Edizione. (2023)

Comando Militare Esercito “Basilicata”
Via Ciccotti 32, 85100 Potenza (PZ)
PEC: cme_basilicata@postacert.difesa.it – PEI: cme_basilicata@esercito.difesa.it

MANUALE DI GESTIONE

per la tenuta del Protocollo Informatico, della gestione dei flussi documentali e degli archivi

Area **O**rganizzativa **O**mogenea

Comando **M**ilitare **E**sercito “Basilicata”
(identificativo:A7D11B4)

ESERCITO

Firmato Digitalmente da/Signed by:
BIAGIO ANTONIO FERRARO

In Data/On Date:
giovedì 5 gennaio 2023 09:51:24

Comando Militare Esercito "Basilicata"

Approvo il presente "Manuale di Gestione per la tenuta del Protocollo Informatico,
della gestione dei flussi documentali e degli archivi".

Esso è stato redatto in conformità al Decreto del Presidente del Consiglio dei Ministri
del 3 dicembre 2013 recante: 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.

Potenza, lì 05.01.2023

La presente pubblicazione abroga e sostituisce l'edizione 2020 dell'analogo documento.

IL COMANDANTE

Col. g. (p.) Biagio A. FERRARO

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

NR.	DATA	DESCRIZIONE

Sommari

Elenco degli allegati

Allegato "A"	Elenco delle U.O. (Unità Organizzative) per la gestione dei flussi documentali nell'ambito dell'Area Organizzativa Omogenea (AOO)
Allegato "B"	Personale incaricato dell'erogazione e gestione del servizio
Allegato "C"	Atto di Nomina del Responsabile e del Vicario del servizio per la tenuta del protocollo e la gestione dei flussi documentali
Allegato "D"	Atto di nomina dei funzionari delegati alla convalida di conformità delle copie informatiche dei documenti originali cartacei da assumere a protocollo in ingresso dell'AOO, mediante l'utilizzo della firma digitale.
Allegato "E"	Richiesta di annullamento di un protocollo
Allegato "F"	Richiesta telefonica per delega o eliminazione delega
Allegato "G"	Richiesta di Variazione/Profilo Utenti

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:

AOO	Area Organizzativa Omogenea
AOO- M_DE 24463	AOO del Comando Militare Esercito "Basilicata"
AGID	Agenzia per l'Italia Digitale
CAD	Codice Amministrazione Digitale D.lgs. 7 marzo 2005 n. 82
CODBCP	Codice dei Beni Culturali e del Paesaggio D.lgs. 22.01.04 n. 41 CODPRI Codice di Protezione dei dati personali D.lgs. 30.06.03 n. 196
DIR	Direttiva SMD-I-004
DPCM	Decreto della Presidenza del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica 30 dicembre 2010 n.445
AIPA	Indice delle Pubbliche Amministrazioni
PA	Pubblica Amministrazione
PEC	Posta Elettronica Certificata
PEI	Posta Elettronica Istituzionale
PI	Protocollo Informatico
RDS	Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
RPA	Responsabile del Procedimento Amministrativo
NdP	Nucleo per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi
UO	Unità Organizzativa
LLGG	Linea Guida Sulla Formazione , Gestione e Conservazione dei Documenti Informatici Riferimenti Normativi

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 PI è piuttosto vasta, per cui 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 Disposizioni legislative 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.

C**ircolare AGIP 23 Gennaio 2013 n. 60 CIRC.**
Regole tecniche per l'interoperabilità dei sistemi di protocollo informatico.

Decreto Legislativo 30 giugno 2003, n. 196. CODPRI
"Codice di protezione dei dati personali", per l'attuazione nelle Pubbliche Amministrazioni delle disposizioni relative, alla gestione delle risorse umane, con particolare riguardo ai soggetti che effettuano il trattamento.

Decreto Legislativo 22 gennaio 2004 n. 41. CODBCP
Codice dei beni culturali e del paesaggio, ai sensi dell'art.10 della legge 6 luglio 2002, n. 137.

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 e successive modifiche ed integrazione.
Codice dell'Amministrazione digitale.
Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n.82 recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n.69.
e stato redatto in conformità alle Linee Guida sulla formazione , gestione e conservazione dei documenti informatici.

LLGG Linea Guida sulla Formazione, Gestione e conservazione dei documenti informatici.
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;

1 PRINCIPI GENERALI

1.1 PREMESSA

Il presente Manuale di Gestione è stato redatto in conformità a quanto previsto dalle Linee Guida sulla formazione , gestionale e conservazione dei documenti informatici.

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

1.2 AMBITO DI APPLICAZIONE DEL MANUALE DI GESTIONE

Il presente manuale di gestione del protocollo, è rivolto al personale interno al' AOO-M_D 24463 e ai soggetti esterni che hanno la necessità di interagire con essa. Esso 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 Comando Militare Esercito "Basilicata" a partire dal 01 gennaio 2017. 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 di tre principi archivistici:

la registrazione di protocollo del documento fa fede, ad ogni effetto, del ricevimento e della spedizione di un documento;

la classificazione del documento, anche non protocollato, lo dota della collocazione logico-funzionale nell'Archivio;

la fascicolazione del documento, protocollato o non protocollato, attesta la sua effettiva gestione nell'ambito di un procedimento amministrativo o di un'attività.

Si ritiene utile ricordare come il registro di protocollo faccia 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 Comando Militare Esercito "Basilicata";
- **Testo Unico**: il Decreto del Presidente della Repubblica 20 dicembre 2000 n.445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **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;
- **Codice**: il decreto legislativo 7 marzo 2005 n.82 – Codice dell'A.D.;Si riportano, di seguito, gli acronimi utilizzati più di frequente:

Area Organizzativa Omogenea (AOO): 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 (DPR art. 50 comma 4). Per ciascun tipo di provvedimento relativo ad atti di propria competenza, è individuata l'UO responsabile dell'istruttoria e di ogni altro adempimento procedimento per l'adozione del provvedimento finale. A tal fine deve essere utilizzato solo ed esclusivamente un unico registro di protocollazione degli atti;

a) **Unità organizzativa (UO)**: è 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;

b) **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;

c) **Responsabile del Nucleo per la tenuta del protocollo informatico, dei flussi documentali e degli archivi (RDS)**: figura prevista dall'art.61 del DPR, i cui compiti, elencati nel citato DPR art.61 e nelle Linee Guide sulla formazione , gestione e conservazione dei documenti informatici.[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;

d) **Manuale di Gestione del protocollo informatico**: documento, previsto dalla Linea Guida sulla formazione , gestione e conservazione dei documeti informatici, descrivere il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del Protocollo Informatico, della gestione dei flussi e degli archivi.

e) **Titolario d'archivio**: 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;

f) **Classificazione**: 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;

g) **Fascicolo**: insieme minimo di documenti, composto dall'ordinata riunione di carte relativa ad uno stesso affare o procedimento amministrativo;

h) **Fascicolazione**: operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi.

i) **Fascicolo/pratica chiuso**: fascicolo che ha completato il suo ciclo all'interno della trattazione dell'affare, ma è conservato all'interno dell'ufficio utente di competenza;

j) **Fascicolo/pratica archiviato**: fascicolo che ha completato il suo ciclo all'interno della trattazione dell'affare e viene trasferito dall'ufficio utente all'Archivio Deposito;

k) **Assegnazione**: operazione di individuazione dell'ufficio utente competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;

l) **Archivio**: 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, per motivi tecnico-organizzativi e di responsabilità, viene suddiviso in tre sezioni: corrente, di deposito e storica;

m) **Archivio corrente**: 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;

n) **Archivio di deposito**: 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;

o) **Archivio storico**: 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;

p) **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 alle AOO e alle funzioni organizzative previste dalle Pubbliche Amministrazioni. Il dominio di PEC per la Difesa è **@postacert.difesa.it.**

q) **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, let. b) del CODPRI;

r) **Dati sensibili**: 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, let. d) del CODPRI;

s) **Dati giudiziari**: 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, let. e) del CODPRI.

t) **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;

u) **Documento informatico**: rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti art.1 lettera p.CAD),

v) **Documento analogico**: rappresentazione non informatica di atti, che contiene la rappresentazione informatica di atti,fatti o dati giuridicamente rivelanti (art 1 lettera Pp – bis -CAD.);

w) **Firma digitale**:Documento Informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art 1 lettera p CAD);

x) **Firma elettronica**: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;

y) **Firma elettronica qualificata**: 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;

z) **Fruibilità di un dato**: possibilità di utilizzare un dato anche trasformandolo nei sistemi informativi automatizzati di un'altra amministrazione;

aa) **Impronta di un documento informatico**: sequenza di simboli binari in grado di identificarne univocamente il contenuto;

bb) **Gestione informatica dei documenti**: 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;

cc) **Segnatura di protocollo**: apposizione o associazione, all'originale del

dd) **Archiviazione ottica**: operazione che genera, su supporto di memorizzazione una registrazione contenente la versione iniziale di una istanza di un documento informatico;

ee) **Busta di trasporto**: documento informatico che contiene il messaggio di posta elettronica certificata;

ff) **Log dei messaggi**: registro informatico delle operazioni relative alle

trasmissioni effettuate mediante posta elettronica certificata tenuta dal gestore;

gg) **Messaggio di posta elettronica certificata**: documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati;

hh) **Posta elettronica**: sistema elettronico di trasmissione dei documenti informatici;

ii) **Riferimento temporale**, l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata;

jj) **Utente di posta elettronica certificata**: 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;

kk) **Password**: è associata ad uno specifico username e serve ad ottenere una identificazione

1.4 AREA ORGANIZZATIVA OMOGENEA

Ai fini della gestione dei documenti del Comando Militare Esercito "Basilicata" è istituita un'Area Organizzativa Omogenea (AOO) denominata Area Organizzativa Omogenea (AOO) del Comando Militare Esercito "Basilicata", codice identificativo: **M_DE24463**

- "**M_D**", è il codice identificativo dell'Amministrazione Difesa;
- **"E",** rappresenta il primo carattere del codice identificativo indicante l'appartenenza del'AOO all'Esercito;

M_DE24463, è la seconda parte del codice identificativo del' OO, che nel caso specifico è riferito al Codice SISME del Comando Militare Esercito "Basilicata".

All'interno del'AOO il sistema di protocollazione è unico e centralizzato per la corrispondenza in entrata, mentre è decentralizzato, per la corrispondenza in uscita, attraverso le UO.

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

Nell'unica AOO-M_DE24463 è istituito un Nucleo per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, secondo le disposizioni dell'art. 61 del DPR.

Alla guida del suddetto servizio è posto il Responsabile del Servizio di Protocollo Informatico, della gestione dei flussi documentali e degli archivi (di seguito RDS).

Nei casi di vacanza, assenza o impedimento del Responsabile, 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 Responsabile del Servizio:

- predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;

- provvedere alla pubblicazione del Manuale (eventualmente anche sul sito Internet dello Stato Maggiore Esercito.);
- presiedere alle attività del Nucleo 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 del registro giornaliero di protocollo;

il C4IE cura 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;

in caso di registrazione di protocollo manuale, conservare in luoghi sicuri le copie dei Registri di Protocollo di emergenza;

autorizzare le operazioni di annullamento di un protocollo;

vigilare sull'osservanza delle disposizioni da parte del personale incaricato.

1.6 CONSERVAZIONE DELLE COPIE DI RISERVA

Entro la giornata lavorativa successiva a quella di riferimento,il registro di protocollo giornaliero viene consolidato dal sistema, firmato digitalmente in modalità automatica ed inviato in conservazione secondo le indicazioni fornite dal Responsabile della Conservazione del dicastero.

1.7 RECAPITO DEI DOCUMENTI

L'AOO-MDE24463 predilige l'invio della corrispondenza in forma telematica alle seguenti caselle di posta elettronica istituzionale:

- posta elettronica ordinaria (PEI): cme_basilicata@esercito.difesa.it
- posta elettronica certificata (PEC): cme_basilicata@postacert.difesa.it

In alternativa, l'indirizzo postale della documentazione analogica diretta all'AOO-M_DE24463 è:

Comando Militare Esercito "Basilicata"
Via Ciccotti, 32 – 85100 POTENZA

La corrispondenza diversamente indirizzata, o diretta a entità non appartenenti all' AOO-M_DE 24463, non sarà accettata.

1.8 **TUTELA DEI DATI PERSONALI**

La documentazione contenente dati personali - comuni, sensibili e/o giudiziari - è gestita in conformità al D.lgs. 196/2003 (Codice di protezione dei dati personali) e 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.

1.8 **ENTRATA IN VIGORE DEL MANUALE**

Le regole indicate nel presente manuale saranno applicate a decorrere dal **28.12.2022**

Il piano di attuazione del protocollo informatico prevede l'eliminazione dei diversi protocolli di Ufficio, di sezione e multipli, seguendo il seguente iter:

1.9 **PIANO DI ATTUAZIONE**

In coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'amministrazione sono registrati all'interno del registro di protocollo informatico.

Il piano di attuazione del protocollo informatico prevede l'eliminazione dei diversi protocolli di sezioni e multipli.

L' RDS esegue comunque, periodicamente, dei controlli a campione sulla corretta esecuzione del piano e sull'utilizzo regolare di un unico registro di protocollo, verificando, attraverso controlli ed ispezioni mirate nelle varie UO, la validità dei criteri di classificazione utilizzati dalle forze dell'ordine.

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 PIANO DI SICUREZZA

Il presente capito 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 [1(*)]:

- protezione periferica della Intranet dell' AOO- M_DE24463;
- protezione dei sistemi di accesso e conservazione delle informazioni [(*)];
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- 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 [(*)];
- conservazione, a cura dell'amministratore di sistema delle copie di riserva dei dati e dei documenti, su infrastruttura diversa da quella utilizzata dal sistema di protocollo [(*)];
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi [(*)];
- archiviazione giornaliera, in modo non modificabile, delle copie del registro 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, comprese le operazioni di backup e manutenzione del sistema [(*)].

I dati personali registrati nel log 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

1 (*) Servizio erogato/assicurato a cura del C4EI

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 del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- 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- M_DE24463 e la cui responsabilità risale al Responsabile della Sicurezza EAD del Comando Militare Esercito "Basilicata".

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

3.1 GENERALITÀ

Per la gestione dei documenti informatici, l' AOO M_DE24463 dispone di due caselle di posta elettronica[2] istituzionale, una di tipo ordinaria (PEI) e l'altra di tipo certificata (PEC):

- posta elettronica ordinaria (PEI): cme_basilicata@esercito.difesa.it
- posta elettronica certificata (PEC): cme_basilicata@postacert.difesa.it

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. Il sistema di posta elettronica non garantisce la ricezione su e-mail ordinaria di messaggi inviati tramite PEC e viceversa;
- 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;
- gli allegati al messaggio devono avere preferenzialmente l'estensione PDF. Sono altresì accettati anche i formati: JPG, P7M, TXT, TIFF, TIF e XML, DOC, PPT, XLS;
- se di numero elevato, i file allegati al documento primario, rispettando i formati anzidetti, possono essere compressi nei formati 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 degli allegati è di 10 (PEI) – 30 (PEC) MB. Superato tale limite, il sistema di posta elettronica non recapiterà il messaggio all'AOO;
- 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

---

2 In aderenza all'art. 2 comma 3 e all'art. 47 del CAD, le comunicazioni dirette all'AOO-MDE24463, mediante l'utilizzo della posta elettronica, sono valide per il procedimento amministrativo se:

- sono sottoscritte con firma digitale;
- ovvero, sono dotate di segnatura di protocollo di cui all'art. 55 del DPR;
- ovvero, sono trasmesse attraverso sistemi di posta elettronica certificata di cui al DPR 68/05.

Inoltre, in conformità all'art. 38 comma 3 del DPR, potranno essere inviate telematicamente all'AOO-MDE24463 istanze sottoscritte, digitalizzate, e presentate unitamente a copie non autenticate di documenti d'identità dei sottoscrittori.

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 S.r.l. 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) l'AOO-M_DE24463 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 in ingresso dematerializzato viene firmata digitalmente[3] 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.

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.

---

3 I documenti informatici sottoscritti digitalmente e derivanti dalla dematerializzazione, devono essere intesi quali copie conformi dei relativi atti cartacei in ragione dell'art.23-ter del CAD.

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 AOO;
- l'interconnessione tra AOO, 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 **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 per l'AOO e per sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro "file" digitale con valenza giuridico- probatoria[4].

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 interessati[5].

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. 20 del CAD).

3.7 **USO DELLA POSTA ELETTRONICA CERTIFICATA**

Nei casi previsti dalla legge, per i quali si renda necessario disporre di una conferma di avvenuta ricezione della corrispondenza, viene utilizzata la casella di PEC, sempre ché anche il corrispondente ne disponga.

Parimenti, si utilizzerà la casella di PEC ogni qualvolta che il corrispondente ne chieda esplicitamente l'impiego.

Negli altri casi il veicolo privilegiato per le comunicazioni è la casella di PEI.

3.8 **GENERALITÀ**

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

- in ingresso;

4 I documenti in uscita contengono anche la marca temporale prevista dalla normativa vigente.

5 I soggetti delegati a rappresentare l'Amministrazione e identificati con i capi delle UO, e il personale responsabile del NdP.

- 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 Comando Militare Esercito "Basilicata" viene registrata in un unico punto (Nucleo del Protocollo Informatico);
- delega alle UO - Articolazioni che hanno facoltà di trasmettere direttamente i documenti sia informatici sia analogici all'esterno dell'AOO.

I documenti in ingresso alla AOO sono assegnati direttamente ai Capi 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 operazioni 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.

3.9 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.

3.10 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 digitazione del "flag" dati sensibili). La posta classificata erroneamente pervenuta al servizio di protocollo sarà consegnata al Punto Controllo 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;

secondo momento, attivare le suddette limitazioni all'accesso.

3.11 DOCUMENTO INFORMATICO

L'AOO è predisposta alla ricezione e alla gestione di documenti informatici sulle caselle di

posta elettronica ordinaria e di una casella di PEC. Se un documento informatico, afferente a pratiche/procedimenti in corso di trattazione, viene inviato ad una casella di posta elettronica ordinaria afferente ad una UO, il titolare di tale casella deve inviare un messaggio al mittente segnalando la necessità di inviare nuovamente il documento alla corretta casella postale dell'AOO.

3.12 DOCUMENTO INFORMATICO IN INGRESSO 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 per i quali l'RDS invia al mittente il messaggio:

- **il messaggio è corrotto o uno dei documenti non è leggibile;**
- **dati non congruenti nella segnatura informatica;**
- **segnatura non conforme alla circolare AIPA/CR/28 7 maggio 20001 ;**
- **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.

Le istanze e le dichiarazioni da presentare alla Pubblica Amministrazione , saranno protocollate se aderenti a quanto disposto dall'art 38.del DPR 445/2000nel rispetto dell'art. 38 del DPR 445/2000

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 P.A., in assenza della firma digitale, è sufficiente che sia presente in allegato il file segnatura. xml, informazioni previste dalla CIRC AIPA/CR/28 7 MAGGIO 2001;

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 sia registrato e assegnato alla Unità Organizzativa, sarà cura di quest'ultima informare l'RDS per le azioni che ogni caso di errore richiede.

3.13 DOCUMENTO INFORMATICO IN INGRESSO 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'accezione della differente coda di arrivo dei messaggi rispetto alla PEI.

3.14 MESSAGGI IN ARRIVO SULLA POSTAZIONE E-MESSAGE

I messaggi telegrafici indirizzati al Comando Militare Esercito "Basilicata" ed ai suoi Uffici sono tutti ricevuti sulla postazione "E – Message" dedicata del Nucleo.

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 come tramite cartella di condivisione /o stampare messagio;
- protocollare il messaggio;
- inoltrare il messaggio alle UO destinatarie in indirizzo.

3.15 DOCUMENTO INFORMATICO IN USCITA

Come già segnalato in precedenza, tutta la documentazione amministrativa dell'AOO è originata e/o gestita in forma elettronica.

Il sistema, sulla base delle informazioni inserite durante la predisposizione, invia ai destinatari, per posta elettronica, il documento primario e tutti gli eventuali allegati presenti. L'utilizzo della casella postale elettronica ordinaria piuttosto che della PEC viene predisposto dall'operatore e può essere modificato fino alla firma del documento stesso da tutti gli utenti che in successione ricevono il documento per il suo perfezionamento (Capo Sezione, Capo Ufficio, ecc.).

Tutti i documenti trasmessi sono corredati del file segnatura. xml, contenente le informazioni previste all' allegato 6 alle Linee Guide sulla formazione , gestione e conservazione dei documenti informatici.

Nelle circostanze di seguito descritte, la formazione e la sottoscrizione dell'atto avviene secondo modalità idonee alla produzione di un originale informatico, mentre la trasmissione

dell'atto, completo di allegati, viene effettuata in forma analogica:

il destinatario è privo di una qualsiasi casella di posta elettronica;

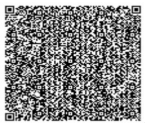
il documento primario è corredato di allegato analogico non digitalizzabile;

il documento primario ha un allegato informatico di dimensione eccessiva o non gestibile dai servizi di posta elettronica.

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. Il re-indirizzamento è automatico per il primo caso, e su indicazione dell'utente, che riporta al sistema la presenza di allegati analogici, per i restanti casi.

In questi casi, il documento, completo di allegati, sarà inviato in forma analogica ai destinatari esterni per competenza attraverso il servizio postale, regolamentato nel capitolo successivo, mentre i destinatari interni e quelli esterni per conoscenza provvisti di e-mail riceveranno solo il documento primario inviato automaticamente dal sistema.

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.



Firmato digitalmente da Col._____ il____/_____2023

Documento M_D A7D11B4 REG.02023 0000____ stampato dall'utenza cmepz_vicario/rds

Per l'avvenuta verifica inviare a cme_basilicata.difesa.it secondo le indicazioni contenute nel sito ww.difesa..it/il Protocollo/Pagine/Glifo.aspx.

Sul documento così stampato con opposto, Glifo sul fronte, con la seguente frase:

L'attestazione dovrà essere sottoscritta da uno dei seguenti funzionari, aventi causa nella formazione dell'atto:

- Dirigente titolare dell'UO;
- Capo della Sezione che ha predisposto l'atto;
- Capo Segreteria dell'UO.

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.

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

nella denominazione dei file non si devono utilizzare caratteri speciali, interpunzioni e/o lettere accentate (esempi di caratteri da non usare: /'°,.^);

il nome dei file non devono superare i venti caratteri.

Qualora come allegato, venga inserito un documento informatico già firmato digitalmente, l'operatore che sta effettuando la predisposizione deve spuntare la voce NO PDF, per evitare la successiva conversione in PDF/A del documento. Tale operazione oltre a non essere utile su un documento già firmato in precedenza, potrebbe generare errori nel sistema informatico idonei a bloccare la fase di protocollazione e trasmissione del documento.

3.16 **<u>MESSAGGI IN PARTENZA SULLA POSTAZIONE E-MESSAGELe UO devono,</u>**

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 spuntata la casella "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" del Nucleo Posta e PII destinatari del messaggio, tra cui quelli eventualmente appartenenti alle UO del Servizio 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.

  Qualora inviato anche via E-Message, alcuni o tutti i destinatari riceveranno il messaggio anche in formato cartaceo (stampa dalla postazione E-Message).

  Nel caso in cui fra i destinatari compaia una lista AIG (Address Indicator Group) e l'inserimento di tutti gli indirizzi nella rubrica di "Adhoc", 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.).

  Il Nucleo protocollo informatico non effettua attività di gestione della corrispondenza in uscita dall'AOO tramite E-Message.

3.17 **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.

Quel documento sarà protocollato solo in uscita dalla UO mittente.

Ogni UO provvederà alla protocollazione e alla conservazione del documento del proprio dipendente , in caso contrario il documento può essere accettato e protocollato dal nucleo preposto alla protocollazione.

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

3.18**DOCUMENTO ANALOGICO**

Non sarà accettata la corrispondenza diretta ad articolazioni estranee all' AOO- M_DE24463 o con indirizzo diverso dal seguente:

DOCUMENTO ANALOGICO INGRESSO

La corrispondenza analogica in arrivo può essere acquisita dalla AOO con diversi mezzi e modalità. In particolare è prevista la consegna[6] della corrispondenza in ingresso da parte del personale dell'agenzia delle Poste Italiane e/o corrieri civili/militari agli addetti del Nucleo Posta. Alla consegna della corrispondenza, presso i locali del Nucleo Posta e PI del Comando, i plichi postali sono sottoposti a verifica di sicurezza mediante apposite apparecchiature elettroniche. 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.

3.18.1 POSTA RACCOMANDATA E ASSICURATA

Il personale del Nucleo Posta e PI 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-MDE24463 dovranno essere ritirati esclusivamente dai destinatari stessi.

3.18.2 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.

3.18.3 REGISTRAZIONE DEI DOCUMENTI ANALOGICI

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

a) 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);

b) scansione massiva dei documenti, a cura di addetti che verificano il buon esito dell'operazione, e assegnazione degli stessi al primo operatore di protocollo libero;

c) 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;

6 Alle ore 11:15 di tutti i giorni (sabati e festivi esclusi)

- eventuale indicazione di Dato Sensibile secondo le disposizioni del CODPRI;
- 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;

d) apposizione della firma digitale sui documenti così elaborati da parte del medesimo operatore responsabile dell'inserimento dei dati di cui al precedente punto c)

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 è custodito nell'archivio istituito presso ciascuna UO che sarà direttamente responsabile della corretta conservazione. Compatibilmente con il carico di lavoro, tutto il processo di protocollazione avviene di norma entro il giorno di ricezione del documento.

3.19 **DOCUMENTO ANALOGICO IN USCITA**

Poiché nell'ambito dell'AOO vengono prodotti esclusivamente documenti originali informatici non avrebbe senso parlare di flusso in uscita di documenti analogici.

Tuttavia, come riportato nel paragrafo inerente al flusso in uscita dei documenti informatici, può essere necessario procedere alla trasmissione attraverso il servizio postale tradizionale di uno o più documenti.

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.

3.20 **DOCUMENTO ANALOGICO INTERNO**

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

3.21 **FAX**

dal comma 2 dell'art.47 comma 2 lettera c recante informazioni relative alla trasmissione informatica dei documenti, è esclusa la trasmissione di documenti a mezzo fax tra PP.AA.

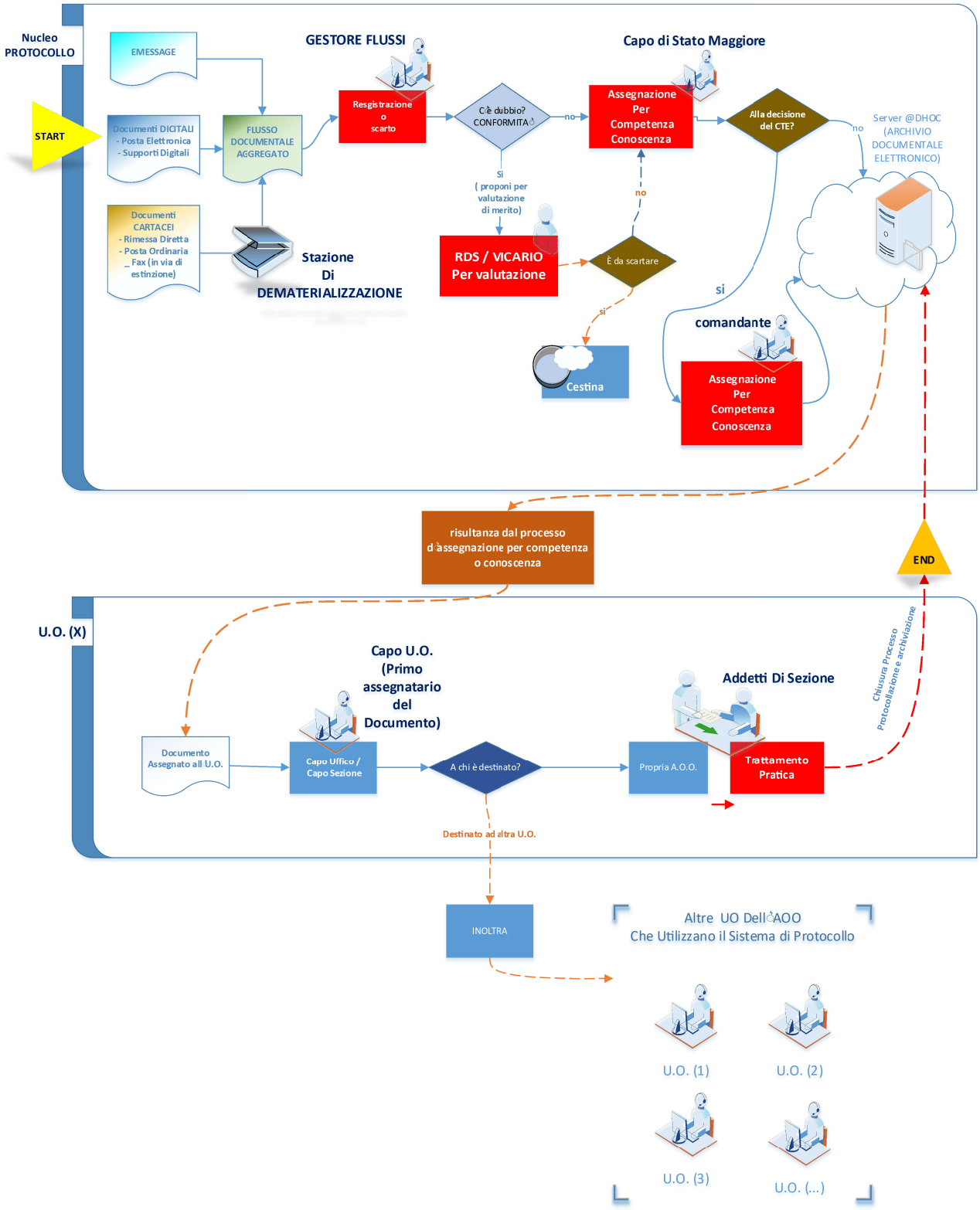
a) Seconda fase

L'Ufficiale che riceve il documento firmato può inoltrarlo, dopo aver apposto eventuali ulteriori decretazioni, al personale che ne curerà:

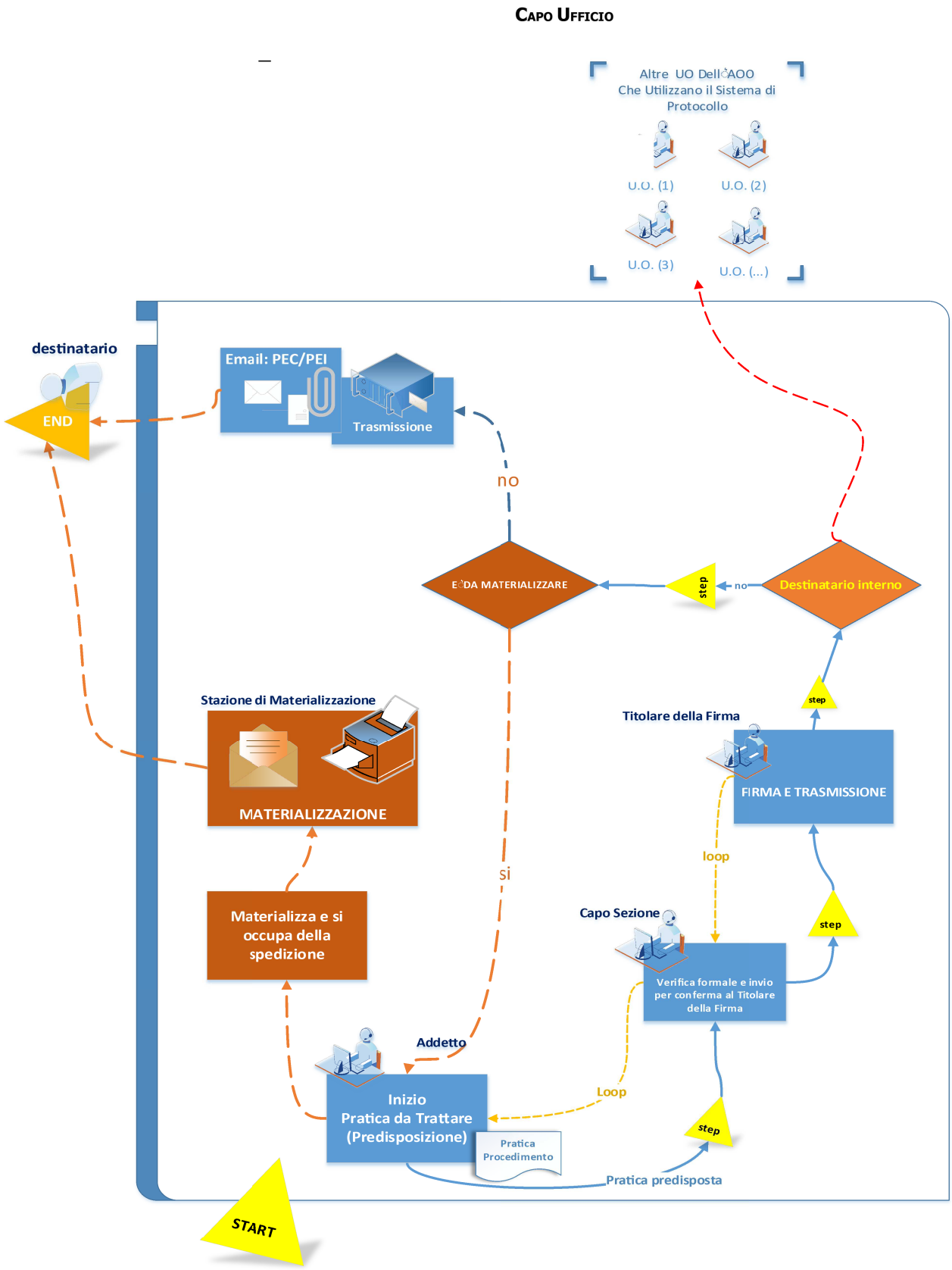
- la fascicolazione e l'archiviazione, nel caso in cui non siano necessarie azioni ulteriori;
- la predisposizione della eventuale lettera da inviare, avendo cura di:
  - preparare un nuovo documento con cui inviare la lettera alla firma, mediante la funzione "Predisposizione";

- selezionare i destinatari della lettera (N.B.: stavolta sono i "veri" destinatari della comunicazione);
- estrarre la lettera da inviare dall'appunto firmato (in tal modo si ha la sicurezza di avere l'ultima versione, contenente tutte le eventuali correzioni effettuate ai vari livelli durante l'iter procedurale);
- provvedere a mantenere traccia dell'appunto originale inserendolo fra i "File accessori" ovvero citandone gli estremi di protocollo nel campo note;
- inoltrare il documento sulla linea gerarchica, per la firma digitale.

3.22**SCHEMA FLUSSO IN INGRESSO**



3.23 SCHEMA FLUSSO IN USCITA



4 MODALITÀ DI PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

4.1 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.

4.2 UNICITÀ DELLA REGISTRAZIONE DEL PROTOCOLLO INFORMATICO

- Nell'ambito della AOO, il registro di protocollo è unico così come la numerazione progressiva delle registrazioni di protocollo. 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.

4.3 REGISTRO GIORNALIERO DI PROTOCOLLO

- Il registro giornaliero di protocollo viene consolidato entro la giornata lavorativa successiva a quella di riferimento.
- Il consolidamento avviene tramite la firma (anche effettuata in modalità digitale automatica) del registro giornaliero di protocollo e con l'invio in conservazione secondo le indicazioni del Responsabile della Conservazione del dicastero.

4.4 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.

4.5 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.
- Per quando attiene alla protoollazione dei documenti in ingresso, vengono utilizzati i dati contenuti nel file segnatura xml, se conforme alle indicazioni dell' LLGG.
- Al File segnatura xml associato ai documenti in uscita, in aderenza alle disposizioni dell' Allegato 6 LLGG, viene apposto il sigillo della AOO.
- Il formato della segnatura di protocollo dell'**AOO-M_DE24463**, conformemente alla normativa, prevede i seguenti dati:
- Codice dell'Amministrazione: **M_D**
- Codice dell'AOO: **A7D11B4**
- Identificativo del Registro: **REG2023**
- Numero di protocollo: <**progressivo di 7 cifre**>
- Data di registrazione: **gg-mm-aa** Esempio di segnatura di protocollo:

M_D A7D11B4 REG2023 0000001 01-01-2023

4.6 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 previa richiesta di annullamento **(Alleg."e").**
- 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.

4.7 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.

4.8 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 E24463 ricalca il "Titolario di archivio dell'Esercito Italiano"[7], 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[8], in particolare:
- il 1° livello del Titolario (titolo) individua 12 voci funzionali [9], 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.

4.9 CLASSIFICAZIONE DEI DOCUMENTI

- La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo

7
8
9

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 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.

4.10 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 un fascicolo 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.

5 ARCHIVIAZIONE DEI DOCUMENTI

5.1 DEPOSITO/ARCHIVIO DELL'AOO- M_DE24463

Sulla base della normativa vigente, per la custodia della documentazione registrata a protocollo, l'AOO-MDE24463 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, atti esauriti da oltre 30 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-MDE24463 produce esclusivamente originali informatici e, inoltre, tutti gli atti cartacei pervenuti vengono dematerializzati e convalidati.

  Pertanto, l'universalità dei documenti originali afferenti all'AOO-MDE24463, 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 nuovo sistema che continueranno ad essere gestiti da parte delle U.O.

5.2 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 dello C4IE, che gestisce anche l'applicativo di protocollazione all'AOO- M_DE24463.

Il sistema è conforme alle norme vigenti, ciascun documento è dotato di firma digitale, di marca temporale, di hash in formato SHA-256 e delle informazioni di registrazione ad esso associate. Ogni giorno viene anche, prodotto, il registro giornaliero delle registrazioni di protocollo, firmato digitalmente dal RDS.

Tutti i documenti sono inoltre fascicolati.

Le regole generali di archiviazioni sono disponibili nel paragrafo inerente alla classificazione.

5.3 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.

  Nell'ambito delle UO dovranno essere stabiliti i responsabili all'archiviazione

documentale attiva e segnalati all'RDS dal quale dipenderanno funzionalmente.

5.4 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_DE24463. 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.

6 ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

6.1 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.

6.2 ACCESSO AL SISTEMA

Per poter accedere al sistema ad ogni utente è assegnata una credenziale 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.

6.3 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 Sezione, 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_DE24463, 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.

6.4 **PROFILI D'ACCESSO**

Nell'ambito dell' AOO-M_DE24463 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.

7 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

7.1 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.

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

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 iniziale n.: ____

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

7.3 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.

7.4 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. Tutte le dichiarazioni dell'RDS di attivazione e chiusura del registro di emergenza sono conservate a cura del RDS.

CHIUSURA DEL REGISTRO DI EMERGENZA

Data di fine 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)

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.

8 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

8.1 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.

8.2 ABROGAZIONE E SOSTITUZIONE DELLE PRECEDENTI NORME INTERNE

Il presente Manuale abroga e sostituisce ogni norma interna all'AOO- MDE24463 che dovesse contrastare con il suo contenuto.

9 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 Uf. Legislativo e non Ufficio Legislativo del Ministero della DIFESA
Sigle in genere	– in maiuscolo e senza punti; esempio: ISTAT.
irgolette 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: 01-01-2016

Allegato "A"

Elenco delle U.O. (Unità Organizzative) per la gestione dei flussi documentali nell'ambito dell'Area Organizzativa Omogenea (AOO) Comando Militare Esercito "Basilicata"

- COMANDO MILITARE ESERCITO "BASILICATA"
  - **COMANDANTE**
    - SEGRETERIA DEL COMANDANTE
    - SEZIONE COORDINAMENTO AMMINISTRATIVO
    - SALA MEDICA
    - RESPONSABILE SERVIZIO DI PREVENZIONE E PROTEZIONE
    - RAPPRESENTANZA MILITARE
    - **CAPO DI STATO MAGGIORE**
      - UFFICIO AFFARI GENERALI
      - UFFICIO PERSONALE LOGISTICA E SERVITU' MILITARI
      - UFFICIO DOCUMENTAZIONE RECLUTAMENTO E COMUNICAZIONE
      - PLOTONE E SUPPORTO GENERALE
      - SEZIONE SICUREZZA

Allegato "B"

PERSONALE INCARICATO DELL'EROGAZIONE E GESTIONE DEL SERVIZIO

Responsabile del Servizio: – Mar Ord. Angelo SABIA

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

Addetto al Protocollo: Ass. Amm.Pasquale RIVIELLO

Allegato "C"

M_D A7D11B4 REG2022 0005832 05-10-2022

COMANDO MILITARE ESERCITO "BASILICATA"

OGGETTO: Nomina del responsabile e del vicario del servizio per la tenuta del protocollo informatico, della gestione documenti e degli archivi del Comando Militare Esercito "BASILICATA".

IL COMANDANTE

VISTO: il DPR 25 Dicembre 2000, n.445 – "Disposizioni legislative in materia di documentazione amministrativa"e successive varianti; e, in particolare l'art .61;

VISTO: il DPCM 3 Dicembre 2013 e, in particolare l'art.3;

VISTO: l'atto Dispositivo n° 1 in data 30.12.2021 "Atto costitutivo dell'Area Organizzativa Omogenea (AOO) di CME "BASILICATA";

VISTO l'atto Dispositivo n° 1 in data 30.12.2021, variante all'atto Dispositivo n 1° in data 09.09.2022.

NOMINA

- il Mar. Ord. Angelo SABIA, Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

IL COMANDANTE
Col. MADDALUNO Ciro

Digitally signed by CIRO MADDALUNO
Date: 2022.10.05 12:38:42 CEST