10° REGGIMENTO GENIO GUASTATORI

Via Brescia 189, 26100 Cremona
PEC: rgtgua10@postacert.difesa.it – PEI: rgtgua10@esercito.difesa.it

MANUALE DI GESTIONE

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

(ai sensi dell'art.3 e 5 del D.C.P.M. 3 dicembre 2013)

Area Organizzativa Omogenea:
10° REGGIMENTO GENIO GUASTATORI
(identificativo: M_D E22045)

2020

Versione 1.0 del 08.09.2017	Elaborato da	Approvato da
Pag.1 di 44	IL RESPONSABILE DEL SERVIZIO Ten.Col. Franco CICOGNA caufmgtpers@rgtgua10.esercito.difesa.it	IL COMANDANTE Col. Giovanni BRAFA MUSICORO

INDICE

Elenco degli allegati

PAGINA NON SCRITTA

10° REGGIMENTO GENIO GUASTATORI

ATTO DI APPROVAZIONE

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

Esso è stato redatto in conformità al Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 recante: Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione digitale di cui al decreto legislativo n.82 del 2005.

Il presente manuale entra in vigore in data 27.07.2020.

Cremona, lì 27 Luglio 2020

IL COMANDANTE
Col. Giovanni BRAFA MUSICORO

Firmato Digitalmente da/Signed by:
GIOVANNI BRAFA MUSICORO
Comandante di reggimento
In Data/On Date:
lunedì 27 luglio 2020 17:36:11

PAGINA NON SCRITTA

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

NR.	DATA	DESCRIZIONE

ELENCO DI DISTRIBUZIONE

UFFICI	N° COPIE
AIUTANTE MAGGIORE IN 1^	1
UFFICIO MAGGIORITA' E PERSONALE	1
UFFICIO OPERAZIONI ADDESTRAMENTO ED INFORMAZIONI	1
UFFICIO LOGISTICO	1
SEZIONE COORDINAMENTO AMMINISTRATIVO	1
COMANDO ALLA SEDE	1
ASSISTENTE SPIRITUALE	1
COBAR	1
UFFICIALE CIS	1
COMANDANTE COMPAGNIA COMANDO E SUPPORTO LOGISTICO	1
COMANDO BATTAGLIONE "TICINO"	1
COMANDANTE 1^ COMPAGNIA GUASTATORI	1
COMANDANTE 4^ COMPAGNIA GUASTATORI	1
COMANDANTE 5^ COMPAGNIA GUASTATORI	1
COMANDANTE 6^ COMPAGNIA SUPPORTO ALLO SCHIERAMENTO	1
UFFICIO GESTIONE PROTOCOLLO INFORMATICO	1
CUSTODE COMSEC	1
UFFICIO PROPAGANDA ED INFORMAZIONE	1
RESPONSABILE DEL SERVIZIO PREVENZIONE E PROTEZIONE	1

ACRONIMI

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

AD	**A**mministrazione **D**ifesa
AGID	**Ag**enzia per l'**I**talia **D**igitale
AOO	**A**rea **O**rganizzativa **O**mogenea
AOO-M_D E 22045	AOO del 10° Reggimento Genio Guastatori
[CAD]	**C**odice **A**mministrazione **D**igitale D.Lgs. 7 marzo 2005 n. 82
[CODBCP]	**Cod**ice dei **B**eni **C**ulturali e del **P**aesaggio D.Lgs 22.01.04 n. 41
[CODPRI]	**Cod**ice di **Pr**otezione dei dati personali D.Lgs 30.06.03 n. 196
D.Lgs.	**D**ecreto **L**egislativo
[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 dicembre 2000 n. 445 ("Testo Unico")
EDRC	**E**nti **D**istaccamenti **R**eparti **C**omandi
FA	**F**orza **A**rmata
FDPI	**F**lussi **D**ocumentali e **P**rotocollo **I**nformatico
IPA	**I**ndice delle **P**ubbliche **A**mministrazioni
MdG	**M**anuale di **G**estione
NdP	**N**ucleo per la tenuta **d**el **P**rotocollo informatico, della gestione dei flussi documentali e degli archivi
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
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 PI è piuttosto vasta: vengono qui riportati solo gli atti principali, rimandando ad eventuali richiami all'interno del Manuale per norme di maggior dettaglio.

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. [DPR]
Testo unico delle disposizioni legislative 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 AIPA 7 maggio 2001 n. 28 [CIRC]
Regole tecniche per l'interoperabilità dei sistemi di protocollo informatico.

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

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

Direttiva SMD-I-004 [DIR]
Il protocollo informatico nella Difesa.

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

Decreto Legislativo 7 marzo 2005, n. 82 [CAD]
Codice dell'Amministrazione digitale.

Decreto Legislativo 30 dicembre 2010, n.235
Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n.82 recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n.69.

Decreto del Presidente del Consiglio dei Ministri 3 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 [CAD], 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 servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi". In questo ambito è previsto che ogni amministrazione pubblica individui una o più AOO, all'interno delle quali sia nominato un RDS per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa ([DPR]).

Obiettivo del manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili per gli addetti al servizio e per i soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

Il manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

Il presente documento, pertanto, si rivolge non solo agli operatori di protocollo, ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

Il manuale è articolato in due parti: nella prima vengono indicati l'ambito di applicazione, le definizioni usate e i principi generali del sistema, nella seconda sono descritte analiticamente le procedure di gestione dei documenti e dei flussi documentali.

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 art. 3 e 5 del [DPCM].

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi del 10° Reggimento Genio Guastatori a partire dal 23 Luglio 2020. 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 che lo dota della collocazione logico-funzionale nell'Archivio;
- la fascicolazione del documento che attesta la sua effettiva gestione nell'ambito di un procedimento amministrativo o di un'attività.

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

1.3. DEFINIZIONI E NORME DI RIFERIMENTO

Ai fini del presente manuale si intende per:

- "amministrazione", il 10° Reggimento Genio Guastatori;
- *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 D.Lgs. n.82 del 2005;

- *Area Organizzativa* Omogenea *(AOO),* l'Unità riconosciuta dall'AGID e dotata di un'autonomia documentale*;*
- *Unità organizzativa (UO),* l'Unità di livello inferiore dell'AOO;
- *Responsabile del Procedimento Amministrativo (RPA)*, è il dipendente della PA cui è affidata la gestione del procedimento amministrativo. È il Dirigente dell'unità organizzativa interessata che assegna a sé, oppure a un altro dipendente dell'unità, il ruolo di responsabile del procedimento;
- *Responsabile del 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, 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;
- *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, costituendo, pertanto, la "carta dei servizi" dell'AOO stessa nella quale gli interessati trovano descritte le modalità di gestione del protocollo nei suoi diversi aspetti.
- *Titolario d'archivio*, è lo strumento dell'archivio che serve per dividere la documentazione prodotta o ricevuta da un soggetto in settori e categorie, schematizzando in maniera logica le sue competenze e funzioni. Il titolario utilizzato dalla AOO M_D E22045 è il Titolario d'archivio dell'Esercito Italiano edizione 2006.
- *Classificazione*, è l'azione che permette, attraverso l'uso appropriato del *Titolario d'archivio*, di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata in fase di lavorazione del documento;
  La classificazione è organizzata su tre livelli:
  - titolo
  - classe
  - sotto classe
- *Fascicolo*, insieme minimo di documenti, composto dall'ordinata riunione di carte relativa ad uno stesso argomento o pratica;
- *Fascicolazione*, l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettante pratiche.
- *Fascicolo archiviato*, il fascicolo che ha completato il suo ciclo all'interno della trattazione della pratica;
- *Assegnazione*, l'operazione di individuazione dell'ufficio utente competente per la trattazione della pratica cui i documenti si riferiscono;
- *Archivio*, la raccolta ordinata degli atti inviati, ricevuti o interni all'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti o pratiche sono ordinati e archiviati in modo coerente e accessibile alla consultazione;
- *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 19 febbraio 2004 n. 11);
- *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];

- *Dati sensibili*, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale: art. 4, comma 1, let. d) del [CODPRI];
- *Documento amministrativo*, ogni rappresentazione, comunque formata, dei contenuti di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività pratica dell'Amministrazione;
- *Documento informatico*, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- *Documento analogico*, la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti: art.1, let. P) –bis del [CAD];
- *Firma digitale*, rappresenta l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica. La firma digitale è normativamente, ai sensi della lettera s comma 1 art. 1 d.lgs. 82/2005, un particolare tipo di firma elettronica qualificata e avanzata basata su un certificato qualificato e un sistema di chiavi crittografiche, una pubblica ed una privata, correlate tra loro, che consente al titolare 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. Tale firma si propone di soddisfare tre esigenze:
  - Autenticità: che il destinatario possa verificare l'identità del mittente;
  - non ripudio: che il mittente non possa disconoscere un documento da lui firmato;
  - integrità che il destinatario non possa inventarsi o modificare un documento firmato da qualcun altro;

  Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'art.71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso;
- *Fruibilità di un dato*, la possibilità di utilizzare un dato anche trasformandolo nei sistemi informativi automatizzati di un'altra amministrazione;
- *Impronta di un documento informatico*, la sequenza di simboli binari in grado di identificarne univocamente il contenuto;
- *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;
- *Segnatura di protocollo*, l'apposizione o associazione, all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso;
- *Nucleo operatori flussi documentali*, 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;
- *Busta di trasporto*, il documento informatico che contiene il messaggio di posta elettronica certificata;
- *Log dei messaggi*, il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuta dal gestore;
- *Messaggio di posta elettronica certificata*, un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati;
- *Riferimento temporale*, l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata;

1.4. AREA ORGANIZZATIVA OMOGENEA

E' 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.

Ai fini della gestione dei documenti del 10° Reggimento Genio Guastatori è istituita un'unica Area Organizzativa Omogenea (AOO) denominata **Area Organizzativa Omogenea (AOO) del 10° Reggimento Genio Guastatori**, codice identificativo:

M_D E22045

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;
- **"22045"**, è la seconda parte del codice identificativo dell'AOO, che nel caso specifico è riferito al Codice SISME del 10° Reggimento Genio Guastatori.

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)

Sono un sottoinsieme dell'AOO rappresentato da un complesso di risorse umane e strumentali cui sono affidate competenze omogenee.

Nell'ambito dell'AOO-E22045, 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 in allegato"A"

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

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

Nell' Area Organizzativa Omogenea (AOO-E22045) è istituito un Nucleo per la tenuta del protocollo informatico, e la gestione dei flussi documentali, secondo le disposizioni dell' art. 61 del [DPR].

Alla guida del suddetto servizio è posto il Responsabile del Sistema di protocollo Informatico, della gestione dei flussi documentali e degli archivi (RDS). Egli ai sensi dell'articolo 61 comma 2 del [DPR] è nominato dal Comandate di Reggimento.

Nei casi di vacanza, assenza o impedimento del Responsabile, la direzione del Servizio è affidata al Vicario. In allegato "B" l'elenco del personale incaricato dell'erogazione e gestione del servizio per l' AOO-E22045.

È compito del RDS o in sua assenza del Vicario:

- predisporre ed aggiornare il Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del Manuale (sia sul sito Intranet dell'amministrazione che sul sito http://www.difesa.it/Protocollo/AOO_Difesa/Esercito/Pagine/E22045.aspx);
- abilitare gli utenti dell'AOO all'utilizzo del Sistema di Protocollo e definire per ciascuno di essi il livello di autorizzazioni per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e modifica delle informazioni;
- presiedere alle attività del Nucleo per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi alle dipendenze della stessa AOO;

- garantire il buon funzionamento degli strumenti interni all'AOO e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
- autorizzare, a seguito di motivata richiesta, le eventuali operazioni di annullamento della registrazione di protocollo;
- disporre, a seguito d'interruzione del Servizio per cause tecniche, l'apertura e l'uso del Registro di protocollo di emergenza con gli strumenti e le funzionalità disponibili dal Sistema di protocollo, e ad avvenuto ripristino del Servizio la chiusura del Registro di protocollo di emergenza con relativa importazione dei protocolli creati con il sistema di emergenza;
- 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;
- vigilare sull'osservanza delle disposizioni delle norme vigenti da parte del personale autorizzato e degli incaricati;

1.7. CONSERVAZIONE DELLE COPIE DI RISERVA

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, al termine della giornata lavorativa e comunque non oltre le 24 ore successive , viene riversato a cura degli Operatori dei flussi documentali , nel rispetto della normativa vigente, su supporti informatici per la conservazione.

1.8. RECAPITO DEI DOCUMENTI

L'AOO-E22045 predilige l'invio della corrispondenza in forma telematica alle seguenti caselle di posta elettronica istituzionale:

- posta elettronica ordinaria (PEI): rgtgua10@esercito.difesa.it
- posta elettronica certificata (PEC): rgtgua10@postacert.difesa.it

In alternativa, l'indirizzo postale della documentazione analogica diretta all'AOO-E22045 è:

10° REGGIMENTO GENIO GUASTATORI
Via Brescia, 189 – 26100 CREMONA

La corrispondenza diversamente indirizzata, o diretta a entità non appartenenti all'AOO-E22045, non sarà accettata.

1.9. TUTELA DEI DATI PERSONALI

La documentazione contenente dati personali - comuni, sensibili e/o giudiziari - è gestita in conformità al Regolamento (UE) 2016/679 e del D.Lgs. 196/2003 (Codice di protezione dei dati personali) e la loro trattazione e visione è consentita esclusivamente agli utenti abilitati.
In particolare, in fase di predisposizione di tali documenti gli utilizzatori del sistema sono obbligati ad identificare il documento come contenente dati personali cliccando sull'apposito campo "dati sensibili" Così facendo i documenti saranno visibili nel sistema solo agli utenti parimenti abilitati a tale trattazione.

1.10. ENTRATA IN VIGORE DEL MANUALE

Le regole indicate nel presente manuale saranno applicate a decorrere dal 23 Luglio 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, fatta eccezione per quei registri di protocollazione imposti da altre leggi, direttive, circolari e disposizioni interne.

2.1. PIANO DI ATTUAZIONE

In coerenza con quanto previsto e disciplinato dal presente manuale, tutti i documenti inviati e ricevuti dall'amministrazione sono registrati all'interno del registro ufficiale di protocollo informatico. Pertanto tutti i registri particolari di protocollo sono 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 di un unico registro ufficiale 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

Considerata la particolare modalità di fruizione del servizio di gestione del protocollo, gran parte delle funzioni/responsabilità di sicurezza sono demandate all'erogatore del Sistema di protocollo. All'AOO, in quanto fruitrice del servizio, è demandata la componente "locale" della sicurezza, poiché attraverso la propria organizzazione, nonché le sue misure e le politiche di sicurezza, essa contribuisce a stabilire adeguati livelli di sicurezza proporzionati al "valore" dei dati/documenti trattati.

Il piano di sicurezza:

- si articola, di conseguenza, in due componenti: una di competenza del Sistema di protocollo, una di competenza della AOO;
- si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e i documenti trattati, rispettivamente, nei locali dove risiedono le apparecchiature utilizzate dal Sistema di protocollo e nei locali della AOO;
- si fonda sulle direttive strategiche di sicurezza stabilite;
- definisce:
  - le politiche generali e particolari di sicurezza da adottare all'interno, rispettivamente, del Centro servizi e della AOO;
  - le modalità di accesso al Sistema di protocollo;
  - gli aspetti operativi della sicurezza, con particolare riferimento alle misure minime di sicurezza, di cui al [CODPRI];
  - i piani specifici di formazione degli addetti;
  - le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione formale con cadenza almeno biennale. Esso può essere modificato a seguito di eventi gravi. 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 conservati secondo le vigenti norme e saranno consultati solo in caso di necessità dal RDS e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

In oltre 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-E22045;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi.
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

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;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

I documenti informatici redatti dall'AOO con altri prodotti di *text editor* sono convertiti, all'atto della loro sottoscrizione con firma digitale, nel formato standard (PDF/A), come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale. Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 ("Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici").

3.4. GESTIONE DEI DOCUMENTI INFORMATICI

II sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente. Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

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

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.

Per la gestione dei documenti informatici all'interno dell' AOO, il RDS fa riferimento alle norme stabilite dal responsabile del sistema informativo dell'AGID.

3.4.1. COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente a quella in essere per tutte le attività svolte presso il sistema informatico dell'AOO-E22045 e la cui responsabilità risale al Responsabile Operativo Locale per la Sicurezza ICT del 10° Reggimento Genio Guastatori.

3.4.2. COMPONENTE LOGICA DELLA SICUREZZA

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente, nell'ambito del sistema di protocollo, è stata realizzata attraverso:

- l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico:
  - identificazione, autenticazione ed autorizzazione degli addetti delle AOO e degli operatori dell'erogatore del sistema di protocollo;

- riservatezza dei dati;
- integrità dei dati;
- integrità del flusso dei messaggi;
- non ripudio dell'origine (da parte del mittente);
- non ripudio della ricezione (da parte del destinatario).

– la ridondanza dei sistemi di esercizio.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura "a strati multipli di sicurezza" conforme alle best practices correnti. L'architettura realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione degli addetti delle AOO e degli operatori dell'erogatore del SdP, con le seguenti caratteristiche:

– unico login server per la gestione dei diritti di accesso ai servizi applicativi;
– unico sistema di repository delle credenziali di accesso degli utenti;
– unico database delle anagrafiche contenente tutti i profili di utenza.

La componente della sicurezza logica dell'AOO viene descritta nel regolamento interno di sicurezza ICT redatto dal Responsabile Operativo Locale per la Sicurezza ICT.

3.5. TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti delle AOO alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche. Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario. Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all' interno della AOO o ad altre AOO, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'AOO, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

– accesso all'indice dei gestori di PEC allo scopo di verificare l'integrità del messaggio e del suo contenuto;
– tracciamento delle attività nel file di log della posta;
– gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal [CODPRI]. Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

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

4.1. GENERALITÀ

Per la gestione dei documenti informatici, l'AOO-E22045 dispone di due caselle di posta elettronica[1] istituzionale, una di tipo ordinaria PEI e l'altra di tipo certificata PEC:

[1] In aderenza all'art. 2 comma 3 e all'art. 47 del [CAD], le comunicazioni dirette all'AOO-E22045, 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.

- posta elettronica ordinaria PEI: rgtgua10@esercito.difesa.it
- posta elettronica certificata PEC: rgtgua10@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 deve essere riportato nell'omonimo campo del messaggio e non deve riportare caratteri speciali quali [, /, °, ^, virgolette, apici ecc..;
- i nomi dei file allegati devono essere privi di caratteri speciali, accenti e interpunzioni. In alternativa a tali caratteri si suggerisce di utilizzare il carattere _ (underscore). Esempi di file validi: richiesta_di_riscatto.pdf, foto_esercitazione.jpg, variazione_dell_utenza.pdf; mentre, non vanno bene nomi come: è il 1° documento.pdf, oppure, si.trasmette.domanda.pdf, o ancora, questa è la mia domanda per entrare a far parte dell'esercito.pdf;
- gli allegati al messaggio devono avere preferenzialmente l'estensione PDF/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 nei formati ZIP o RAR;
- 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_E E22045 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. 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;

Inoltre, in conformità all'art. 38 comma 3 del [DPR], potranno essere inviate telematicamente all'AOO-E22045 istanze sottoscritte, digitalizzate, e presentate unitamente a copie non autenticate di documenti d'identità dei sottoscrittori.

[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],

- 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 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 (fino a querela di falso della provenienza delle dichiarazioni da parte di chi ha sottoscritto il documento);
- soddisfa il requisito legale della forma scritta (art. 21 del [CAD]).

[3] 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.

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 che il corrispondente ne chieda esplicitamente l'impiego.

4.8. ARCHIVIAZIONE DEL DOCUMENTO INFORMATICO

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

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, la totale corrispondenza indirizzata al 10° Reggimento Genio Guastatori viene registrata in un unico punto (Nucleo Protocollo Informatico) situato presso l'Ufficio Maggiorità e Personale;
- delega alle UO-Articolazioni che hanno facoltà di trasmettere direttamente i documenti sia informatici sia analogici all'interno dell'AOO.

I documenti in ingresso alla AOO , in seguito alla registrazione, saranno assegnati, entro la giornata di ricezione, all'Aiutante Maggiore in 1ª, il quale provvederà ad inoltrare gli stessi ai Capi delle UO interessate (Responsabili del Procedimento Amministrativo) che provvederanno 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 08:00 alle ore 16:30;
- venerdì dalle ore 08:00 alle ore 12:00.

Per i documenti in uscita, il servizio di protocollazione sarà fruibile per l'intero arco della giornata.

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". La posta classificata erroneamente pervenuta al Sistema di protocollo sarà consegnata al Punto Controllo del Comando.
Inoltre, a mente dell'art. 53 comma 5 del [DPR], sono esclusi dalla registrazione di protocollo:

- le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione;
- le note di ricezione delle circolari e altre disposizioni;
- i materiali statistici, i giornali, le riviste e i libri;
- i materiali pubblicitari, gli inviti a manifestazioni;
- documenti già soggetti a registrazione particolare dell'Amministrazione;
- fogli di viaggio;

- documentazione caratteristica;
- registro delle presenze;
- modelli 730;
- licenze, permessi;
- esposti anonimi;

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'Aiutante Maggiore in 1ª, ovvero, essere inviati in un apposito elenco gestito dal RDS qualora siano rilevate anomalie.

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

In particolare, il sistema prevede sette casi pre-impostati per i quali l'RDS invia al mittente il messaggio:

- il messaggio è corrotto o uno dei documenti non è leggibile;
- dati non congruenti nella segnatura informatica;
- segnatura non conforme alla circolare AIPA/CR/28 7 maggio 2001;
- 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 PEI.

5.7. MESSAGGI IN ARRIVO SULLA POSTAZIONE E-MESSAGE

I messaggi telegrafici indirizzati al Comando del 10° Reggimento Genio Guastatori ed ai suoi Uffici sono **tutti** ricevuti sulla postazione "E – Message" del Comando.

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 all'Aiutante Maggiore in 1ª.

5.8. DOCUMENTO INFORMATICO IN USCITA

Come già segnalato in precedenza tutta la documentazione amministrativa dell'AOO è originata e/o gestita in forma elettronica.
A seguito della formazione degli atti, i Capi Ufficio delle UO provvedono al loro perfezionamento, attraverso le funzioni del sistema, inoltrando gli stessi alle uniche figure che hanno facoltà di firma, quindi di assumere a protocollo, i documenti in uscita dalla AOO, ovvero il Comandante di Reggimento e il Capo Sezione Coordinamento Amministrativo (per i soli atti amministrativi).
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.

Cremona, 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:

- Capo Ufficio dell'UO;
- Capo della Sezione che ha predisposto l'atto.

Dopo la firma di tale attestazione il documento primario e gli eventuali allegati vengono spediti all'indirizzo postale del corrispondente, secondo le usuali procedure analogiche.

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

- nella denominazione dei file non si devono utilizzare caratteri speciali, interpunzioni e/o lettere accentate (esempi di caratteri da non usare: /'°,.^);
- 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")**;
- inviare il messaggio al Comandante di Reggimento, il quale apponendo la firma digitale e la marcatura temporale assumerà a protocollo il messaggio;
- inoltrare il documento a tutti gli indirizzi indicati in sede di predisposizione.

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

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

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

Nel caso in cui fra i destinatari compaia una lista AIG (Address Indicator Group) e l'inserimento di tutti gli indirizzi nella rubrica di "Adhoc", o la loro selezione, risulti troppo laboriosa si può provvedere a registrare il codice identificativo dell'AIG (es.: AIG 2395) nella tabella degli indirizzi, senza associare ad esso altri dati (indirizzi postale, e- mail, ecc.).
Il Nucleo protocollo informatico **non effettua attività di gestione della corrispondenza in uscita** dall'AOO **tramite E-Message**.

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 Capo Ufficio 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-E22045 o con indirizzo diverso dal seguente:

10° Reggimento Genio Guastatori
Via Brescia, 189 – 26100 CREMONA

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 della corrispondenza in ingresso da parte del personale dell'agenzia delle Poste Italiane e/o corrieri civili/militari al Sottufficiale d'Ispezione in orario di servizio o Ufficiale / Sottufficiale di Picchetto fuori dall'orario di servizio.

Per quanto attiene alla corrispondenza soggetta a protocollazione che dovesse giungere direttamente alle UO, essa sarà consegnata al Nucleo Posta preferibilmente nella stessa giornata di ricezione, altrimenti dovrà riportare in calce: la data e l'ora in cui è stata consegnata per la protocollazione, seguita dalla sigla dell'UO.

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

5.12.1. POSTA RACCOMANDATA E ASSICURATA

La posta raccomandata verrà ritirata dal Sottufficiale d'Ispezione in orario di servizio o Ufficiale / Sottufficiale di Picchetto fuori dall'orario di servizio.
La corrispondenza raccomandata verrà segnata su un apposito registro dal personale di servizio e consegnata tempestivamente al Nucleo posta dell'Ufficio Maggiorità e Personale.

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 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;

d. apposizione della firma digitale sui documenti così elaborati da parte del medesimo operatore responsabile dell'inserimento dei dati di cui al precedente punto c).
   Tale operazione attesta la conformità della copia per immagine al documento cartaceo originale e consente la contestuale protocollazione e assegnazione dei documenti stessi.
   Ogni documento cartaceo potrà essere accompagnato da allegati informatici memorizzati su CD, DVD e supporti con connessione USB. Tali allegati devono rispondere alle medesime regole di comunicazione indicate al precedente capitolo.
   Quando possibili, anche gli allegati informatici saranno importati nel sistema e associati al documento primario di appartenenza, subito dopo il processo di scansione di quest'ultimo.
   I **supporti fisici** degli allegati informatici **non saranno restituiti al mittente** poiché parte integrante dei rispettivi documenti cartacei. Inoltre, non saranno accettate tipologie di supporto fisico diverse da quelle menzionate.
   Il documento analogico originale è custodito nell'archivio istituito presso ciascuna UO che sarà direttamente responsabile della corretta conservazione. Compatibilmente con il

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

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 paragrafo inerente il documento informatico in uscita.

5.15. FAX

Con l'Art. 31, D.Lgs. 30 dicembre 2010, n.235, sono state soppresse le parole "*, ivi compreso il fax*" dal comma 1 dell'art.45 del CAD recante informazioni relative alla trasmissione informatica dei documenti, escludendo pertanto il fax dai mezzi aventi valore giuridico di trasmissione.

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 10° Reggimento Genio Guastatori 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-E22045 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 10° Reggimento Genio Guastatori (sede dell'AOO-E22045), indirizzati nominativamente al personale dell'AOO-E22045, dovranno essere ritirati all'ingresso dai diretti interessati o da loro delegati che saranno contattati dal personale ivi in servizio.

5.18. APPUNTI E NOTE

Nelle more del rilascio dello specifico modulo del sistema di PI, deputato alla gestione degli appunti/note, tale documentazione può essere predisposta mediante l'utilizzo di una procedura che permette di gestire appunti/note e il carteggio loro associato (allegati, lettere alla firma, ecc.) limitando la produzione di documentazione cartacea.

La procedura di cui sopra è articolata in due fasi:

a. **Predisposizione**
   Utilizzando la funzione "Predisposizione" viene redatto l'appunto (in formato DOC o RTF), completo degli allegati, avendo cura di:
   - nominare i singoli file in maniera da renderli facilmente riconoscibili;
   - selezionare il corpo dell'appunto come documento primario;

- spuntare la casella “No PDF” in particolare per le lettere alla firma (sempre in formato DOC, RTF), che potrebbero subire modifiche durante l’iter;
- selezionare, quale unico destinatario, l’Ufficiale immediatamente inferiore in linea gerarchica all’autorità cui l’appunto è destinato (per approvazione o informazione): sarà quell’Ufficiale destinatario a ricevere sulla propria scrivania l’appunto, di ritorno dopo la firma.

L’appunto così predisposto viene inviato sulla linea gerarchica ascendente; durante l’iter, ciascuno degli aventi causa può apporre le proprie decretazioni nel campo note, correggere i documenti, rimandarlo indietro per approfondimenti e revisioni, inoltrarlo all’autorità superiore.

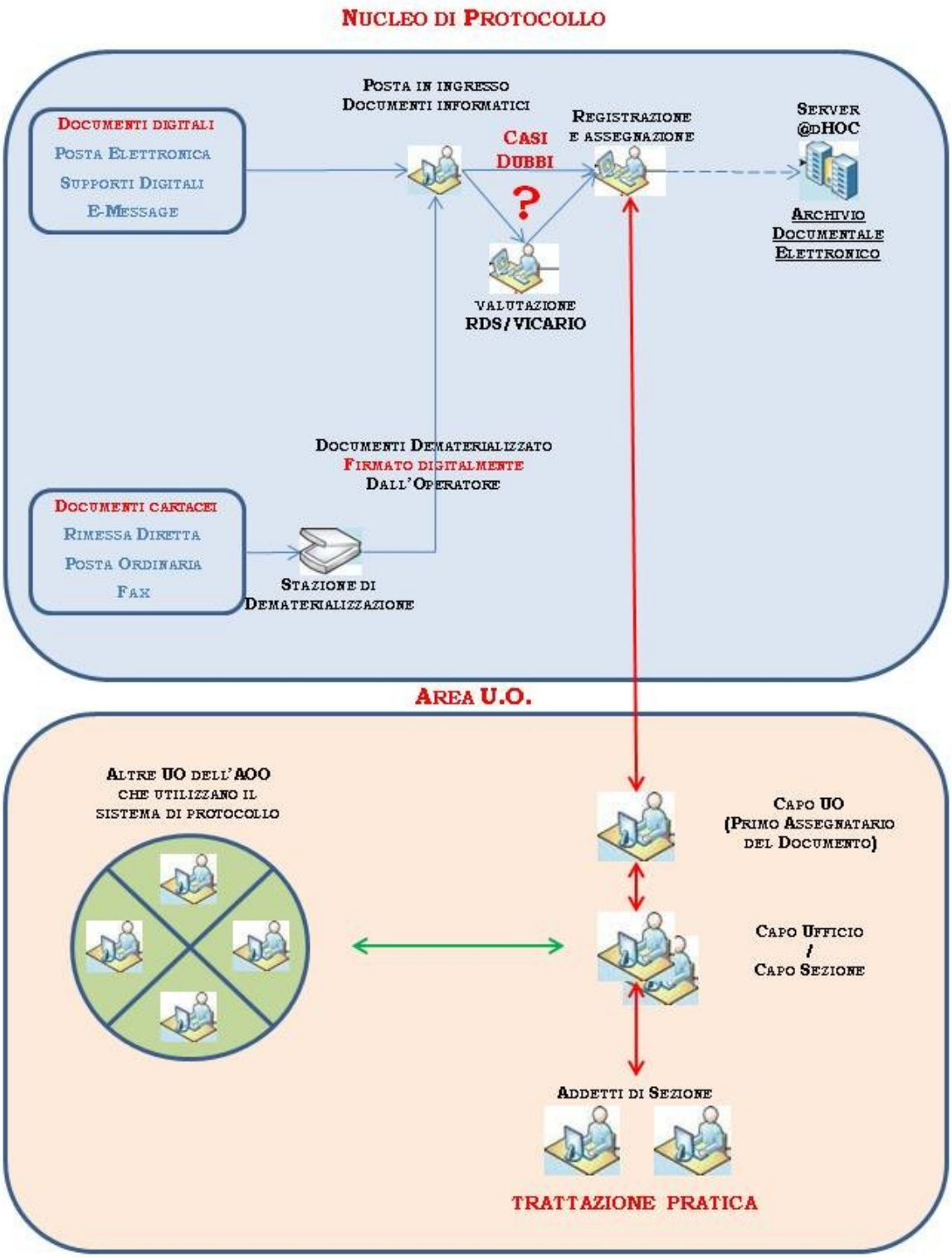
Completato l’iter l’appunto viene firmato digitalmente per l’approvazione (o per la presa visione in caso di appunto “per informazione”): contestualmente il documento viene protocollato, inviato al destinatario (precedente quarto alinea) e visibile (evidenziato, ora, in verde) sulla scrivania dell’operatore che ne ha curato la predisposizione.

b. Seconda fase

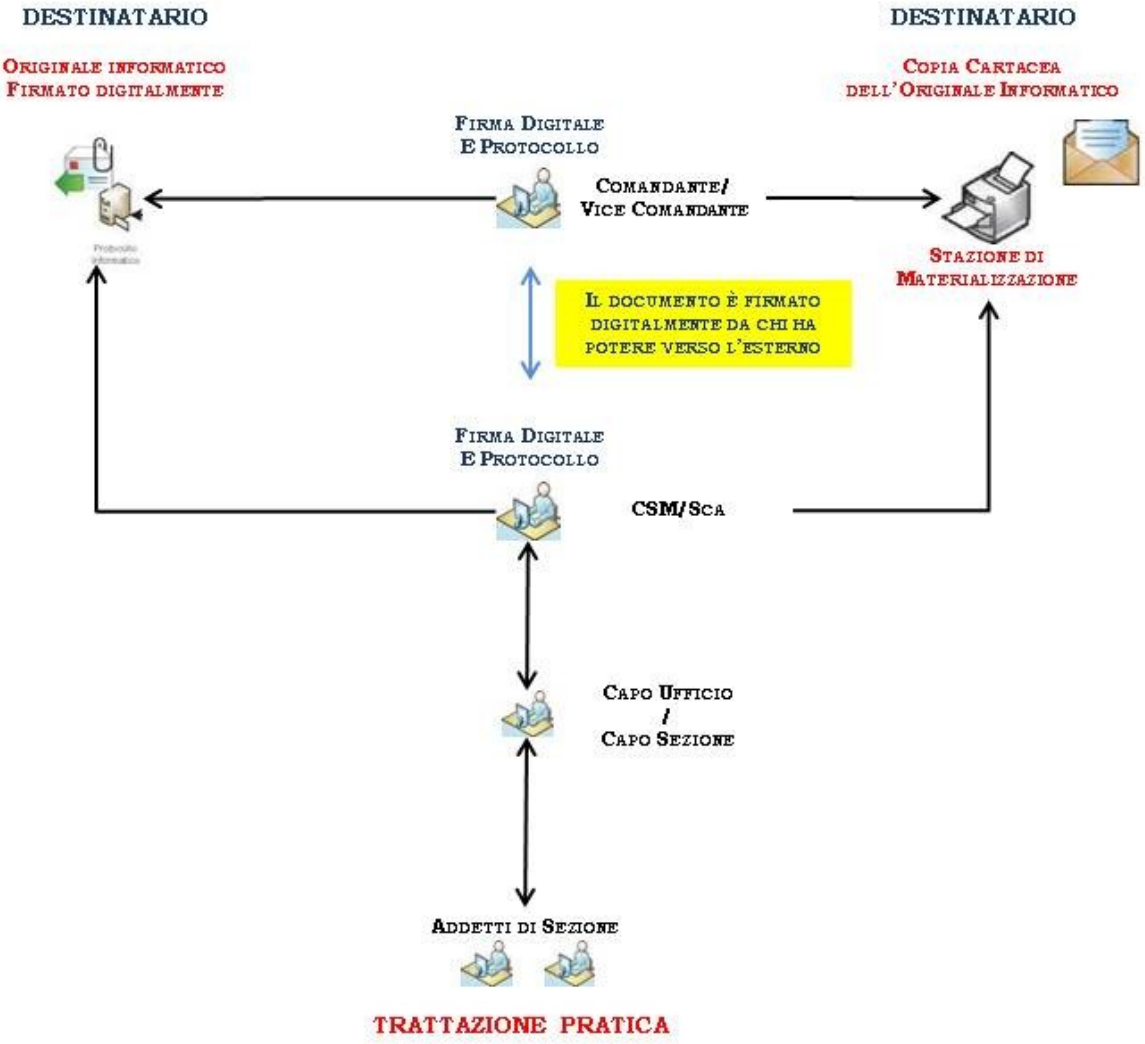
L’Ufficiale che riceve il documento firmato può inoltrarlo, dopo aver apposto eventuali ulteriori decretazioni, al personale che ne curerà:

- la fascicolazione e l’archiviazione, nel caso in cui non siano necessarie azioni ulteriori;
- la predisposizione della eventuale lettera da inviare, avendo cura di:
  - preparare un nuovo documento con cui inviare la lettera alla firma, mediante la funzione “Predisposizione”;
  - selezionare i destinatari della lettera (N.B.: stavolta sono i “veri” destinatari della comunicazione);
  - estrarre la lettera da inviare dall’appunto firmato (in tal modo si ha la sicurezza di avere l’ultima versione, contenente tutte le eventuali correzioni effettuate ai vari livelli durante l’iter procedurale);
  - provvedere a mantenere traccia dell’appunto originatore inserendolo fra i “File accessori” ovvero citandone gli estremi di protocollo nel campo note;
  - inoltrare il documento sulla linea gerarchica, per la firma digitale (che, al solito, ne determinerà assunzione a protocollo e invio).

5.19. SCHEMA FLUSSO IN INGRESSO



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

6.3. REGISTRO GIORNALIERO DI PROTOCOLLO

Ogni giorno, il RDS o il Vicario RDS provvede alla generazione, ed alla firma digitale, della stampa delle registrazioni di protocollo relative al giorno precedente. Questa procedura si avvia in automatico per mezzo del sistema HSM (Hardware Secure Mode) che provvede ad effettuare la firma a norma di legge del registro di protocollo. 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 a cura degli operatori flussi documentali 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.

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-E22045, conformemente alla normativa, prevede i seguenti dati:

- Codice dell'Amministrazione: M_D
- Codice dell'AOO: E22045
- Identificativo del Registro: E22045AAAA
- Numero di protocollo: <progressivo di 7 cifre>
- Data di registrazione: gg-mm-aaaa

Esempio di segnatura di protocollo:
M_D E22045 E20452017 1234567 21-01-2017

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.

E' cura del RDS autorizzare i ruoli che possono effettuare le operazioni di annullamento delle registrazioni di protocollo;
Dalla visualizzazione del 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 tramite mail.

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-E22045 ricalca il "Titolario di archivio dell'Esercito Italiano"[5], 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[6], in particolare:

- il 1° livello del Titolario **(titolo)** individua 12 voci funzionali[7], corrisponde ad aggregazioni di funzioni e si indica con il numero arabo;
- il 2° **(classe),** 3° **(sottoclasse)** livello del Titolario corrispondono alle successive articolazioni, mediante l'associazione alle suddette funzioni di 1° livello, delle rispettive sotto-funzioni e/o attività e/o materie di pertinenza, individuate mediante una preventiva analisi di studio del modello di Ente militare di riferimento. Si individuano anch'essi con il numero arabo.

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

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

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

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 archivio.

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

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

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

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

[6]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.

[7]**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

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 vengono creati di volta in volta da utenti appositamente abilitati alla apertura, gestione e chiusura dei fascicoli.
L'RDS, sentito il parere dei Capi UO, abiliterà uno o più utenti per ogni singola UO.
Gli utenti abilitati alla creazione dei fascicoli accedendo alla funzione *apertura fascicolo* nella voce di menù *archivio* dovranno indicare la classificazione a cui il fascicolo sarà associato.
Il sistema, sulla base di tale informazione, predisporrà l'identificativo del fascicolo, con la seguente sintassi:
ANNO di creazione-CodiceTitolo/CodiceClasse/CodiceSottoclasse.numeroProgressivo
A titolo esemplificativo un fascicolo avrà il seguente formato: 2017- 1/10/5.20.

Per quanto attiene alla descrizione occorre attenersi alle regole generali di scrittura dei dati, indicate nell'apposito paragrafo, inoltre appare opportuno evidenziare che **non possono essere creati fascicoli con denominazione generica come ad es. "Varie"**.

Per quanto riguarda la creazione dei sottofascicoli vale la stessa procedura di quanto descritto per la creazione dei fascicoli.
Per maggiori dettagli si rimanda al bollettino per gli utenti del Sistema di Protocollo Informatico e Gestione Documen tale ADhOC n. 22 rilasciato in data 26 aprile 2017.

7. ARCHIVIAZIONE DEI DOCUMENTI

7.1. DEPOSITO/ARCHIVIO DELL'AOO-E22045

L'AOO-E22045 produce esclusivamente originali informatici e, inoltre, tutti gli atti cartacei pervenuti vengono dematerializzati e convalidati.

Pertanto, l'universalità dei documenti originali afferenti all'AOO-E22045, 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. e conservati presso l'archivio centralizzato nelle modalità previste dal "REGOLAMENTO PER L'ARCHIVIO CENTRALIZZATO"**

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 COMC4EI, che gestisce anche l'applicativo di protocollazione all'AOO-E22045.

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.
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:

- Presso l'archivio corrente (a cura di ogni UO) saranno custodite tutte le cartelle dell'anno corrente fino al 31 dicembre dello stesso anno;
- Presso l'archivio centralizzato del 10° Reggimento Genio Guastatori saranno custoditi i documenti dal 1° anno dalla loro creazione fino alla loro prevista conservazione. Al termine della validità di conservazione, il personale archivista sottoporrà la raccolta dei documenti archiviati al Capo Ufficio/C.te di reparto originatore. Verificata l'effettiva perdita di interesse della documentazione il personale archivista procederà alla distruzione in base a quanto previsto dal "REGOLAMENTO PER L'ARCHIVIO CENTRALIZZATO".

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 Sistema di protocollo, in base alle rispettive competenze, hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza.

8.2. ACCESSO AL SISTEMA

Ad ogni utente autorizzato all'accesso sul sistema di gestione documentale AdHOC è assegnata una credenziale composta da:

- RUOLO: la funzione che l'utente ricopre all'interno della UO;
- PROFILO: autorizzazioni concesse al ruolo per svolgere specifiche operazioni;

Per poter accedere al sistema AdHOC esistono due modalità di accesso:

- TRAMITE CMD e PIN CARTA: il sistema riconoscerà tramite CMD e PIN CARTA l'utente che richiede di accedere al sistema. L'accesso al ruolo assegnato all'utente avviene tramite l'associazione dell'anagrafica al ruolo di pertinenza.
- TRAMITE RUOLO E PASSWORD: il sistema riconoscerà l'anagrafica associata a quel ruolo che in combinazione con la password (stringa segreta e riservata all'utente) consente di accedere al sistema.

L'RDS, avvalendosi dei propri collaboratori (amministratori AdHOC), 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, alla propria anagrafica.

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 questo, è necessario ricorrere allo strumento delle deleghe, ogni volta che il titolare di un ruolo si assenti e debba essere sostituito, in quel ruolo, da personale appositamente designato (ad esempio, il Capo Ufficio da uno dei Capi Sezione, ecc.). La gestione delle deleghe risulta di primaria importanza per assicurare la continuità e correttezza dei flussi documentali e, in particolare, per l'apposizione della firma digitale.

Nei periodi di assenza, tali ruoli potranno essere assunti, con le relative funzioni, da altri utenti. 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-E22045 o che a seguito di nuovo impiego presso gli uffici della AOO stessa, che ha bisogno di impiegare il sistema di protocollazione, dovrà essere tempestivamente richiedere agli amministratori AdHOC, tramite Ticket alla sezione HelpDesk del sito del 10°Reggimento Genio Guastatori e corredata dal modulo per l'autorizzazione al trattamento dei dati personali, il nuovo ruolo indicando le sue generalità e il profilo utente da assegnargli. Gli amministratori AdHOC previa autorizzazione del RDS provvederanno all'inserimento del nuovo ruolo.
Parimenti, dovrà essere comunicato il personale in via di trasferimento, o di cui si preveda una lunga assenza o che non sarà più impiegato presso quella UO, per sostituirne o disattivarne l'utenza e impedire l'accumulo di pratiche inevase.
In tale situazione, eventuali giacenze dovranno essere verificate a cura dell'UO e riassegnate dai diretti interessati, quando possibile, o da altri utenti temporaneamente autorizzati dal RDS.

8.4. PROFILI D'ACCESSO

Nell'ambito dell'AOO-E22045 la strutturazione degli accessi prevede la realizzazione di una serie di profili sulla base della struttura ordinativa e delle rispettive competenze.
Le principali profilazioni riguardano le funzioni di:

- *amministrazione del sistema,* è assegnata dal RDS ad alcuni collaboratori per la gestione dell'organigramma, dei ruoli e dei profili, nonché la gestione dell'anagrafica utenti;
- *lista dei documenti da materializzare*, consente la stampa dei documenti che per le loro caratteristiche non possono essere inviati per posta elettronica. L'unica postazione designata a tale funzione è l'ufficio protocollo;
- *trasmissione dei documenti*, è assegnata ai titolari di ciascuna UO e ai loro delegati ;
- *predisposizione dei documenti*, consente di preparare gli atti che potranno essere in seguito firmati e trasmessi;
- *consultazione*, consente di cercare documenti memorizzati nell'archivio, di visualizzarne i dati di protocollazione e, se di pertinenza della propria UO, il documento medesimo.
- *accesso alla scrivania*, consente la trattazione dei documenti assegnati in arrivo e quelli predisposti in partenza, per l'eventuale successiva trasmissione;
- *dati sensibili*, da abilitare solo agli utenti che gestiscono atti soggetti al [CODPRI];
- *Capo UO*, è una funzione legata al titolare di ciascuna UO al fine di ricevere la posta di propria pertinenza protocollata in ingresso dal NdP e assegnarla ai propri dipendenti.

I profili ora delineati non vanno considerati esaustivi delle molteplici possibilità fornite dal sistema informatico e, inoltre, è possibile anche creare profili ex-novo che contengano un mix di quelli ora elencati.
L'assegnazione dei profili ed il loro aggiornamento sono stabiliti dal RDS, tale operazione per la sua importanza andando a modificare l'ordinamento delle UO, viene determinata solo ed esclusivamente previo formali richieste dei responsabili delle diverse UO.

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 non funzionamento del sistema informatico, predisposte tenendo in considerazione quanto detto 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 del non funzionamento e il relativo motivo.

APERTURA DEL REGISTRO DI EMERGENZA

Causa dell'interruzione: _____

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

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

Timbro e firma del Responsabile del Sistema di protocollo (RDS)

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

Durante il periodo di non funzionamento del sistema informatico NON sarà comunque possibile protocollare documenti informatici in ingresso, poiché tale attività è strettamente correlata alle funzionalità del sistema stesso.

Se, invece, tra i documenti analogici pervenuti, venisse riscontrato un atto che per la sua rilevanza fosse necessario protocollare immediatamente, si procederà al suo inserimento nel registro di emergenza, provvedendo alla trasmissione del medesimo all'UO di competenza.

Per quanto riguarda la documentazione in uscita, essendo possibile solo attraverso l'apposizione della firma digitale e tramite la posta elettronica, la funzione di registrazione a protocollo non sarà disponibile.

Se vi fosse un atto che per la sua rilevanza dovesse comunque essere trasmesso, verrà prodotto con metodologie alternative dall'UO di competenza e portato all'attenzione del RDS per la relativa protocollazione di emergenza e successiva trasmissione per canali analogici.

Appare evidente che non è conveniente procedere con tali modalità ed è buona norma ridurre al minimo indispensabile l'accesso a tali funzioni.

Vale anche la pena sottolineare che l'eventuale mancato funzionamento del sistema inibisce anche l'accesso all'archivio informatico e alle funzioni di ricerca in generale, determinando il sostanziale blocco operativo dell'AOO.

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 iniziale: _____ Pagina finale n.: _____

Timbro e firma del Responsabile del Sistema di protocollo (RDS)

Dopo la riattivazione sia i documenti in ingresso sia i documenti in uscita protocollati in emergenza, verranno importati all'interno del sistema dall'amministratore ADhOC o suo delegato.

10. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

10.1. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE DI GESTIONE

Il presente manuale di gestione è adottato su proposta del Responsabile del Sistema 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 ogni norma interna all'AOO-E22045 che dovesse contrastare con il suo contenuto.

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; • in maiuscolo il cognome e il primo carattere del nome; • esempio: ROSSI Mario
Titoli di cortesia, nobiliari, ecc.	• sempre omessi.
Nomi di città e di stati	• in lingua italiana, se disponibile.
Nomi di ditte e società	• se riportano nomi di persona valgono le precedenti regole; • usare sigle, in maiuscolo o senza punti o, in alternativa, denominazioni ridotte; • la forma societaria va in minuscolo senza punti; • esempi: BIANCO Giuseppe srl, ACME spa.

Enti della Difesa	• denominazione telegrafica in maiuscolo se disponibile.
Enti e associazioni in genere	• usare sigle, in maiuscolo e senza punti o, in alternativa, denominazioni ridotte; • esempio: ASS. NAZ. PARACADUTISTI D'ITALIA.
Ministeri	• usare la forma ridotta; • esempi: MIN. DIFESA, MIN. INTERNO.
Enti di secondo livello	• esempio: utilizzare MIN. DIFESA Uf. Legislativo e non Ufficio Legislativo del Ministero della DIFESA
Sigle in genere	• in maiuscolo e senza punti; • esempio: ISTAT.
Virgolette e apici	• digitare il carattere direttamente dalla tastiera; • non eseguire la funzione copia e incolla di Windows.
Date	• usare il seguente formato numerico: GG-MM-AAAA; • esempio: 01-01-2016

Allegato "A"

Elenco delle U.O. (Unità Organizzative) per la gestione dei flussi documentali nell'ambito dell'Area Organizzativa Omogenea (AOO):

1	COMANDANTE DI REGGIMENTO
2	AIUTANTE MAGGIORE IN 1^
3	ASSISTENTE SPIRITUALE
4	BATTAGLIONE TICINO
5	1^ COMPAGNIA GUASTATORI
6	4^ COMPAGNIA GUASTATORI
7	5^ COMPAGNIA GUASTATORI
8	6^ COMAGNIA SUPPORTO ALLO SCHIERAMENTO
9	CO.BA.R.
10	COMANDO ALLA SEDE
11	COMPAGNIA COMANDO E SUPPORTO LOGISTICO
12	CUSTODE COMSEC
13	PROPAGANDA E INFORMAZIONE
14	RESPONSABILE DEL SERVIZIO DI PREVENZIONE E PROTEZIONE
15	UFFICIALE SICUREZZA CIS
16	SEZIONE COORDINAMENTO AMMINISTRATIVO
17	UFFICIO LOGISTICO
18	UFFICIO MAGGIORITA' E PERSONALE
19	UFFICIO OPERAZIONI ADDESTRAMENTO ED INFORMAZIONI

Allegato "B"

Personale incaricato dell'erogazione e gestione del servizio

Responsabile del Servizio: Ten.Col. Franco CICOGNA

Vicario del RDS: Serg. Alessandro BRUNO

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 AdHOC: Serg. Alessandro BRUNO (titolare-effettivo presso il Nu.Ge.S.I.)
C.le Magg. Ca. Giulio SANTILLO (1°sostituto – effettivo presso il Nu.Ge.S.I.)