica l'utente mediante i dati personale (nominativo, luogo di nascita, etc.);
- PASSWORD: stringa segreta e riservata all'utente che, in combinazione con il ruolo, consente di accedere al sistema. Essa è associata allo USERID.

L'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, secondo le esigenze prospettate formalmente dal titolare di ciascuna UO.
Ogni persona fisica può ricoprire più ruoli mantenendo, comunque, la stessa password di accesso legata, quest'ultima, al proprio USERID.

7.3. UTENTI ASSENTI, TRASFERITI O NEO ASSEGNATI

Se non diversamente pianificato, la scrivania degli utenti che per qualsiasi motivo sono assenti continuerà a ricevere corrispondenza che potrà giacere anche per lungo tempo.
Per questo, è necessario ricorrere allo strumento delle deleghe, ogni volta che il titolare di un ruolo si assenti e debba essere sostituito, in quel ruolo, da personale appositamente designato (ad esempio, il Capo Ufficio da uno dei Capi Nucleo, ecc.). La gestione delle deleghe risulta di primaria importanza per assicurare la continuità e correttezza dei flussi documentali e, in particolare, per l'apposizione della firma digitale.
Nei periodi di assenza, tali ruoli potranno essere assunti, con le relative funzioni, da altri utenti, se preventivamente autorizzati dal RDS. Così facendo, il personale facente funzione potrà controllare indipendentemente tra loro sia la propria scrivania, sia quella del ruolo sostituito.
I documenti così originati avranno il gruppo firma dei titolari degli anzidetti ruoli e quello dei loro facenti funzione che, con le prescritte diciture, firmeranno i documenti in parola.
Inoltre, il personale neo assegnato all'AOO-M_D E25800, che ha bisogno di impiegare il sistema di protocollazione, dovrà essere tempestivamente e formalmente segnalato al RDS indicando le sue generalità e il profilo utente da assegnargli.
Parimenti, dovrà essere comunicato il personale in via di trasferimento, o di cui si preveda una lunga assenza, per sostituirne o disattivarne l'utenza e impedire l'accumulo di pratiche inevase.
In tale situazione, eventuali giacenze dovranno essere verificate a cura dell'UO e riassegnate dai diretti interessati, quando possibile, o da altri utenti temporaneamente autorizzati dal RDS.

7.4. PROFILI D'ACCESSO

Nell'ambito dell'AOO-M_D E25800 la strutturazione degli accessi prevede la realizzazione di una serie di profili sulla base della struttura ordinativa e delle rispettive competenze.
Le principali profilazioni riguardano le funzioni di:

- *amministrazione del sistema,* è assegnata dal RDS ad alcuni collaboratori ed a pochi altri utenti delle UO per la sola gestione della tabella dei corrispondenti;
- *lista dei documenti da materializzare*, consente la stampa dei documenti che per le loro caratteristiche non possono essere inviati per posta elettronica. E' consigliabile abilitare questa funzione a pochi utenti di ciascuna UO, in genere, al personale della segreteria;

- *trasmissione dei documenti*, è assegnata ai titolari di ciascuna UO e ai loro delegati per firmare digitalmente i documenti;
- *predisposizione dei documenti*, consente di preparare gli atti che potranno essere in seguito firmati e trasmessi;
- *consultazione*, consente di cercare documenti memorizzati nell'archivio, di visualizzarne i dati di protocollazione e, se di pertinenza della propria UO, il documento medesimo.
- *accesso alla scrivania*, consente la trattazione dei documenti assegnati in arrivo e quelli predisposti in partenza, per l'eventuale successiva trasmissione;
- *dati sensibili*, da abilitare solo agli utenti che gestiscono atti soggetti al [CODPRI];
- *Capo UO*, è una funzione legata al titolare di ciascuna UO al fine di ricevere la posta di propria pertinenza protocollata in ingresso dal NDP e assegnarla ai propri dipendenti.

I profili ora delineati non vanno considerati esaustivi delle molteplici possibilità fornite dal sistema informatico e, inoltre, è possibile anche creare profili ex-novo che contengano un mix di quelli ora elencati.

L'assegnazione dei profili ed il loro aggiornamento sono stabiliti dal RDS, tale operazione per la sua importanza andando a modificare l'ordinamento delle UO, viene determinata solo ed esclusivamente previo formali richieste dei responsabili delle diverse UO.

8. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

8.1. PREMESSA

La normativa (art 63 [DPR]) disciplina in modo piuttosto puntuale la materia del registro di emergenza, che è stato pensato per sopperire ad eventuali malfunzionamenti del sistema informatico.
Tuttavia è necessario sottolineare come le norme risalgano al 2000, prima comunque dell'entrata in vigore del [CAD], che impone la redazione di originali informatici.
Tale regola, infatti, muta radicalmente lo scenario in cui il registro di emergenza deve agire, rendendo, inoltre, di fatto, le funzioni di protocollazione molto meno rilevanti di quanto non lo erano nell'impianto normativo previsto dal [DPR].
Di seguito, quindi, verranno descritte le procedure previste nei casi di non funzionamento del sistema informatico, predisposte tenendo in considerazione quanto detto in precedenza.

8.2. ATTIVAZIONE DEL REGISTRO DI EMERGENZA

Ogni qualvolta, per motivi accidentali o programmati, non fosse possibile utilizzare il sistema informatico per le attività di protocollazione per un periodo di tempo significativo, il RDS adotterà il registro di emergenza emettendo la seguente dichiarazione:

APERTURA DEL REGISTRO DI EMERGENZA

Causa dell'interruzione: _____

Data d'inizio interruzione: GG-MM-AAAA ora dell'evento: HH:MM

Numero di protocollo iniziale: _____ Pagina finale n.: _____

Timbro e firma del Responsabile del Servizio di Protocollo (RDS)

La dichiarazione sarà mantenuta agli atti, nella quale indica, con esattezza, la data e l'ora di inizio del non funzionamento e il relativo motivo.

8.3. ATTIVITÀ POSSIBILI DURANTE L'ATTIVAZIONE DEL REGISTRO DI EMERGENZA

Durante il periodo di non funzionamento del sistema informatico non sarà comunque possibile protocollare documenti informatici in ingresso, poiché tale attività è strettamente correlata alle funzionalità del sistema stesso.
Se, invece, tra i documenti analogici pervenuti, venisse riscontrato un atto che per la sua rilevanza fosse necessario protocollare immediatamente, si procederà al suo inserimento nel registro di emergenza, provvedendo alla trasmissione del medesimo all'UO di competenza.
Per quanto riguarda la documentazione in uscita, essendo possibile solo attraverso l'apposizione della firma digitale e tramite la posta elettronica, la funzione di registrazione a protocollo non sarà disponibile.
Se vi fosse un atto che per la sua rilevanza dovesse comunque essere trasmesso, verrà prodotto con metodologie alternative dall'UO di competenza e portato all'attenzione del RDS per la relativa protocollazione di emergenza e successiva trasmissione per canali analogici.
Appare evidente che non è conveniente procedere con tali modalità ed è buona norma ridurre al minimo indispensabile l'accesso a tali funzioni.
Vale anche la pena sottolineare che l'eventuale mancato funzionamento del sistema inibisce anche l'accesso all'archivio informatico e alle funzioni di ricerca in generale, determinando il sostanziale blocco operativo dell'AOO.

8.4. RIATTIVAZIONE DEL SISTEMA INFORMATICO

Quando il sistema informatico riprende il suo normale funzionamento, il RDS produce una ulteriore dichiarazione, con l'esatta indicazione della data e dell'ora della ripresa del servizio, come di seguito indicato:

CHIUSURA DEL REGISTRO DI EMERGENZA

Data d'inizio interruzione: GG-MM-AAAA ora dell'evento: HH:MM

Numero di protocollo iniziale: _____ Pagina finale n.: _____

Timbro e firma del Responsabile del Servizio di Protocollo (RDS)

Tutte le dichiarazioni del RDS di attivazione e chiusura del registro di emergenza sono conservate a cura del RDS.
Dopo la riattivazione sia i documenti in ingresso sia i documenti in uscita protocollati in emergenza, verranno immessi all'interno del sistema con le usuali metodologie.
In particolare per i documenti in ingresso nell'oggetto dovrà essere riportato il numero del registro di emergenza in maniera che in caso di ricerca il numero di registrazione del documento informatico sia associato a quello di emergenza, es.: [RE xxxxxx gg-mm-aaaa].
Parimenti, si riprodurranno, a cura delle UO di competenza, i documenti protocollati in uscita durante l'emergenza, con l'accortezza di farli confluire all'interno della lista dei documenti da materializzare: tale azione consentirà di avere il nuovo numero di protocollo senza la necessità di ritrasmettere il documento stesso.
In entrambi i casi, gli operatori che hanno registrato nuovamente i documenti nel sistema informatico dovranno riportare il numero di protocollo d'emergenza nei previsti campi dell'applicativo: descrizione o note.

9. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

9.1. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE DI GESTIONE

Il presente manuale di gestione è adottato su proposta del Responsabile del Servizio di protocollo informatico e gestione documentale (RDS).
Esso potrà essere aggiornato a seguito di:

- sopravvenute normative;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- modifiche apportate dal RDS agli allegati del presente manuale.

9.2. ABROGAZIONE E SOSTITUZIONE DELLE PRECEDENTI NORME INTERNE

Il presente Manuale abroga e sostituisce ogni norma interna all'AOO-M_D E25800 che dovesse contrastare con il suo contenuto.

10. REGOLE GENERALI DI SCRITTURA DEI DATI ALL'INTERNO DEL SISTEMA INFORMATICO

In tutti i sistemi informatici è di particolare importanza la qualità delle informazioni che vengono inserite al suo interno. Ancora più rilevante è tale importanza in un sistema diffuso e capillare come quello di PI e gestione documentale.
È facilmente intuibile, infatti, come, in assenza di regole comuni e coerenti, non sia possibile ottenere tutti i benefici attesi dal sistema, in quanto, semplicemente, i documenti potrebbero essere difficilmente rintracciabili o, nei casi peggiori, non reperibili.
Vengono di seguito riportate alcune 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.

TIPO DI DATI	REGOLE
Nomi di persona	• prima il cognome e poi il nome; • in maiuscolo il cognome e il primo carattere del nome; • esempio: ROSSI Mario
Titoli di cortesia, nobiliari, ecc.	• sempre omessi.
Nomi di città e di stati	• in lingua italiana, se disponibile.
Nomi di ditte e società	• se riportano nomi di persona valgono le precedenti regole; • usare sigle, in maiuscolo o senza punti o, in alternativa, denominazioni ridotte; • la forma societaria va in minuscolo senza punti; • esempi: BIANCO Giuseppe srl, ACME spa.
Enti della Difesa	• denominazione telegrafica in maiuscolo se disponibile.
Enti e associazioni in genere	• usare sigle, in maiuscolo e senza punti o, in alternativa, denominazioni ridotte; • esempio: ASS. NAZ. PARACADUTISTI D'ITALIA.
Ministeri	• usare la forma ridotta; • esempi: MIN. DIFESA, MIN. INTERNO.
Enti di secondo livello	• esempio: utilizzare MIN. DIFESA Uff. Legislativo e non Ufficio Legislativo del Ministero della DIFESA
Sigle in genere	• in maiuscolo e senza punti; • esempio: ISTAT.
Virgolette e apici	• digitare il carattere direttamente dalla tastiera; • non eseguire la funzione copia e incolla di Windows.
Date	• usare il seguente formato numerico: GG-MM-AAAA; • esempio: 01-01-2020

Allegato “A”

Elenco delle U.O. (Unità Organizzative) per la gestione dei flussi documentali nell’ambito dell’Area Organizzativa Omogenea (AOO) Reggimento Logistico “Folgore”:

BATTAGLIONE LOGISTICO
COBAR
COMANDO ALLA SEDE
COMPAGNIA COMANDO E SUPPORTO LOGISTICO
DIRIGENTE SERVIZIO SANITARIO
MATRICOLA CISAM_CEVA
SERVIZIO PREVENZIONE E PROTEZIONE
SEZIONE COORDINAMENTO AMMINISTRATIVO
SOTTUFFICIALE DI CORPO
UFFICIO LOGISTICO
UFFICIO MAGGIORITÀ E PERSONALE
UFFICIO OPERAZIONI ADDESTRAMENTO E INFORMAZIONI

Allegato “B”

Personale incaricato dell’erogazione e gestione del servizio

Responsabile del Servizio: Magg. Alessandro COLACCHIO

Vicario del RDS: 1°Lgt. Dimitri DARIO

Amministratore di Sistema: C.le Magg. Ca. Sc. “QS” Antonio DE TINTIS

In caso di contemporanea assenza del RDS e del suo Vicario, anche per un solo giorno, deve comunque, con atto formale, essere nominato un dipendente della AOO che svolga il ruolo di RDS.