COMANDO MILITARE ESERCITO "SICILIA"

SISTEMA DI GESTIONE DOCUMENTALE

Manuale di Gestione

del Protocollo Informatico

(DPCM 03 dicembre 2013)

ISTRUZIONI PER IL CORRETTO FUNZIONAMENTO DEL SERVIZIO "*ADHOC*"

Edizione 2020

AVVERTENZE

La presente pubblicazione è diramata con la lettera in Annesso I.

ATTO DI APPROVAZIONE

Approvo la pubblicazione del documento "Manuale di Gestione del Protocollo Informatico - Adhoc" – Edizione 2020, che abroga e sostituisce le precedenti versioni.

Palermo,_____

Il Comandante Militare dell'Esercito in Sicilia
Generale di Divisione Maurizio Angelo SCARDINO

Firmato Digitalmente da/Signed by:
MAURIZIO ANGELO SCARDINO

In Data/On Date:
mercoledì 18 novembre 2020 14:18:40

INDICE

ALLEGATI

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

1	
2	
3	
4	
5	

ELENCO DI DISTRIBUZIONE

SEGRETERIA DEL GENERALE COMANDANTE	COPIA N°	"1"
SOTTUFFICALE ADDETTO AL VICE COMANDANTE	COPIA N°	"2"
CAPO DI STATO MAGGIORE	COPIA N°	"3"
SEZIONE COORDINAMENTO AMMINISTRATIVO	COPIA N°	"4"
UFFICIO PERSONALE LOGISTICA E SERVITU' MILITARE	COPIA N°	"5"
UFFICIO AFFARI GENERALI	COPIA N°	"6"
UFFICIO RECLUTAMENTO E COMUNICAZIONE	COPIA N°	"7"
SEZIONE SICUREZZA	COPIA N°	"9"
SEZIONE PROT. INF. E FLUSSI DOC	COPIA N°	"10"
REPARTO DI SUPPORTO GENERALE	COPIA N°	"11"
COMANDO ALLA SEDE	COPIA N°	"12"
UFFICIO DOCUMENTALE	COPIA N°	"13"
CIRCOLO UNIFICATO PALERMO	COPIA N°	"14"
LEGAD	COPIA N°	"15"
SPP	COPIA N°	"16"

Sul sito WEB del Comando è pubblicato analogo documento in formato digitale "pdf".

ABBREVIAZIONI

Per facilitare la consultazione della presente direttiva, si riporta il riepilogo delle abbreviazioni utilizzate all'interno di essa:

AOO **A**rea **O**rganizzativa **O**mogenea
CIRC **Circ**olare AIPA 7 maggio 2001 AIPA/CR/28
CNIPA **C**entro **N**azionale per l'**I**nformatica nella **P**ubblica **A**mministrazione
DPCM **D**ecreto del **P**residente del **C**onsiglio dei **M**inistri 03 dicembre 2013
DPR 445/00 **D**ecreto del **P**residente della **R**epubblica **445/2000**
DPR 428/98 **D**ecreto del **P**residente della **R**epubblica **428/98**
IPA **I**ndice delle **P**ubbliche **A**mministrazioni
Manuale **Manuale** di Gestione
PEC **P**osta **E**lettronica **C**ertificata
PI **P**rotocollo **I**nformatico
RDP **R**egistrazione **d**i **P**rotocollo
RDS **R**esponsabile **d**el **S**ervizio di protocollo informatico
RE **R**egistro di **e**mergenza
RPA **R**esponsabile del **P**rocedimento **A**mministrativo
SDP **S**egnatura **d**i **P**rotocollo
UO **U**nità **O**rganizzativa
UU **U**fficio **U**tente

1. PRINCIPI GENERALI

1.1 Ambito di applicazione e Organizzazione

Il presente manuale di gestione dei documenti è redatto ai sensi degli articoli 3 e 5 del DPCM 03 dicembre 2013. Descrive le regole tecniche per il protocollo informatico e fornisce le istruzioni per il corretto funzionamento del relativo servizio.
Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti amministrativi del ***Comando Militare Esercito "SICILIA" con sede in Palermo, Piazza del Parlamento n. 5*****.**
Su indicazione del Responsabile del Servizio, di seguito sono definiti i tempi, le modalità, le misure organizzative e tecniche relative al protocollo informatico.

1.2 Individuazione dell' Area Organizzativa Omogenea e relative UO

Per la gestione dei documenti l'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) – con codice **E26346** – denominata ***Comando Militare Esercito "SICILIA"*** che è composta dall'insieme di tutte le UO articolati come riportato nell'allegato **"12.3"**
All'interno della AOO il sistema di protocollazione è unico.
Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
Nel medesimo allegato sono riportati la denominazione, il codice identificativo della AOO e l'insieme delle UO che la compongono con la loro articolazione.
All'interno della AOO il sistema di protocollazione è centralizzato per la corrispondenza in entrata, mentre è decentralizzato, per la corrispondenza in uscita, attraverso tutte le UO che svolgono anche i compiti di protocollo.
L'allegato **"12.3"** è suscettibile di modifica in caso di inserimento di nuove UO o di riorganizzazione delle medesime.
Le modifiche sono comunicate al Referente per il Protocollo Informatico della Difesa dal RDS.
Nelle UO sarà utilizzato il medesimo sistema di numerazione di protocollo e l'operatore incaricato dell'attività di protocollazione dovrà essere abilitato dal RDS che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

1.3 Individuazione del Responsabile del Servizio e Compiti

A capo del servizio per la gestione del protocollo informatico è posto un Ufficiale, Dirigente ovvero Funzionario con il compito di gestire il protocollo informatico, i flussi documentali e gli archivi , ai sensi dell'art. 61, comma 2, del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. Nell'allegato **"12.3"**, sono riportati:

- i dati identificativi dell'Area;
- il nominativo del Responsabile del Servizio [art. 61, comma 2, del testo unico];
- il nominativo del Vicario del Responsabile del Servizio nei casi di vacanza, assenza o impedimento di questi [cfr. art. 3, comma 1, lettera b), DPCM 31ottobre 2000];

Al Responsabile del Servizio sono assegnati i compiti di cui all'art. 61,comma 3, del testo unico. In particolare:

- predispone lo schema del manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- attribuisce il livello di autorizzazione per l'accesso alle funzioni del sistema di protocollo informatico, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
- si assicura che le copie dei dati di protocollo e dei documenti archiviati su supporto informatico vengano custoditi in luoghi sicuri e differenti;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 del testo unico e le attività di gestione dell'archivio di cui agli articoli 67, 68 e 69 dello stesso;
- effettua le operazioni di annullamento delle registrazioni di protocollo;
- vigila sull'osservanza delle disposizioni del presente regolamento da parte del personale autorizzato e degli incaricati;
- verifica la corretta apertura e chiusura del registro di protocollazione di emergenza.

Al Responsabile del Servizio compete il costante aggiornamento di tutti gli allegati al presente manuale.

1.4 Tutela dei dati personali

L'amministrazione titolare dei dati di protocollo e dei dati personali – comuni, sensibili e/o giudiziari – contenuti nella documentazione amministrativa di propria pertinenza dà attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 con atti formali aventi rilevanza interna ed esterna.

- Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema protocollo informatico e a trattare i dati di protocollo veri e propri, sono stati incaricati dal titolare dei dati e, se nominato, dal responsabile.
- Relativamente agli adempimenti esterni, l'amministrazione si è organizzata per garantire che i certificati ed i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relativi a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente.

Le regole e le modalità operative stabilite dall'amministrazione sono riportate successiva SEZIONE III " misure di sicurezza adottate".

In relazione alla protezione dei dati personali trattati al proprio interno l'amministrazione dichiara di avere ottemperato a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196 e dal Regolamento (UE) 2016/679 con particolare riferimento:

- al principio di necessità nel trattamento dei dati;
- al diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.

1.5 Casella di Posta Elettronica Istituzionale

L'AOO è dotata di una casella di posta elettronica istituzionale attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità:

- del Servizio di Protocollo per la corrispondenza in ingresso;
- a tutti gli uffici (UO) per la corrispondenza in uscita.

Il Servizio di Protocollo procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta e adotta gli opportuni metodi di conservazione in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.

1.6 Casella di Posta Elettronica Certificata (PEC)

L'AOO è dotata di una casella di posta elettronica certificata per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'indice delle Pubbliche Amministrazioni (IPA). Tale casella costituisce l'indirizzo virtuale della AOO.

1.7 Sistema di classificazione dei documenti

Con l'inizio della attività operativa del protocollo è adottato un unico "Titolario di classificazione", redatto dallo Stato Maggiore dell'Esercito. Si tratta di un sistema logico che suddivide i documenti secondo la funzione esercitata, permettendo di organizzare in maniera omogenea i documenti che si riferiscono a medesimi argomenti o a medesimi procedimenti amministrativi.
L'aggiornamento del titolario avverrà a cura dello Stato Maggiore dell'Esercito.

1.8 ACCREDITAMENTO DELL'AOO ALL'IPA

L'AOO nell'ambito degli adempimenti previsti è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) tenuto e reso pubblico dal CNIPA fornendo le seguenti informazioni che individuano la AOO stessa con l'indicazione:

- della denominazione;
- del nominativo del RDS;
- del nominativo del VICARIO;

- dell'indirizzo della sede principale;
- della casella di posta elettronica certificata.

L'Indice delle Pubbliche Amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati. L'A.D. comunica tempestivamente all'IPA ogni successiva modifica delle credenziali di riferimento e la data in cui la modifica stessa sarà operativa in modo da garantire l'affidabilità dell'indirizzo di posta elettronica.

2. ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

2.1 Piano di attuazione

Con l'entrata in funzione del sistema di gestione informatica dei documenti sono eliminati tutti i sistemi di registrazione dei documenti alternativi al protocollo informatico [cfr. art. 3, comma 1), DPCM 03 dicembre 2013].

Rimangono tuttavia in vigore i registri di protocollo per la corrispondenza **"CLASSIFICATA".**

3. SICUREZZA

3.1 Generalità

Al fine di assicurare la sicurezza del sistema informatico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, si adottano le misure tecniche e organizzative di seguito specificate:

- protezione periferica della intranet dell'AOO;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- piano di continuità del servizio con particolare riferimento alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera;
- gestione delle situazioni di emergenza informatica attraverso l'utilizzo di un server ausiliario nel quale riversare l'ultima copia di backup per il proseguo dell'attività;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service patch) correttivi dei sistemi operativi;

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

3.2 Formazione dei documenti – Aspetti di sicurezza

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 prodotti dall' AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML, e TIFF) 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 una data certa a un documento informatico prodotto all'interno di una 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 del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).
L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'AOO.

3.3 Gestione documenti informatici

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

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette 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 all'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

3.4 Trasmissione e interscambio dei documenti informatici

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 pubbliche amministrazioni, 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'amministrazione, (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/ AOO) oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata 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 di amministrazioni 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 decreto legislativo del 30 giugno 2003, n. 196 e dal Regolamento (UE) 2016/679.

3.4.1 All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).
La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28.

3.4.2 All'interno della AOO

Gli uffici dell'amministrazione (UO) si scambiano i documenti informatici protocollati attraverso l'utilizzo dell'opzione "INVIA AD ALTRO UTENTE".

3.5 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso autorizzato (user id e password) IP basato sulla profilazione degli utenti in via preventiva. La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

3.5.1 Utenti interni all'AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RDS dell'AOO. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione alla registrazione, abilitazione alla trasmissione e alla modifica dei documenti.

3.6 Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene con le modalità e con le tecniche indicate nel DPCM 03 dicembre 2013 Regole tecniche per la conservazione e secondo le indicazioni del Responsabile della Conservazione del Ministero della Difesa.

3.6.1 Conservazione dei documenti informatici e delle registrazioni di protocollo

Il responsabile della conservazione digitale:

- adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale utilizzando gli strumenti digitali;
- assicura il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti in caso di aggiornamento del sistema di conservazione;
- verifica periodicamente, con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati.

4. MODALITA' DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DEI DOCUMENTI

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'AOO.
Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in flussi:

- entrata;
- uscita;
- interno.

Il documento amministrativo, in termini tecnologici, è classificabile in:

- informatico;
- analogico.

4.1 Documento in entrata

Per documenti in entrata si intendono i documenti che hanno rilevanza giuridico-probatoria, acquisiti dall'AOO nell'esercizio delle proprie funzioni. I documenti su supporto cartaceo possono pervenire all'Amministrazione, ritirati o acquisiti dagli addetti al Servizio di protocollo informatico, attraverso:

- Posta Elettronica Certificata (PEC)

- Posta Elettronica Istituzionale (PEI)
- il servizio postale;
- la consegna diretta agli uffici/sezioni (UO);
- Istanze per il personale in quiescenza o comunque non in servizio attivo.

4.2 Documento in uscita

Per documenti in uscita si intendono i documenti che hanno rilevanza giuridico-probatoria prodotti dal personale delle UO nell'esercizio delle proprie funzioni.
La registrazione dei documenti in partenza viene effettuata in automatico dal sistema tramite rilascio della segnatura e firma digitale. Il singolo operatore si occupa della gestione del fascicolo relativo al documento.

4.3 Documento interno

Per documenti interni si intendono i documenti scambiati tra le diverse Unità Organizzative (UO) dell'Area Organizzativa Omogenea (AOO).
I documenti interni di preminente carattere *giuridico-probatorio* sono quelli redatti dal personale nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi, e, come tali, devono essere protocollati secondo le disposizioni previste nelle sezioni seguenti.

4.4 Documento informatico

Per documento informatico si intende il documento elettronico che contiene la rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti (art.1 lettera p-bis CAD). Gli originali dei documenti dell'Amministrazione, inclusi quelli inerenti ad albi, elenchi e pubblici registri, sono formati con mezzi informatici (art. 40 comma 1 CAD). I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato dalla loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione [Allegato 2 DPCM 03 dicembre 2013]

4.5 Documento - cartaceo (analogico)

Per documento cartaceo (analogico) è la rappresentazione non informatica di atti, fatti, o dato giuridicamente rilevanti (Art.1 lettera p-bis CAD).

4.6 Formazione dei documenti – aspetti operativi

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa.
Ogni documento formato per essere inoltrato all'esterno o all'interno in modo formale:

- tratta un unico argomento indicato in maniera sintetica ma esaustiva a cura dell'autore nello spazio riservato all'oggetto;

- è riferito ad un solo protocollo;
- può far riferimento a più fascicoli.

Le firme necessarie alla redazione e perfezione giuridica del documento in partenza possono essere apposte prima della sua protocollazione.
Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabili delle singole UO.
Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della AOO e dell'UO che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione (via, numero, CAP, città, provincia);
- il numero di telefono/fax della UO.

Il documento deve inoltre recare almeno le seguenti informazioni:

- luogo di redazione del documento;
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- se trattasi di documento digitale, firma elettronica avanzata o qualificata da parte dell'istruttore del documento e sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale;

Per agevolare il processo di formazione dei documenti informatici e consentire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'AOO rende disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge.

4.7 Uso della Posta Elettronica Certificata

La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta ed ha **valore legale equiparato ad una raccomandata con ricevuta di ritorno.**

La data e l'ora di trasmissione e ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili a terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.

L'utilizzo della Posta Elettronica Certificata (PEC) consente di:

- conoscere in modo inequivocabile la data e l'ora di trasmissione;

- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema della AOO ricevente. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato.

Il termine "certificata" si riferisce al fatto che il gestore del servizio rilascia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio ed eventuali allegati. Allo stesso modo, il gestore del destinatario invia al mittente la ricevuta di avvenuta consegna.

I gestori certificano quindi con le proprie "ricevute" che:

- il messaggio è stato spedito;
- il messaggio è stato consegnato;
- il messaggio non è stato alterato.

In ogni avviso inviato dai gestori è apposto un **riferimento temporale che certifica data ed ora** di ognuna delle operazioni descritte. I gestori inviano ovviamente avvisi anche in caso di errore in una qualsiasi delle fasi del processo (accettazione, invio, consegna) in modo che non ci siano mai dubbi sullo stato della spedizione di un messaggio. Se il mittente dovesse smarrire le ricevute, la traccia informatica delle operazioni svolte, **conservata dal gestore *Telecompost***, consente la riproduzione, con lo stesso valore giuridico, delle ricevute stesse.

5 DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

5.1 Generalità

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni. Per il flusso pratico dei documenti si rimanda all'allegato **"12.4"** (Regolamento interno sul servizio postale).

5.2 Flusso dei documenti ricevuti dall'AOO

5.2.1 Provenienza esterni dei documenti

I documenti che sono trasmessi da soggetti esterni all'amministrazione sono, oltre quelli richiamati nel capitolo precedente, le istanze, i telegrammi e i supporti digitali rimovibili.
I documenti che transitano attraverso il Servizio Postale sono consegnati quotidianamente al Servizio di Protocollo**.**

L'operazione di protocollazione per i documenti in arrivo (vds. flusso documentale in allegato **"12.5"**) **è effettuata centralmente presso il Servizio di Protocollo Informatico.**

5.2.2 Ricezione dei documenti informatici PEC e PEI

Di norma la ricezione dei documenti informatici è assicurata tramite PEC e PEI che vengono recapitate in maniera informatica al Servizio di Protocollo dell'AOO.
Gli indirizzi PEC e PEI del *Comando Militare Esercito "Sicilia"* sono i seguenti:

- **cmepa@postacert.difesa.it ;**
- **cmepa@esercito.difesa.it .**

Quando i documenti informatici pervengono al Servizio di Protocollo, la stessa unità procede alla registrazione di protocollo.
Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente illustrate.
L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti recanti standard del formato dei documenti, modalità di trasmissione, definizione dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.
Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.
L'addetto protocollatore controlla quotidianamente i messaggi pervenuti nelle caselle PEI – PEC ed E-Message e verifica se sono da protocollare.

5.2.3 Ricezione dei documenti cartacei a mezzo posta convenzionale

I documenti pervenuti transitano attraverso il Servizio Postale che provvede a recapitarle al Servizio di Protocollo.

5.2.4 Errata ricezione dei documenti cartacei

Nel caso in cui pervengano per errore documenti indirizzati ad altre AOO:

a) se la busta non viene aperta e rimane integra, si invia alla AOO corretta;

b) se la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia alla AOO destinataria apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

5.2.5 Attività di protocollazione dei documenti

Superati tutti i controlli precedenti, i documenti sono protocollati e segnati nel protocollo generale secondo gli standard e le modalità dettagliate nel capitolo 10 (Modalità di produzione e di conservazione delle registrazioni di protocollo informatico) del presente manuale.

5.2.6 Ricevute attestanti l'invio e la ricezione dei documenti informatici

L'invio e la ricezione dei documenti comporta l'invio al mittente della ricevuta legata al servizio di protocollazione informatica.

La notifica al mittente dell'avvenuto recapito del messaggio è assicurato dal servizio di posta elettronica istituzionale utilizzato dall'AOO con gli standard specifici.

5.2.7 Rilascio di ricevute attestanti la ricezione dei documenti cartacei

Per i documenti cartacei, consegnati direttamente dal mittente o da altra persona incaricata, viene rilasciata una ricevuta attestante l'avvenuta consegna. il Servizio Postale che lo riceve è autorizzato a:

- fotocopiare la prima pagina del documento;
- apporre sulla copia realizzata il timbro dell'amministrazione con la data e l'ora di arrivo e la sigla dell'operatore.

5.2.8 Conservazione delle rappresentazione digitale di documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine attraverso un processo di scansione.

Il processo di scansione avviene in diverse fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico file;
- verifica della leggibilità e della qualità delle immagini acquisite;
- collegamento delle immagini alle rispettive registrazioni di protocollo in modo non modificabile.

I documenti cartacei dopo l'operazione di riproduzione in formato immagine sono conservati presso l'archivio centralizzato dell'AOO ed inviati solo in formato elettronico alle UO destinatarie.
Gli allegati/annessi particolari (Libretti Personali, Stato di Servizio, elaborati tecnici, ecc.) non vengono riprodotti in formato immagine e, prima dell'inoltro della relativa lettera di accompagnamento, sarà apposta nell'apposito campo l'annotazione: "Allegato analogico" da ritirare presso il Servizio di Protocollo.
Qualora l'UO, nell'espletamento del proprio mandato istituzionale ha necessità di acquisire il documento ricevuto in "originale" potrà richiederlo al competente Servizio Protocollo. Di tale documento viene fotocopiata la prima pagina e sulla copia realizzata è apposto apposito timbro di ricevuta con la data di ritiro e la firma del nominativo cui questi viene consegnato.

5.2.9 Classificazione, assegnazione e presa in carico dei documenti

Gli addetti del Servizio di Protocollo provvedono ad inviare il documento al responsabile dell'UO di destinazione. Quest'ultimo:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore il documento è riassegnato all'UO corretta o al RDS;
- in caso di verifica positiva, provvede a smistare il documento al proprio interno e lo assegna al personale all'uopo preposto per la classificazione, fascicolazione e trattazione.

5.3 Flusso dei documenti inviati dall'AOO

5.3.1 Sorgente interna dei documenti

Per sorgente interna (all'AOO) dei documenti si intende l'unità organizzativa (UO) mittente che invia la corrispondenza nelle forme e nelle modalità più opportune ad altra AOO, ovvero ad altra UO della stessa AOO.

Per documenti in partenza s'intendono quelli prodotti dal personale degli uffici (vds. flusso documentale in allegato **"12.5"**) dell'AOO nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra AOO, ovvero ad altro ufficio (UO) della stessa AOO.

5.3.2 Verifica formale dei documenti

Ogni UO è autorizzata dall'AOO per il tramite del RDS a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita.
Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dalle UO.
Le UO provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.

5.3.3 Registrazione di protocollo e segnatura

La classificazione e la segnatura della corrispondenza in partenza in formato digitale è effettuata direttamente dalle singole UO abilitati in quanto collegati al sistema di protocollo informatico dell'AOO a cui appartengono.
Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatura della missiva da inviare sono effettuate dal personale designato dal responsabile dell'UO.

5.3.4 Trasmissione dei documenti informatici

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta istituzionale

5.3.5 Trasmissione dei documenti cartacei a mezzo posta

L'UO provvede direttamente alla trasmissione "fisica" del documento in partenza e alla spedizione del documento, di norma il giorno lavorativo in cui è stato protocollato.

6. REGOLE DI SMISTAMENTO ED ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

6.1 Smistamento, assegnazione e presa in carico

L'attività di smistamento consiste nell'operazione di recapitare un documento protocollato e segnato ai responsabili di ciascun UO, attraverso funzioni specifiche del sistema di protocollo informatico.
Quest'ultimi, dopo averne preso visione, provvedono ad accettarli ed assegnarli al proprio personale dipendente, oppure in caso di errore a smistare la notifica ad altro UO.
Con l'assegnazione (vds. Allegato **"12.6"**) si provvede al conferimento della responsabilità del procedimento amministrativo ad un soggetto fisico.
Nel caso in cui venga recapitato per errore un documento indirizzato ad altra UO destinataria, lo stesso è inviato dal responsabile ricevente all'UO competente con la seguente decretazione: documento pervenuto per errore - non di competenza di questo Ufficio/Sz. Aut..
Il responsabile dell'UO competente è incaricato della gestione del procedimento a cui il documento si riferisce e prende in carico il documento.
I termini per la definizione del procedimento amministrativo decorrono comunque dalla data di protocollazione.
Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.
La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

6.2 Regole assegnazione documenti

Per assegnazione si intende l'azione di conferimento:

- della Responsabilità del Procedimento Amministrativo ad un soggetto fisico;
- materiale documentario da lavorare.

Successivamente all'assegnazione il RPA esegue l'operazione di presa in carico del documento.
La "presa in carico" dei documenti informatici viene registrata dal sistema di protocollo in modo automatico e la data di ingresso dei documenti nelle UO di competenza coincide con la data di assegnazione degli stessi.

I termini per la definizione del procedimento amministrativo che prende avvio dal documento, decorrono comunque dalla data di protocollazione.
Il sistema di gestione informatica dei documenti tiene traccia di tutti i passaggi, memorizzando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

Lo smistamento iniziale eseguito dal Servizio di Protocollo Informatico, avviene recapitando ai Responsabili di ciascuna UO, attraverso funzioni specifiche del sistema di protocollo informatico, la notizia circa i documenti destinati all'UO medesimo.
Questi dopo averne preso visione, provvedono ad assegnarli o a se stessi o ai propri UU/RPA per la trattazione.

6.3 Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati alle UO competenti al termine delle operazioni di registrazione e segnatura di protocollo.
I destinatari del documento lo ricevono esclusivamente in formato digitale.

6.4 Assegnazione dei documenti ricevuti informato cartaceo

I documenti ricevuti dall'amministrazione in formato cartaceo, *successivamente acquisiti in formato immagine con l'ausilio dello scanner*, una volta concluse le operazioni di registrazione, segnatura e di assegnazione, sono fatti pervenire al personale di competenza attraverso la rete interna (allegati analogici). L'originale cartaceo viene conservato dal Servizio Protocollo e ritirato dall'UO assegnataria tramite il personale designato con segnatura digitale tramite la propria CMD.

Il responsabile dell'UO/UU può visualizzare i documenti, attraverso l'utilizzo dell'applicazione di protocollo informatico e in base alle abilitazioni previste potrà:
- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare come assegnatario il personale competente sulla materia oggetto del documento.

La "presa in carico" dei documenti informatici viene registrata dal sistema in modo automatico e la data di ingresso dei documenti negli Uf./Sz.Aut. di competenza coincide con la data di assegnazione degli stessi.
Il ritiro giornaliero della corrispondenza "annessa/allegata" al documento originale in arrivo da parte delle UO avviene presso il Servizio Protocollo.

6.5 Modifica delle assegnazioni

Nel caso di assegnazione errata, l'UO che riceve il documento comunica l'errore all'operatore che ha erroneamente inoltrato il documento, che procederà ad una nuova assegnazione.
Nel caso in cui un documento assegnato erroneamente ad un UU afferisca a competenze attribuite ad altro UU della stessa UO, l'abilitazione al relativo cambio di assegnazione è attribuita al responsabile dell'UO medesimo o a persona da questi incaricata.
Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

7. UO RESPONSABILI DELLE ATTIVITA' DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI

Il presente capitolo individua le unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e tenuta dei documenti all'interno della AOO in base al modello organizzativo adottato dall'Amministrazione.
Relativamente alla organizzazione e alla tenuta dei documenti dell'amministrazione all'interno dell'AOO è istituito il servizio archivistico per la conservazione dei documenti.

7.1 Servizio archivistico

Il servizio archivistico è funzionalmente integrato nel servizio per la tenuta del protocollo informatico.
Alla gestione del servizio archivistico è preposto personale all'uopo incaricato designato dal Responsabile del Servizio.
Dopo la scansione i documenti cartacei vengono custoditi in raccoglitori settimanali, presso la stessa UO Protocollo.
Per particolari documenti, definiti dal RDS (quali documenti del Servizio Coordinamento Amministrativo, documenti Sanitari, libretti personali, ecc.), ritiro giornaliero a cura delle UO.

8. ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE

8.1 Documenti esclusi

Sono esclusi dalla registrazione i documenti classificati.

9. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

9.1 TITOLARIO O PIANO DI CLASSIFICAZIONE

9.1.1 Titolario

Il piano di classificazione fornito dallo Stato Maggiore Esercito è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'AOO.
Il piano di classificazione si suddivide in voci di titolo, classe, sottoclasse.
L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione.

9.1.2 Classificazione dei documenti

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze dell'Amministrazione (AOO) ed è di competenza dell'UO.

9.2 Fascicoli

9.2.1 Fascicolazione dei documenti

I documenti assunti a protocollo nel Sistema informatico vengono smistati all'UO che a sua volta verranno classificati e riuniti in fascicoli.
Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento.
I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza, sottofascicolo, secondo l'ordine cronologico di registrazione.

9.2.2 Apertura del fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'ente, il soggetto preposto, provvede all'apertura di un nuovo fascicolo su indicazione del Capo UO.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

- indice di classificazione, (cioè titolo, classe, sottoclasse, etc.);
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall' AOO;
- data di apertura del fascicolo;
- template abilitazione della propria UO.

9.2.3 Chiusura del fascicolo

Il fascicolo viene chiuso al termine del procedimento amministrativo, all'esaurimento dell'affare o a termine anno solare.
La data di chiusura si riferisce alla data dell'ultimo documento prodotto.
Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.
Gli elementi che individuano un fascicolo sono gestiti dal soggetto di cui al paragrafo 9.2.2, primo capoverso.

10. MODALITA' DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

10.1 Unicità del Protocollo Informatico

Nell'ambito della AOO il registro di protocollo è unico e la numerazione delle registrazioni di protocollo è unica e rigidamente progressiva.
Essa si chiude al 31 dicembre di ogni anno e ricomincia da 0000001 all'inizio dell'anno successivo.

Il numero di protocollo è costituito da almeno sette cifre numeriche, ai sensi dell'articolo 57 del testo unico.
La numerazione di protocollo è unica, sia per i documenti in entrata, interni, in uscita.

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.
La documentazione che non è stata registrata presso il Servizio di Protocollo viene considerata giuridicamente inesistente presso l'amministrazione.

10.2 Conservazione Registri Giornalieri di Protocollo

Il registro di protocollo è qualificato atto pubblico originario che fa fede, fino a querela di falso, della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità di esso. RDS, qualora non vi sia attivata la modalità di firma automatica HSM, provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno [cfr. art. 53, comma 2, del testo unico].

10.2.1 Registro informatico di protocollo

Al fine di garantire la non modificabilità delle operazioni di registrazione l'integrità del registro di protocollo, il registro viene inviato, seguendo le indicazioni fornite dal Responsabile della Conservazione del Ministero dell Difesa, al Centro di dematerializzazione e conservazione unico della Difesa (CEDECU). Se è attivo il servizio di firma automatica, viene anche firmato digitalmente in modalità automatica.

10.3 Registrazione di Protocollo

Per ogni documento ricevuto o spedito dall'Amministrazione, è effettuata una registrazione di protocollo, consistente nella memorizzazione dei dati obbligatori.

Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive, ai sensi dell'articolo 53, comma 3, del testo unico.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti ***dati obbligatori*** [cfr. articolo 53, comma 1, del testo unico]:

- numero di protocollo, 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 che ha prodotto il documento, registrato in forma non modificabile (codice SISME);
- destinatario o destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- classificazione.

10.3.1 Documenti informatici

La registrazione di protocollo di un documento informatico è eseguita dopo che l'operatore addetto ne ha verificato l'autenticità, la provenienza e l'integrità. Nel caso di documenti informatici in partenza, questa verifica è estesa alla validità amministrativa della firma [cfr. Circolare AGID 23 gennaio 2013 n. 60].

Per i documenti informatici è prevista la registrazione delle stesse informazioni indicate per quelli su supporto cartaceo, con l'aggiunta, tra i dati obbligatori, dell'impronta del documento informatico, generata impiegando la funzione di hash SHA-2 e registrata in forma non modificabile [cfr. articolo 53, comma 1, lettera f), del testo unico].

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio e sia ad uno o più file ad esso allegati [cfr. articolo 18 DPCM 03 dicembre 2013].

Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto [cfr. art. 19 DPCM 03 dicembre 2013].

10.3.2 Documenti analogici (cartacei e supporti rimovibili)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza.

La registrazione di protocollo di un documento analogico cartaceo ricevuto viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.

Nel caso di corrispondenza in uscita o interna, l'UO esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

10.4 Elementi Facoltativi delle Registrazione di Protocollo

I dati facoltativi sono modificabili senza la necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

Di seguito vengono riportati gli elementi facoltativi finalizzati alla conservazione e gestione della documentazione:

- data di arrivo;
- luogo di provenienza, o di destinazione, del documento;
- tipo di documento;
- mezzo di ricezione/spedizione (ordinaria, espressa, corriere, raccomandata, telefax, ecc.);
- numero degli allegati;
- descrizione sintetica degli allegati;
- estremi del provvedimento di differimento dei termini di registrazione;
- mezzo di ricezione o, in alternativa, mezzo di spedizione;
- ufficio di competenza;
- copie per conoscenza.

10.5 Segnatura Di Protocollo Dei Documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo [cfr. art. 55, comma 2, del testo unico].
La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.
Essa consente di individuare ciascun documento in modo inequivocabile.

10.5.1 Documenti informatici

I dati della segnatura di protocollo di un documento informatico sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD) reso disponibile dall'AIPA [Circolare AGID n. 60 23 gennaio 2013].

- mittente;
- destinatario o destinatari.

Nel caso di documenti informatici in partenza, vengono specificate le seguenti informazioni [cfr. art. 21, DPCM 03 dicembre 2013]:

- persona o ufficio destinatario;
- identificazione degli allegati;
- informazioni sul procedimento e sul trattamento.

La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche di cui alla Circolare AIA 7 maggio 2001, n. 28.

10.5.2 Documenti cartacei

La segnatura di protocollo di un documento cartaceo è realizzata dal sistema, in forma permanente e non modificabile. Le informazioni minime previste sono:

- codice identificativo dell'AD;
- codice identificativo del dell'Area Organizzativa Omogenea (AOO);
- numero di protocollo e data del documento.

La registrazione e la segnatura costituiscono un'operazione unica e contestuale avente entrambe la natura di atto pubblico

10.6 Annullamento delle Registrazioni Di Protocollo

Le registrazioni annullate rimangono memorizzate nel registro informatico del protocollo e sono evidenziate dal sistema con un simbolo o una dicitura [cfr. art. 54, del testo unico].

L'operazione di modifica o di annullamento di una registrazione di protocollo è eseguita con le modalità di cui all'articolo 8 del DPCM 03 dicembre 2013.
L'annullamento di una registrazione di protocollo deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RDS.
Solo il RDS è autorizzato ad annullare, ovvero dare disposizioni di annullamento delle registrazioni di protocollo.

10.7 Casi Particolari di Registrazioni di Protocollo

10.7.1 Documenti cartacei in partenza con più destinatari

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica.

10.7.2 Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma inoltrati al Servizio di protocollo come documenti senza firma, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

10.7.3 Protocollazione di documenti inerenti a gare di appalto confezionati su supporti cartacei.

La corrispondenza riportante l'indicazione "offerta" - "gara d'appalto" o simili, o comunque dalla cui confezione si evince la partecipazione ad una gara, non viene aperta, ma viene protocollata in arrivo con l'apposizione del numero di protocollo e della data di registrazione direttamente sulla lettera di trasmissione e inviata all'ufficio interessato, dall'ottobre 2018, ai sensi dell'art. 40 del Dlgs 50/2016, le gare possono essere gestite solo in modalità telematica. Pertanto o si utilizzano strumenti CONSIP oppure le procedure di gara previste da @D[h]OC e descritte nel Bollettino n. 31 e n. 33.

10.7.4 Documenti non firmati

L'operatore di protocollo attesta la data, la forma e la provenienza per ogni documento. Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "Mittente sconosciuto o anonimo" e "Documento non sottoscritto".
Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.
E' poi compito dell'UO di competenza valutare se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

10.7.5 Differimento delle registrazioni

Le registrazioni di protocollo dei documenti ricevuti sono effettuate nella giornata di arrivo e comunque non oltre le quarantotto ore dal ricevimento degli atti.

10.7.6 Corrispondenza personale

La corrispondenza nominativamente intestata non è aperta e viene consegnata al destinatario il quale, dopo averne preso visione, se valuta che i documenti ricevuti non siano personali, è tenuto a trasmetterli al Servizio Protocollo Informatico per la registrazione dei documenti in arrivo.

10.7.7 Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto in ogni caso a registrare il documento ed eventuali allegati.
Tale verifica spetta all'UO assegnataria che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

10.8 Registrazioni di Protocollo

Al fine di assicurare l'immodificabilità il sistema *adhoc*, emette un protocollo con apposizione di un riferimento temporale come previsto dalla normativa vigente.
Come previsto dalla normativa in materia di tutela dei dati personali, gli addetti al protocollo adottano tutti gli accorgimenti necessari per la tutela dei dati sensibili/giudiziari non inserendoli nel campo "oggetto" del registro di protocollo.

11. MODALITA' DI UTILIZZO DEL REGISTRO DI EMERGENZA

11.1 Il Registro di Emergenza

Qualora non fosse disponibile fruire del servizio di protocollo informatico per una interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza.
Qualora nel corso di un anno non venga utilizzato il registro di emergenza, il RDS annota sullo stesso il mancato uso.
Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite su registro di protocollo generale.
Ad ogni registrazione recuperata dal registro di emergenza viene attributo un nuovo numero di protocollo, continuando la numerazione del protocollo raggiunta al momento dell'interruzione del servizio.
A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.
I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale.
La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.
La gestione del registro di emergenza è illustrata nell'allegato **"12.9"** (Gestione registro di emergenza).

11.2 Modalità di apertura del Registro di Emergenza

Il RDS assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica, le operazioni di protocollo sono svolte manualmente sul registro di emergenza, su postazioni di lavoro operanti fuori linea.
Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il RDS imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare.
Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo.
Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il RDS autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

11.3 Modalità di utilizzo del Registro di Emergenza

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro il numero totale di operazioni registrate manualmente.
La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.

11.4 Modalità di chiusura e recupero del Registro di Emergenza

E' compito del RDS verificare la chiusura del registro di emergenza.
E' compito della persona delegata dal RDS riportare dal registro di emergenza al sistema di protocollo le registrazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.

Una volta ripristinata la piena funzionalità del servizio di protocollo informatico, il RDS provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e l'ora di chiusura.

11.5 Gestione Registro di Emergenza

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico, ogni evento deve essere registrato su un supporto alternativo (cartaceo), denominato ***Registro di emergenza*** **(RE).**
Su questo registro devono essere riportate **la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora del ripristino della piena funzionalità del sistema, nonché eventuali annotazioni ritenute rilevanti dal responsabile del protocollo informatico**.
Il registro di emergenza viene sostanzialmente a configurarsi come un repertorio del protocollo unico**: ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo senza soluzioni di continuità la**
numerazione del protocollo unico raggiunta al momento dell'interruzione del servizio.
A tale registrazione nelle note sarà associato anche il **numero di protocollo** e la **data** di registrazione del relativo **protocollo di emergenza**. I documenti annotati nel registro di emergenza e trasferiti nel protocollo unico recheranno, pertanto, **due numeri**: **uno del protocollo di emergenza e uno del protocollo unico.**
Il registro di emergenza, in unico esemplare, deve essere gestito dal responsabile del Nucleo Protocollo; tutte le UO, che dovranno protocollare in entrata ed in uscita, dovranno contattare detto responsabile per l'acquisizione del numero di protocollo. Al ripristino dei servizi informatici, ogni UO, previo autorizzazione del RDS, procederà alla trascrizione nella banca dati dei protocolli utilizzati nel periodo di interruzione.

Allegato "A"

DEFINIZIONI

Ai fini del presente manuale s'intende:

- **per *testo unico***, il DPR 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- per ***Area Organizzativa Omogenea*** *(AOO)*, un insieme di funzioni e di strutture, individuate dall'Amministrazione che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato (cfr. art. 2, comma 1, lettera n), del DPCM 03 dicembre 2013];
- per ***Unità Organizzativa (UO)*****,** un ufficio o sezione dell'area organizzativa omogenea che utilizza i servizi messi a disposizione dal sistema di gestione informatica dei documenti (cfr. art. 2, lettera o), del DPCM 03 dicembre 2013];
- per ***Ufficio Utente (UU)*****,** un ufficio dell'area organizzativa omogenea che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto, destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali;
- per ***Responsabile del Procedimento Amministrativo (RPA)*****,** è la persona, alla quale è stata affidata la trattazione di un affare amministrativo ivi compresa la gestione/creazione del relativo fascicolo dell'archivio corrente;
- per ***documento amministrativo*** ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa [cfr. art. 1, comma 1, lettera a), del testo unico];
- per ***documento informatico*****,** la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti [cfr. art. 1, comma 1, lettera b), del testo unico];
- per ***firma digitale*****,** il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici [cfr. art. 1, comma 1, lettera n), del testo unico];
- per ***gestione dei documenti*****,** l'insieme delle attività finalizzate alla formazione, ricezione, registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dall'Amministrazione, nell'ambito del sistema di classificazione d'archivio adottato

(Titolario di archivio) adottato dall'Esercito [cfr. art. 1, comma 1, lettera q), del testo unico];

- per ***sistema di gestione informatica dei documenti,*** l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dall'Amministrazione per la gestione dei documenti [cfr. art. 1, comma 1, lettera r), del testo unico];

- per ***segnatura di protocollo,*** l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile, delle informazioni che consentono di identificare/individuare in modo inequivocabile il documento stesso [cfr. art. 1, comma 1, lettera s), del testo unico];

- per ***archivio corrente,*** la parte di documentazione relativa ai procedimenti in corso di istruttoria e di trattazione, o comunque verso i quali sussiste un interesse corrente;

- per ***archivio storico,*** il complesso di documenti relativi a procedimenti esauriti e destinati alla conservazione permanente;

- per ***titolario di classificazione,*** uno schema generale di voci logiche che identificano le funzioni e le attività di una UO. E' articolato in modo gerarchico al fine di identificare, secondo uno schema che va dal generale al particolare, il fascicolo;

- per ***piano di conservazione di un archivio,*** il piano, integrato con il titolario di classificazione, contenente i criteri di organizzazione dell'archivio, di selezione periodica e conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali [cfr. art. 68, comma 1, del testo unico];

- per ***fascicolo,*** l'unità di base indivisibile di un archivio che raccoglie i documenti relativi ad un procedimento amministrativo;

- per ***Servizio,*** il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi [cfr. art. 61, comma 1, del testo unico].

La gestione dei documenti è effettuata mediante il sistema operativo informatico denominato *Adhoc*.

ALLEGATO "B"

NORMATIVA DI RIFERIMENTO

- Regolamento (UE) 2016/679, "Regolamento generale per la protezione dei dati personali";
- DPCM 3 DICEMBRE 2013 Regole tecniche per il protocollo informatico
- DPCM 3 DICEMBRE 2013 Regole tecniche per la conservazione
- DPCM 13 NOVEMBRE 2014 Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni.
- DPCM 22 FEBBRAIO 2013 Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali
- Decreto del Presidente della Repubblica 11 **febbraio 2005, n. 68**
- Circolare n. 60 AGID 23 gennaio 2013
- Codice dell'Amministrazione Digitale (Dlgs 7 marzo 2005 n. 82 e s.m.i.)
- Codice in materia di protezionedei dati personali (Dlgs 30 giugno 2003 n. 196 e s.m.i.)
- SGD –VI reparto I° Ufficio Referente Unico del Protocollo Informatico per la Difesa ("Linee guida per l'implementazione del protocollo informatico: La registrazione e la segnatura di protocollo ed altri problemi pratici")- **Marzo 2004**
- SMD – Reparto TEI (Let. 155/0503/121/01-SRL1 datata **19 gennaio 2004**);
- SMD – Reparto TEI (Direttiva SMD-I-002 "Formati di scambio di documenti in ambito Difesa");
- SMD – Reparto TEI (Direttiva SMD-I-003 "La posta elettronica in ambito Difesa" **dell'8 luglio 2004**);
- SMD – Reparto TEI (Direttiva SMD-I-004 "Il protocollo informatico in ambito Difesa" **dell'8 luglio 2004**);
- Direttiva 18 **dicembre 2003** - Linee guida in materia di digitalizzazione dell'Amministrazione per l'anno 2004 (GU n. 28 del 4 Aprile 2004)
- Direttiva 1999/93/CE del parlamento Europeo e del Consiglio del 13 **dicembre 2003**
- Direttiva MIT 27 **novembre 2003** - Impiego della posta elettronica nelle pubbliche amministrazioni. (GU n. 8 del 12-1-2004)
- Decreto del 14 **ottobre 2003** - Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi. (GU n. 249 del 25-10-2003)
- D. Lgs. N. 196 del 30 **giugno 2003** - Codice in materia di protezione dei dati personali.
- Legge n. 289 del 27 **dicembre 2002** – Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
- Direttiva del Ministro per l'innovazione e le tecnologie, 20 **dicembre 2002** - Linee guida in materia di digitalizzazione dell'amministrazione
- Direttiva del Ministro per l'innovazione e le tecnologie, 9 **dicembre 2002 -**Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali

- SGD –VI reparto I° Ufficio Referente Unico del Protocollo Informatico per la Difesa ("Linee guida per l'implementazione del protocollo informatico: Riferimenti normativi ed operazioni da effettuare")- **Ottobre 2002**;
- SGD –VI reparto I° Ufficio Referente Unico del Protocollo Informatico per la Difesa ("Linee guida per l'implementazione del protocollo informatico: Schema esemplificativo del manuale di gestione e Nucleo Minimo di Protocollo")- **Marzo 2003**
- Direttiva n. 16 **gennaio 2002**, Dipartimento per l'innovazione e le tecnologie - Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali
- Direttiva del Ministro per la funzione Pubblica del 13 **dicembre 2001** – Formazione del Personale (GU. n. 26 del 31 gennaio 2002)
- Circolare AIPA 21 **giugno 2001**, n. AIPA/CR/**31** (Art. 7, comma 6, del decreto del Presidente del Consiglio dei ministri del 03 dicembre 2013, recante "Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428" - requisiti minimi di sicurezza dei sistemi operativi disponibili
- DLgs n. 165 del 30 **marzo 2001** - "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche"
- Circolare del 16 **febbraio 2001**, n. AIPA/CR/**27** - art. 17 del DPR 10 novembre 1997, n. 513: utilizzo della firma digitale nelle Pubbliche Amministrazioni.
- Testo unico sulla documentazione amministrativa (GU. n. 42 del 20.2.2001) DPR 28 **dicembre 2000** n. - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- Decreto del Presidente della Repubblica 8 gennaio **2001**, n. 37 (Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato - n. 42, allegato 1, della legge n. 50/1999);
- Autorità Garante per la protezione dei dati personali, Provvedimento 8/P/2001 del 14 marzo **2001** (Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici);
- Decreto legislativo 29 **ottobre 1999**, n. 490 (GU. n. 302 del 27.12.1999) Testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dell'articolo 1 della legge 8 ottobre 1997, n. 352.
- Decreto Legislativo 30 luglio **1999**, n. 281 (Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica);
- DPR 20 **ottobre 1998**, n. 428 (GU. n. 291 del 14.12.1998)Regolamento per la tenuta del protocollo amministrativo con procedura informatica.
- DPR 27 **giugno 1992**, n. 352 (GU. n. 177 del 29.7.1992)Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della legge 7 agosto 1990,n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
- Legge n. 241 del 7 **agosto 1990 -** Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (GU. n. 192 del 18.8.1990)
- Regio Decreto 25 **gennaio 1900**, n. 35 (Gazz. Uff. n. 44 del 22.2.1900) Regolamento per gli uffici di registratura e di archivio delle amministrazioni centrali.
- Giornale Militare Ufficiale – Dispensa n. 54 – **Circolare 18/10/29** Norme per la conservazione e l'eliminazione degli atti da carteggio.

- Giornale Militare Ufficiale – Dispensa n. 24 Circolare 02/05/30 Norme per la conservazione e l'eliminazione degli atti da carteggio.
- Circolari del Gabinetto del Ministro del 22/11/30 e del 12/01/31 Norme per la conservazione e l'eliminazione degli atti da carteggio.
- Circolare del Ministero dell'Interno 1 marzo 1937 n. 17200-2 Norme per la conservazione e l'eliminazione degli atti da carteggio.
- Decreto del Presidente della Repubblica 30 settembre 1963, n. 1409 Norme relative all'ordinamento e al personale degli Archivi di Stato.
- Decreto Legislativo 29 ottobre 1999, n. 490 Testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dell'articolo 1 della legge 8 ottobre, n. 352.
- Decreto del Presidente della Repubblica 30 settembre 1963, n. 1409.

ALLEGATO "C"

ARTICOLAZIONE DI CIASCUNA UNITÀ ORGANIZZATIVA (UO) NELL'AMBITO DELL'AOO.

Denominazione dell'Area: **Comando Militare Esercito "SICILIA"**
Codice identificativo dell'Area: **M_D E26346**

Data di istituzione: **05 LUGLIO 2016**

Indirizzo di posta elettronica istituzionale dell'Area: cmepa@esercito.difesa.it
Indirizzo di posta elettronica certificata dell'Area: cmepa@postacert.difesa.it

Responsabile del Servizio:..... Serg.Magg.Ca.Q.S. Ignazio D'ANTONI;
Vicario del RDS:.....C.le.Magg.Ca.Sc.Q.S. Marcello Anitra;

Il vicario del RDS interverrà in caso di assenza del titolare, come previsto dall'art. 3 lettera b. del DPCM. *In caso di contemporanea assenza del RDS e del suo vicario, anche per un solo giorno, sarà indispensabile nominare comunque, con atto formale , un dipendente dell'AOO che svolga, per il tempo strettamente necessario, il ruolo di RDS.*

Insieme delle Unità Organizzative che compongono l'AOO con la loro articolazione gerarchica e relativa denominazione del Servizio istituito:

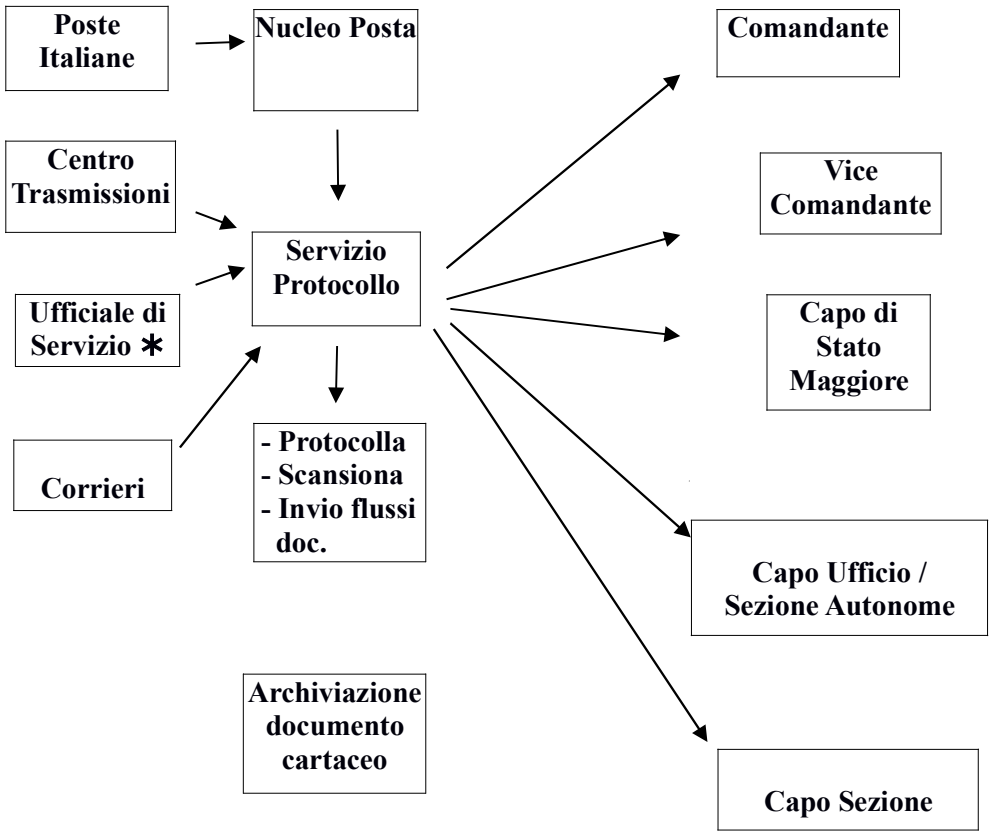
1° LIVELLO	2° LIVELLO	3° LIVELLO	4° LIVELLO	5° LIVELLO
COMANDANTE				
	SEGRETERIA DEL COMANDANTE			
	SOTTUFFICIALE DI CORPO			
	LEGAD			
	SERVIZIO DI PROTEZIONE E PREVENZIONE			
	BIBLIOTECA			
	COMANDO ALLA SEDE			
	UFFICIALE DI SERVIZIO AL COMANDO			
	COBAR			
	RSU			
	SEZ. COORD. AMMINISTRATIVO			
		NU. FONDI PERMANENTI		
		NU. MATERIALI		

		NU.MATRICOLA		
		NU.TRAT. ECONOMICO		
	VICE COMANDANTE			
		SEGRETERIA DEL VICE COMANDANTE		
		CIRCOLO UNIFICATO PALERMO		
			CRDD	
		CAMPO ONORATO		
	CAPO DI STATO MAGGIORE			
		SEZ.SICUREZZA		
		SEZ. PROT. INFO. E FLUSSI DOCUMENTALI		
		REPARTO DI SUPPORTO GENERALE		
			COMPAGNIA COMANDO E SERVIZI	
			PLOTONE TRASPORTI	
			PLOTONE INFRASTR.	
		UFFICIO PERSONALE LOGISTICA E SERVITU' MILITARE		
			SEZ. PERSONALE MILITARE	
			SEZ. PERSONALE CIVILE	
			SEZIONE LOGISTICA	
			SEZIONE C3I	
		UFFICIO RECLUTAMENTO E COMUNICAZIONE		
			SEZIONE PI/PR Info Pubblico	
			SEZIONE RECLUTAMENTO	
			SEZIONE SOSTEGNO ALLA RICOLLOCAZIONE PROFESSIONALE	
		UFFICIO AFFARI GENERALI		
			SEZIONE ALLOGGI	

			SEZIONE A.G. PRES/BEN E COOP	
			SEZIONE SANITARIA E GRAVI PATOLOGIE	
		UFFICIO DOCUMENTALE		
			REPARTO ATTIVITA' TERRITORIALI	
				SEZ. SEGRETERIA E PERSONALE
				SEZIONE ARCHIVIO
				SEZIONE DEMATERIALIZZAZIONE
				SEZIONE INFOPUBBLICO
				SQUADRA SERVIZI E MINUTO MANTENIMENTO
			SEZIONE DOCUMENTAZ	
			SEZIONE SEGRETERIA	
			SZ MATRIC DISCIP ANAGR E GEST ARCH	
			SZ PROVV MEDICO LEGALI	

ALLEGATO "D"

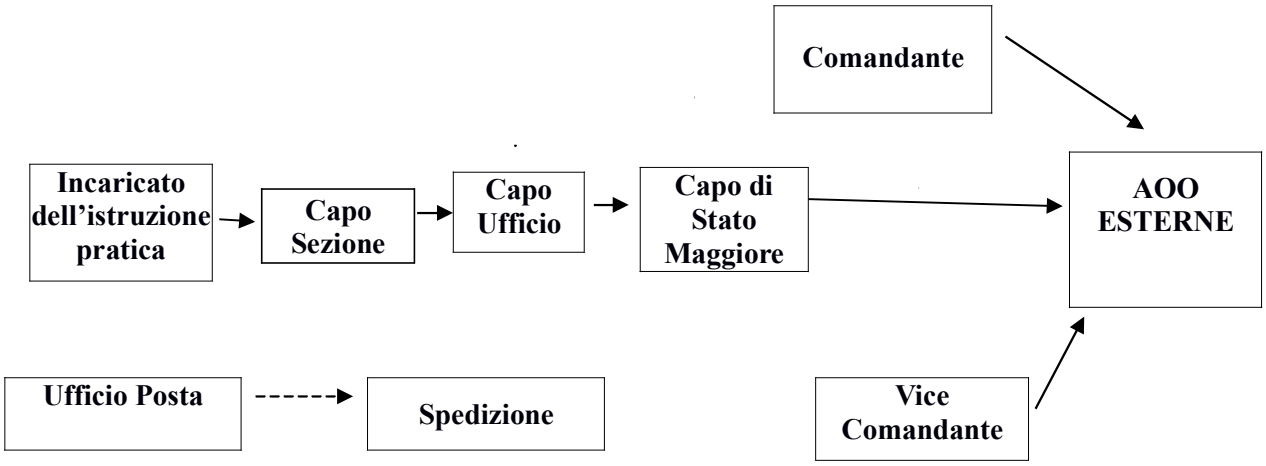
FLUSSO SINOTTICO DELLA POSTA IN ENTRATA



Legenda :
⇐ **Smista la posta classificata alla Sz. Sicurezza.**

ALLEGATO "E"

FLUSSO SINOTTICO DELLA POSTA IN USCITA



ALLEGATO "F"

Attribuzioni di funzioni connesse con il servizio di protocollo informatico

RESPONSABILE DEL SERVIZIO

RESPONSABILE DEL SERVIZIO		
Nominativo	:	Serg. Magg. Ca. Q.S. Ignazio D'ANTONI
Incarico	:	Responsabile del Servizio
Indirizzo	:	Piazza della Vittoria, 14 - 90100 Palermo
Telefono/ Fax	:	091 2193869 - 2193908 (linea civile) 1672869 - 1672908 (linea militare)
E-MAIL	:	ignazio.dantoni@esercito.difesa.it rdsadhoc@cmepa.esercito.difesa.it vadhoc@cmepa.esercito.difesa.it

VICARIO DEL RESPONSABILE DEL SERVIZIO		
Nominativo	:	C.le Magg. Ca. Sc- Q.S. Marcello ANITRA
Incarico	:	Vicario del Responsabile del Servizio
Indirizzo	:	Piazza della Vittoria, 14 - 90100 Palermo
Telefono	:	091 2193872 (linea civile) 1672872 (linea militare)
E-MAIL	:	marcello.anitra@esercito.difesa.it adadhoc@cmepa.esercito.difesa.it