# REGGIMENTO GENIO FERROVIERI

- COMANDO -

Viale Rimembranze, 1 – 40013 – Castel Maggiore (BO)
PEC: rgtgfv@postacert.difesa.it – PEI: rgtgfv@esercito.difesa.it


# MANUALE DI GESTIONE

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

(ai sensi degli artt.3 e 5 del D.C.P.M. 3 dicembre 2013)

## **A**rea **O**rganizzativa **O**mogenea
## REGGIMENTO GENIO FERROVIERI
## (identificativo: M_D E12988)

## Edizione 2020

| Versione 3.1 del 17 agosto 2020 | Elaborato da | Approvato da |
|---|---|---|
| Pag. 01 di 44 | IL RESPONSABILE DEL SERVIZIO<br>Magg. g.(fv.) Salvatore Antonino IANNUZZO | IL COMANDANTE<br>Col. g.(fv.) t.ISSMI Cesare CANICCHIO |

PAGINA NON SCRITTA

# REGGIMENTO GENIO FERROVIERI

## ATTO DI APPROVAZIONE

Approvo il presente “Manuale di Gestione per la tenuta del Protocollo Informatico, della gestione dei flussi documentali e degli archivi, edizione 2020 - AOO Reggimento Genio Ferrovieri M_D E12988”.

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 e s.m.i., Regolamento Generale sulla Protezione dei Dati – Regolamento UE n. 2016/679.

Il presente manuale entra in vigore in data 1° settembre 2020 ed abroga e sostituisce la precedente versione 3.0 dell’11 agosto 2020.

Castel Maggiore, lì *18 agosto 2020*

IL COMANDANTE
Col. g.(fv.) t.ISSMI Cesare CANICCHIO
(*firmato digitalmente*)

PAGINA NON SCRITTA

# REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

| NR. | DATA | DESCRIZIONE |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

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:

| | |
|---|---|
| **AOO** | **A**rea **O**rganizzativa **O**mogenea |
| **AOO-M_D E12988** | AOO del Reggimento Genio Ferrovieri |
| **AGID** | **Ag**enzia per l'**I**talia **D**igitale |
| **[CAD]** | **C**odice **A**mministrazione **D**igitale D.Lgs. 07.03.2005, n. 82 e s.m.i. |
| **[CIRC]** | **Cir**colare dell'Autorità per l'Informatica nella P.A. 07.05.2001, n. 28 |
| **[CODBCP]** | **Cod**ice dei **B**eni **C**ulturali e del **P**aesaggio D.Lgs. 22.01.2004, n. 42 |
| **[CODPRI]** | **Cod**ice di **Pr**otezione dei dati personali D.Lgs. 30.06.2003, n. 196 |
| **[DEPRI]** | Decreto Legislativo 10 agosto 2018, n. 101 |
| **[DIR]** | **Dir**ettiva SMD-I-004 |
| **[DPCM]** | **D**ecreto della **P**residenza del **C**onsiglio dei **M**inistri 31.10.2000 |
| **[DPR]** | **D**ecreto del **P**residente della **R**epubblica 28.12.2000, n. 445 |
| **[GDPR]** | **G**eneral **D**ata **P**rotection **R**egulation - Regolamento UE |
| **IPA** | **I**ndice delle **P**ubbliche **A**mministrazioni |
| **[NOPA]** | Decreto Legislativo 30 marzo 2001, n. 165 |
| **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 |
| **NdP** | **N**ucleo per la tenuta **d**el **P**rotocollo informatico, della gestione dei flussi documentali e degli archivi |
| **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.

**Regolamento Generale sulla Protezione dei Dati – Regolamento UE n. 2016/679 [GDPR]**
"Regolamento del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

**Regio Decreto 35 del 25 gennaio 1900**
"*Regolamentazione della gestione del protocollo dei documenti amministrativi*" Tale norma è stata rinnovata con il DPR 428/1988 che tuttavia ha mantenuto impianto e principi del provvedimento originario.

**Decreto Legislativo 30 marzo 2001, n. 165 [NOPA]**
"*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*." Con il D.Lgs n. 165 vengono disciplinate l'organizzazione degli uffici e i rapporti di lavoro e di impiego alle dipendenze delle amministrazioni pubbliche.

**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.

**Circolare Agenzia Italia Digitale 23 gennaio 2013, n. 60 [CIRC]**
Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le P.A..

**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 10 agosto 2018, n. 101 [DEPRI]**
*"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE)"*che recepisce formalmente il *General Data Protection Regulation* – GDPR, nella normativa italiana.

**Decreto Legislativo 22 gennaio 2004, n. 42 [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 07 marzo 2005, n. 82 e s.m.i. [CAD]**
Codice dell'Amministrazione Digitale.

**Decreto Legislativo 30 dicembre 2010, n. 235**
Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82 riguardante il Codice dell'Amministrazione Digitale, a norma dell'art. 33 della legge 18 giugno 2009, n. 69.

**Decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013 [DPCM]**
Regole tecniche per il PI 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. In attuazione ad alcune disposizioni contenute nel CAD è stato emanato il presente DPCM, che indica, nel dettaglio, le regole tecniche per l'attuazione della normativa e abroga il corrispondente DPCM del 31 ottobre 2000.

# 1. PRINCIPI GENERALI

## 1.1. PREMESSA

Il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "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", prevede per tutte le amministrazioni di cui all'art. 2 comma 2 del Codice l'adozione del Manuale di gestione.

Quest'ultimo, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del Nucleo 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, dei documenti e degli archivi è redatto ai sensi degli artt. 3 e 5 del [DPCM], ed è rivolto al personale interno all'AOO-M_D E12988 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 Reggimento Genio Ferrovieri a partire dal 29 giugno 2017 (data di attivazione del sistema).

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 che fa fede, ad ogni effetto, del ricevimento e della spedizione di un documento;
- la classificazione del documento, anche non protocollato, che lo dota della collocazione logico-funzionale nell'Archivio;
- la fascicolazione del documento, protocollato o non 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:

a. *Amministrazione*, il Reggimento Genio Ferrovieri;
b. *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;
c. *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;
d. *Codice*, il Decreto Legislativo 7 marzo 2005 n. 82 – Codice dell'Amministrazione Digitale.

Si riportano, di seguito, gli acronimi utilizzati più di frequente:

a. *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 ([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 procedimentale per l'adozione del provvedimento finale. A tal fine deve essere utilizzato solo ed esclusivamente un unico registro di protocollazione degli atti;

b. *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 una unità dipendente dall'Area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico;
c. *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;
d. *Responsabile del Nucleo per la tenuta del protocollo informatico, 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;
e. *Manuale di Gestione del protocollo informatico*, 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, nel quale gli interessati vi trovano descritte le modalità di gestione del protocollo nei suoi diversi aspetti;
f. *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;
g. *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;
h. *Fascicolo*, insieme minimo di documenti, composto dall'ordinata riunione di atti relativa ad uno stesso affare o procedimento amministrativo;
i. *Fascicolazione*, l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi;
j. *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;
k. *Fascicolo/pratica archiviato*, il fascicolo che ha completato il suo ciclo all'interno della trattazione dell'affare e viene trasferito dall'utente all'Archivio Deposito;
l. *Assegnazione*, l'operazione di individuazione dell'ufficio utente competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
m. *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,

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

n. *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;
o. *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;
p. *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;
q. *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 (art. 1 della Deliberazione CNIPA ora AGID del 19 febbraio 2004, n. 11);
r. *Casella di Posta Elettronica Istituzionale (PEI)*, la email istituita da ciascuna AOO attraverso la quale possono essere ricevuti i messaggi da protocollare;
s. *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;
t. *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, let. n) del [CODPRI];
u. *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];
v. *Dati sensibili*, sono quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche ed altro, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazione a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale (art. 9 GDPR);
w. *Dati giudiziari*, i dati personali idonei a rivelare provvedimenti di cui all'art. 10 GDPR, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
x. *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;
y. *Documento informatico*, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
a. *Documento analogico*, la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti: art. 1, let. P) –bis del [CAD];
b. *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;
c. *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;
d. *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;

e. *Fruibilità di un dato*, la possibilità di utilizzare un dato anche trasformandolo nei sistemi informativi automatizzati di un'altra amministrazione;
f. *Impronta di un documento informatico*, la sequenza di simboli binari in grado di identificarne univocamente il contenuto;
g. *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;
h. *Segnatura di protocollo*, l'apposizione o associazione, all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso;
i. *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;
j. *Supporto di memorizzazione*, mezzo fisico atto a registrare permanentemente informazioni rappresentate in modo digitale, su cui l'operazione di scrittura comporti una modifica permanente ed irreversibile delle caratteristiche del supporto stesso;
k. *Archiviazione ottica*, operazione che genera, su supporto di memorizzazione una registrazione contenente la versione iniziale di una istanza di un documento informatico;
l. *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;
m. *@DhOC*, software di gestione del protocollo informatico;
n. *Busta di trasporto*, il documento informatico che contiene il messaggio di PEC;
o. *Log dei messaggi*, il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuta dal gestore;
p. *Messaggio di posta elettronica certificata*, un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati;
q. *Posta elettronica*, un sistema elettronico di trasmissione dei documenti informatici;
r. *Riferimento temporale*, l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata;
s. *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;
t. *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**.

## 1.4. AREA ORGANIZZATIVA OMOGENEA

Ai fini della gestione dei documenti del Reggimento Genio Ferrovieri è stata istituita l' Area Organizzativa Omogenea (AOO) denominata **Area Organizzativa Omogenea (AOO) del Reggimento Genio Ferrovieri**, codice identificativo:

**M_D E12988**

Laddove:

- **"M_D"**, è il codice identificativo dell'Amministrazione Difesa;
- **"E"**, rappresenta il primo carattere del codice identificativo indicante l'appartenenza della AOO all'Esercito;
- **"12988"**, è la seconda parte del codice identificativo dell'AOO, che nel caso specifico è riferito al Codice SISME del Reggimento Genio Ferrovieri.

All'interno della 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. UNITÀ ORGANIZZATIVE (UO)

Nell'ambito dell'AOO-M_D E12988, 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 normalmente retta da un dirigente/funzionario responsabile per le funzioni di competenza. Inoltre, esistono una serie di articolazioni (Sezioni, 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. Sono state inoltre previste alcune U.O. dipendenti dall'AOO per la quale non è stata prevista la possibilità di produrre/predisporre documenti. In particolare tali U.O. sono:

- COBAR: destinata alla ricezione dei documenti inerenti gli organismi della rappresentanza militare;
- R.S.U.: destinata alla ricezione dei documenti inerenti la rappresentanza sindacale;
- SMISTATORE: unità "funzionale" destinata alla distribuzione nell'ambito dell'AOO della documentazione pervenuta ed assunta a protocollo.

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

Nell'unica AOO-M_D E12988 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). Egli è funzionalmente individuato nell'ambito dell'Ufficio Maggiorità e Personale (S1) e si identifica con il Capo Ufficio/Aiutante Maggiore.
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 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 Intranet dell'amministrazione);

- 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 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;
- 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;
- 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.

## 1.7. RECAPITO DEI DOCUMENTI

L'AOO-M_D E12988 predilige l'invio della corrispondenza in forma telematica alle seguenti caselle di posta elettronica:

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

In alternativa, l'indirizzo postale della documentazione analogica diretta all'AOO-M_D E12988 è:

**REGGIMENTO GENIO FERROVIERI**
**Viale Rimembranze, 1 – 40013 Castel Maggiore (BO)**

La corrispondenza diversamente indirizzata, o diretta a entità non appartenenti all'AOO-M_D E12988, non sarà accettata.

## 1.8. PRIVACY E PROTEZIONE DEI DATI PERSONALI

La trattazione e la visione dei documenti contenenti dati sensibili e giudiziari, deve avvenire nel rispetto della legge (D.Lgs. 196/2003 come modificato dal D.Lgs 101/2018 Regolamento UE n. 2016/679 "Regolamento Generale sulla Protezione dei Dati" GDPR, in vigore dal 25 maggio 2018) ed è consentita esclusivamente agli utenti abilitati.

Al riguardo, i documenti contenenti:

- dati sensibili: sono quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche ed altro, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazione a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale (art. 9 GDPR);
- dati giudiziari: sono quelli contenenti i dati personali idonei a rivelare provvedimenti di cui all'art. 10 GDPR, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Tali dati, come previsto dal GDPR, devono essere trattati in modo adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono trattati.

In particolare, nella protocollazione o predisposizione di tali documenti gli utilizzatori del sistema sono obbligati a selezionare l'apposizione del *fleg* sull'apposito campo dati sensibili.

## 1.9. ENTRATA IN VIGORE DEL MANUALE

Le regole indicate nel presente manuale saranno applicate a decorrere dal 1° settembre 2020.

# 2. ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

Il presente capitolo riporta la pianificazione, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli diversi dal protocollo informatico che, per qualsiasi motivo, non sono stati già eliminati alla data di entrata in vigore del protocollo informatico.

## 2.1. 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. Pertanto non vi sono registri particolari di protocollo in quanto già aboliti ed eliminati.
Il piano di attuazione del protocollo informatico prevede l'eliminazione dei diversi protocolli di ufficio, di sezione e multipli, seguendo il seguente iter:

- svolgimento di una riunione di coordinamento con i Responsabili delle UO interessate, al fine di:
  - · presentare la procedura informatica nel suo complesso;
  - · analizzare l'incidenza dell'applicazione delle sue funzionalità nelle procedure lavorative consolidate;
  - · effettuare un'attività informativa sulle modalità di creazione e gestione della documentazione;
  - · definire il piano di visibilità;
- acquisizione dei dati anagrafici e di riferimento delle UO e dei suoi utenti;
- configurazione della procedura per l'accesso delle nuove UO;
- formazione degli utenti sull'impiego delle funzionalità della procedura informatica;
- avvio del Servizio;
- assistenza alle UO sul servizio.

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

# 3. 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.

## 3.1. 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.

## 3.2. 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 Intranet dell'AOO-M_D E12988;
- 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 (username) di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione. Al riguardo, fermo restando la predisposizione del sistema, per motivi di sicurezza l'accesso al sistema è consentito esclusivamente con la carta CMD. Pertanto, sono stati momentaneamente sospesi gli accessi con ruolo e password, intendendo come perentoria tale disposizione;
- cambio delle password con frequenza almeno bimestrale durante la fase di esercizio;

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 RDS e dal titolare dei dati e, ove previsto, dall'Autorità Giudiziaria.

## 3.3. FORMAZIONE DEI DOCUMENTI - ASPETTI DI SICUREZZA

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

- l'identificabilità del soggetto che ha formato il documento e l'AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti 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.

## 3.4. 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 unicamente mediante la piattaforma del protocollo informatico in modo da impedirne l'accesso al di fuori del sistema di gestione documentale da parte di utenti non autorizzati;

- 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.

### 3.5. 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_D E12988 e la cui responsabilità risale al Responsabile della Sicurezza EAD del Reggimento Genio Ferrovieri.

## 4. FORMAZIONE, TRASMISSIONE, SOTTOSCRIZIONE E ARCHIVIAZIONE DEI DOCUMENTI INFORMATICI.

### 4.1. GENERALITÀ

Per la gestione dei documenti informatici, l'AOO-M_D E12988 dispone di due caselle di posta elettronica[1] istituzionale, una di tipo ordinaria (PEI) e l'altra di tipo certificata (PEC):

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

### 4.2. 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 delle comunicazioni deve essere riportato nell'omonimo campo del messaggi e non deve riportare caratteri speciali quali [, /, °, ^, virgolette, apici ecc.;

[1] In aderenza all'art. 2 comma 3 e all'art. 47 del [CAD], le comunicazioni dirette all'AOO-M_D E12988, 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-M_D E23471 istanze sottoscritte, digitalizzate, e presentate unitamente a copie non autenticate di documenti d'identità dei sottoscrittori.

- 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/A o 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 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 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 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).

## 4.3. FORMAZIONE DEI DOCUMENTI - ASPETTI OPERATIVI

In aderenza alla normativa vigente (art. 40 del CAD) l'AOO-M_D E12988 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 dematerializzata viene firmata digitalmente[2] dal personale del Nucleo di Protocollo a ciò delegato che provvede anche alla distribuzione del documento cartaceo all'U.O. deputata alla custodia. 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.

## 4.4. 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

[2] 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].

uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità (vedasi art. 3 comma 3 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004).

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.

## 4.5. 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.

## 4.6. 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[3].

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[4].

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 "*la scrittura privata fa piena prova, fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritta";*
- soddisfa il requisito legale della forma scritta (art. 21 del [CAD]).

## 4.7. 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, sempreché anche il corrispondente ne disponga.

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

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

## 4.8. ARCHIVIAZIONE DEL DOCUMENTO INFORMATICO

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

[3] I documenti in uscita contengono anche la marca temporale prevista dalla normativa vigente.

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

# 5. LA GESTIONE DEI DOCUMENTI – ASPETTI FUNZIONALI

## 5.1. GENERALITÀ

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

- in ingresso;
- in uscita;
- interno.

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

- centralità, per quanto concerne la posta in ingresso, tutta la corrispondenza indirizzata al Reggimento Genio Ferrovieri viene registrata in un unico punto (Nucleo Protocollo Informatico - NdP);
- delega alle UO, 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 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.

## 5.2. ORARIO DI EROGAZIONE DEL SERVIZIO

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

- lunedì – giovedì dalle ore 08:15 alle ore 16:25;
- venerdì dalle ore 08:15 alle ore 11:55.

Per i documenti in uscita, il servizio di protocollazione sarà fruibile dalle 08:15 alle 23:59 di ciascun giorno lavorativo. Questo poiché il cambio data richiede la chiusura del registro di protocollo giornaliero da parte del RDS che la effettuerà entro le ore 08:15 del giorno lavorativo successivo.

## 5.3. 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" e classifiche equivalenti (mediante digitazione del *fleg* dati sensibili). La posta classificata erroneamente pervenuta al servizio di protocollo sarà consegnata al Punto Controllo del Comando di Reggimento.

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 ed apocrifi;
- informazioni elettroniche superiori ai 30 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 Nucleo Protocollo, di un filtro elettronico. L'UO competente per la trattazione può comunque, anche in un secondo momento, attivare le suddette limitazioni all'accesso.

## 5.4. 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 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.

## 5.5. 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 AGID 60 del 23 gennaio 2013;
- mancata sottoscrizione del documento primario;
- destinatario errato;
- verifica di integrità dei documenti negativa;
- il documento o gli allegati dichiarati all'interno del file segnatura.xml non corrispondono a quanto ricevuto.

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 P.A., in assenza della firma digitale, è sufficiente che sia presente in allegato il file segnatura.xml, informazioni previste dalla [CIRC].

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

## 5.6. 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 Posta Elettronica Istituzionale (PEI).

## 5.7. MESSAGGI IN ARRIVO SULLA POSTAZIONE E-MESSAGE

I messaggi telegrafici indirizzati al Reggimento Genio Ferrovieri ed ai suoi Uffici sono tutti ricevuti sulla postazione "EI*Message*" dedicata.

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.

## 5.8. DOCUMENTO INFORMATICO IN USCITA

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

A seguito della formazione degli atti, i titolari delle UO o gli addetti da questi delegati provvedono al loro perfezionamento, attraverso le funzioni del sistema, 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 presenti. L'utilizzo della casella postale elettronica ordinaria piuttosto che della PEC viene programmato dall'operatore che ha predisposto la pratica 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 dalla [CIRC] riguardanti la segnatura di protocollo.

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 reindirizzamento 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.
Sul documento così stampato sarà apposta, sul retro, la seguente frase:

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

*Castel Maggiore (BO), 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:

- Titolare dell'UO;
- Delegato del Titolare 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:
- utilizzare preferibilmente file con estensione RTF;
- nella denominazione dei file non si devono utilizzare caratteri speciali, interpunzioni e/o lettere accentate (esempi di caratteri da non usare: / ‘ ° , . ^);
- i 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.

## 5.9. 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 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, laddove ritenuto necessario, anche tramite la postazione "E-Message" della UO.

I destinatari del messaggio, tra cui quelli eventualmente appartenenti alle UO del Servizio stesso, 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**.

## 5.10. 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 titolare competente dell'UO destinataria.

Quel documento sarà protocollato solo in uscita dalla UO mittente.

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

## 5.11. DOCUMENTO ANALOGICO

Non sarà accettata la corrispondenza diretta ad articolazioni estranee all'AOO-M_D E12988 o con indirizzo diverso dal seguente:

**REGGIMENTO GENIO FERROVIERI**
**Viale Rimembranze, 1 – 40013 Castel Maggiore (BO)**

## 5.12. DOCUMENTO ANALOGICO INGRESSO

La corrispondenza analogica in arrivo può essere acquisita dalla AOO con diversi mezzi e modalità. In particolare è prevista la consegna[5] della corrispondenza in ingresso da parte del personale dell'agenzia delle Poste Italiane e/o corrieri civili/militari agli addetti del Nucleo Posta.

Per quanto attiene alla corrispondenza soggetta a protocollazione che dovesse giungere direttamente alle UO, essa sarà consegnata al Nucleo Posta 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.

[5] Di massima alle ore 11:00 di tutti i giorni (sabati e festivi esclusi).

### 5.12.1. 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-M_D E12988 dovranno essere ritirati esclusivamente dai destinatari stessi; il personale del Nucleo Posta o di servizio NON è autorizzato al ritiro.

### 5.12.2. 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.

### 5.12.3. 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;
   - 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 su cui verrà apposta la dicitura:
   "*Il presente documento e' copia informatica conforme al documento amministrativo analogico da cui e' tratta (art. 23ter/3 D.Lgs. 82/2005 e art. 10/1 DPCM 13/11/2014)*;

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 contenuti su CD, DVD e supporti con connessione USB. Tali allegati devono rispondere alle medesime regole di comunicazione indicate al precedente capitolo.
   Quando possibile, 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.

## 5.13. 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.

## 5.14. DOCUMENTO ANALOGICO INTERNO

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

## 5.15. FAX

In linea a quanto disposto dall'articolo 47 comma 2 lettera c del C.A.D. è stata esclusa la trasmissione di documenti a mezzo fax le P.A. Pertanto, nell'ambito di questo Reggimento, non è più utilizzato il FAX.

## 5.16. 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.

## 5.17. DOCUMENTI ESCLUSIVI PER IL TITOLARE O INDIRIZZATI ALLE PERSONE

La corrispondenza analogica indirizzata direttamente al personale del Reggimento Genio Ferrovieri, 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-M_D E12988 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 Nucleo Posta. In tal caso, essa dovrà riportare tale volontà con una dichiarazione sottoscritta e apposta in calce al documento: a esempio "protocollare", seguita dal timbro dell'UO e dalla data. Inoltre, i plichi presentati all'ingresso del Reggimento Genio Ferrovieri (sede dell'AOO-M_D E12988) 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.

## 5.18. DOCUMENTI DI GARE: RICHIESTE DI PRESENTAZIONE E RICEZIONE DELLE OFFERTE

L'art. 40 del D.Lgs 50/2016 prevede, a partire dal 18 ottobre 2018, l'obbligo di uso dei mezzi di comunicazione elettronici nello svolgimento di procedure di aggiudicazione. Molte delle attività relative a tale argomento vengono svolte su piattaforme del MEF o CONSIP, tuttavia alcune di esse vengono effettuate attraverso l'utilizzo del sistema AdHoc.

Allo scopo di consentire una più agevole procedura gestionale viene utilizzata la tipologia documentale "gare" che è idonea alla trasmissione, in sicurezza, delle richieste di presentazione delle offerte.

Tale procedura consta di due macro fasi, ovvero:

- invio della richiesta di presentazione delle offerte;
- ricezione delle offerte da parte delle aziende contattate.

La prima fase, inizia selezionando la tipologia documentale "gare" mediante la quale avviene un'unica predisposizione indicando tutte le aziende interessate, sarà poi il sistema a:

- produrre protocolli diversi;
- effettuare trasmissioni separate;

  per ciascuna azienda interessata allo scopo di garantire la riservatezza della trasmissione stessa affinché ciascuna azienda non possa venire a conoscenza delle altre interessate.

La produzione di protocolli diversi per le comunicazioni prodotte saranno raccordate tra di loro dalla generazione di un "codice pratica" unico per tutti.

Terminate la fase di predisposizione, l'iter successivo sarà quello normale, di qualunque documento predisposto per la partenza dopodiché il sistema effettuerà tutta l'attività prevista in modo automatico:

- protocollazione differenziata;
- generazione del codice pratica univoco;
- apposizione del codice pratica nell'oggetto;
- generazione dell'allegato con l'indirizzo dell'azienda e il codice pratica;
- trasmissione differenziata delle richieste di offerte.

La seconda fase, invece, consente, in completa sicurezza (affinché solo chi è autorizzato, possa accedere al contenuto delle offerte), la ricezione via PEC verso il sistema AdHoc di questa AOO, delle offerte richieste prevenute da parte delle aziende interessate[6].

I passaggi di questa fase possono essere riassunti in 5 punti che sono:

- individuazione del funzionario preposto all'apertura delle "buste" di offerta;
- esportazione della chiave pubblica presente nella carta CMD Multiservizi Difesa del funzionario di cui sopra;
- trasmissione attraverso il sistema, dell'invito a partecipare, comprendente i due certificati di cifrature, le istruzioni di dettaglio e ogni altra informazione utile;
- predisposizione, a cura delle aziende interessate, della documentazione, con la necessità di cifrare i file da trasmettere, secondo le indicazioni ricevute.
- invio della documentazione all'AOO.

La protocollazione delle offerte avverrà nel registro generale in quanto la tipologia documentale gare è selezionabile solo per il flusso in uscita. Al riguardo va evidenziato che gli addetti al protocollo potranno unicamente visionare la PEC dal quale desumere solo che l'azienda mittente ha presentato un'offerta per il codice pratica corrispondente senza alcun accesso alle informazioni riguardanti l'offerta.

## 5.19. ORDINI DEL GIORNO ED ORDINI DI SERVIZIO

Con tale tipologia documentale vengono creati, protocollati e gestiti, all'interno della AOO gli:

- ordini del giorno OdG;
- ordini dei servizi OdS.

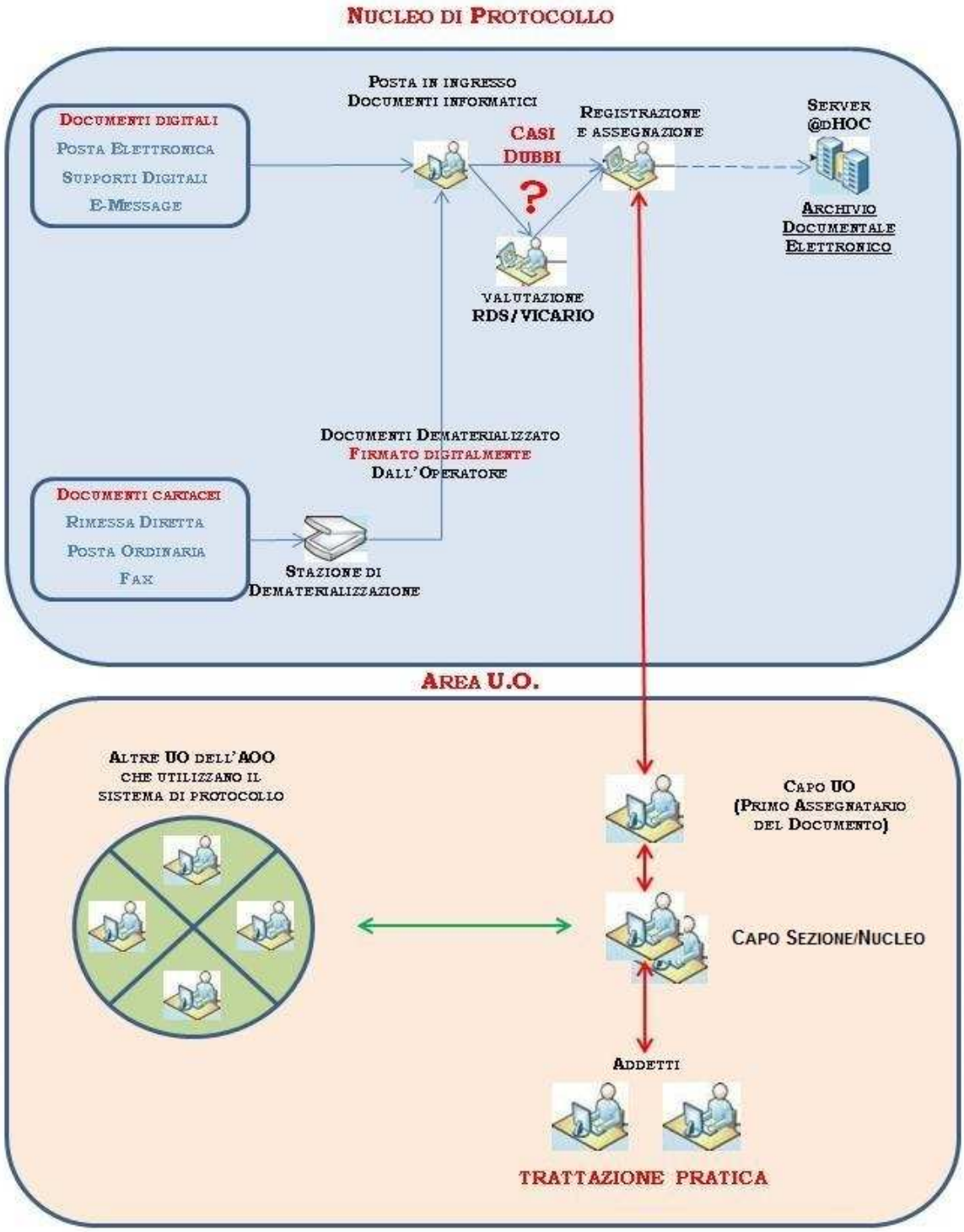
Seppur analoghi tra loro, la tipologia OdG consente la creazione, numerazione progressiva e datazione (in automatico) di un solo documento per giorno mentre la tipologia OdS consente la creazione anche di due o più documenti per giorno.

## 5.20. DECRETI

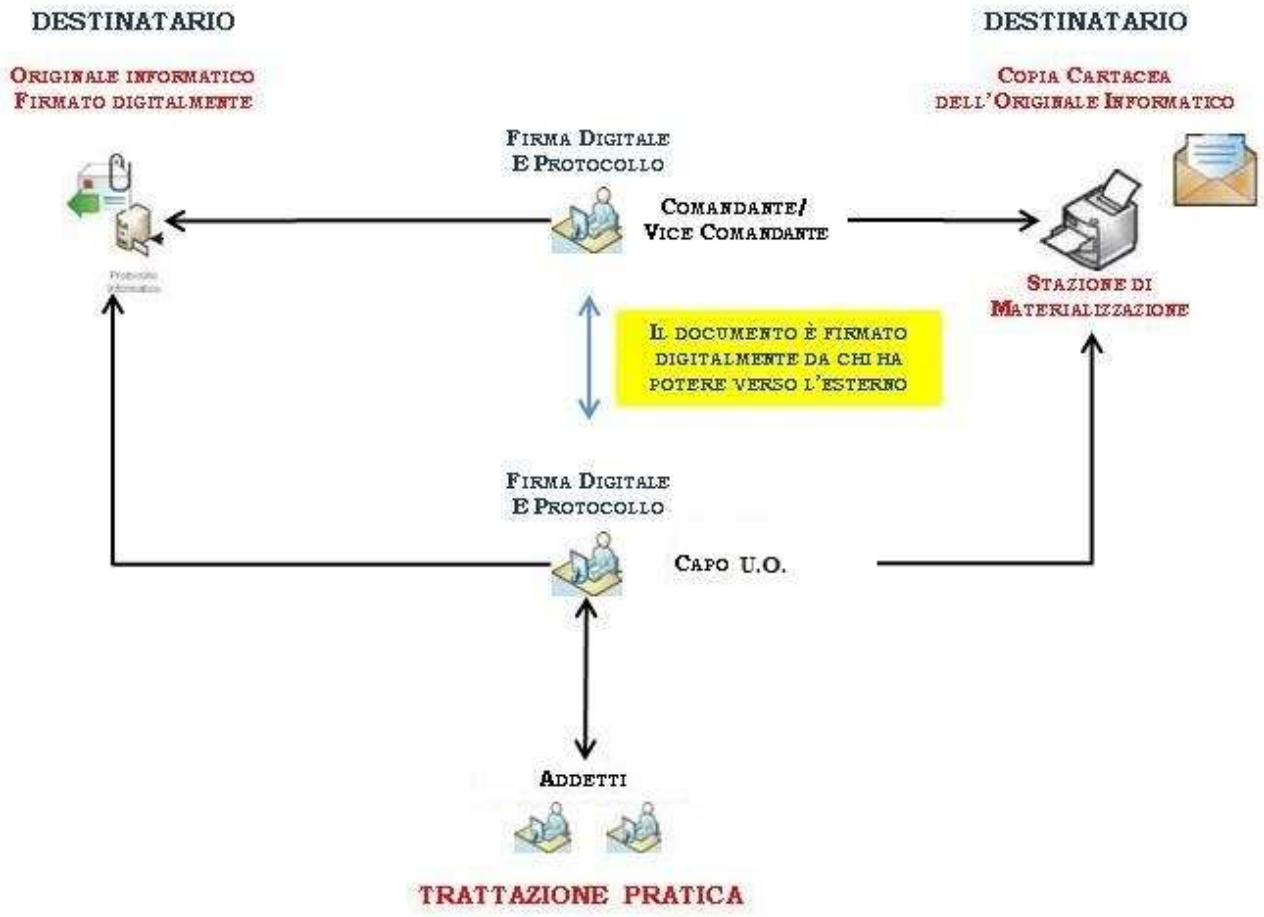
Con tale tipologia documentale vengono creati, protocollati e gestiti, all'interno della AOO i provvedimenti di natura amministrativa-contabile (ad esempio: determinazioni di "fuori uso", decreti ingiuntivi, svincolo cauzioni nell'ambito di gare e contratti, definizione di riscossione somme erogate a vuoto, ecc.)

[6] Le aziende interessate non devono dotarsi di nessun strumento informatico particolare oltre quelli basilari per la gestione delle PEC ad eccezione di un software di gestione di firma digitale fornito da un prestatori di servizi fiduciari relativi alla firma digitale presso l'AGID.

## 5.21. SCHEMA FLUSSO IN INGRESSO



## 5.22. SCHEMA FLUSSO IN USCITA



# 6. MODALITÀ DI PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

## 6.1. 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.

## 6.2. 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 archiviata. 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.

## 6.3. REGISTRO GIORNALIERO DI PROTOCOLLO

Ogni giorno, entro le ore 08:15, il RDS provvede alla generazione, ed alla firma digitale, della stampa delle registrazioni di protocollo relative al giorno precedente. A partire dalla mezzanotte e fino al termine di tale attività, della durata di pochi minuti, non sarà possibile protocollare atti né in uscita né in entrata. La stampa viene archiviata sia su supporto non modificabile esterno all'applicativo che all'interno del sistema stesso ed è sempre possibile effettuarne copie cartacee o digitali.

## 6.4. 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.

## 6.5. 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, se presente, vengono utilizzati dati contenuti nel file segnatura xml, purché conforme alle indicazioni della [CIRC], Sui documenti in uscita la segnatura di protocollo viene impressa sul primo foglio del documento informatico, sul lato sinistro.

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-M_D E12988, conformemente alla normativa, prevede i seguenti dati:

- Codice dell'Amministrazione: M_D
- Codice dell'AOO: E12988
- Identificativo del Registro: REGAAAA
- Numero di protocollo: <progressivo di 7 cifre>
- Data di registrazione: GG-MM-AAAA

Esempio di segnatura di protocollo:
M_D E E12988 REG2019 0000001 01-01-2019

## 6.6. 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.

## 6.7. 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.

## 6.8. 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 E12988 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) e 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.

## 6.9. 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.

## 6.10. 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:

---

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

[8] II 3° livello corrisponde al 3°e 4° livello del Titolario dell'Esercito Italiano che sono stati accorpati per rispondere al requisito del sistema "@dHoc" che prevede la classificazione archivistica fino al terzo livello.

[9] Le 12 voci di 1° Livello: 1-Organizzazione, 2-Pianificazione, 3-Programmazione, 4-Studi, Ricerche e Sviluppo progetti, 5-Gestione delle risorse umane, 6-Gestione delle risorse finanziarie, 7-Gestione delle risorse logistiche, 8-Formazione, Addestramento ed Aggiornamento, 9-Impiego dello Strumento Operativo, 10-Impiego dello Strumento Logistico, 11-Controllo, 12-Pubblica Informazione, Comunicazione e Stampa.

- 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, indicati nell'apposito paragrafo, inoltre:

- la stessa deve essere preceduta da una stringa alfanumerica che identifica l'U.O. originatrice;
- **non devono 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.

# 7. ARCHIVIAZIONE DEI DOCUMENTI

## 7.1. DEPOSITO/ARCHIVIO DELL'AOO-M_D E12988

Sulla base della normativa vigente, per la custodia della documentazione registrata a protocollo, l'AOO-M_D E12988 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 E12988 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 E12988 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.**.

## 7.2. 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 CSIE, che gestisce anche l'applicativo di protocollazione all'AOO-M_D E12988

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.

## 7.3. ARCHIVIAZIONE/CUSTODIA DEI DOCUMENTI ANALOGICI

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

- archivio corrente:
- vi saranno custoditi tutte le cartelle dell'anno corrente e del precedente (due anni), già suddivisi in ordine cronologico fino ad arrivare al secondo anno;

- allo scadere del secondo anno verrà fatta un a valutazione dei documenti da scartare secondo modalità stabilite da ciascuna UO interessata nel rispetto della normativa vigente in materia di conservazione della documentazione amministrativa. I documenti non scartati saranno conservati nell'archivio di deposito.
- archivio di deposito: verranno custoditi tutti i documenti fino al termine previsto dalla normativa in vigore. Alla scadenza del termine, si procederà in aderenza alle direttive emanate in materia dall'Ufficio Storico di Forza Armata.

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.

### 7.4. 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 E12988. 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.

## 8. ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

### 8.1. 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 (username e password) sono del tutto personali e il loro uso ricade sotto la responsabilità di ciascun utente cui sono assegnate**.

### 8.2. 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;
- USERNAME: identifica l'utente mediante i dati personale (nominativo, luogo di nascita, ecc.);
- PASSWORD: stringa segreta e riservata dell'utente che, in combinazione con il ruolo, consente di accedere al sistema. Essa è associata allo USERNAME.

Al riguardo, fermo restando la predisposizione del sistema all'accesso con RUOLO e PASSWORD, per motivi di sicurezza l'accesso al sistema è consentito esclusivamente con la carta CMD. Pertanto, sono stati momentaneamente sospesi gli accessi con RUOLO e PASSWORD;

Il RDS, avvalendosi di una utenza privilegiata (amministratore di sistema), assegna agli utenti diversi livelli di autorizzazione; tali utenti, una volta identificati, sono suddivisi secondo diversi profili di accesso, 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 USERNAME.

## 8.3. 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 quanto sopra è necessario ricorrere allo strumento della delega 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 degli addetti, 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 E12988, che ha necessità 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 ai diretti interessati, quando possibile, o ad altri utenti temporaneamente autorizzati dal RDS.

## 8.4. PROFILI D'ACCESSO

Nell'ambito dell'AOO-M_D E12988 la struttura degli accessi prevede la realizzazione di una serie di profili sulla base della struttura ordinativa e delle rispettive competenze.

I principali profili 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;
- 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] [GDPR];
- 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; risulta infatti possibile 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 previa formale richiesta del responsabile della UO di riferimento.

# 9. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

## 9.1. 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 interruzione del funzionamento del sistema informatico, predisposte tenendo in considerazione quanto scritto in precedenza.

## 9.2. 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 dell'interruzione di 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)

## 9.3. ATTIVITÀ POSSIBILI DURANTE L'ATTIVAZIONE DEL REGISTRO DI EMERGENZA

Durante il periodo di interruzione del 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 tale 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.

### 9.4. 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 dichiarazione del 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 finale: _____ 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.

## 10. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

### 10.1. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE DI GESTIONE

Il presente manuale di gestione è predisposto dal 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.

### 10.2. ABROGAZIONE E SOSTITUZIONE DELLE PRECEDENTI NORME INTERNE

Il presente manuale abroga e sostituisce la precedente versione 3.0 dell' 11 agosto 2020 unitamente ad ogni norma interna all'AOO-M_D E12988 che dovesse contrastare con il contenuto del presente.

## 11. 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;<br>· in maiuscolo il cognome e il primo carattere del nome;<br>· 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;<br>· usare sigle, in maiuscolo o senza punti o, in alternativa, denominazioni ridotte;<br>· la forma societaria va in minuscolo senza punti;<br>· 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;<br>· esempio: ASS. NAZ. PARACADUTISTI D'ITALIA. |
| Ministeri | · Usare la forma ridotta;<br>· 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;<br>· esempio: ISTAT. |
| Virgolette e apici | · Digitare il carattere direttamente dalla tastiera;<br>· non eseguire la funzione copia e incolla di Windows. |
| Date | · Usare il seguente formato numerico: GG-MM-AAAA;<br>· 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 Genio Ferrovieri

| | | |
|---|---|---|
| 0 | COMANDANTE | |
| 1 | UFFICIO MAGGIORITÀ’ E PERSONALE | |
| 3 | UFFICIO O.A.I. | |
| 4 | UFFICIO LOGISTICO | |
| 5 | UFFICIO AMMINISTRAZIONE | |
| 6 | UFFICIO PROGETTI E DIREZIONE LAVORI | |
| 7 | BATTAGLIONE GENIO FERROVIERI | |
| | 1 | COMPAGNIA ARMAMENTO E PONTI |
| | 2 | COMPAGNIA ESERCIZIO |
| | 3 | COMPAGNIA ATTREZZATURE SPECIALI E COSTRUZIONI |
| | 4 | COMPAGNIA VIABILITÀ' E LAVORI IN TERRA |
| 8 | COMPAGNIA COMANDO E SUPPORTO LOGISTICO | |
| 9 | COMANDO ALLA SEDE | |
| 10 | SERVIZIO PREVENZIONE E PROTEZIONE | |
| 11 | SERVIZIO SANITARIO | |
| 12 | SOTTUFFICIALE DI CORPO | |
| 13 | *CO.BA.R. n.8* | |
| 14 | SALA OPERATIVA[10] | |
| 15 | *R.S.U.* | |
| 16 | *SMISTATORE* | |

[10] U.O. attivabile per le esigenze istituzionali di Forza Armata

Allegato“B”

## Personale incaricato dell’erogazione e gestione del servizio

**Responsabile del Servizio**: Magg. Salvatore Antonino IANNUZZO.

**Vicario del RDS**: 1° Lgt. Antonio PECORELLA

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.

**Amministratori di Sistema**: Serg. Magg. Alessandro CARFAGNA;

C.le Magg. Ca.Sc. Angelo IGLINA;

C.le Magg. Sc. Antonino LA ROSA.