8°REGGIMENTO BERSAGLIERI

VELOX AD IMPETUM

MANUALE DI GESTIONE

ED ISTRUZIONI PER IL CORRETTO FUNZIONAMENTO DEL "SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO E LA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI" DELL'AREA ORGANIZZATIVA OMOGENEA "8° REGGIMENTO BERSAGLIERI"

AVVERTENZE

La presente pubblicazione è stata approntata secondo quanto previsto dalla Circolare 1001 dello Stato Maggiore dell'Esercito-Ed. 2016. Fatte salve le esigenze di servizio, ufficio o istituto, nessuna parte di questa pubblicazione può essere riprodotta in qualsiasi forma a stampa, fotocopia, microfilm, scansione digitalizzata o altri sistemi, senza l'autorizzazione scritta dell'originatore.

La presente pubblicazione è diramata con la lettera in Annesso I e sarà visionabile sul sito del reggimento.

ATTO DI APPROVAZIONE

Approvo il presente Manuale di gestione ed istruzioni per il corretto funzionamento del "Servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi" dell'Area Organizzativa Omogenea "8° reggimento bersaglieri".

Il documento, redatto in ottemperanza all'art. 5 del DPCM 3/12/2013 *"Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis , 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005"* ha lo scopo di:

- descrivere il sistema di gestione e conservazione dei documenti;
- fornire le istruzioni per il corretto funzionamento del servizio per la tenuta del Protocollo Informatico, della gestione dei flussi documentali e degli archivi.

Esso abroga la circolare interna "Norme procedurali" ed. 2019,

Caserta, 24 settembre 2020.

Il COMANDANTE
Col. f.(b.) t.ISSMI Giampiero BISANTI

INDICE

1. AMBITO DI APPLICAZIONE DEL MANUALE E DEFINIZIONI

1.1. Introduzione

L'art. 50 del DPR n. 445/2000 recante il *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*, stabilisce che tutte le Pubbliche Amministrazioni debbano introdurre il protocollo informatico in luogo di quelli analogici esistenti.

L'art. 3 del DPCM del 03 dicembre 2013, contenente le *"Regole tecniche per il protocollo informatico"* ha previsto che, con l'entrata in vigore del protocollo informatico, le Pubbliche Amministrazioni, ciascuna nel rispetto del proprio ordinamento, perseguano alcuni obiettivi di adeguamento organizzativo e funzionale, quali:

- individuazione delle Aree Organizzative Omogenee (AOO);
- nomina del Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi;
- tempi, modalità e misure organizzative e tecniche finalizzate alla eliminazione dei protocolli interni;
- redazione di un Manuale per la gestione del protocollo informatico.

Gli obiettivi sopra indicati sono stati conseguiti dal reggimento in data 03 luglio 2017, giorno in cui l'Area Organizzativa Omogenea (AOO) – 8° REGGIMENTO BERSAGLIERI è transitata dalla procedura "PROMIL" alla procedura AD[h]OC, nuovo sistema di gestione informatico dei flussi documentali NON CLASSIFICATI, assicurando il mantenimento del Codice Amministrazione M_D-E21263 e abrogando, in pari data, qualsiasi altro tipo di protocollo analogico.

In particolare, nell'ambito dell'AOO-8° REGGIMENTO BERSAGLIERI il registro di protocollo è unico così come la numerazione progressiva delle registrazioni di protocollo, a mente degli artt. 50, 51 e 52 del DPR 445/2000.

Il Sistema di Protocollo Informatico in uso è: AD[h]OC (il software viene aggiornato dal COMC4EI sulla base dei rilasci disponibili in ambito difesa).

La numerazione si apre al 1° gennaio e si chiude al 31 dicembre.

Il numero di protocollo individua un unico documento, quindi ogni documento reca un solo numero di protocollo.

La documentazione non registrata presso l'AOO è considerata giuridicamente inesistente presso l'Amministrazione.

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

1.2. Area Organizzativa Omogenea (AOO)

L'individuazione delle AOO, previste dall'art. 2, c. 2, DPR 20 ottobre 1998 n. 428 e dal successivo art. 50, c. 4, DPR 28 dicembre 2000 n. 445, ha come obiettivo primario la determinazione degli ambiti di competenza del nuovo sistema di protocollo informatico.

Per AOO si intende un insieme di unità organizzative di un'amministrazione che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. In particolare, ciascuna AOO mette a disposizione delle Unità Organizzative Responsabili (UOR) dipendenti:

– il servizio di protocollo dei documenti in entrata ed in uscita, utilizzando un'unica sequenza numerica propria dell'AOO;
– un complesso di risorse umane e strumentali che costituisce il "Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi" (Servizio) cui sono affidate la gestione ed il funzionamento del sistema di gestione informatica documentale (art. 61, DPR 445/2000).

Nell'AOO – 8° REGGIMENTO BERSAGLIERI è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Gli atti previsti per l'avvio del Servizio sono:

– atto di costituzione e organigramma della AOO - 8° REGGIMENTO BERSAGLIERI (All. D)
– atto di nomina del Responsabile del Servizio, unitamente a quella del Vicario (All. E);
– richiesta di avvio del Servizio AD[h]OC della AOO-8° REGGIMENTO BERSAGLIERI (All. F);
– prospetto dati per la pubblicazione sull'Indice della Pubblica Amministrazione (IPA) (All. G);
– Manuale di Gestione.

1.3. Unità Organizzative Responsabili (UOR)

Una Unità Organizzativa Responsabile è un sottoinsieme di una AOO, ovvero un complesso di risorse umane e strumentali cui sono state affidate competenze omogenee nell'ambito delle quali i dipendenti assumono la responsabilità nella trattazione di pratiche o procedimenti amministrativi.

Le Unità Organizzative Responsabili che afferiscono all'AOO-8° REGGIMENTO BERSAGLIERI (a mente dell'art. 50, c. 4, DPR 445/2000) sono:

– LIVELLO I: COMANDANTE DI REGGIMENTO
– LIVELLO II : OPERATORI FLUSSO DOCUMENTALE
– LIVELLO III:01 UFFICIO MAGGIORITA' E PERSONALE
– LIVELLO III:02 UFFICIO OAI
– LIVELLO III:03 UFFICIO LOGISTICO
– LIVELLO III:04 SEZIONE COORDINAMENTO AMMINISTRATIVO
– LIVELLO III:05 3° BATTAGLIONE BERSAGLIERI "CERNAIA"
– LIVELLO III:06 COMPAGNIA COMANDO E SUPPORTO LOGISTICO

1.4. Il Responsabile del Servizio (RdS)

E' il responsabile delle operazioni di registrazione, di protocollo, di organizzazione e tenuta dei documenti all'interno dell'AOO.

In particolare, a mente dell'art. 61, c. 3, DPR 445/2000, ha i seguenti compiti:

– predisporre lo schema del Manuale di Gestione;
– predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, all'interscambio, all'accesso, alla conservazione dei documenti nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione e il responsabile dei sistemi informativi;
– presiedere alle attività del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi alle dipendenze della stessa AOO;

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

1.5. Il Vicario

Contestualmente alla nomina del RDS deve essere individuato e nominato il relativo vicario che 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.

1.6. Il manuale di gestione (MdG)

Il presente documento costituisce il "Manuale di Gestione del Protocollo Informatico" dell'AOO-8° REGGIMENTO BERSAGLIERI, redatto ai sensi dell'art. 5, DPCM del 03 dicembre 2013.

Il MdG descrive il sistema di gestione dei documenti presso l'AOO-8° REGGIMENTO BERSAGLIERI fornendo le istruzioni per il corretto funzionamento del "Servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi".

Nel manuale di gestione sono riportati, in particolare:

- il piano di sicurezza dei documenti informatici;
- le modalità di utilizzo di strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'AOO, ivi comprese le caselle di posta elettronica, anche certificata, utilizzate;
- la descrizione di eventuali ulteriori formati utilizzati per la formazione del documento informatico in relazione a specifici contesti operativi esplicitati e motivati;
- l'insieme minimo dei metadati associati ai documenti soggetti a registrazione particolare e gli eventuali ulteriori metadati rilevanti ai fini amministrativi, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce;
- la descrizione del flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione, tra i quali, in particolare, documenti informatici pervenuti attraverso canali diversi da quelli previsti dagli articoli 16

e 17 del DPCM 3 dicembre 2013, come ad esempio raccomandate o assicurate;
- l'indicazione delle regole di smistamento ed assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso AOO della stessa amministrazione o verso altre amministrazioni;
- le modalità di formazione, implementazione e gestione dei fascicoli informatici relativi ai procedimenti e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;
- l'indicazione delle unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e tenuta dei documenti all'interno dell'AOO;
- l'elenco dei documenti esclusi dalla registrazione di protocollo, ai sensi dell'art. 53, comma 5, del testo unico;
- l'elenco dei documenti soggetti a registrazione particolare e le relative modalità di trattamento;
- il sistema di classificazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;
- le modalità di produzione e di conservazione delle registrazioni di protocollo informatico e, in particolare, l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire l'immodificabilità della registrazione di protocollo, la contemporaneità della stessa con l'operazione di segnatura ai sensi dell'art. 55 del Testo Unico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione;
- la descrizione funzionale ed operativa del componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti con particolare riferimento alle modalità di utilizzo;
- i criteri e le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali;
- le modalità di utilizzo del registro di emergenza ai sensi dell'art. 63 del testo unico, inclusa la funzione di recupero dei dati protocollati manualmente.

Sarà cura del RdS procedere al periodico aggiornamento del MdG, al variare degli elementi organizzativi, procedurali e tecnologici cui si riferisce.

2. LE TIPOLOGIE DOCUMENTARIE

2.1. Il documento amministrativo

Per **documento amministrativo** s'intende una rappresentazione formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o comunque utilizzati ai fini dell'attività amministrativa, così come prevede l'art. 1, DPR 28 dicembre 2000 n. 445.

Le tipologie di documenti trattati dall'AOO sono:
- Lettera;
- Messaggio/telegramma;
- E-message;
- E-mail (PEI/PEC/personale);

- Ordine del giorno;
- Atto dispositivo;
- Disposizioni Permanenti;
- Lettera di trasmissione di documenti analogici "non dematerializzati".

A livello generale, è comunque opportuno prendere in considerazione tutti i documenti, anche quelli informali, in particolare tutti quelli che concorrono a determinare gli *iter* di processo, in quanto non solo garantiscono la trasparenza dell'azione amministrativa, ma costituiscono per l'Amministrazione un preciso *know-how* di cui fare patrimonio.

Il Sistema di Gestione Documentale è abilitato soltanto alla trattazione dei documenti **non classificati**, compresi quelli trattanti dati sensibili (secondo il D.Lgs. 196/03).

Il documento amministrativo è classificabile in termini operativi in:

- ricevuto (in arrivo);
- inviato (in uscita);
- interno,

ovvero in termini tecnologici in:

- informatico;
- analogico (cartaceo o altro formato).

2.2. Il documento informatico

Per documento informatico s'intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. I documenti informatici da chiunque formati, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni stabilite dalle regole tecniche del Codice dell'Amministrazione Digitale (CAD), D.Lgs. n.82 del 2005.

In particolare, ove siano state rispettate le suddette regole tecniche, il documento informatico sottoscritto con firma elettronica qualificata o con **firma digitale** soddisfa il requisito della forma scritta (art.1350, Codice Civile), mentre la data e l'ora di formazione sono opponibili ai terzi (art. 2702, Codice Civile).

2.3. Il documento analogico

Per documento analogico, si fa' riferimento ad un **documento amministrativo cartaceo** che può essere prodotto sia in maniera tradizionale (lettera scritta a mano o a macchina), sia con strumenti informatici (lettera prodotta tramite sistema di videoscrittura) e poi stampato.

Si definisce **originale** il documento cartaceo nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali comprendente tutti gli elementi di garanzia e di informazione del mittente e del destinatario, stampato e dotato di firma autografa.

La mail-personale in arrivo può essere considerata documento amministrativo analogico, se risponde al requisito di **ragionevole certezza del mittente**.

Un documento analogico viene convertito in documento informatico tramite opportune procedure di "*dematerializzazione*" (es. scanner).

2.4. Documenti in entrata

Per **documenti in entrata** s'intendono gli atti acquisiti/ricevuti dall'AOO e che ne riguardino le funzioni istituzionali, d'interesse amministrativo, operativo e funzionale.

2.5. Documenti in uscita

Per **documenti in uscita** si intendono gli atti che sono diretti, e cioè spediti, ad altre AOO anche della stessa amministrazione o a privati (persone fisiche o giuridiche).

Si sottolinea che la fascicolazione dei documenti in partenza è di competenza del Responsabile del Procedimento Amministrativo (Utente), mentre il protocollo viene effettuato automaticamente dal sistema di Protocollo.

2.6. Documenti interni

I documenti interni sono scambiati tra le diverse UOR facenti capo alla medesima AOO e non vengono protocollati, salvo abbiano **preminente carattere amministrativo**, ovvero siano 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.

La corrispondenza interna che deve avere valenza amministrativa ed essere smistata all'interno dell'AOO dovrà avere un solo numero di protocollo, attribuito dal Sistema al documento interno prodotto dall'UOR mittente, invece all'UOR destinatario, sulla scrivania virtuale del **capo articolazione**, il sistema fornirà la visualizzazione del documento assegnato.

3. I FLUSSI DOCUMENTALI.

3.1. Descrizione del Flusso documentale

La descrizione del flusso di lavorazione dei documenti è un'attività prevista dall'art. 5, c. 2, let. "f", DPCM 03 dicembre 2013.

3.2. Flusso documentale in entrata

I **documenti analogici** giungono al Nucleo Posta/Servizio AD[h]OC dell'Ufficio Maggiorità e Personale del reggimento, che è **l'unico punto di raccolta, protocollazione e smistamento** dei documenti in ingresso per l'AOO:

- tramite il servizio postale convenzionale;
- a mano (tramite consegna diretta da corrieri espressi o militari, giro posta).

I **documenti informatici** possono giungere via posta elettronica, istituzionale o certificata (trattata esclusivamente dal Nucleo Posta/AD[h]OC)

Il Nucleo Posta è l'unico soggetto alla trattazione del Flusso in Entrata, ovvero:

- **Flusso Informatico PEI/PEC**;
- **Posta Ordinaria** in arrivo non classificata e che soddisfa i criteri di autenticità ed inalterabilità ritirata presso gli Uffici Postali, corrieri militari e civili (solo se indirizzate al Comando ed escluse le "**ASSICURATE**", che saranno consegnate chiuse esplicitamente alla Segreteria in indirizzo).

3.2.1. Compiti del Nucleo Posta

Il **Nucleo Posta**, dovrà prestare attenzione alla **corrispondenza ordinaria** in Entrata, in particolare:

- effettua verifiche preliminari alla registrazione, eseguite sia **prima dell'apertura** della posta, sulle buste e sui contenitori della corrispondenza pervenuta su canali tradizionali (correttezza indirizzo destinatario), sia **successivamente** sui documenti cartacei ivi contenuti (completezza dati identificativi, ovvero data, provenienza/mittente, firma);

- il documento cartaceo, una volta protocollato, è consegnato alla Segreteria di UOR di competenza;
- cura il tempestivo recapito dei documenti cartacei ricevuti per "ASSICURATA" all'Ufficio indirizzato, per l'apertura e il controllo;
- NON apre la corrispondenza personale (anche se indicante grado o incarico) e non ne effettua la protocollazione, ma deve essere consegnata al destinatario che ne valuterà il contenuto e provvederà a farla protocollare su sua esplicita indicazione alla propria Segreteria di UOR;
- le **ricevute di ritorno** della posta raccomandata vanno firmate dal personale del Nucleo Posta, per ritiro dall'Ufficio Postale di Poste Italiane. Viene successivamente compilato un apposito registro e le consegna alla Segreteria di UOR previa contro firma del registro per avvenuta consegna. Le ricevute originali sono conservate "allegate" alla copia cartacea conservata agli atti della Segreteria di UOR o, qualora conservata in modo sostitutivo si procederà alla "dematerializzazione" e protocollazione come un documento analogico, avendo cura di utilizzare il medesimo oggetto della relativa lettera e il riferimento alla lettera cui si attesta la ricevuta.

3.2.2. Recapito di plichi presso il Corpo di Guardia

Per la Posta Ordinaria recapitata da corrieri civili presso i Corpi di Guardia, si prevedono 2 situazioni:

- **Orario di servizio e personale del Nucleo Posta presente**: il Personale di Guardia avvisa il Nucleo Posta della presenza del corriere. Il Personale del Nucleo firma per il ritiro e compila un apposito registro da custodire in Ufficio e procederà secondo quanto previsto per la corrispondenza ordinaria. Se il plico è indirizzato a un Ufficio per "**Uso esclusivo d'Ufficio**" o **personale**, questo sarà ritirato direttamente dal personale destinatario;
- **Orario di servizio e personale del Nucleo Posta assente o fuori orario di servizio**: il Personale di Guardia contatterà il personale di Servizio al reggimento per il ritiro del plico, per la successiva consegna e gestione ordinaria al personale del Nucleo Posta.

3.3. Flusso documentale in uscita

I documenti possono essere spediti tramite:

- via interoperabilità (PEI o PEC direttamente dal Servizio di Protocollo Informatico AD[h]OC);
- via Posta Ordinaria;
- via corriere civile o militare.

Tutti i documenti in uscita dalle UOR, destinati all'esterno dell'AOO, nonché i documenti interni che necessitano, per risvolti amministrativi, di un protocollo devono avere una segnatura di protocollo (informatica o analogica tramite timbratura).

La loro predisposizione dovrà essere principalmente e preferibilmente quella informatica.

La spedizione avviene principalmente e preferibilmente per via "interoperabilità".

Solo eccezionalmente i documenti vengono predisposti e/o spediti in forma cartacea, dopo la procedura di "materializzazione" e l'apposizione della segnatura di protocollo tramite timbratura. Qualora il documento cartaceo sia copia di un originale informatico l'UOR dovrà altresì apporvi una dicitura che attesta essere un documento conforme all'originale informatico firmato digitalmente e custodito presso l'Archivio del Sistema di Protocollo Informatico o più semplicemente stamparlo con il "GLIFO" direttamente dalla "Lista dei Documenti da Materializzare", dal menù "Protocollo".
I documenti vengono spediti sempre in forma cartacea se destinati a privati sprovvisti di PEC o ad AOO dell'Amministrazione o di altre Amministrazioni che non siano ancora conformi alle regole di interoperabilità del protocollo informatico ai sensi del DPR 445 del 2000 o se il Documento non è "de-materializzabile". In tal caso è da preferire la "raccomandata con ricevuta A/R."
Le ricevute di ritorno dovranno essere trattate secondo quanto già indicato al sottopara. 3.2.1, 5° alinea.

3.4. Flusso documenti informatici

3.4.1. Canali di ricezione/spedizione

Per la ricezione e la spedizione di documenti informatici l'AOO dispone dei seguenti canali istituzionali:

- casella di posta elettronica ordinaria: **rgtb8@esercito.difesa.it** (interoperabile);
- casella di PEC: **rgtb8@postacert.difesa.it** (interoperabile);
- indirizzo Ente:

8° REGGIMENTO BERSAGLIERI
Via Laviano n. 8
81100 CASERTA,

Nel rispetto dell'art. 38, DPR 445/2000 **vengono comunque accettati** e protocollati tutti i documenti inviati telematicamente (e-mail personali/funzionali) se "*sottoscritte mediante la firma digitale o quando il sottoscrittore é identificato dal sistema informatico con l'uso della carta di identità elettronica*" o comunque riconosciuti attendibili dal Destinatario.

Dei Documenti non accettati dovrà essere dato riscontro al Mittente a cura del RDS.

3.4.2. Caratteristiche del Documento informatico per la interoperabilità

L'AOO accetta documenti informatici conformi alle seguenti regole tecniche:

- il formato preferibilmente accettato per file allegati ai messaggi di posta elettronica, come **documenti primari** è **unicamente** il **PDF** e **PDF/A**;
- sono accettati anche i formati JPG, P7M, TXT, TIFF, XML e tutti i formati del pacchetto Libre Office;
- i file allegati al documento primario possono essere dei formati del pacchetto Libre Office, ZIP;
- in un singolo messaggio di posta elettronica dev'essere associata la documentazione relativa a un **unico argomento** (pertanto se un

mittente deve inviare cinque documenti afferenti cinque pratiche differenti, dovrà inviare cinque mail);
- la massima dimensione complessiva degli allegati è di 100 MB (per la PEC questo valore dev'essere diviso per il numero di destinatari, es. file da 10Mb inviato a 10 destinatari = 100Mb);
- la casella postale del mittente, in caso di persone giuridiche, deve essere riferita alla persona giuridica medesima, e non alle persone fisiche che la compongono;
- il nome degli eventuali file allegati deve essere contenuto e ristretto al minimo necessario;
- il nome degli eventuali file allegati deve essere di lunghezza moderata, non contenere spazi e/o caratteri speciali. Si suggerisce di utilizzare il carattere "underscore" (_) al posto di tali caratteri;
- la ricezione di allegati non "apribili" o non coerenti con quanto indicato nel documento primario (o lettera di trasmissione), comporta la trasmissione al mittente di una comunicazione (stesso canale, oggetto, indicazione del problema riscontrato e indicando l'identificativo del messaggio se trattasi di PEC) a cura del RDS.

3.4.3. Gestione del Flusso Documentale in entrata via PEI

Il Flusso PEI in entrata è gestito, normalmente, dal Sistema di Protocollo Informatico scaricandolo dal server del gestore e veicolandolo presso le postazioni di protocollazione degli Operatori del Servizio AD[h]OC.

Ogni Operatore del Servizio AD[h]OC provvederà alle seguenti operazioni:

- controllo dell'integrità e coerenza della documentazione; in particolare della presenza della lettera di trasmissione, degli allegati/annessi dichiarati e della corretta visualizzazione di tutto il documento;
- procedere alla protocollazione e assegnazione alla UOR.

Nel caso di documento incoerente, corrotto, mancante di parti o non visualizzabile, l'Operatore AD[h]OC lo invierà al RDS a seconda dei casi per la trattazione.

Vengono altresì trasmessi dagli addetti al protocollo al RDS per la valutazione, anche tutti quei messaggi che si presumono erroneamente pervenuti all'AOO o di cui non si riconosca l'attendibilità del mittente.

Il Sistema ha la possibilità di gestire le eventuali anomalie secondo uno schema di risposte pre-impostate direttamente al mittente, a cura e responsabilità del RDS.

ATTENZIONE: *Le mail che vengono considerate SPAM (indirizzi con domini stranieri o particolari, nickname o che non offrano adeguata informazione circa il mittente) non vengono protocollate e non viene spedito nessun messaggio al mittente. Questo al fine di prevenire eventuali attacchi informatici (virus, fishing, trojan, back doors, etc) attivabili inconsapevolmente all'apertura del file o miranti esclusivamente alla "certificazione dell'esistenza" del destinatario per popolare mailing-list.*

3.4.4. Gestione del Flusso Documentale in entrata via PEC

Il Flusso PEC in entrata è gestito dal Sistema di Protocollo Informatico scaricandolo dal server del gestore e veicolandolo presso le postazioni di protocollazione degli Operatori del Nucleo AD[h]OC.

Ogni Operatore provvederà alle seguenti operazioni:

- controllo dell'integrità e coerenza della documentazione; in particolare della presenza della lettera di trasmissione, degli allegati/annessi dichiarati e della corretta visualizzazione di tutto il documento;
- procedere alla protocollazione e assegnazione alla UOR.

Nel caso di documento incoerente, corrotto, mancante di parti o non visualizzabile, l'operatore lo invierà al RDS a seconda dei casi per la trattazione.

***ATTENZIONE**: Al fine di minimizzare eventuali possibili perdite di Documenti per cancellazione incidentale o mancata protocollazione, l'Amministratore AD[h]OC, su delega del RdS, procede mensilmente al downlad del **Flusso PEC** direttamente dal sito del Gestore.*

3.4.5. Gestione del Documento Informatico ricevuto via email funzionale

Se un documento informatico viene inviato ad una casella di posta elettronica ordinaria afferente una UOR (*incarico@rgtb8.esercito.difesa.it*) o anche personale (*nome.cognome@esercito.difesa.it*), 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 ovvero rgtb8@esercito.difesa.it

Nel rispetto dell'art. 38 del DPR 445/2000 vengono comunque accettati e protocollati tutti i documenti informatici riconosciuti attendibili dal destinatario.

Nel caso in cui il titolare di quella casella ritenesse utile al procedimento amministrativo e quindi accettabile, provvederà a farla acquisire a protocollo secondo le procedure previste per i flussi cartacei (stampandola in PDF e procedendo alle operazioni di protocollazione).

Dei documenti non accettati dovrà essere dato riscontro al Mittente a cura dell'UOR.

3.4.6. Gestione delle Ricevute informatiche

Il Sistema provvede, automaticamente, alla gestione delle Ricevute informatiche.

Le Ricevute con validità legale sono generate **esclusivamente** per il Flusso in interoperabilità via PEC e si distinguono in 4 tipologie:

- **Ricevuta di Assegnazione,** certificante **l'assunzione** in carico del documento trasmesso da parte del gestore di PEC del mittente;
- **Ricevuta di Non Avvenuta Assegnazione,** certificante la **non assunzione** in carico del documento trasmesso da parte del gestore di PEC del mittente;
- **Ricevuta di Consegna**, certificante la **presa in carico** del documento trasmesso da parte del gestore di PEC e **disponibilità** dello stesso presso la casella di PEC del destinatario (equiparata alla"**ricevuta di A/R**" prevista dalla legge);
- **Ricevuta di Non Avvenuta Consegna,** certificante la **non presa in carico** del documento trasmesso da parte del gestore di PEC e

quindi la **non disponibilità** dello stesso presso la casella di PEC del Destinatario).

***ATTENZIONE**: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) **senza che il Servizio AD[h]OC ne abbia conoscenza**.*

*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 sulle caratteristiche che deve avere un documento informatico (**vds 3.4.2**) può:*

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

  Nel caso non vi sia modo di spedirlo via interoperabilità si dovrà:
- *stampare l'intero Documento e inviarlo via Posta Ordinaria;*
- *contattare il RDS per un invio PEC del Documento (verranno inviate, via mail funzionale, le relative Ricevute di Consegna. Nessuna Ricevuta sarà consegnata se il Destinatario non ha una casella di PEC).*

3.4.7. Predisposizione per una trasmissione in interoperabilità

Per le caratteristiche che deve avere un documento per essere inviato tramite interoperabilità vedasi il **paragrafo 3.4.2**

Il sistema informatico, sulla base delle informazioni inserite nella fase di predisposizione di quel documento, provvede ad inviare, per posta elettronica, il documento primario e tutti gli allegati presenti agli aventi causa indicati, distinguendo fra destinatari "per competenza" e "per conoscenza".

L'utilizzo della PEI piuttosto che la PEC viene selezionato dall'operatore che ha predisposto la pratica e può essere modificato da tutti coloro i quali hanno titolo a farlo fino alla firma del documento stesso. Di *default* è selezionato l'invio tramite PEC.

A tutti i documenti trasmessi viene allegato il file ***segnatura.xml***, contenente le informazioni previste dalla art.3, let. c, Circ. AgID 23/01/2013 n.60, necessarie per la **validità legale del Documento informatico**.

Il file *segnatura.xml* **non viene generato** nei seguenti casi, per i quali si procederà, successivamente, all'invio tramite Posta Ordinaria e per i quali farà fede il "**timbro postale**":

- corrispondente privo di una qualsiasi casella di posta elettronica;
- documento primario a cui è associato un allegato analogico non *de-materializzabile*;
- documento primario cui è associato un allegato informatico che per caratteristiche proprie non può essere trasmesso per posta elettronica.

Quando il documento non deve essere trasmesso per posta elettronica, il sistema informatico, completa le operazioni di firma digitale, apposizione della marca temporale e protocollazione del documento, senza procedere alla successiva trasmissione. Il Documento sarà disponibile, protocollato, nella "**Lista di Materializzazione**" dell'**Operatore che ne ha effettuato la predisposizione** iniziale per la successiva stampa, imbustamento e invio via Posta Ordinaria.

***ATTENZIONE**: È necessario segnalare che, qualora come allegato, venga inserito un documento informatico **già firmato digitalmente**, l'operatore che sta effettuando la predisposizione deve cliccare sulla voce **NO FIRMA**, 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.*

4. REGISTRAZIONE DEI DOCUMENTI NON IN INTEROPERABILITÀ

4.1. Il Protocollo

Il protocollo è, in senso lato, il libro dove vengono registrati progressivamente gli estremi di documenti e atti, in entrata e in uscita, da un soggetto o ente (pubblico o privato). Questa registrazione, se condotta a norma di legge, ha carattere di pubblica e riconosciuta certezza, cioè "fa fede fino a prova di falso" in caso di controversia giuridica (validità probatoria).

Il protocollo serve ad attribuire ad un determinato documento data, forma e provenienza certa attraverso la registrazione dei seguenti elementi (art. 53, c. 1, DPR 445/2000):

- numero di protocollo del documento generato automaticamente dal Sistema;
- data di registrazione;
- data di emissione del documento;
- mittente per il documento in entrata;
- destinatario/i per il documento in uscita;
- oggetto del documento;
- data e n. di protocollo del documento ricevuto, se disponibili;

L'insieme di tali elementi è denominato "registrazione di protocollo" (RdP) ed è memorizzata nel Registro di Protocollo in modo non modificabile.

Il Registro di Protocollo Informatico, va da sé, offre una maggiore velocità di consultazione e ricerca, rispetto a quello tradizionale cartaceo, attraverso l'uso di una maschera di ricerca.

4.1.1. La Rubrica

Per l'inserimento del mittente/destinatario è opportuno far riferimento ai nomi eventualmente pubblicati per ciascuna AOO sull'Indice delle Pubbliche Amministrazioni (IPA). Tuttavia, una rubrica è costantemente aggiornata dal RDS secondo quanto indicato dalle varie AOO. Eventuali aggiunte/varianti alla rubrica potranno essere segnalate al RDS da ogni UOR.

4.1.2. L'Oggetto

Per la descrizione dell'oggetto è opportuna una esplicitazione per esteso, per facilitare successive operazioni di ricerca del documento. Per le

pratiche riguardanti il Personale è opportuno indicare il cognome nel **campo oggetto**.

4.1.3. La Segnatura di Protocollo del Mittente

La segnatura di protocollo è l'apposizione o l'associazione al documento, in forma permanente non modificabile, delle informazioni minime riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile.

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

Durante l'operazione di protocollazione è necessario riportare con attenzione il numero di protocollo del mittente e la data.

4.2. Protocollo di documenti cartacei in entrata all'AOO

La protocollazione informatica di un documento cartaceo prevede una procedura detta di "*dematerializzazione*"

Questa procedura prevede le attività di "acquisizione", "completamento" e "firma per conformità" del documento cartaceo.

4.2.1. Acquisizione

- inserimento del documento nello scanner a disposizione delle UOR;
- acquisizione del documento attraverso la scannerizzazione;
- verifica della qualità della risoluzione del documento così acquisito (dev'essere leggibile);
- verifica dell'integrità e coerenza con l'originale.

4.2.2. Completamento

Per ogni documento accettato si dovranno completare le seguenti informazioni:

- indicazione del mittente (persona fisica, giuridica, altro soggetto);
- del numero di protocollo mittente;
- della data di emissione;
- dell'oggetto del documento.

Il Sistema impedisce di procedere con la registrazione di protocollo qualora si ometta di specificare i precedenti campi obbligatori, tuttavia, allorché non sia presente un protocollo mittente, la segnatura di protocollo univoca può essere prodotta dal sistema stesso (genera segnatura).

4.2.3. Firma digitale dell'addetto per conformità

Apposizione, da parte dell'addetto, della firma digitale sul file ottenuto dal processo di scansione.

Questa attività è necessaria per garantire la "*conformità*" del documento dematerializzato col suo originale e solamente chi ha effettuato l'operazione può assicurare.

Digitati i campi obbligatori e accettato il documento (con apposizione firma digitale), il Sistema genera automaticamente un numero di protocollo univoco di ingresso, con la data corrente e tutte le informazioni di completamento precedentemente inserite dall'operatore.

4.2.4. Il ritiro degli originali cartacei

L'introduzione del sistema ha sensibilmente ridotto la necessità di gestire documenti in formato cartaceo, tuttavia una certa quantità di carta, continua a pervenire all' Area Organizzativa Omogenea.
I rispettivi Responsabili del Servizio potranno procedere alla consegna dell'originale cartaceo alle Unità Organizzative interessate garantendo sia al Responsabile del Servizio sia all'Unità Organizzativa competente, la gestione in sicurezza.
Il sistema presenta, esclusivamente ai Responsabili del Servizio, una funzione nella voce di menù Protocollo, denominata Ritiro Originali Cartacei, attraverso la quale è possibile fare quanto sopra descritto.
La funzione produce l'elenco dei documenti cartacei che vengono consegnati ad una determinata Unità Organizzativa.
Questo elenco, che può essere generato in modalità manuale oppure automatica, in formato PDF, sarà firmato digitalmente dall'operatore che provvede materialmente al ritiro.
L'attività sarà tracciata e consultabile da apposite funzioni di riepilogo storico dell'attività.
È gestito anche il caso di successiva restituzione di un documento

4.3. Protocollo di documenti cartacei 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 già spiegato nel paragrafo inerente il flusso dei documenti informatici, può essere necessario procedere alla trasmissione attraverso il servizio postale tradizionale di uno o più documenti.
Ferme, pertanto, le procedure di preparazione dell'atto da parte dell'operatore incaricato, già descritte nel citato paragrafo inerente al flusso dei documenti informatici, dopo la firma digitale e l'apposizione della timbratura che attesta essere copia di un documento originale informatico o più semplicemente del "*Glifo*" (vedasi pag.10), le UOR provvederanno alla spedizione delle copie destinate all'esterno dell'AOO, mediante i tradizionali canali di posta.

4.4. Protocollo di mail-funzionale

In ingresso

l documento pervenuto attraverso mail-personale deve sempre rispondere al requisito di **leggibilità** e di **chiarezza** riguardo la fonte di provenienza; qualora il supporto cartaceo non ne assicuri la corretta conservazione nel tempo, lo stesso **dovrà essere fotocopiato**.
L'utilizzo della mail-personale soddisfa il prescritto requisito della forma scritta e, se il documento risponde al requisito della ragionevole certezza del mittente, verrà registrato dal Servizio di protocollo.
In aderenza alla normativa vigente, il mittente che invia il documento via mail-personale **non deve inviare** anche la copia del documento originale con altri mezzi; ciò per evitare che uno stesso documento possa avere due protocolli diversi.
Prima di effettuare una registrazione, pertanto, sarà opportuno, tramite il motore di ricerca del Sistema, che l'operatore di protocollo verifichi la presenza di altri documenti registrati con la stessa anagrafica, stesso numero di protocollo mittente e pari data.

4.5. La segnatura di Protocollo

La segnatura di protocollo generata dal Sistema contiene gli elementi essenziali di identificazione del documento:

- indicazione dell'Amministrazione (denominazione e codice identificativo: M_D per il Dicastero Difesa);
- indicazione del Registro annuale a cui fa riferimento (es. REG2020);
- indicazione dell'AOO (denominazione, anche telegrafica, e codice identificativo: E21263, il primo carattere identifica l'Area di appartenenza, ovvero ESERCITO);
- numero progressivo di protocollo (minimo 7 cifre; per numerazione di lunghezza inferiore si aggiungono zeri di riempimento sulla sinistra) numerazione rinnovata ogni anno solare (art. 57, DPR 445/2000);
- data di registrazione (standard gg-mm-aaaa, con zeri di riempimento per giorni e mesi inferiori a dieci ed utilizzando il trattino di separazione codice ASCII45).

Esempio di Segnatura di Protocollo:
M_D E21263 REG2019 1234567 14-08-2019

Il documento, così digitalizzato e protocollato, sarà smistato a seconda dell'organizzazione interna alla UOR competente per la successiva assegnazione al responsabile del procedimento amministrativo (RPA).

4.6. Annullamento di una registrazione

L'annullamento di una registrazione di protocollo, prevista dall'art. 8 del DPCM 03.12.2013, è prerogativa del **Responsabile del Servizio di Protocollo**. L'annullamento deve essere chiesto al RDS con specifica nota motivata da parte del RPA, indicandola sulle "Note" e inviandola, via AD[h]OC, al RDS.

L'RDS non entrerà nel merito e rispetterà la motivazione, insindacabile, addotta.

Le informazioni relative alla registrazione di protocollo annullata (data, autore annullamento, estremi autorizzazione RDS) rimangono memorizzate nel registro informatico di protocollo per essere sottoposte a tutte le elaborazioni previste dalla procedura, comprese visualizzazioni e stampe. La procedura riporta la dicitura "annullato" in posizione visibile e tale da consentire comunque la lettura delle informazioni originarie.

4.7. Documenti da protocollare

La *ratio* che deve governare il comportamento di un operatore durante la fase di protocollo di un documento in arrivo, deve essere improntata alla **valutatività** e alla **attestazione**. In altre parole, l'addetto al protocollo deve valutare:

- l'attendibilità del mittente;
- leggibilità e coerenza del Documento;
- riconoscerne le eventuali priorità.

Inoltre, l'operatore deve attestare che un determinato documento così come si registra è pervenuto.

Si tratta dunque di una delicata competenza di tipo "notarile", attestante la certezza giuridica di:

- data;

– forma;
– provenienza per ogni documento, **senza interferire su di esso**.

I documenti da protocollare sono tutti quelli previsti dal relativo piano di classificazione, con eccezione dei documenti elencati nell'art. 53, c. 5, DPR 445 del 2000 e al punto seguente.

4.8. Documenti da non protocollare

Di seguito sono riportati i **documenti esclusi** dalla registrazione di protocollo (esplicitati dal par.5.6.2.11, Circ.SMD-I-2004):

– gazzette ufficiali;
– bollettini ufficiali P.A.;
– notiziari P.A.;
– note di ricezione circolari o altre disposizioni;
– materiali statistici;
– giornali, riviste, libri;
– materiali pubblicitari;
– inviti a manifestazioni, cartoline e biglietti d'auguri
– certificati medici (riportanti la diagnosi della malattia);
– modelli per la dichiarazione dei redditi;
– lettere personali e corrispondenza "e.p.t." (esclusivo per il titolare);
– provvedimenti medico-legali;
– fogli di viaggio;
– note caratteristiche, rapporti informativi;
– registro delle presenze;
– licenze, permessi, istanze del personale che non attivano procedimenti amministrativi;
– esposti anonimi;
– documenti classificati;
– tutti i documenti già soggetti a registrazioni particolari dell'Amministrazione.

4.9. Privacy e protezione dei dati personali

La trattazione dei documenti contenenti dati personali sensibili e giudiziari deve avvenire nel rispetto della L. n. 675 del 1996 e successive disposizioni di modifica ed integrazione e, a decorrere dal 1 gennaio 2004, da quelle previste dal D.Lgs. n.196 del 2003 "*Codice in materia di protezione dei dati personali*".

I documenti contenenti dati sensibili (cioè quelli idonei a rivelare: l'origine razziale ed etnica, la fede religiosa o filosofica, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale) e i dati giudiziari non devono essere trattati all'interno del sistema automatizzato di gestione documentale, dove dev'essere registrata **la sola lettera di trasmissione o il solo protocollo del documento**, avendo cura di inoltrare lo stesso, secondo i tradizionali sistemi di gestione della posta, in busta chiusa recante l'apposita dicitura:

– *"CONTIENE DATI SENSIBILI DA TRATTARE AI SENSI DELLA L. N. 675/96";*
– "*CONTIENE DATI GIUDIZIARI DA TRATTARE AI SENSI DELLA D.LGS. N. 196/03" e custoditi negli archivi fisici della UOR.*

4.10. Registro giornaliero di protocollo

La registrazione di protocollo è un atto pubblico che consente di verificare l'effettivo ricevimento o spedizione di un documento. Ciascuna registrazione di protocollo è annotata sul registro di protocollo, che è un repertorio dal quale si evince l'effettiva ricezione/spedizione di un documento, indipendentemente dalla regolarità del documento stesso.

Al fine di tutelare l'integrità e la regolarità delle registrazioni, il sistema provvede quotidianamente alla stampa del **registro giornaliero di protocollo**, firmata digitalmente dal RDS (tramite firma remota HSM) e archiviata all'interno del sistema.

Entro il mese di gennaio, il RDS provvede alla stampa del registro di protocollo dell'anno precedente, lo firma digitalmente e ne custodisce una copia agli atti, insieme all'indice delle PEC ricevute in quell'anno.

Per evitare vuoti nella sequenzialità della numerazione del registro, il sistema assegna il numero di protocollo e la data di registrazione solo dopo che sono stati inseriti gli atri dati (mittente/destinatario, data e protocollo del documento ricevuto).

La numerazione di protocollo è unica, sia per i documenti in entrata che per quelli in uscita.

Non è assolutamente consentito, ancorché impossibile, "prenotare" o "lasciare in sospeso" numeri di protocollo.

5. GESTIONE DELL'ARCHIVIO DEI DOCUMENTI INFORMATICI

5.1. L'archivio

Il sistema di archiviazione di seguito descritto mira al rispetto della normativa vigente in materia di diritti civili e responsabilità amministrativa, recata dal codice civile agli articoli 2946 e 2947, dalla L. 20 del 1994 e dal D.Lgs. 41 del 2004.

L'archivio è definito come il complesso dei documenti prodotti e acquisiti dal soggetto produttore nell'esercizio delle sue funzioni.

Esso si distingue in:

- archivio corrente: costituito dall'insieme dei documenti correnti, relativo a procedimenti in atto;
- archivio di deposito: rappresentato dall'insieme dei documenti definiti semi-correnti (o semi-attivi), ovvero non più necessari allo svolgimento delle attività correnti, ma ancora utili per finalità amministrative;
- archivio storico: è l'insieme dei documenti storici, ovvero riferiti a procedimenti amministrativi conclusi da oltre 40 anni, opportunamente conservati.

I documenti, conseguentemente, si distinguono in:

- **correnti**: i documenti relativi a procedimenti correnti, documenti dell'anno in corso;
- **di deposito o semi-correnti**: i documenti ancora utili per finalità amministrative, ma non più necessari allo svolgimento delle attività correnti;
- **storici**: i documenti relativi a procedimenti amministrativi esauriti da oltre 40 anni e selezionati per la conservazione permanente.

5.2. Il Sistema di Conservazione

Il sistema di Conservazione verrà utilizzato nell'ambito delle disposizioni che saranno impartire dal Responsabile della Conservazione del dicastero.

5.3. Organizzazione archivistica dell'AOO

A partire dalla data di avvio del servizio, l'AOO produce principalmente originali informatici, mentre tutti gli atti cartacei prodotti o pervenuti vengono "***de-materializzati***" e sottoposti a "**conservazione sostitutiva**". Pertanto l'universalità dei documenti originali afferenti all'AOO 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 col vecchio sistema di protocollo (PROMIL e cartaceo) in modalità cartacea che saranno gestiti con il sistema di **custodia decentrato** da parte delle UOR. Presso ogni UOR l'archiviazione è così articolata:

- uno stesso archivio contiene i documenti relativi all'anno in corso (correnti) e ai 10 anni precedenti (semi correnti), opportunamente distinti;
- un archivio di deposito contiene i documenti archiviati oltre i 10 anni precedenti, che si intendono esauriti;
- un archivio storico contiene quei documenti esauriti da oltre 40 anni e selezionati per la conservazione permanente, sulla base della normativa vigente.

5.4. La Conservazione

Seguendo quanto indicato dalle Regole tecniche vigenti e sulla base del modello OAIS (*open archival information system*) che definisce le caratteristiche di un archivio finalizzato alla conservazione a lungo termine di Documenti informatici e alla fruizione degli stessi da parte di una comunità di riferimento, si possono identificare i seguenti ruoli fondamentali: Produttore, Responsabile della Conservazione, Responsabile del Servizio di Conservazione, Utente.

5.4.1. Produttore

È il soggetto che affida la conservazione dei propri Documenti informatici al Centro di Dematerializzazione e Conservazione Unico della Difesa (CEDECU).

Nel ruolo del Produttore possono essere definiti tutti gli Enti della Difesa e di altre Pubbliche Amministrazioni nonché terzi privati che trasmettono al CeDeCU i documenti e i fascicoli da conservare, in continuità con il proprio processo di gestione documentale.

I rapporti tra l'AID, tramite il CeDeCU, e i Produttori vengono formalizzati e regolati per mezzo di due documenti fondamentali: la Convenzione e il Disciplinare tecnico *(L'attivazione della convenzione fra il Rds dell'Aoo e il RSC sarà effettuata entro l'anno 2020).*

Il Produttore, secondo quanto previsto nella convenzione, si impegna a depositare i documenti informatici e le loro aggregazioni documentali informatiche nei modi e nelle forme definite da AID, garantendone l'autenticità e l'integrità nelle fasi di produzione e di archiviazione corrente, effettuata nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando

formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente. Si impegna inoltre a depositare e mantenere aggiornati, nei modi e nelle forme definite da AID, tramite il CeDeCU, gli strumenti di ricerca e gestione archivistica elaborati a supporto della formazione dei documenti e della tenuta degli archivi.

Il Produttore mantiene la titolarità e la proprietà dei documenti depositati.

Le tipologie documentarie da trasferire, le modalità di versamento e i metadati sono concordati e specificati nel Disciplinare tecnico, redatto a cura dei referenti e responsabili di riferimento del Produttore e del CeDeCU per l'erogazione dei servizi per le diverse tipologie documentarie indicati in esso. È formato da specifiche parti relative alle diverse tipologie documentarie oggetto di conservazione. Potrà essere aggiornato in caso di modifiche nelle modalità di erogazione dei servizi, anche a seguito di eventuali modifiche normative. Viene validato dal Responsabile del Servizio del CeDeCU.

Il Produttore resta il responsabile del contenuto del Pacchetto di Versamento (d'ora in poi PdV) ed è obbligato a trasmetterlo al servizio di conservazione secondo le modalità operative descritte genericamente nel presente Manuale e in dettaglio nel Disciplinare tecnico e nella documentazione tecnica di riferimento

5.4.2. Utente

L'utente è la persona fisica o giuridica, interna o esterna al Sistema di conservazione, secondo il modello organizzativo adottato, che interagisce con i servizi di un Sistema di gestione informatica dei documenti e/o di un Sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

L'utente è un soggetto riconosciuto dal Servizio di conservazione autorizzato ad usufruire del servizio.

Il Sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un Pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati.

Nel ruolo dell'Utente sono definiti gli specifici soggetti abilitati dal Produttore, in particolare gli operatori eventualmente indicati dal Produttore e riportati nel Disciplinare tecnico, che possono accedere esclusivamente ai documenti versati dal Produttore stesso o solo ad alcuni di essi secondo le regole di visibilità e di accesso concordate tra Produttore e Conservatore.

Altri utenti sono identificabili con figure tecniche o funzionali interne alla struttura del CeDeCU che hanno la necessità di interagire con il Sistema di Conservazione per garantire il relativo servizio.

L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione, e nel rispetto delle misure di sicurezza previste dalla normativa vigente.

5.4.3. Il Responsabile della Conservazione di UOR

Il Responsabile della Conservazione si trova presso il Produttore ed affida le attività della conservazione al Responsabile del Servizio della Conservazione che opera all'interno del CeDeCU.

Il Responsabile della Conservazione, tramite il CeDeCU, si impegna alla conservazione dei documenti trasferiti e ne assume la funzione di Responsabile della conservazione ai sensi della normativa vigente.

Per l'**AOO-8°rgt. b.**, considerata la struttura, la vastità e complessità delle Materie trattate, ogni UOR dovrà nominare un ARCHIVISTA di **UOR** (di Sezione) i quali, supervisionati dal RDS, effettueranno le attività della gestione archivistica, in particolare, provvederà a:

- individuare, in concerto con il proprio Responsabile di UO, di quale tipologia e argomento documentale procedere alla Fascicolazione;
- creare i Fascicoli secondo il Piano di Classificazione (art. 5.5 del Manuale di Gestione) con la decodifica individuata nell'art .5.6 del Manuale di Gestione;
- abilitare il Personale di UOR alla **Fascicolazione** o alla semplice **Consultazione**;
- procedere alla fascicolazione dei Documenti Informatici in Entrata e in Uscita dalla UOR (qualora non abbia abilitato altro Personale della UOR, *vds. lettera precedente*);
- procedere alla chiusura dei Fascicoli al termine dell'iter amministrativo o secondo quanto disposto dal RDS.

5.5. Piano di Classificazione

In un sistema di gestione e tenuta dei documenti è fondamentale conoscere l'insieme delle relazioni che un documento ha con tutti gli altri e, più in particolare, con quelli che riguardano il medesimo procedimento amministrativo. A tale scopo ciascun documento deve essere classificato.

La normativa vigente, in particolare l'art. 50, c. 4, DPR n. 445 del 2000 ed il DPCM 03.12.2013, stabilisce che la classificazione d'archivio deve adottare principi di coerenza funzionale nell'ambito di ciascuna AOO e presentare modalità di articolazione uniformi. L'applicazione di un piano di classificazione o titolario di archivio, che si presenta come un sistema integrato di informazioni sui documenti basato sul loro ordinamento funzionale, costituisce un presupposto indispensabile per la realizzazione e lo sviluppo della gestione informatica dei flussi documentali.

Il piano di classificazione consiste in uno schema generale di voci logiche, stabilite in modo uniforme, articolate tendenzialmente in modo gerarchico, che identificano l'unità archivistica, cioè l'unità di aggregazione di base dei documenti all'interno dell'archivio (fascicolo).

Nell'unità archivistica i documenti sono ordinati tipicamente per data di acquisizione.

E' necessario che le voci del **Titolario di Archivio** non si identifichino con la struttura organizzativa della relativa amministrazione poiché la stessa struttura può essere soggetta a trasformazioni.

Tutti i documenti di una pubblica amministrazione, a prescindere dallo stato di trasmissione (in arrivo, in uscita, interni), sono soggetti a classificazione. Uno stesso documento può essere classificato più volte.

Il Titolario di archivio consente di definire i criteri di formazione e di organizzazione dei fascicoli e delle serie di documenti logicamente simili (circolari, verbali, registri contabili, ecc.); consente di reperire tutti i documenti relativi ad una specifica attività o procedimento amministrativo; consente, inoltre, di selezionare i documenti archiviati ai fini della loro conservazione ovvero della loro distruzione.

Per l'AOO viene adottato il **Titolario d'archivio di Forza Armata**, il cui piano di classificazione si suddivide in **titoli**, **classi** e **sottoclassi**:

- il titolo individua le c.d. Macrofunzioni (funzioni primarie e di organizzazione dell'Ente);
- le altre partizioni corrispondono a specifiche competenze che si collegano alla macrofunzione descritta nel titolo, secondo un'articolazione gerarchica che scende a un progressivo dettaglio.

Il titolario non è retroattivo, quindi si applica ai documenti protocollati dopo la sua introduzione. L'aggiornamento del titolario compete allo SME-IV Reparto Sistemi C3I.

Qualunque sia la tipologia (elettronico, cartaceo, ecc.), **tutti i documenti devono essere classificati** e inseriti nel fascicolo di riferimento; il piano di classificazione costituisce, pertanto, lo strumento principale per identificare la posizione logica del documento.

5.6. I fascicoli

Il fascicolo è l'insieme ordinato di documenti, relativi ad uno stesso procedimento amministrativo, a una stessa materia, a una stessa tipologia, che si forma nel corso dell'attività amministrativa allo scopo di riunire tutti i documenti utili per il procedimento stesso.

I fascicoli possono essere organizzati:

- **per oggetto**: il fascicolo contiene i documenti relativi ad una materia specifica o a una persona fisica o giuridica;
- **per procedimento amministrativo**: il fascicolo contiene tutti i documenti ricevuti, spediti, interni relativi ad un medesimo procedimento amministrativo;
- **per anno**, specificando o meno la tipologia di documento/i inserita.

Un Documento può essere classificato e fascicolato in più fascicoli.

5.7. Archiviazione dei documenti informatici nel server dell'AD[h]OC

I documenti informatici sono archiviati su supporti di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo e custoditi presso i server.

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 prodotto il **registro giornaliero** delle registrazioni di protocollo, firmato digitalmente in modalità automatica con le credenziali di Firma Digitale del RDS attraverso un "***Hardware Security Module***" **(**HSM) depositato presso un certificatore accreditato alla DigitPA (**http://archivio.digitpa.gov.it/firma-elettronica/firma-remota**).

I Documenti sottoposti alla fascicolazione sono definiti e gestiti dal responsabile di UOR (vds. Art.5.4).
Presso la AOO, a cura dell'RDS, sono conservate copia delle PEC ricevute e spedite, in quanto l'Ente Gestore le conserva nei propri *server* per un massimo di 30 mesi.

6. PIANO DI SICUREZZA

6.1. Analisi dei rischi

I documenti informatici sono oggetto di un apposito piano di sicurezza. L'analisi dei rischi è stata effettuata al fine di garantire sia l'integrità fisica delle differenti tipologie documentarie, sia la tutela e la riservatezza delle informazioni contenute nei predetti documenti, ferme restando le predisposizioni di competenza delle singole UO sugli allegati analogici ricevuti a corredo dei relativi documenti informatici, in ingresso e/o prodotti, di competenza.

6.2. Documenti oggetto di analisi

Le tipologie documentarie che caratterizzano l'AOO-8° rgt. b. possono, a loro volta, essere suddivise in documenti:

- sprovvisti di una qualsiasi delle classifiche di segretezza, denominati "ordinari";
- contenenti dati personali, a norma del D.lgs. 30 giugno 2003 – 196, Art. 4, comma 1, lettere a, b, c;
- contenenti dati sensibili e/o giudiziari, a norma del D.lgs. 30 giugno 2003 – 196, Art. 4, comma 1, lettere b, d, e, ed a mente del Decreto del Ministro della Difesa 13 aprile 2006, n. 203;
- contenenti una qualsiasi delle classifiche di segretezza.

6.3. Provvedimenti adottati

Alla luce di quanto esposto e tenuto conto delle funzionalità che caratterizzano la procedura AD[h]OC e l'intero sistema di gestione del Servizio (software di base, software applicativo, LAN e singole stazioni di lavoro), il RdS ha definito i seguenti provvedimenti:

- sono oggetto di trattazione del Servizio tutti i documenti ordinari;
- sono oggetto di trattazione del Servizio tutti i documenti contenenti dati personali e dati sensibili, per i quali dovranno essere adottate le procedure atte a garantirne la riservatezza delle informazioni e la sicurezza dei dati di seguito descritte;
- non sono oggetto di trattazione del Servizio tutti i Documenti riportanti una delle classifiche di segretezza.

6.4. Procedure per la riservatezza e la sicurezza dei dati

Allo scopo di garantire la riservatezza e la sicurezza dei dati contenuti nei documenti riportanti informazioni personali o sensibili di cui ai precedenti sottopara. 2.2 e 2.3, il RdS dispone quanto segue:

6.4.1. Apertura plichi.

I plichi destinati alle UO che fruiscono del Servizio devono essere aperti esclusivamente dal personale del Nucleo Legale dell'Ufficio Maggiorità e Personale, in possesso della nomina quale "incaricato del trattamento dei dati personali ai sensi del D.lgs. 196/2003 e 66/2010" ed opportunamente istruito sulle responsabilità connesse, consegnando

successivamente, il tutto all'Addetto AD[h]OC per la registrazione e segnatura dei documenti.
I Documenti riportanti informazioni personali, sensibili e/o giudiziarie devono essere sottoposti alle attività di Registrazione e di Segnatura, esclusivamente da parte del personale operatore SU./Grd. Incaricato per il trattamento dei dati personali".

6.4.2. Accesso al sistema

L'accesso al sistema avviene per mezzo di un **processo di autenticazione** che funziona mediante piattaforma Windows e che consente l'utilizzo della postazione di lavoro. Questo è verificato in tempo reale su un apposito sistema di autenticazione fornendo le proprie **credenziali d'accesso**.
Gli utenti del Servizio di Protocollo, in base alle rispettive competenze, hanno **autorizzazioni di accesso differenziate** in base alle tipologie di operazioni da effettuare.
Ad ogni utente è assegnata una credenziale di accesso, costituita da:
- "*user name*", che permette l'identificazione dell'utente da parte del sistema;
- "*password*" riservata di autenticazione;
- profilo assegnato, ovvero autorizzazione di accesso specifica per determinate/limitate operazioni di protocollo e gestione documentale;
- accesso tramite **Carta Multi-Servizi della Difesa** (CMD) attraverso i codici CARTA in possesso all'Utente.

Il sistema consente di registrare le seguenti informazioni relative a:
- accessi al sistema effettuate da un dato operatore;
- operazioni effettuate su un dato documento;
- operatore che ha effettuato una certa operazione;
- operazioni effettuate nell'ambito di una data sessione.
- Il sistema consente inoltre la riconfigurazione del modello sicurezza attraverso:
- creazione e cancellazione di utenti;
- configurazione dei diritti di utenti;
- configurazione dei diritti di accesso ad un documento;
- configurazione dei diritti di accesso ai fascicoli;
- configurazione dei diritti di accesso attraverso le voci di titolario.

***ATTENZIONE**: Tutti gli Utenti dovranno essere edotti, a cura delle rispettive UOR d'appartenenza, sulle norme relative al Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", c.d. "Legge sulla privacy"*

6.4.3. Abilitazioni di accesso

Il RDS, avvalendosi di un'utenza privilegiata (amministratore del sistema), assegna agli utenti i diversi livelli di autorizzazione all'accesso, sulla base delle rispettive competenze.
Una singola persona può ricoprire più ruoli funzionali all'interno del sistema, comunque mantenendo la stessa *password* di accesso, in quanto legata alla persona fisica.

Tutti gli utenti dell'AOO sono abilitati ad accedere al Sistema, ma **il livello di autorizzazione per l'accesso alle funzioni della procedura assegnato sarà diversificato**.

L'operazione di aggiornamento dei profili stabiliti dal RDS, andando a modificare l'ordinamento delle UO, viene determinata solo ed esclusivamente previo formali richieste dei responsabili delle diverse UO rivolte al RDS.

6.4.4. Gestione delle registrazioni di protocollo

Nella registrazione di protocollo, i campi relativi al numero di protocollo, data di registrazione e numero di allegati non sono alterabili da alcuno, neanche dall'amministratore; le informazioni relative al mittente, ai destinatari e all'oggetto possono essere modificati da chi possiede il relativo privilegio.

Ogni operazione di modifica viene registrata. Il sistema è in grado di generare l'elenco delle modifiche effettuate su una data registrazione ottenendo in dettaglio:

- nome dell'utente che ha eseguito l'operazione;
- data e ora;
- valore precedente dei campi soggetti a modifica, permettendo quindi una completa *ricostruzione cronologica di ogni registrazione e successiva lavorazione.*

Il Sistema non consente di effettuare cancellazioni: in alternativa è previsto, per gli utenti abilitati, l'annullamento di un numero di protocollo accompagnato da una motivazione.

Giornalmente ad un'ora prestabilita, la procedura consente di produrre e archiviare il Registro di protocollo. L'archiviazione avviene sui server del CSIE in Roma e sono accessibili al RDS.

6.5. Registro di Emergenza

Il DPR n. 445 del 28 dicembre 2000 all'art. 63, comma 1, stabilisce che, *"ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica, ogni evento deve essere registrato manualmente su uno o più supporti alternativi, denominati "Registro di emergenza".*

6.5.1. Attivazione

Il Registro di Emergenza sarà attivato da un "Provvedimento di attivazione" da parte del RdS, contenente data, causa ed ora di interruzione del Servizio, con la seguente procedura:

- dalla emanazione del Provvedimento di attivazione, il RdS trascrive, sul Registro di Emergenza, gli estremi del Provvedimento di attivazione e le indicazioni relative alla data, causa ed ora di interruzione del Servizio in esso contenuti;
- durante il periodo di interruzione del Servizio, le UO che hanno necessità di Protocollare in entrata/uscita documenti che presentino improcrastinabili esigenze di carattere amministrativo/operativo, si recapiteranno all'operatore al protocollo presso i locali del Servizio AD[h]OC i registri/documenti per la trascrizione manuale del Registro di Emergenza.

6.5.2. Modalità di compilazione

Alla ricezione del "Provvedimento di attivazione", il RdS trascrive sul primo rigo utile gli estremi del suddetto Provvedimento.

Dal rigo successivo, rispettando la numerazione progressiva, ogni Registrazione di Emergenza sarà effettuata mediante la trascrizione dei seguenti dati:

- Numero di protocollo costituito dal Codice identificativo della UO (Cod. id.), seguito dal numero progressivo;
- Data di arrivo del documento;
- Mittente (per i documenti in entrata);
- Data e protocollo del documento;
- Oggetto;
- Data di partenza del documento (se trattasi di documento in uscita);
- Destinatari;
- Indice di classificazione.

6.5.3. Sospensione del registro di emergenza per ripristino del servizio

All'atto del ripristino del Servizio, sarà emesso un "Provvedimento di sospensione" con la data e l'ora di riavvio del Servizio.

6.5.4. Modalità di sospensione

All'atto della emanazione del "Provvedimento di sospensione", il RdS trascrive, sul primo rigo utile successivo all'ultima Registrazione di Emergenza, gli estremi del Provvedimento.

Ogni qualvolta il Registro di Emergenza sarà riattivato, la numerazione progressiva del protocollo riprenderà dal numero successivo all'ultimo utilizzato.

6.6. Attività informativa e disposizioni finali.

I documenti oggetto della presente trattazione devono essere inoltrati alle UO destinatarie da parte dello stesso personale mediante l'utilizzo della specifica funzione della procedura che consente di apporre il "flag" alla voce "Dati Sensibili".

Tale protezione consentirà la visibilità del documento e dei suoi dati di registrazione esclusivamente ai diretti destinatari ed ai titolari dei successivi inoltri, se provvisti dell'autorizzazione alla trattazione dei dati sensibili predisposta dal RdS su richiesta del Resp. dell'UO di appartenenza.

Tali disposizioni sono:

- oggetto di attività informativa rivolta al personale utente della procedura AD[h]OC, che si svolge all'atto dell'avvio del Servizio presso ciascuna UO;
- consultabili sul presente MdG, diramato a tutte le UO dell'AOO-8° rgt. b. e pubblicato sul sito web intranet dello SME;
- oggetto di attività informativa di aggiornamento svolta periodicamente da parte del RdS, soprattutto a vantaggio del personale neo-assegnato.

6.6.1. Modalità di aggiornamento del manuale

Il Responsabile del Servizio di Protocollo ha il compito di garantire la corretta applicazione delle regole contenute nel manuale di gestione nonché di curarne l'aggiornamento a seguito di:

- normativa sopravvenuta;
- in relazione alle eventuali/nuove esigenze di ordine organizzativo;
- modifiche apportate negli allegati;
- cambio del RDS;
- qualsiasi altro evento che ne alteri significativamente l'aderenza allo "status quo".

ALLEGATO A

RIFERIMENTI NORMATIVI

Di seguito sono riportati i riferimenti normativi di maggior rilevanza costituenti argomento di questo Manuale con le relative abbreviazioni indicate tra parentesi quadre 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: sono qui riportati solo gli atti principali, rimandando a eventuali richiami all'interno del Manuale per le norme di maggior dettaglio.

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013
Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 " Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5– bis, 23 – ter, comma 4, 43, commi 1 e 3, 44, 44 – bis e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005." e, " Regole tecniche per il protocollo informatico ai sensi degli articoli 40 – bis, 41,47,57-bis e 71, del del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005.

Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445. [DPR]
Disposizioni legislative in materia di documentazione amministrativa. Con il DPR n. 445 si effettua una razionalizzazione e semplificazione della normativa inerente al PI. Viene, pertanto, abrogato (art. 77 DPR) 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 DPR. Il DPR è il documento di riferimento principale per il PI.

Decreto Legislativo 30 giugno 2003 n. 196 e successive modificazioni [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.

Circolare Agid n.60 del 23 gennaio 2013.
Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni.

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

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

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

ALLEGATO B

ABBREVIAZIONI IN USO

Per rendere più snello il testo del presente Manuale sono utilizzate una serie di sigle, acronimi e abbreviazioni riportate di seguito con il relativo significato.
Per alcune delle abbreviazioni usate sono forniti ulteriori dettagli nel Glossario.

A.D. – Amministrazione Difesa.

Ad. – Addetto.

AOO Area Organizzativa Omogenea

[CAD] Codice Amministrazione Digitale **-** D.Lgs 7 marzo 2005 n. 82

[CIRC] Circolare AIPA 7 maggio 2001 n. 28

[CODBCP] Codice dei Beni Culturali e del Paesaggio **-** Decreto Legislativo n. 22. 01.2004 n. 41

[CODPRI] Codice di Protezione dei dati Personali **-** Decreto Legislativo 30 giugno 2003 n.196

DigitPa Ente Nazionale per la digitalizzazione della Pubblica Amministrazione

[DIR] Direttiva SMD-I-004

[DPCM] Decreto della Presidenza del Consiglio dei Ministri 31 ottobre 2000

DPR Decreto del Presidente della Repubblica

[DPR] DPR 30 dicembre 200 n. 445

D.Lgs Decreto Legislativo

l. Legge

IPA Indice delle Pubbliche Amministrazioni

Mdg – Manuale di Gestione.

P.A. Pubblica Amministrazione

PEC Posta Elettronica Certificata

PEI Posta Elettronica Istituzionale

PI Protocollo Informatico

RDS Responsabile del Servizio

RPA Responsabile del Procedimento Amministrativo

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

UO Unità Organizzativa

UOR – Unità organizzativa Responsabile**.**

ALLEGATO C

GLOSSARIO

L'applicazione della normativa inerente al Protocollo Informatico introduce una serie di termini e concetti nuovi che, nel presente paragrafo, sono definiti e spiegati.

Amministrazioni Pubbliche
Per Amministrazioni Pubbliche si intendono quelle indicate nell'art. 1, comma 2 del D.Lgs n. 165 del 30 marzo 2001.

Archivio
L'archivio è la raccolta ordinata degli atti spediti, inviati o comunque formati dall'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali.
Gli atti formati e/o ricevuti dall'Amministrazione o dall'AOO sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono. Essi sono ordinati e archiviati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico.

Archiviazione elettronica
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).

Area Organizzativa Omogenea (AOO)
Una AOO rappresenta un insieme di Unità Organizzative (UO) facenti capo alla stessa Amministrazione che usufruiscono, in modo omogeneo e coordinato, dei servizi informatici per la gestione dei flussi documentali e, in particolare, del servizio di protocollazione (art. 50, comma 4 del [DPR]).
Per ciascun tipo di provvedimento relativo ad atti di propria competenza, è individuata l'UO responsabile dell'istruttoria e di ogni altro adempimento instaurato per l'adozione del provvedimento finale. Dove in precedenza potevano esistere una serie di registri di protocollo, in una AOO è previsto l'utilizzo di un unico registro.

Documento analogico
Rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, let. p)-bis del [CAD]).

Dati anonimi
Dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile (art. 4, comma 1, let. n) del [CODPRI]).

Dati giudiziari
I dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1 del [DPR]. Dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile (art.4, comma 1, let. n) del [CODPRI]).

Documento informatico
Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, let. p) del [CAD]).

Dati personali
Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificata o identificabile, 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]).

Fascicolazione
L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi.

Fascicolo
Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento/processo amministrativo, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi tutti i documenti utili allo svolgimento di tali attività.

Firma digitale
Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e un sistema chiavi crittografate, una pubblica e 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 un insieme di documenti informatici.

Manuale di Gestione del Protocollo Informatico
Il Manuale, previsto dall'art. 5 del [DPCM], 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
Il Manuale deve essere predisposto dal RDS quale garante dell'applicazione, nell'ambito dell'AOO di pertinenza, delle procedure indicate al suo interno ed il suo contenuto può essere organizzato da ciascun RDS secondo le specifiche della rispettiva AOO.

Posta Elettronica Istituzionale (PEI)
La PEI è la e-mail istituita da ciascuna AOO attraverso la quale possono essere ricevuti i messaggi da protocollare.

Posta Elettronica Certificata (PEC)
La PEC, fornisce un servizio di messaggistica che sfrutta gli standard propri della posta elettronica ed assicura al mittente l'attestazione di avvenuta ricezione del messaggio ed al destinatario la garanzia dell'identità del mittente. Questo servizio, strettamente connesso all'utilizzo della firma digitale per l'individuazione dei soggetti intervenuti nel processo di trasmissione e ricezione del documento, comprende altre funzionalità al fine di permettere confidenzialità, integrità, tracciabilità e storicizzazione del messaggio.

Responsabile del Procedimento Amministrativo (RPA)
Il RPA si identifica con il dipendente della PA cui è affidata la gestione del procedimento amministrativo. E' il Dirigente/Comandante dell'UO interessata che assegna a sé, oppure a un altro dipendente dell'unità, il ruolo di responsabile del procedimento.

RDS - Responsabile del Servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi
Il RDS è una ulteriore novità di rilievo introdotta dall'art. 61 del [DPR]. In sostanza si tratta di una figura ben diversa dal classico Capo Ufficio Posta o figure similari da sempre presenti nell'Amministrazione della Difesa. I suoi compiti, elencati nell'art. 61 del [DPR] e nell'art. 4 del [DPCM], 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 dei cittadini/ditte/altre Pubbliche Amministrazioni.

Titolario e relativa classificazione d'archivio
Unitamente al Manuale, è redatto, per ciascuna AOO, anche il Titolario con la relativa classificazione d'archivio. Esso è uno schema generale di voci logiche rispondenti alle esigenze funzionali articolato in modo gerarchico, al fine di identificare, partendo dal generale al particolare, l'unità di aggregazione di base dei documenti all'interno dell'archivio.
Tutti i documenti che entrano a far parte dell'archivio dell'AOO, sono soggetti a classificazione.
Inoltre, uno stesso documento può essere classificato più volte in base alla molteplicità di funzioni individuate, cercando di contenerne il numero. Tale molteplicità, peraltro, comporta, in un ambiente tradizionale, la duplicazione del documento mentre, in un ambiente digitale, sono duplicate solo le informazioni di collegamento.

Unità organizzativa (UO)
Per UO s'intende uno dei sottoinsiemi dell'AOO rappresentato da un complesso di risorse umane e strumentali cui sono state affidate competenze omogenee nell'ambito delle quali il Capo Ufficio/Sezione o Comandante risulta essere il Responsabile del Procedimento Amministrativo (RPA) nella trattazione dei documenti o procedimenti amministrativi.

ALLEGATO D

8° REGGIMENTO BERSAGLIERI

Oggetto: Atto costitutivo dell'Area Organizzativa Omogenea (AOO)

IL COMANDANTE DELL'ENTE

VISTO l'art. 50 del DPR del 28 dicembre 2000, n. 445 recante Disposizioni legislative in materia di documentazione amministrativa.

D I S P O N E

A decorrere dal 03 luglio 2017 la costituzione dell'Area Organizzativa Omogenea codice **M_D E21263** dell'8° reggimento bersaglieri così articolata:

E21263
LIVELLO I: COMANDANTE DI REGGIMENTO
LIVELLO II : OPERATORE FLUSSO DOCUMENTALE
LIVELLO III:01 AIUTANTE MAGGIORE
LIVELLO III:02 CAPO UFFICIO OAI
LIVELLO III:03 CAPO UFFICIO LOGISTICO
LIVELLO III:04 CAPO SEZ. COORDINAMENTO AMMINISTRATIVO
LIVELLO III:05 COMANDANTE DI BATTAGLIONE
LIVELLO III:06 COMANDANTE CCSL

ALLEGATO E

8° REGGIMENTOBERSAGLIERI

Oggetto: Nomina del responsabile e del Vicario del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi dell'8° reggimento bersaglieri.

IL COMANDANTE

VISTO il DPR 28 dicembre 2000, n. 445 – "Disposizioni legislative in materia di documentazione amministrativa" e successive varianti e, in particolare, l'art. 61;

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

NOMINA *

- il Magg. Daniele COLELLA, Responsabile del Servizio di gestione dei flussi documentali e del protocollo informatico presso l'8° reggimento bersaglieri;

- il C.le Magg. Ca. Sc. Qs. Massiminiano PATELLA, Vicario nei casi di assenza o impedimento del Responsabile del servizio. Inoltre svolge funzioni di Amministrazione locale del Sistema di Protocollo Informatico.

IL COMANDANTE

Col. f. (b.) t. ISSMI Giampiero BISANTI

Caserta, _____

Per ricevuta e accettazione.

data, _____ firma RDS _____

data, _____ firma VICARIO _____

***originale custodita agli atti di questo Comando.**

Allegato F

Richiesta di avvio del Servizio AD[h]OC dell'AOO – 8° RGT. B.

(originale custodita agli atti di questo Comando)

Allegato G

PROSPETTO DATI PER LA PUBBLICAZIONE DELL'AREA ORGANIZZATIVA SUL SITO DIFESA E SULL'IPA

<< 8° REGGIMENTO BERSAGLIERI>>

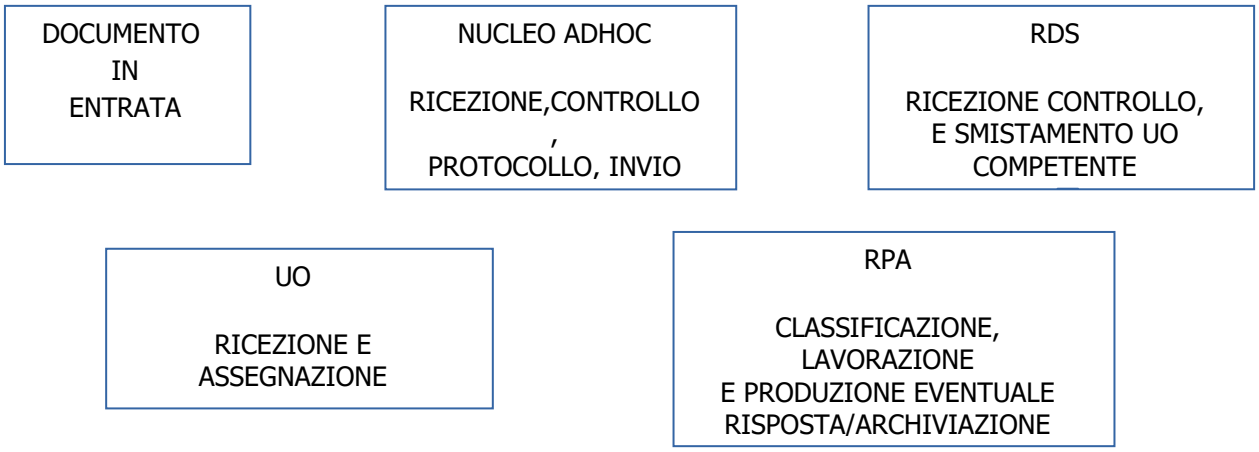
Identificativo	E21263
Descrizione	8° REGGIMENTO BERSAGLIERI
Descrizione abbreviata	rgtb8
Email istituzionale PEI	rgtb8@esercito.difesa.it
Email istituzionale PEC	rgtb8@postacert.difesa.it
Indirizzo	Via Laviano, 8 - 81100 CASERTA
Telefono su linea militare	1525274
Telefono su linea militare per contatti con rds	1525489
Linea commerciale	0823215273

SERVIZIO PER LA GESTIONE INFORMATICA DEI DOCUMENTI, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

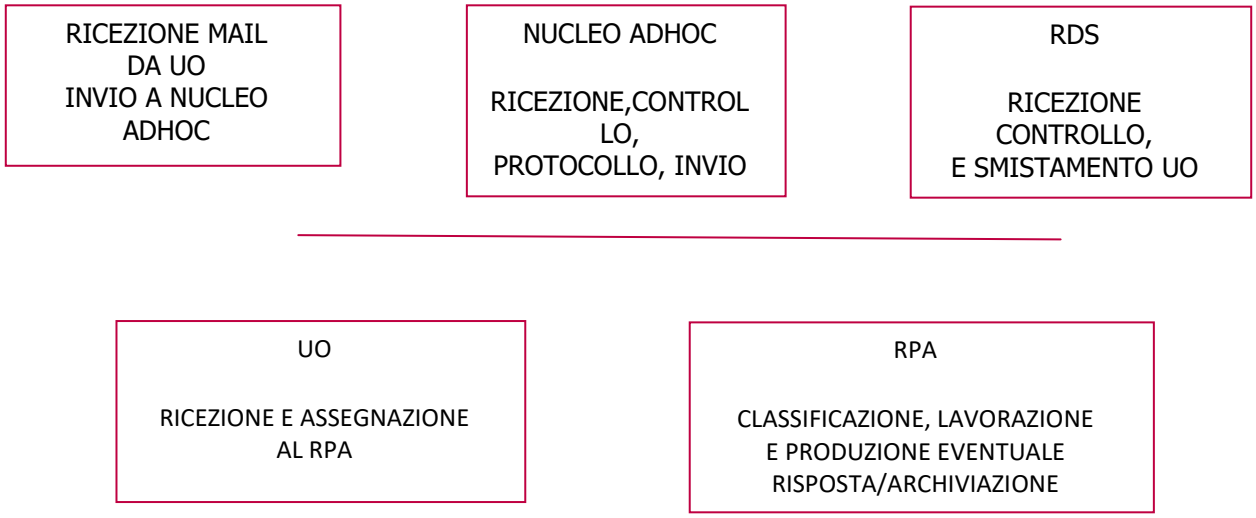
RUOLO	NOMINATIVO:	TEL.	E-MAIL :
RESPONSABILE DEL SERVIZIO	MAGG. DANIELE COLELLA	1525489	uadmag@rgtb8.esercito.difesa.it
VICARIO	C.LE MAGG. CA. SC. Q.S. MASSIMINIANO PATELLA	15255300	suadsegr@rgtb8.esercito.difesa.it
AMMINISTRATORE AD[h]OC	C.LE MAGG. SC. MASSIMO ESPOSITO	1525461	admadhoc@rgtb8.esercito.difesa.it
SOSTITUTO AMMINISTRATORE AD[h]OC	SERG. MAGG. FRANCESCO ANTONUCCI	1525461	admadhoc@rgtb8.esercito.difesa.it
OPERATORE/ADDETTO AL PROTOCOLLO	C.LE MAGG. CA. SC. LUIGI DELLA VECCHIA	15255294	suadpromil@rgtb8.esercito.difesa.it
OPERATORE/ADDETTO AL PROTOCOLLO	C.LE MAGG. SC. RAFFAELE ADDEO	15255294	suadpromil@rgtb8.esercito.difesa.it

Allegato H

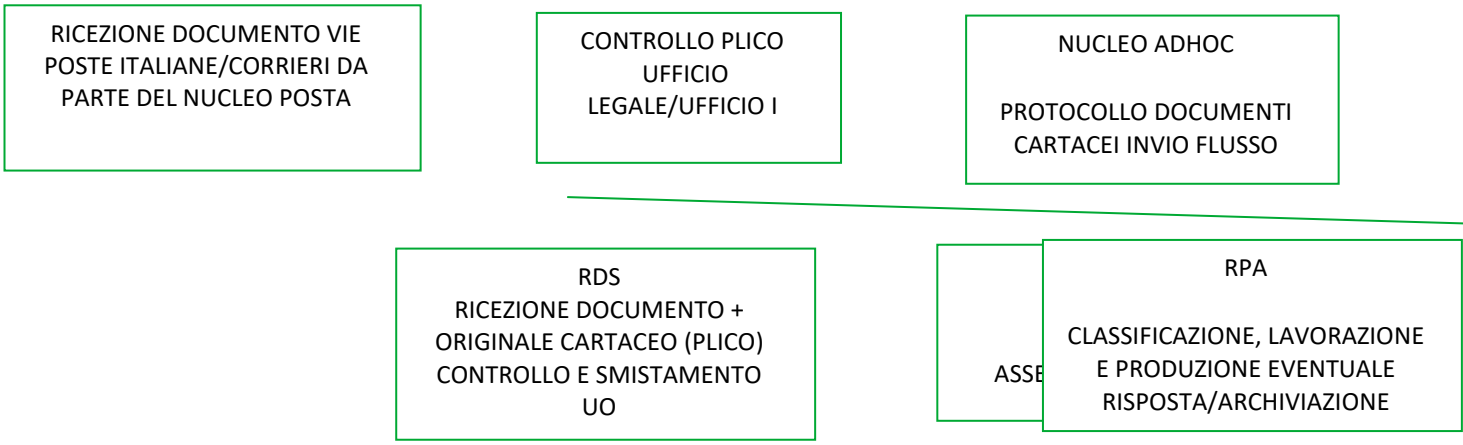
Flusso di lavorazione dei documenti informatici in ENTRATA ricevuti in "interoperabilità" PEI,PEC



Flusso di lavorazione dei documenti informatici in ENTRATA ricevuti in NON "interoperabilità"/e-mail



Flusso di lavorazione dei documenti analogici in ENTRATA (posta ordinaria)



ALLEGATO I

UBICAZIONE DEI LOCALI DI UF. FDPI DESTINATI ALLA GESTIONE DEI FLUSSI DOCUMENTALI

LOCALITÀ: CASERTA;
INDIRIZZO: VIA LAVIANO, 8
CASERMETTA N. 1
PIANO TERRA
STANZA N. 30

ALLEGATO J

REGISTRI IN USO

REGISTRO GENERALE

REGISTRO ORDINI DEL GIORNO

REGISTRO VARIAZIONI

REGISTRO DI EMERGENZA

ALLEGATO K

8° REGGIMENTO BERSAGLIERI

Nucleo Gestione Sistemi Informatici
VLaviano, 8 -81100 Caserta
PEI: rgtb8@esercito.difesa.it PEC: rgtb8@postacert.difesa.it

Caserta, _____

Oggetto: Scheda per la richiesta dei servizi di RETE.

^^^ ^^^ ^^^ ^^^

Si chiede l'accesso ai seguenti servizi di rete per il: _____

(Grado, Cognome e Nome)
in forza presso _____

(Ufficio -Sezione) (Recapito Ufficio)
con incarico _____C.F._____e-mail_____@esercito.difesa.it
(posta elettronica Istituzionale)

SERVIZI E FUNZIONI DA ABILITARE

☐ **POSTA ELETTRONICA FUNZIONALE**
Ind. email_____@rgtb8.esercito.difesa.it

☐ **RILEVAZIONE PRESENZE**
Specificare Permessi e Cartelle
Numero CMD_____
(a cura dell'Utente)

☐ **ADHOC**
Unità Organizzativa*_____
(a cura del Responsabile del Servizio)

Timbro e Firma dell' R.D.S._____

☐ **AGENDA COMANDO**
☐ Capo Ufficio
☐ Capo Sezione

Timbro e Firma del Comandate_____
(a cura dell'Ufficio scrivente)

☐ **CONDIVISIONI**
☐ Aree Comuni in ambito Ufficio di appartenenza:
_____

Lettura Scrittura_____
☐ Lettura Scrittura_____
☐ Lettura Scrittura_____
☐ Lettura Scrittura_____

☐ ☐

Aree Protette in ambito reggimento:
☐ _____

Specificare Permessi e Cartelle
☐ Lettura Scrittura_____
☐ Lettura Scrittura_____
☐ Lettura Scrittura_____
☐ Lettura Scrittura_____

AREA S.I.G.E

☐ SIGE-IMPIEGO
☐ SIGE-DENARO
SIGE-MATERIALI

☐ SIGE-PARCHI
☐ SIGE-SANITA'

SIGE-MATRICOLA

AREA WEB

☐ SITO WEB
☐ CALENDARIO EVIDENZA
☐ FTP

ALLEGATO L

REGOLAMENTO DI SERVIZIO

1. L'accesso ai servizi di rete avviene tramite l'inserimento di un Nome Utente (Username) ed una parola chiave (password); tali codici, presumibilmente identici per ogni servizio, sono **STRETTAMENTE** personali;
2. La conoscenza degli identificativi e delle password da parte di terzi consentirebbe a questi ultimi l'utilizzo dei servizi di rete in nome dell'utente. L'utente è pertanto tenuto a conservare la password con la massima cura e con la massima diligenza. Egli sarà ritenuto responsabile di qualsiasi danno o conseguenza pregiudizievole arrecata all'Amministrazione od a terzi in dipendenza della mancata osservanza di quanto sopra esposto.
3. È necessario proteggere il proprio Personal Computer con password di BIOS, sistema e screen-saver.
4. La posta elettronica potrà essere impiegata per relazioni anche con organizzazioni NON militari purché per motivi di servizio e per argomenti non coperti dal Segreto di Stato.
5. Tutti gli accessi alla rete sono registrati.
6. È vietato far viaggiare in rete:
   a. informazioni sensibili, di vietata divulgazione o a qualunque titolo classificate;
   b. materiale pornografico e a sfondo sessuale o di natura oscena;
   c. materiale di contenuto pedofilo; materiale che viola i diritti d'autore, ed in particolare software pirata (Warez, Crack), file musicali, immagini, video, testi protetti da copyright;
   d. materiale offensivo incluse espressioni diffamatorie, di fanatismo, razzismo, odio, irriverenza o minaccia;
   e. materiale che promuove o fornisce informazioni che istruiscono su attività illegali o che possono causare pregiudizio a terzi;
   f. software, informazioni o altro materiale contenente virus o componenti dannosi;
   g. iniziative legate al gioco d'azzardo, concorsi, giochi che richiedono una partecipazione a titolo oneroso;
   h. pubblicità o sponsorizzazioni a pagamento;
   i. "chain letters" (catene di Sant' Antonio elettroniche);
   j. ogni altro elemento indicato dal "Regolamento interno di sicurezza EAD" come sensibile o classificati ed in particolare nominativi del personale, incarico ricoperto, requisiti di sicurezza posseduti.
7. L'utente è responsabile per i contenuti direttamente immessi nella rete o, comunque, a lui attribuibili in virtù del codice di identificazione e della password.
8. L'utente ha l'obbligo di verificare l'assenza di virus informatici sui dischetti immessi nel computer e di non aprire allegati ai messaggi di posta elettronica di dubbia provenienza.
9. È vietato effettuare interventi sull'Hardware. In caso di necessità deve essere inviata una richiesta d'Intervento tecnico al Nucleo Gestione Sistemi Informatici.
10. L'elaboratore elettronico gli viene affidato dall'A.D. per adempiere alle sole esigenze d'Istituto a lui demandate e che non gli è consentito di detenere sullo stesso dati, propri di terzi, a carattere strettamente privato/intimo la cui visione possa ledere il diritto di privacy.
11. L'A.D., ai fini della salvaguardia della rete e del rispetto delle leggi vigenti in materia, ha il diritto di ispezionare il citato elaboratore in quanto strumento di lavoro assegnato all'utente esclusivamente per l'assolvimento dell'incarico.
12. L'indirizzo di posta elettronica (e-mail) affidatogli in uso, per l'assolvimento dell'incarico nella forma incarico@rgtb8.esercito.difesa.it non ha caratteristiche di privatezza personale e costituisce normale strumento di lavoro e ne è vietato l'utilizzo per scopi personali.
13. Chiunque abusivamente duplica software per uso su elaboratori o sapendo o, avendo motivi di sapere che si tratta di copie non autorizzate, lo distribuisce, vende, detiene a scopi commerciali/personali, è soggetto alla pena prevista dalla vigente legislazione che comporta reclusione e sanzioni economiche. Alla stessa pena è soggetto chi mette in atto sistemi tendenti a facilitare la rimozione arbitraria o l'esclusione funzionale dei dispositivi applicati a protezione dei software per uso su elaboratori.
14. Non sono consentite azioni di spamming, spoofing, hijacking o comunque tendenti a nascondere la propria identità, a molestare o arrecare danno all'attività degli elaboratori di altri utenti o ad acquisire dati/informazioni/privilegi a cui non si ha diritto.

Apponendo la propria firma,

DICHIARA

di essere a conoscenza di tutte le norme di sicurezza riguardanti l'utilizzo di *Personal Computer* , di aver preso visione del **"Regolamento Interno di Sicurezza delle Risorse ICT"**, del **"Regolamento Interno di Sicurezza EAD"** e del presente "**Regolamento di Servizio"**.

Caserta,_____

ALLEGATO M

MODULO VARIAZIONE RUOLO AD[h]OC

DA: _____ A: Ufficio Logistico – NGSI

Si comunicano i dati anagrafici relativi al: (nel caso di delega, indicare i dati del delegato)

Grado: _____ Cognome, Nome_____
Nato a _____ il gg/mm/aaaa _____
Codice fiscale _____ Rep./Uf./Sez.:_____
Ruolo_____ Telefono: _____
a cura amministratore ADHOC

☐ AUTORIZZATO alla trattazione dei dati sensibili Posta elettronica _____

per il/i seguenti motivo/i

☐ Nuova Attivazione
☐ Cambio ruolo
☐ Promozione al grado superiore
☐ Tresferito presso altro ruolo
☐ Altri interventi (specificare in Note)

NOTE VARIAZIONE DATI

DA COMPILARE ESCLUSIVAMENTE PER LE DELEGHE

☐ Attivazione "Delega firma" (**) ☐ Disattivazione "Delega firma" (**)

NOTE DELEGA

(*) Specificare nel campo note:data di decorrenza della variazione di ruolo, ruolo assunto e relativo sostituto da associare (anagrafica utente). (Es. Da trascrivere fedelmente nel campo note: 12/01/2010 ruolo da variare: Capo Sezione Flussi (anagrafica associata al ruolo: Ten. Col. Rssi Marco – nuova anagrafica da associare al ruolo: Ten. Col. Verde Marco).

(**) Indicare nel campo noteRuolo e anagrafica Delegante e data di decorrenza dell'operazione richiesta (Es: dalle ore 08:00 del 01/01/2013).

Gli utenti (anagrafica utente), possono essere associati a più di un "Ruolo" (accedendo con account diversi).

Si rammente che per poter consentire agli amministgratori di sistemna di dar seguito alle operazioni chieste, bisogna comunicare tutti I dati anagrafici richiesti sul modulo , che sono necessari per il conseguimento dei associazione Ruolo – Anagrafica.

Caserta _____

IL RESPONSABILE DELLA UO

ALLEGATO N

MODULO DI RICHIESTA INSERIMENTO ENTE IN RUBRICA AD[h]OC

INSERIMENTO ENTE IN RUBRICA AD[h]OC	
NOMINATIVO INTERNO	
INDIRIZZO:	
CITTÀ :	
CAP.:	
PROVINCIA	
STATO:	
TELEFONO:	
E-MAIL	
E-MAIL CERTIFICATA	
ISTITUZIONALE:	

Caserta lì _____

Ufficio del richiedente

Grado, Nome e cognome del richiedente

ALLEGATO 0

MODULO SCARICO DOCUMENTI DEMATERIALIZZATI

8° REGGIMENTO BERSAGLIERI
UFFICIO MAGGIORITÀ E PERSONALE
SEZIONE ADOCH

CASERTA 07/07/2020
PDC: C.le Magg. Sc. xxxxxxxxxxxx
Voip: 1525294 – 0823215294 Linea Civile
suadpromil@rgtb8.esercito.difesa.it

POSTA CONSEGNATA ALL' INFERMERIA DI CORPO/COMANDO BRIGATA

NR	PROTOCOLLO	UFFICIO DESTINATARIO
1	001001 del 07-07-2020	INFERMERIA"DOCUMENTAZIONE SANITARIA DEL xxxxxxxxxxxxx
2	0010011 del 07-07-2020	INFERMERIA"DOCUMENTAZIONE SANITARIA DEL xxxxxxxxxxxxx

PARTE CEDENTE

_____

PARTE RICEVENTE

_____

ALLEGATO P

8° REGGIMENTO BERSAGLIERI

UFFICIO/CP

ELENCO DELLA CORRISPONDENZA

N. Ord.	DESTINAZION	LOCALITÀ	N. PROTOCOLLO	OGGETTO
1	COMANDO ENTE	PALERMO	1234567 DEL 10/09/2020	LIBRETTO PERSONALE
2				

SPAZIO RISERVATO AL DESTINATARIO

LOCALITÀ

DATA

IL RESPONSABILE DEL RITIRO
(firma leggibile)