BASE MILITARE ITALIANA DI SUPPORTO

GIBUTI

MANUALE DI GESTIONE

DEL PROTOCOLLO INFORMATICO, DEI FLUSSI

DOCUMENTALI E DEGLI ARCHIVI

Edizione 2020

Firmato Digitalmente da/Signed by:
MICHELE CHIEDI
In Data/On Date:
lunedì 10 agosto 2020 09:22:59

BASE MILITARE ITALIANA di SUPPORTO GIBUTI

ATTO DI APPROVAZIONE

Approvo il

"MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI" DELLA BASE MILITARE ITALIANA DI SUPPORTO DI GIBUTI EDIZIONE 2020 CHE ABROGA E SOSTITUISCE L'EDIZIONE 2019.

Gibuti,

IL COMANDANTE
Col. a.(AVES) Michele CHIEDI

INDICE

ATTO DI APPROVAZIONE..... I

ELENCO DI DISTRIBUZIONE..... VI

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI..... VII

ACRONIMI..... VIII

RIFERIMENTI NORMATIVI …..... IX

GLOSSARIO X

1. MODELLO ORGANIZZATIVO..... 1
   a. Premessa..... 1
   b. b. Aree Organizzative Omogenee..... 1
   c. Coordinatore della gestione documentale..... 1
   d. Responsabile del servizio..... 1
   e. Vicario dell'RDS..... 2
   f. Manuale di Gestione del protocollo informatico, dei flussi documentali e degli archivi dello Stato Maggiore della Difesa …… 2
   g. Applicabilità del "Manuale"..... 2
   h. Manuali di Gestione delle AOO..... 2
   i. Servizio di protocollo informatico e gestione documentale..... 3
   j. Caratteristiche gestionali..... 3
   k. Applicativo utilizzato..... 3
   l. Il sistema dei Registri e le tipologie documentali..... 3
2. FORMAZIONE E REGISTRAZIONI DEI DOCUMENTI. 4
   a. Formazione..... 4
   b. Flussi della documentazione..... 4
   c. Protocollazione e registrazione..... 5
   d. Unicità delle registrazioni..... 5
   e. Dati della registrazione di protocollo..... 5
   f. Segnatura di protocollo dei documenti..... 6
   g. Documenti provenienti da applicativi interni al dicastero..... 6
   h. Documenti esclusi dalla protocollazione..... 7
   i. Annullamento delle registrazioni di protocollo..... 7
   j. Privacy e tutela dei dati personali..... 8

k. Produzione dei registri giornalieri. 8
3. LA GESTIONE DEI DOCUMENTI INFORMATICI. 8
a. Specifiche dei documenti informatici in ingresso..... 8
b. Procedure per il protocollo dei documenti informatici in ingresso..... 9
c. Documenti informatici provenienti da altre pubbliche amministrazioni..... 10
d. Documenti informatici provenienti da aziende e liberi professionisti..... 10
e. Documenti informatici provenienti da privati cittadini..... 10
f. Messaggi di notifica di eccezione..... 11
g. Specifiche dei documenti informatici in uscita..... 11
h. Utilizzo casella PEC o PEI in uscita..... 11
i. Ricevute dei documenti informatici..... 12
j. Documento interno..... 12
4. LA GESTIONE DEI DOCUMENTI ANALOGICI. 12
a. Documento analogico..... 12
b. Tipologia di spedizioni..... 13
c. Ritiro della corrispondenza..... 13
d. Corrispondenza che non deve essere aperta..... 13
e. Eventuali plichi con documenti classificati..... 14
f. Registrazioni delle consegne della posta..... 14
g. Controlli all’apertura dei plichi provenienti dai servizi postali..... 14
h. Personale abilitato alle attestazioni di conformità delle copie informatiche..... 14
i. Procedure per la registrazione..... 14
j. Documento in uscita..... 15
k. Predisposizioni dei plichi..... 15
l. Fax..... 16
m. Documento non firmato..... 16
5. SISTEMA CLASSIFICAZIONE, FASCICOLAZIONE E ARCHIVIO..... 16
a. Titolario..... 16
b. Classificazione dei documenti..... 16
c. Fascicolazione dei documenti..... 17
d. Deposito/Archivio dell’AOO..... 17
e. Archiviazione dei documenti informatici..... 17
f. Archiviazione/custodia dei documenti analogici..... 17

g. Conservazione..... 18
6. SICUREZZA ED ABILITAZIONI DI ACCESSO 19
a. Piano di Sicurezza..... 19
b. Accesso al sistema. 19
c. Profili di accesso..... 19
7. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA. 20
a. Attivazione..... 20
b. Svolgimento delle attività. 21
c. Riattivazione del sistema informatico..... 21
8. CARATTERISTICHE SPECIFICHE DELL'AOO DELLA BMIS..... 21
a. Premessa..... 21
b. Unità organizzative responsabili dei documenti..... 21
c. Caselle di posta elettronica ed indirizzo postale..... 22
d. Unità Organizzativa responsabile della gestione del protocollo e del sistema documentale, con relativi orari..... 22
e. Servizio di scambio posta..... 23
f. Titolario..... 23
g. Postazione del registro di emergenza..... 23
Elenco Allegati:
Allegato "A": SCHEMI DI FLUSSO IN ENTRATA ED USCITA DEI DOCUMENTI …….. 24
Allegato "B": REGOLE GENERALI DI SCRITTURA DEI DATI …….. 25
Allegato "C": NOMINA DEGLI INCARICATI ALLA DEMATERIALIZZAZIONE …… 26
Allegato "D": IL TITOLARIO O PIANO DI CLASSIFICAZIONE …… 27

ELENCO DI DISTRIBUZIONE

DISTRIBUZIONE ESTERNA

- Stato Maggiore della Difesa.

DISTRIBUZIONE INTERNA

- Segreteria
- RDS
- Vicario
- Sostituto

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

1	
2	
3	
4	
5	
6	

ACRONIMI

All'interno del documento saranno utilizzati una serie di acronimi, abbreviazioni e sigle che vengono di seguito riportati, con il relativo significato. Per alcune delle abbreviazioni usate, sono forniti ulteriori dettagli nel Glossario.

AD	Amministrazione Difesa
ADHOC	Applicativo per il protocollo informatico e la gestione documentale in uso presso lo Stato Maggiore della Difesa
AgID	Agenzia per l'Italia digitale
AOO	Area organizzativa omogenea
[CAD]	Decreto Legislativo 7 marzo 2005 n. 82
[CIRC]	Circolare AgID del 23 gennaio 2013 n. 60
CGD	Coordinatore della gestione documentale dell'area tecnico operativa interforze
[CODBCP]	Decreto Legislativo 22 gennaio 2004 n. 41
[CODPRI]	Decreto Legislativo 30 giugno 2003 n. 196
[DIR]	Direttiva SMD-I-004
[DPCM]	Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013, recante regole tecniche per il protocollo informatico
DPR	Decreto del Presidente della Repubblica
[DPR]	DPR 28 dicembre 2000 n. 445
D.Lgs.	Decreto Legislativo
[GDPR]	Regolamento UE n. 2016/679
INCC	Informazioni non Classificate controllate
IPA	Indice delle Pubbliche Amministrazioni
l.	Legge
P.A.	Pubblica Amministrazione
PEC	Posta elettronica certificata
PEI	Posta elettronica istituzionale
PI	Protocollo informatico
RDS	Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi
RPA	Responsabile del procedimento amministrativo
UO	Unità organizzativa

RIFERIMENTI NORMATIVI

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. [DPR] Disposizioni legislative e regolamentari in materia di documentazione amministrativa" e s.m.i.
- Decreto Legislativo 30 giugno 2003, n. 196. [CODPRI] Codice in materia di protezione dei dati personali" e s.m.i.
- Decreto Legislativo 22 gennaio 2004 n. 41. [CODBCP] "Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137" e s.m.i.
- SMD I 004 - Edizione 2004 "Il protocollo informatico nella Difesa"
- Decreto Legislativo 7 marzo 2005, n. 82 [CAD] "Codice dell'Amministrazione digitale" e s.m.i.
- Decreto del Presidente della Repubblica 11 febbraio 2005, n.68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata"
- Circolare AgID n. 60 23.01.2013 [CIRC] Regole tecniche per interoperabilità dei sistemi di protocollo informatico"
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013. [DPCM] "Regole tecniche per il Protocollo Informatico"
- Regolamento UE n. 2016/679 [GDPR] "Regolamento Generale sulla Protezione dei Dati"
- SMD I 002 – Edizione 2016 "Standardizzazione dei formati dei documenti elettronici della Difesa"
- SMD I 003 - Edizione 2017 "Disciplinare interno all'AD sull'utilizzo dei servizi informatici non classificati erogati in ambito Difesa, quali i servizi di posta elettronica, instant messaging ed accesso a internet"
- SMD I 009 - Edizione 2017 "Norme di gestione e d'impiego per il rilascio in formato elettronico della tessera personale di riconoscimento Modello ATe e dei certificati digitali emessi dalla Public Key Infrastructure (PKI) della Difesa"
- SMD I 024 - Edizione 2017 "Procedure sulla gestione in sicurezza dei servizi informatici non classificati dell'AD"
- MANUALE DI CONSERVAZIONE DELLA DIFESA - Edizione 2019
- MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI DEL COMANDO OPERATIVO DI VERTICE INTERFORZE – Edizione 2020

GLOSSARIO

L'applicazione della normativa inerente al Protocollo Informatico introduce una serie di termini e concetti che, nel presente paragrafo, saranno definiti ed utilizzati quali "principi di base".

Archivio

L'archivio è la raccolta ordinata degli atti formati o ricevuti dall'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali.

Gli atti 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.

Area Organizzativa Omogenea (AOO)

Una AOO (artt. 50, comma 4, e 61 del DPR) costituisce un insieme di unità organizzative (UO) facenti capo allo stesso Ente/Comando che usufruiscono, in modo omogeneo e coordinato, dei servizi informatici per la gestione dei flussi documentali e, in particolare, del servizio di protocollazione. Dove, in precedenza, venivano utilizzati una serie di registri di protocollo, suddivisi per i diversi livelli gerarchici degli Enti, ora è necessario effettuare una reductio ad unum di tali registri, associando un insieme di uffici con ricadute sugli aspetti pratici, funzionali e logistici. In pratica, la costituzione di una AOO comporta la chiusura dei vari Uffici di Protocollo intermedi, esistenti prima dell'entrata in funzione del PI.

Classificazione d'archivio

Classificare vuol dire attribuire a ciascun documento un indice (di classificazione) inserito in una struttura di voci (piano di classificazione) e associarlo ad una definita unità archivistica generalmente identificata come fascicolo. Attraverso la classificazione deve essere possibile:

- identificare responsabilità specifiche per la gestione dei documenti;
- rendere possibile la gestione integrata di documenti;
- collegare le finalità documentali e quelle amministrative relative al trattamento delle pratiche, eventualmente in associazione a programmi di work flow;
- facilitare le operazioni di selezione per la conservazione o lo scarto dei documenti. La classificazione non deve mai essere applicata a posteriori per esigenze occasionali.

Coordinatore della gestione documentale (CGD)

Ove nominato, nell'ambito delle amministrazioni con più AOO, ai sensi di quanto disposto dall'art. 3 del DPCM 3/12/2013, definisce e assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione e archiviazione, nonché di comunicazione interna tra le AOO.

Documento analogico

Rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Documento informatico

Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Per documento elettronico si intende qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.

Dati personali

Informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relative all'ubicazione, un'identificazione online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati sensibili

Dati personali attraverso i quali sia possibile rivelare l'origine razziale o etnica, le opinion politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, oltre ai dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dati giudiziari

I dati personali idonei a rivelare provvedimenti di cui all'art. 10 [GDPR], in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale.

Fascicolazione

L'operazione di raccolta dei singoli atti/documenti raggruppati in tanti fascicoli inerenti ad altrettanti affari o procedimenti amministrativi.

Fascicolo

Insieme ordinato di atti e 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, con lo scopo di riunire, a fini decisionali o informativi, tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formato, natura, contenuto giuridico, ecc., anche se non è rara la creazione di fascicoli formati da un insieme di documenti della stessa tipologia e forma, raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc.).

I fascicoli costituiscono il tipo di unità archivistica più diffusa degli archivi contemporanei e sono costituiti, in base alle esigenze di servizio, secondo criteri che sono stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento. I fascicoli possono essere organizzati secondo i seguenti criteri:

- per oggetto;
- per processo o procedimento amministrativo;
- per tipologia di forma del documento (cartaceo, digitale, fax, e-mail, ecc.).

Indirizzo di posta elettronica certificata (PEC)

La posta elettronica certificata (PEC), fornisce un servizio di messaggistica che sfrutta gli standard propri della posta elettronica e assicura al mittente l'attestazione di avvenuta ricezione del messaggio e al destinatario la garanzia dell'identità del mittente. Questo servizio comprende alter funzionalità

per permettere confidenzialità, integrità, tracciabilità e storicizzazione del messaggio.

Sono inoltre disponibili strumenti per l'individuazione dei soggetti intervenuti nel processo di trasmissione e ricezione del documento, del quale si hanno informazioni quali la data, l'ora, il mittente, il destinatario, l'oggetto, il contenuto e quanto necessario per la trasmissione di un atto o documento informatico. La PEC è strettamente connessa all'IPA (Indice delle Pubbliche Amministrazioni), ove sono pubblicati gli indirizzi di posta certificata associati alle AOO e alle funzioni organizzative previste dalle Pubbliche Amministrazioni. È necessario tenere presente che, utilizzando la PEC, viene rilasciata al mittente una ricevuta di avvenuta consegna del messaggio, contestualmente alla disponibilità del messaggio stesso nella casella di posta elettronica del destinatario, indipendentemente all'avvenuta lettura da parte del soggetto destinatario. Tale ricevuta indica al mittente che il messaggio è effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario e certifica la data e l'ora dell'evento.

Indirizzo di posta elettronica istituzionale (PEI)

La casella di posta elettronica è istituita da ciascuna AOO, attraverso la quale possono essere ricevuti i documenti elettronici da protocollare.

Manuale di gestione (Manuale)

Descrive il sistema di gestione 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 per un corretto ed efficace funzionamento del sistema di protocollo, dei procedimenti amministrativi informatici e del sistema documentale, costituendo, pertanto, la "carta dei servizi" nella quale gli interessati trovano descritte le modalità di gestione del protocollo nei suoi diversi aspetti. Il Manuale è un documento dinamico, che deve essere aggiornato in dipendenza delle modifiche alle procedure manuali, organizzative ed informatiche applicate alla gestione del protocollo.

Responsabile del Servizio (RDS)

Il Responsabile del Servizio per la tenuta del protocollo informatico è previsto dall'art. 61 [DPR] ed è una figura ben diversa dal classico Capo Ufficio Posta o figure simili, da sempre presenti nell'AD.

I suoi compiti non sono meramente burocratici, ed hanno, principalmente, una valenza di tipo legale: il RDS, ovvero il suo vicario in caso di assenza, garantisce il corretto funzionamento (a norma di legge) del sistema di PI anche nei confronti dei cittadini/ditte/altre Pubbliche

Amministrazioni

Servizio di protocollo informatico e gestione documentale. All'interno di ogni singola AOO è istituito, ai sensi dell'art. 61 [DPR], un servizio per la tenuta del protocollo e la gestione dei flussi documentali e degli archivi, al quale spetta il compito di garantire il corretto impiego del sistema di protocollo informatico e assicurare, in generale, il funzionamento del sistema di gestione documentale.

Titolario

La realizzazione di una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione o Titolario che, unitamente al Manuale, è redatto, per ciascuna AOO, con la relativa classificazione d'archivio. Il Titolario di archivio è uno schema generale di voci logiche rispondenti alle esigenze funzionali e articolate in modo gerarchico, al fine di identificare, partendo dal generale al particolare, l'unità di aggregazione di base dei documenti all'interno dell'archivio. 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 di una AOO, cioè un complesso di risorse umane e strumentali cui sono state affidate competenze omogenee nell'ambito delle quali il Capo Reparto/Ufficio/Servizio è il Responsabile del Procedimento Amministrativo (RPA) nella trattazione dei documenti o dei vari procedimenti.

1. MODELLO ORGANIZZATIVO

a. Premessa

Il presente documento è stato predisposto secondo le regole ed i principi definiti nel "Manuale di Gestione del protocollo informatico, dei flussi documentali e degli archivi dello Stato Maggiore della Difesa – Edizione 2020" (in seguito denominato per semplificazione "Manuale").

Il "Manuale" fornisce, in qualità di documento di riferimento, le istruzioni per il corretto funzionamento dei servizi per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi da parte degli enti dell'Area Tecnico-Operativa Interforze (T.O.I) dipendenti dallo Stato Maggiore della Difesa.

L'Area T.O.I. è composta da una pluralità di Enti e Comandi articolati su più Aree Organizzative Omogenee (AOO) di cui la Base Militare Italiana di Supporto (BMIS) è parte integrante.

b. Aree Organizzative Omogenee

Ai sensi dell'art. 50 del Testo Unico, le AOO sono gli insiemi di "uffici da considerare ai fini di una gestione unica e coordinata dei documenti". L'elenco delle AOO dell'Area T.O.I., pubblicato sul sito della Difesa, è suscettibile di modifiche in relazione all'esigenza di nuove AOO o alla loro riorganizzazione.

c. Coordinatore della gestione documentale

Al fine di garantire criteri uniformi per la gestione dei documenti nelle diverse AOO appartenenti all'Area Tecnico-Operativa Interforze, lo Stato Maggiore della Difesa ha assegnato i compiti di Coordinatore della Gestione Documentale (CGD) al Capo Ufficio Protocollo Unico dello Stato Maggiore della Difesa. Il CGD assolve ai compiti indicati nell'art. 4 del [DPCM] e, in particolare:

- definisce ed assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna tra le AOO;
- predispone il "Manuale", anche ai fini della conservazione, dei documenti informatici, e le istruzioni per il corretto funzionamento dei servizi per la tenuta dei protocolli informatici, della gestione dei flussi documentali e degli archivi;
- è sostituito dal Capo Sezione Protocollo dell'Ufficio Protocollo Unico, in qualità di vicario, nei casi di vacanza, assenza o impedimento.

d. Responsabile del servizio

Per ogni AOO è necessario nominare il Responsabile della gestione documentale o Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (RDS), secondo quanto previsto dalla normativa vigente. In particolare, l'RDS:

- garantisce lo svolgimento ed il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, nel rispetto delle normative vigenti;
- predispone, ai fini della gestione dei documenti informatici, il Manuale di Gestione della AOO di cui è il responsabile e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
- attribuisce il livello di autorizzazione per l'accesso alle funzioni del sistema di protocollo informatico e di gestione documentale;

- autorizza le operazioni di annullamento delle registrazioni di protocollo di cui all'articolo 54 del DPR 445/2000;
- autorizza l'apertura del registro di emergenza dopo aver accertato l'indisponibilità del sistema e, dopo aver verificato il ripristino del suo corretto funzionamento, ne dispone la chiusura.

Per la rilevanza dei compiti assegnati e per la funzione da svolgere, anche verso l'esterno dell'AOO, la nomina del RDS viene effettuata con un atto formale dell'Ente di appartenenza (Ordine di servizio, Decreto, Ordine del Giorno, Atto Dispositivo, ecc.).

e. Vicario dell'RDS

Per i casi di vacanza, assenza, impedimento o, comunque, nelle veci dell'RDS, interviene il "Vicario" appositamente individuato per tale funzione. In caso di contemporanea assenza dell'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.

f. Manuale di Gestione del protocollo informatico, dei flussi documentali e degli archivi dello Stato Maggiore della Difesa ("Manuale")

Il "Manuale" contiene le regole per la gestione dei servizi di protocollo, l'uso dei titolari di classificazione e le regole per la costituzione e manutenzione dei fascicoli elettronici nell'ambito dell'Area T.O.I. In particolare esso:

- definisce le modalità di relazione con l'utenza, con particolare riferimento alla ricezione dei documenti cartacei;
- descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, all'AOO individuando le responsabilità connesse alla relativa gestione;
- definisce le regole di registrazione, di smistamento e di assegnazione dei documenti ricevuti;
- indica le UO responsabili delle attività di registrazione di protocollo e i relativi orari di operatività, l'incaricato che svolge la funzione di RDS ed il suo Vicario, le UO responsabili per l'organizzazione e la tenuta dei documenti all'interno dell'AOO;
- individua le tipologie di documenti esclusi dalla registrazione di protocollo o soggetti a registrazione particolare;
- riporta le modalità di utilizzo del registro di emergenza.

g. Applicabilità del "Manuale"

I principi contenuti nel "Manuale" si applicano ai protocolli informatici, ai flussi documentali ed agli archivi delle AOO dell'Area T.O.I. dipendenti dallo Stato Maggiore della Difesa, che utilizzano il sistema ADHOC. Il "Manuale" è aggiornato a cura del Capo Ufficio Protocollo Unico dello SMD ed inviato alle AOO dell'Area T.O.I. che lo utilizzeranno come modello di riferimento nella redazione dei Manuali di AOO.

h. Manuali di Gestione delle AOO

Gli RDS assicurano il rispetto, nell'ambito della propria AOO, delle indicazioni contenute nel suddetto "Manuale". A tale scopo, questi devono predisporre il Manuale di Gestione dell'AOO, sulla base di quanto riportato nel "Manuale", con l'aggiunta delle scelte organizzative e delle disposizioni particolari valide esclusivamente per la propria AOO. Il Manuale di AOO entra in vigore con un atto formale dell'Ente di appartenenza (Ordine di servizio, Decreto, Ordine del Giorno, Atto Dispositivo, ecc.) e viene aggiornato ogni qualvolta l'RDS lo ritiene opportuno.

L'RDS richiede tempestivamente la pubblicazione di ogni nuova versione del Manuale di AOO sul sito internet della Difesa, nella pagina dell'Ente.

Nel caso di avvicendamento dell'RDS, il nuovo Responsabile deve prendere visione del Manuale di gestione di pertinenza, verificare le regole in esso contenute ed, eventualmente, provvedere alle modifiche. Le regole contenute nel Manuale si intenderanno valide fino alla pubblicazione della nuova versione.

i. Servizio di protocollo informatico e gestione documentale

Si tratta di una funzione svolta da appositi Uffici, Sezioni o Nuclei, in relazione alle dimensioni dell'AOO. L'UO responsabile delle attività di registrazione di protocollo ed i relativi orari di servizio devono essere indicati nel Manuale di AOO.

j. Caratteristiche gestionali

La gestione dei documenti informatici nelle AOO dell'Area T.O.I. avviene secondo un modello di protocollazione:

- accentrata, per la posta in ingresso, in quanto tutta la corrispondenza indirizzata alle AOO viene registrata in un unico punto dagli addetti dell'UO a livello di Sezione o Nucleo, che assicura il Protocollo Informatico;
- distribuita, per i documenti informatici in uscita o interni, in quanto le UO (Reparti/Uf.Gen./Uf./Servizi) possono protocollare e trasmettere direttamente la documentazione prodotta. In Allegato "A" sono riportati gli schemi di flusso in entrata ed uscita dei documenti informatici per la BMIS.

k. Applicativo utilizzato

L'intero processo di gestione dei documenti e del processo di protocollazione sono gestiti attraverso il sistema di protocollo informatico e gestione documentale ADHOC. Tutte le informazioni di dettaglio inerenti alle funzionalità presenti nel sistema ADHOC sono reperibili in una raccolta online sulla maschera "cruscotto" dell'applicativo, nella voce "Bollettini" e nella voce "Guida".

Per le specifiche procedure di accesso ai vari menù e funzionalità, si rinvia alla consultazione della predetta documentazione.

l. I sistema dei Registri e le tipologie documentali

I documenti, analogici o informatici, vengono gestiti dalle AOO suddivisi nel seguente modo:

- in ingresso;
- in uscita;
- interno.

In ciascuna AOO è istituito il Registro Generale di Protocollo, per la registrazione delle comunicazioni ricevute, spedite ed interne alla AOO. Inoltre, il sistema ADHOC prevede appositi registri aggiuntivi che possono essere attivati dall'RDS per registrazioni in ingresso (ad esempio le fatture) riguardanti gli atti interni (ordini del giorno e decreti) o particolari procedimenti (le gare). Le funzioni correlate alla gestione dei registri particolari nel sistema sono denominate "Tipologia Documentale" o "Tipologia Registro", in relazione alle diverse funzioni interessate. Ciascun registro è identificato da:

- un codice, utilizzato come prefisso nella segnatura di protocollo, di tre caratteri, a cui sarà

automaticamente aggiunto l'anno nel quale si effettua la registrazione dei documenti (REG2019, per il Registro Generale del 2019);

- una descrizione che, di norma è fissa, predefinita nel sistema, in alcuni casi è personalizzabile.

Di seguito si riporta la configurazione dei registri della BMIS, indentificati con il codice di 3 caratteri e la relativa descrizione, suddivisi tra "attivi" e "disattivati:

- Attivati:
  - REG Generale.
- Disattivati:
  - APT Note/Appunti;
  - ODG Ordini del Giorno;
  - ODS Ordini di Servizio;
  - FAT Fatture;
  - RFT Rifiuto Fatture;
  - GEP Gestione Personale;
  - RVA Richiesta variazioni;
  - GAR Gare;
  - DE1 Decreti ed atti a rilevanza esterna (personalizzabile).

2. FORMAZIONE E REGISTRAZIONI DEI DOCUMENTI.

a. Formazione

In aderenza alla normativa vigente (art. 40 del CAD) le AOO producono esclusivamente documenti originali informatici con l'uso della firma digitale. I titolari che hanno capacità di firma sono indicati dai capi delle AOO/UO.

I documenti cartacei in ingresso vengono dematerializzati in modo che l'intero flusso documentale venga gestito in maniera elettronica.

Il documento deve trattare un unico argomento, indicato in maniera sintetica nello spazio riservato all'oggetto.

L'intera documentazione amministrativa, in pratica tutti i documenti informatici firmati digitalmente, viene gestita nel formato PDF/A.

Gli allegati che, per la loro natura o per il loro utilizzo, non possono o non devono essere convertiti, sono conservati nel loro formato originale.

I documenti, analogici o informatici, vengono gestiti in relazione al loro formato, nell'ambito delle AOO, suddivisi nel seguente modo:

- in ingresso;
- in uscita;
- interno.

b. Flussi della documentazione

Per quanto attiene ai documenti informatici, le AOO utilizzano tre canali principali:

- casella di Posta Elettronica Istituzionale (PEI);
- casella di Posta Elettronica Certificata (PEC, riceve esclusivamente messaggi inviati da altre caselle PEC);
- applicativi interni al dicastero interfacciati direttamente al sistema documentale.

La posta analogica viene inviata e ricevuta attraverso i seguenti canali:

- servizi postali ufficiali ed altri operatori abilitati;
- a mezzo "corriere militare".

Le documentazioni pervenute attraverso canali differenti non assumono rilevanza ufficiale e il loro eventuale assoggettamento a protocollo deve essere valutato alla luce delle normative vigenti.

Le caselle di posta elettronica e l'indirizzo postale per la ricezione della corrispondenza cartacea sono resi pubblici con le modalità previste dalle normative vigenti e, in particolare, nel Manuale dell'AOO e sul sito internet dell'AD.

c. Protocollazione e registrazione

All'interno dell'AOO tutti i documenti devono essere oggetto di registrazione (tranne le eccezioni esplicitamente previste).

In particolare, per I documenti ricevuti o inviati dall'AOO, la registrazione di protocollo prevista dall'art. 53 del DPR 445/2000 ha la funzione giuridica di garantire la trasparenza amministrativa in relazione alle operazioni di ricezione e di invio.

Tramite i registri di Protocollo (Generale e gli altri registri istituiti con le finalità indicate nel "Manuale") è possibile registrare ufficialmente l'esistenza di un documento all'interno delle AOO e tenere traccia delle sue movimentazioni.

d. Unicità delle registrazioni

Le registrazioni di protocollo sono uniche, cosi come la numerazione progressiva delle stesse. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo. I numeri di protocollo individuano un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Il numero di protocollo è costituito da almeno sette cifre numeriche. Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.

Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione non registrata presso l'AOO è considerata giuridicamente inesistente presso l'Amministrazione. Non è consentita la protocollazione di un documento già protocollato. In sintesi, i registri quali atti pubblici originari che fanno fede della formazione, tempestività e dell'eventuale ricevimento o spedizione dei documenti, indipendentemente dalla regolarità degli stessi, sono idonei a produrre effetti giuridici.

e. Dati della registrazione di protocollo

Il sistema, per ciascuna registrazione di protocollo prevede l'inserimento dei dati previsti all'art. 53 [DPR] con le regole ivi descritte. In particolare:

- il numero progressivo: viene generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione: è assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente per i documenti ricevuti o, in alternativa, il/i destinatario/i per i documenti spediti: sono registrati in forma non modificabile e reperiti nella tabella dei mittenti e destinatari del sistema informatico;
- l'oggetto del documento: registrato in forma non modificabile; gli addetti devono seguire le regole generali di codifica delle informazioni;
- la data ed il protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico: calcolata con l'algoritmo SHA-256.

Nella redazione dei campi "oggetto" e in generale, ogni qualvolta sia necessario digitare una descrizione nel sistema informatico, è necessario riferirsi a quanto riportato in Allegato "B". Nel caso in cui si tratti di un documento informatico proveniente da una P.A., dotato di *file* "*segnatura.xml*", il sistema completa automaticamente le informazioni afferenti alla registrazione di protocollo.

f. Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione.

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.

Sui documenti in ingresso, se presente, vengono utilizzati dati contenuti nel file "segnatura.xml", purché conforme alle indicazioni della [CIRC].

Se è attivata la produzione e la firma automatica del registro giornaliero di protocollo, la segnatura di protocollo viene anche apposta nella porzione in alto a sinistra della prima pagina del documento primario. Tale segnatura viene anche firmata in modalità automatica dal RDS.

Il file "segnatura.xml" viene allegato a tutti i documenti in uscita per posta elettronica.

Il formato della segnatura di protocollo delle AOO della BMIS, conformemente alla normativa, prevede i seguenti dati:

- Codice dell'Amministrazione: M_D;
- Codice dell'AOO: S89307;
- Codice del registro: REG 2020 (registro del 2020);
- Numero di protocollo: 1234567 (7 cifre);
- Data di registrazione: gg-mm-aaaa;

La segnatura di protocollo risulterà, pertanto: M_D S89307 REG2020 1234567 gg-mm-aaaa.

g. Documenti provenienti da applicativi interni al dicastero

La documentazione amministrativa proveniente da applicativi della Difesa è gestita con il sistema ADHOC sulla base di accordi di carattere tecnico e funzionale.

L'applicativo trasmittente sarà opportunamente identificato con gli strumenti messi a disposizione dal sistema documentale, garantendo, in tal modo, la certezza del mittente.

La documentazione pervenuta con le modalità sopra descritte potrà essere sottoposta a processi di protocollazione automatica o manuale, in dipendenza delle necessità del procedimento amministrativo in trattazione.

h. Documenti esclusi dalla protocollazione

Il sistema documentale utilizzato è abilitato alla trattazione dei documenti "NON CLASSIFICATI". La posta classificata, erroneamente pervenuta al protocollo, deve essere consegnata agli organi di sicurezza delle AOO.

Inoltre, sono esclusi dalla registrazione di protocollo:

- gazzette ufficiali;
- bollettini ufficiali P.A.;
- notiziari P.A.;
- note di ricezione circolari:
- note di ricezione altre disposizioni;
- materiali statistici;
- giornali, riviste e libri;
- materiali pubblicitari;
- inviti a manifestazioni che non attivino procedimenti amministrativi;
- documenti classificati;
- documenti già soggetti a registrazione particolare dell'AD;
- fogli di viaggio;
- note caratteristiche;
- registro delle presenze;
- modelli 730;
- posta classificabile come *spam*.

i. Annullamento delle registrazioni di protocollo

La necessità di modificare anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrati in forma non modificabile, per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.

In particolare, è possibile annullare una registrazione di protocollo per un documento erroneamente fatto entrare nel patrimonio documentale dell'AOO nei casi di:

- duplicazioni di protocollo, per documenti inviati più volte dai mittenti;
- documenti erroneamente protocollati.

Solo l'RDS è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo. Il registro elettronico, mediante la funzione "visualizza gli annullati", riporta i motivi dell'annullamento.

L'annullamento di una registrazione di protocollo può avvenire anche su richiesta delle UO, specificando, in una apposita nota, i motivi, ma non può riguardare i contenuti trattati nel documento. In tali casi è l'UO assegnataria, competente per la materia, che deve provvedere ad informare il mittente, con apposite comunicazione PEI/PEC, sulla base di quanto ricevuto.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data e l'ora dell'annullamento.

È sempre possibile visualizzare, per gli utenti abilitati, i documenti annullati e le relative motivazioni di annullamento.

L'annullamento di una registrazione di protocollo comporta l'invio automatico, da parte del sistema ADHOC, di un messaggio al mittente con la motivazione che è stata inserita nella fase di annullamento (es: esigenza della firma elettronica, della copia di un documento d'identità o quanto necessario per la corretta registrazione a protocollo).

j. Privacy e tutela dei dati personali

La trattazione dei documenti contenenti dati personali, sensibili e giudiziari deve avvenire nel rispetto della legge. Per i documenti contenenti dati personali o dati sensibili (cioè quelli idonei a rivelare: l'origine razziale ed etnica, le convinzioni religiose, filosofiche o altro, le opinioni politiche, l'adesione a partiti, sindacati, organizzazioni o associazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale) e dati giudiziari,sono previste particolari forme di riservatezza e di accesso controllato, mediante la selezione di un filtro elettronico. I dati in questione devono essere individuati come tali nel sistema di protocollo, selezionando l'apposita casella di spunta, sin dal momento della loro protocollazione in ingresso o in uscita.

Qualora un documento contenente dati sensibili e personali non venga individuato al momento della protocollazione, è compito di chiunque ne riconosca le caratteristiche provvedere ad integrare la registrazione di protocollo attribuendo al documento la spunta prevista. In generale, è opportuno che venga posta particolare attenzione, a partire dal momento della protocollazione, alla redazione dell'oggetto del documento per escludere la possibilità che da esso possano desumersi dati sensibili e personali (anonimizzazione).

k. Produzione dei registri giornalieri

Il sistema provvede alla generazione delle registrazioni di protocollo della giornata. Durante tale attività, della durata di pochi minuti, non è possibile protocollare atti né in uscita né in entrata. I registri particolari entrano nella gestione quotidiana al pari del Registro Generale e, dopo aver staccato il primo numero di protocollo, anche tali registri vengono firmati ogni giorno per consentire successive protocollazioni.

Le registrazioni giornaliere vengono firmate digitalmente in modalità automatica a cura del RDS. Le registrazioni vengono archiviate all'interno del sistema ed è sempre possibile effettuarne copie cartacee o digitali.

3. LA GESTIONE DEI DOCUMENTI INFORMATICI

a. Specifiche dei documenti informatici in ingresso

Le AOO dell'Area T.O.I. sono predisposte alla ricezione e gestione di documenti informatici

tramite una casella PEI ed una casella PEC, pubblicate anche sulle pagine del protocollo informatico della AD.

Sono accettati i documenti informatici conformi alle seguenti regole:

- il formato preferibile per file allegati ai messaggi di posta elettronica, come documenti primari, sono il PDF ed il PDF/A;
- sono accettati anche i formati JPG, P7M, TXT, TIFF, TIF, XML;
- i file allegati al documento primario, oltre ai predetti formati, possono essere in formato ZIP o nei formati concordati con l'UO interessata;
- l'invio di allegati non previsti comporta la ritrasmissione al mittente del messaggio;
- le marche temporali apposte alle firme digitali devono essere in formato embedded e non detached;
- l'apposizione di firma digitale non valida rende inutilizzabile il file trasmesso;
- ad ogni trasmissione deve essere associata la documentazione relativa ad un unico argomento: il mittente che deve inviare cinque diverse pratiche dovrà effettuare cinque diversi invii;
- la casella postale del mittente deve essere riferita alla persona giuridica (ad esempio, la ditta ROSSI SPA dovrà inviare la propria documentazione dalla casella postale *rossispa@xxxxx.it* e non dalla casella postale *mario.rossi@rossispa.xxxxx.it*);
- il nome dei file allegati deve essere di lunghezza moderata, non contenere spazi, lettere accentate, caratteri speciali, virgolette e apici. Si suggerisce di utilizzare il carattere_(underscore) al posto dei predetti caratteri (esempi di nomi di file validi: richiesta_di_risarcimento.pdf; foto_di_citta.jpg; attivazione_dell_utenza. Non vanno bene nomi come: questo è il 1° documento.pdf; si.trasmette.domanda.pdf.

Se un documento informatico viene inviato ad una casella di posta elettronica ordinaria personale o funzionale, il titolare di tale casella deve inviare un messaggio al mittente segnalando la necessità di inviare nuovamente il documento alla corretta casella postale PEI/PEC dell'AOO.

b. Procedure per il protocollo dei documenti informatici in ingresso

I messaggi giunti sulle caselle di posta vengono inseriti in un'apposita coda alla quale accedono gli addetti al protocollo.

Gli addetti protocollano il messaggio, procedendo alla successiva assegnazione all'UO competente ovvero, nei casi dubbi, inviano il messaggio ad un apposito elenco, denominato "lista RDS".

Se la protocollazione di un messaggio non viene completata, il messaggio viene nuovamente presentato nella coda dei messaggi.

I documenti inseriti nella "lista RDS" vengono gestiti dal RDS e possono essere protocollati, rispediti al mittente (solo per la PEI) o gestiti dal personale incaricato, secondo le deleghe ed i profili di accesso assegnati dal RDS.

Gli addetti al protocollo inviano anche i messaggi erroneamente pervenuti all'AOO alla predetta "lista RDS".

Se l'RDS accerta un errore di spedizione provvede affinché venga inviato al mittente una

comunicazione tramite un'apposita lettera o una notifica di eccezione.

I documenti in ingresso sono assegnati giornalmente, tramite le UO, ai Responsabili del Procedimento Amministrativo (RPA) e/o ai sostituti da essi incaricati, che provvedono alla successiva gestione interna. Gli utenti, tramite la funzionalità "Gestione delle deleghe", possono stabilire l'utente che subentra nella gestione della corrispondenza durante il loro periodo di assenza.

Il controllo della completezza formale e sostanziale della documentazione pervenuta è di competenza del personale dell'UO che tratta la specifica tematica. Qualora sia necessario acquisire ulteriori documenti, l'UO provvede direttamente a richiederli al mittente.

Le e-mail considerate spam non vengono protocollate e non viene spedito nessun messaggio al mittente.

c. Documenti informatici provenienti da altre pubbliche amministrazioni

La documentazione proveniente da altre pubbliche amministrazioni sarà oggetto di protocollazione e successiva gestione all'interno dell'AOO, nel rispetto dell'art. 47 CAD.

Pertanto, è necessario che la stessa rientri in almeno una delle sottoelencate casistiche:

- sia firmata digitalmente;
- risponda alle regole dell'interoperabilità promulgate dall'AgID;
- la casella postale mittente sia certificata.

L'Ufficio si riserva di protocollare o non protocollare gli atti che non rispondono ad almeno uno dei requisiti di cui sopra, in relazione alla possibilità di determinare la provenienza del documento.

d. Documenti informatici provenienti da aziende e liberi professionisti

Le aziende devono inviare le proprie comunicazioni utilizzando la casella di posta elettronica certificata (secondo le disposizioni del DPCM 21 marzo 2011) utilizzando come canale preferenziale quella registrata nell'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata istituito dal Ministero dello Sviluppo Economico (INI-PEC).

Anche i liberi professionisti dovranno utilizzare, preferibilmente, il canale di posta elettronica certificata registrato nell'INI-PEC.

In entrambi i casi è opportuna l'apposizione della firma digitale, da parte del rappresentante legale, sui documenti trasmessi.

È necessario che risulti possibile l'accertamento della provenienza del documento, ai sensi dell'art. 45 del CAD.

e. Documenti informatici provenienti da privati cittadini

I privati cittadini, in funzione della tipologia di casella disponibile, possono utilizzare entrambe le caselle di posta elettronica dell'AOO. Non è possibile inviare sulla casella PEC una e-mail normale. Per la protocollazione è necessario attenersi alle disposizioni dell'art. 45 del CAD, che prevede, in ogni caso, l'accertamento della provenienza.

A tal fine, è necessario inviare i documenti avendo cura di apporre la firma digitale ovvero di allegare scansione del proprio documento di identità in corso di validità o, comunque, di seguire quanto prescritto dall'art. 38 del DPR 445/2000 in combinato disposto con l'art. 65 del CAD.

f. Messaggi di notifica di eccezione

Il sistema prevede sette casi preimpostati di restituzione al mittente dei documenti pervenuti tramite PEI:

- il messaggio è corrotto o uno dei documenti non leggibile;
- dati non congruenti nella segnatura informatica;
- segnatura non conforme alla circolare AgID n. 60 del 23.01.2013;
- mancata sottoscrizione del documento primario;
- destinatario errato;
- verifica di integrità dei documenti negativa;
- il documento o gli allegati dichiarati all'interno del file "segnatura.xml" non corrispondono a quanto ricevuto.

Oltre ai casi suindicati è possibile inviare un messaggio non preimpostato, riportando i motivi della restituzione.

g. Specifiche dei documenti informatici in uscita

A tutti i documenti trasmessi viene allegato il file "segnatura.xml", contenente le informazioni previste dalla [CIRC].

Il corretto invio dei documenti richiede l'osservanza delle seguenti regole:

- utilizzo di formati previsti nell'AD (ODT/DOCX/RTF);
- la denominazione non deve contenere caratteri speciali (*, ', ^, ecc.);
- la denominazione non deve essere usato il carattere . (punto).

In caso di inserimento, come allegato, di un documento già firmato che non deve essere modificato, è necessario che nella predisposizione venga selezionata la voce "NO FIRMA".

Per quanto riguarda le dimensioni complessive dei file, si evidenzia che:

- la posta elettronica istituzionale può trasmettere documenti di dimensioni non superiori a 30 MB per ogni destinatario;
- la posta elettronica certificata può trasmettere fino a 100 MB da suddividere per ogni destinatario (ad esempio: 1 destinatario - 100 MB, 3 destinatari - 33 MB ciascuno).

Tutta la documentazione amministrativa dell'AOO viene prodotta in originale in modalità informatica con l'apposizione della firma digitale e della marca temporale.

h. Utilizzo casella PEC o PEI in uscita

Il sistema informatico, sulla base delle informazioni inserite, provvede ad inviare, per posta elettronica, il documento primario e gli allegati a tutti i destinatari inseriti.

L'utilizzo della casella PEI, piuttosto che della PEC, può essere impostato durante la predisposizione e può essere modificato da tutti coloro che visionano il documento, fino alla firma dello stesso.

Nei casi previsti dalla legge o qualora si renda necessario disporre di una ricevuta di ricezione della corrispondenza inviata, viene utilizzata la casella di posta elettronica certificata (PEC). Parimenti si utilizzerà la casella di PEC ogni qualvolta che il corrispondente richieda esplicitamente l'impiego di tale strumento. Negli altri casi è possibile utilizzare anche la casella

PEI.

In particolare, è necessario utilizzare:

- con le altre PA, la casella di posta PEI o PEC, in funzione delle specifiche esigenze della pratica in trattazione (se disponibile PEC – IPA);
- con le imprese ed i professionisti la PEC (preferibilmente INI-PEC);
- con i cittadini, il canale indicato dagli stessi nelle istanze presentate, significando che, l'assolvimento di eventuali "obblighi di comunicazione", richiede l'utilizzo dei canali previsti dalla normativa vigente.

i. Ricevute dei documenti informatici

Il sistema gestisce in automatico:

- le ricevute generate dal sistema di PEC;
- le ricevute previste dalla [CIRC] per i documenti dotati di file "segnatura.xml" delle P.A.;
- i messaggi di "eccezione" che segnalano un problema di ricezione nella casella postale del destinatario (ad esempio, destinatario sconosciuto, casella postale del destinatario piena, ecc.).

La messaggistica di cui trattasi viene automaticamente inserita in allegato al documento di origine ed è consultabile con le normali funzioni di consultazione. In caso di "posta non consegnata" il documento viene evidenziato sulla scrivania virtuale dell'utente che lo ha predisposto. Dopo le verifiche del caso, è possibile:

- inviare nuovamente il documento alla stessa casella postale iniziale;
- inviare il documento ad una casella postale diversa;
- provvedere alla materializzazione del documento per la successiva trasmissione per posta ordinaria.

Almeno una volta al giorno è necessario verificare la presenza di eventuali messaggi di "posta non consegnata".

In alcuni casi, la procedura automatica non riesce a gestire alcune tipologie di ricevute, con particolare riferimento alle notifiche delle "eccezioni". In tal caso, il messaggio deve essere acquisito a protocollo ed inviato all'UO interessata.

j. Documento interno

Per documenti interni si intendono quelli scambiati tra le diverse articolazioni (UO) afferenti alla medesima AOO.

Se tra gli indirizzi per competenza o per conoscenza viene inserita una UO interna all'AOO, il sistema informatico provvede ad inviare il documento sulla scrivania virtuale dell'UO destinataria.

Rimangono invariate le susseguenti attività gestionali, compresa l'eventuale necessità di ricorrere alla materializzazione del documento.

4. LA GESTIONE DEI DOCUMENTI ANALOGICI

a. Documento analogico

Per documento analogico si intende la rappresentazione non informatica di atti, fatti o dati

giuridicamente rilevanti.

Di norma, nell'attività amministrativa il documento analogico è un documento stampato su carta, prodotto con strumenti informatici. L'originale analogico (il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali e sostanziali, dotato di firma autografa) deve comprendere tutti gli elementi di garanzia e di informazione del mittente e del destinatario.

I documenti analogici devono pervenire in originale o in copia autentica attraverso il servizio postale o consegnati direttamente agli indirizzi preposti alla ricezione della corrispondenza analogica di ciascuna AOO riportati nel presente documento e pubblicati sul sito internet della Difesa. La documentazione così pervenuta sarà in ogni caso soggetta a processo di scansione, ai sensi dell'art. 23 ter comma 3 del CAD, allo scopo di effettuarne, nel limite di quanto possibile rispetto alla natura e consistenza degli allegati, una gestione digitalizzata.

b. Tipologia di spedizioni

Il servizio postale deve essere utilizzato nei casi di necessità e per esigenze d'ufficio, rispettando i criteri di economia e speditezza. Di seguito si riportano le principali tipologie di spedizioni attualmente previste:

- prioritaria, consente di spedire documenti fino a 2 kg, senza tracciatura;
- raccomandata, prevede la ricevuta dell'avvenuta spedizione (fino a 2 kg). Su richiesta è previsto l'avviso di ricevimento per la notifica dell'avvenuta consegna;
- assicurata, con le stesse modalità della raccomandata, con possibilità di stabilire il valore assicurabile in caso di smarrimento, furto o danneggiamento;
- pacco ordinario, per spedizioni fino a 20 kg di peso. Il servizio di "corrieri militari" viene assicurato secondo le seguenti modalità:
- senza tracciatura;
- con tracciatura, qualora sia necessaria la prova dell'invio.

c. Ritiro della corrispondenza

Il personale preposto deve provvedere, giornalmente, alla consegna della posta analogica da spedire, e al ritiro di quella indirizzata all'AOO, presso il servizio postale di riferimento.

Le modalità di consegna e ritiro devono essere riportate nel Manuale di AOO.

Il militare incaricato deve verificare che su tutti i documenti prelevati risulti l'indirizzo dell'AOO o di una delle sue UO.

La corrispondenza che risulti indirizzata ad altra AOO, deve essere restituita con apposto il timbro / dicitura "NON INDIRIZZATA ALL'AOO".

In caso di parziale o totale lacerazione del plico si riporta, sull'involucro, la dicitura "GIUNTO LACERO" con timbro e firma dell'incaricato.

d. Corrispondenza che non deve essere aperta

Il personale preposto non è autorizzato all'apertura di buste, plichi o pacchi che:

- riportano una delle seguenti diciture: Grado Nome Cognome; ESCLUSIVO PER IL TITOLARE; ESCLUSIVO PER (Grado, Nome, Cognome); PERSONALE PER (Grado, Nome, Cognome); Al Capo del Reparto o dell'Ufficio;
- abbiano come destinatario gli organi di sicurezza;

- evidenziano "fascette di sicurezza" anche se prive dell'indicazione della classifica di segretezza del documento contenuto.

Tale corrispondenza viene consegnata direttamente alle UO. Sarà cura dei destinatari provvedere alla riconsegna di quanto ricevuto, per l'eventuale registrazione a protocollo. Si precisa che, per motivi di sicurezza, plichi e pacchi, a "titolo personale" non possono essere ricevuti tramite i canali della corrispondenza di servizio.

e. Eventuali plichi con documenti classificati

Nel caso in cui, successivamente all'apertura di un plico ordinario o di una "raccomandata/assicurata", si rinvenga una seconda busta o un documento riportante una "classifica di segretezza" si richiude il plico con i sistemi normalmente in uso (nastro adesivo, punti metallici, spago, ecc.) apponendo il timbro previsto e si informa il PCN.

f. Registrazioni delle consegne della posta

Di norma, il ritiro della posta ordinaria non prevede registrazioni di dettaglio, ad eccezione delle eventuali "distinte di consegna", da custodire per almeno un anno. Per quella tracciata, raccomandate, assicurate, pacchi e atti giudiziari è necessaria la registrazione dei vari passaggi, con particolare riferimento alla documentazione che viene:

- restituita perché non diretta all'AOO;
- consegnata ai destinatari, senza apertura della busta e registrazione di protocollo.

Ciascuna AOO, sulla base delle dimensioni dei flussi di corrispondenza analogica, adatta le registrazioni e le ricevute alle proprie esigenze.

g. Controlli all'apertura dei plichi provenienti dai servizi postali

Il personale preposto adotta opportune modalità organizzative atte a prevenire e limitare eventuali rischi e pericoli di contaminazione per i plichi provenienti dal servizio postale.

In caso di corrispondenza sospetta, deve essere avvertito con immediatezza il diretto superiore ed il Nucleo M.P.

h. **Personale abilitato alle attestazioni di conformità delle copie informatiche**

La scansione ed il protocollo con il sistema ADHOC consente la dematerializzazione della documentazione analogica in ingresso. L'intero flusso documentale viene gestito in maniera elettronica, con un processo di validazione ai sensi dell'art. 23 ter comma 3 del CAD e art. 10/1 del DPCM 13.11.2014 - Regole per la gestione dei documenti informatici. Il personale delegato a tale attività all'interno della BMIS è generalmente il vicario che deve essere individuato con apposito ordine di servizio, secondo il modello in Allegato "C".

i. Procedure per la registrazione

Per la protocollazione in ingresso gli addetti abilitati procedono alla scansione massiva dei documenti e all'inserimento dei seguenti dati essenziali:

- Codice Amministrazione mittente, se presente;
- Codice AOO mittente, se presente;
- Mittente;
- Oggetto;
- Protocollo mittente;

- Data protocollo mittente.

Gli allegati cartacei, vengono inseriti nella fase di scansione massiva del documento di riferimento.

Gli allegati digitali sono accettati, se forniti, su supporto ottico (CD ovvero DVD) ovvero su memoria con connessione USB.

Non possono essere accettati allegati informatici su supporti diversi da quelli indicati. In ogni caso i supporti informatici non vengono riconsegnati al mittente ma rimangono associati al documento cartaceo originario.

Il contenuto del supporto, qualora la dimensione non sia eccessiva, può essere associato al documento primario di appartenenza, subito dopo il processo di scansione di quest'ultimo.

Il processo di acquisizione termina con l'apposizione della firma digitale (e la marca temporale) sul file ottenuto dal processo di scansione massiva e con l'invio alla UO destinataria.

Il documento analogico originale e gli eventuali allegati vengono custoditi presso l'AOO/UO ai soli fini di eventuali verifiche.

Le operazioni di dematerializzazione avvengono di norma entro il giorno successivo alla ricezione del documento.

j. Documento in uscita

La procedura standard prevede l'invio automatico dei documenti all'indirizzo e-mail dei destinatari interessati. Tuttavia, è possibile inviare la documentazione nella "Lista dei documenti da materializzare" e procedere alla stampa, nei seguenti casi:

- documento che non deve essere trasmesso per posta elettronica;
- destinatario senza casella di posta elettronica;
- documento primario associato ad un allegato analogico, non dematerializzabile, o informatico, non inviabile per posta elettronica (ad esempio, quando risulta di dimensioni eccessive).

I documenti confluiti nella lista da materializzare possono essere stampati dagli operatori abilitati con l'apposizione di glifo ai sensi dell'art. 23 comma 2 bis del CAD e della Circolare AgID n. 62.

Il destinatario può verificare l'origine del documento, avvalendosi delle procedure presenti sul sito *www.difesa.it/Protocollo/Pagine/Glifo.aspx*.

k. Predisposizioni dei plichi

Le AOO predispongono la corrispondenza analogica da spedire, tramite il servizio postale o i corrieri militari, con buste di dimensioni ridotte e, per l'inoltro di stampe e pacchi, i mezzi più idonei (cellofan, carta resistente, etc.). Per la corrispondenza "assicurata" è necessario utilizzare buste resistenti ed accertarsi che il plico non sia lacero. I plichi ed i pacchi devono essere ben chiusi con nastro adesivo, spago, ecc..

La posta da spedire deve essere predisposta, utilizzando la modulistica prevista significando che, in aderenza alla vigente normativa in materia di trasparenza amministrativa, è fatto obbligo di compilare in maniera leggibile ed in tutta la sua interezza la modulistica a corredo di ciascuna tipologia di spedizione.

Inoltre, al fine di evadere tempestivamente il flusso della corrispondenza in uscita, essa deve essere consegnata al personale preposto per consentirne in tempo utile la consegna al servizio postale o ai corrieri.

l. Fax

Tra le Pubbliche Amministrazioni e tra le stesse e le imprese vige l'obbligo di comunicare esclusivamente con le tecnologie dell'informazione e della comunicazione ovvero per via telematica e la BMIS pertanto, non ha attivo nessun apparato FAX. L'eventuale trasmissione / ricezione di documentazione con il sistema FAX è ancora ammessa da parte dei privati cittadini e può essere effettuata solo qualora la UO ne abbia la disponibilità. A tale riguardo, si precisa che:

- un documento inviato via fax non deve essere recapitato anche con altri strumenti (art 45 del CAD);
- è necessario allegare una fotocopia del documento d'identità (art. 38 [DPR]).

m. Documento non firmato

I documenti cartacei privi di mittente, qualora configurabili quali esposti anonimi, sono trattati nell'ambito delle AOO procedendo alla scansione solo della busta ed all'apposizione del protocollo e della data sulla stessa e sul primo foglio (con apposito timbro o a mano).

5. SISTEMA CLASSIFICAZIONE, FASCICOLAZIONE E ARCHIVIO

a. Titolario

Le AOO definiscono nel Manuale di AOO la gestione degli archivi sulla base dei riferimenti normativi e metodologici in vigore. In particolare, il "Titolario di archivio" deve:

- discendere dal modello funzionale che caratterizza le attività svolte;
- svilupparsi su funzioni, sotto funzioni, attività;
- prevedere non più di 3 livelli.

La sua struttura deve presentare caratteri di generalità e di completezza necessari per soddisfare le esigenze di classificazione delle UO.

L'aggiornamento del Titolario compete esclusivamente al vertice dell'AOO, su proposta dell'RDS. Ciascuna UO può chiedere integrazioni, varianti e aggiunte al Titolario sulla base delle proprie necessità. Dopo ogni modifica il RDS provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

È possibile, registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.

Il Titolario non è retroattivo, significando che le sue variazioni non possono applicarsi ai documenti classificati in precedenza.

In Allegato "D" sono stati riportati utili approfondimenti sullo specifico argomento.

b. Classificazione dei documenti

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO. Tutti i documenti

ricevuti e prodotti delle UO dell'AOO, indipendentemente dal supporto sul quale sono formati, sono classificati in base Titolario.

Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse), il fascicolo di appartenenza ed, eventualmente, il sottofascicolo nonché l'UO di competenza.

c. Fascicolazione dei documenti

Lo strumento di base per gestire la classificazione è il "fascicolo".

Il sistema prevede che i primi tre livelli del Titolario (titolo, classe e sottoclasse) vengano precaricati e gestiti in modalità accentrata dall'RDS.

I fascicoli ed i sottofascicoli sono invece gestiti direttamente dagli interessati ai relativi procedimenti.

In particolare, per poter classificare un documento è necessario inserirlo in un fascicolo oppure in un sottofascicolo.

Per quanto riguarda la descrizione occorre attenersi alle regole generali di scrittura dei dati, indicate in Allegato "B". Inoltre, è opportuno evidenziare che non possono essere creati fascicoli con denominazione generica, come ad esempio "Varie", e che il sistema mantiene traccia della data di creazione del fascicolo e degli autori.

d. Deposito/Archivio dell'AOO

Le AOO producono esclusivamente originali informatici e, inoltre, tutti gli atti cartacei pervenuti vengono dematerializzati rendendoli validi a tutti gli effetti di legge.

Pertanto, l'universalità dei documenti originali afferenti all'AOO, a partire dalla data di avvio del servizio, sono archiviati all'interno del sistema informatico, che ne consente la gestione e l'accesso, secondo le norme di legge previste.

Tuttavia esiste un consistente numero di atti cartacei che, fino alla loro dematerializzazione, devono essere gestiti con il sistema di custodia da parte delle UO.

e. Archiviazione dei documenti informatici

I documenti informatici sono archiviati in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo, sui supporti di memoria del sistema ADHOC.

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.

f. Archiviazione/custodia dei documenti analogici

Per quanto attiene l'organizzazione degli archivi cartacei si precisa che nell'archivio corrente attivo si custodiscono le cartelle dell'anno corrente, già suddivisi in ordine cronologico fino ad arrivare al 10° anno precedente; allo scadere del 10° anno saranno valutati i documenti da scartare.

Si sottolinea che i documenti cartacei sono conservati in cartelline da carteggio, indicando il

giorno in cui la documentazione viene trattata, e custodite presso le UO.

Si evidenzia che, ogni giorno, il personale delle UO deve ritirare la documentazione analogica pervenuta, firmando apposite ricevute/registro.

g. Conservazione

La conservazione è disciplinata dal Manuale di Conservazione della Difesa che illustra nel dettaglio l'organizzazione del processo, i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività.

(1) Servizio di conservazione dei registri giornalieri di protocollo

Il Responsabile della Conservazione della Difesa ha dato disposizioni (luglio 2020) per l'avvio del servizio di consevazione a norma della documentazione elettronica. Il servizio, che in futuro verrà esteso a tutta la documentazione elettronica, al momento non è ancora pienamente operativo ed è per ora limitato alla conservazione a norma dei registri giornalieri di protocollo.

Il servizio sarà erogato dall'infrastruttura del Centro di Dematerializzazione e Conservazione Unico della Difesa (CE.De.C.U.), situato a Gaeta.
Tale Ente, come previsto dalla normativa vigente, è un Conservatore Accreditato presso l'Agenzia per l'Italia Digitale, avendo superato il complesso processo di certificazione previsto dalla normativa vigente e, pertanto, può erogare servizi di conservazione a norma alle Pubbliche Amministrazioni.

Si riepilogano di seguito i passaggi che saranno necessari per l'invio dei registri giornalieri di protocollo in conservazione:

i. ciascun Responsabile del Servizio di protocollo, con una cadenza concordata con l'Ente erogatore del servizio, riceverà, dalla casella postale *supporto.conservazione@aid.difesa.it*, la convenzione che il Responsabile del Servizio deve firmare digitalmente, nell'apposito spazio riservato a tale scopo, in formato PADES, utilizzando il kit di firma del Comando per le Operazioni in Rete (disponibile al link *pki.difesa.it*). La convenzione inviata sarà già completa di tutti i dati e le informazioni necessarie. Sarà cura di ciascun Responsabile del Servizio verificare l'esattezza delle informazioni indicate e segnalare le eventuali incongruenze alla casella postale mittente;
ii. dopo aver provveduto alla firma della convenzione, ciascun Responsabile del Servizio provvederà a trasmetterla, tramite casella di posta elettronica certificata, via sistema di protocollo informatico, alla casella *postale cor@postacert.difesa.it*;
iii. il Responsabile della Conservazione della Difesa, previa verifica del documento, provvederà a controfirmare tale convenzione, inviandola all'Ente erogatore del Servizio (e, per conoscenza, anche al Responsabile del Servizio interessato);
iv. il Centro di Dematerializzazione e Conservazione Unico della Difesa, al ricevimento della convenzione così controfirmata, provvederà ad attivare l'utenza del Responsabile del Servizio interessato e a fornirgli le credenziali di attivazione, tramite posta elettronica. Le credenziali così ricevute dovranno essere inserite all'interno del sistema ADHOC.

Una volta avviato il servizio, i registri giornalieri di protocollo dovranno essere di norma inviati in conservazione entro la giornata lavorativa successiva alla chiusura del registro.

Per i dettagli tecnici relativi alla procedura da utilizzarsi si rimanda al Bollettino per gli utenti ADHOC n. 34 del 2 dicembre 2019.

6. SICUREZZA ED ABILITAZIONI DI ACCESSO

a. Piano di Sicurezza

La sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici archiviati sono garantiti dal sistema ADHOC, gestito presso il Centro di Elaborazione Dati Unificato dell'Area Tecnico Amministrativa, che ne cura anche i processi di backup.

Il Piano della Sicurezza informatica, relativo ai collegamenti, alle modalità di trasmissione ed interscambio dei documenti, viene predisposto ed aggiornato dagli Enti preposti, in quanto parte del più ampio Piano di Sicurezza Informatica dell'AD.

Di seguito, pertanto, saranno riportate le misure di controllo per l'impiego dei servizi del sistema ADHOC.

b. Accesso al sistema

I vari processi sono caratterizzati da utenti che accedono a procedure (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).

Agli utenti del sistema documentale vengono riconosciute autorizzazioni di accesso differenziate, sulla base delle tipologie di operazioni stabilite dall'ufficio di appartenenza.

L'accesso al sistema avviene tramite CMD nel seguente modo:

- inserimento della CMD all'interno del lettore di smart card collegato al computer;
- digitazione nell'apposito campo del proprio pin carta.

In caso di indisponibilità della CMD è possibile accedere tramite apposite credenziali, per un limitato periodo di tempo. L'attivazione della deroga, considerata la sua rilevanza ai fini della sicurezza, deve essere autorizzata dall'RDS o dal personale da questi delegato.

L'RDS, avvalendosi di una utenza privilegiata (amministratore di sistema), assegna agli utenti diversi livelli di autorizzazione; tali utenti una volta identificati, sono suddivisi secondi diversi profili di accesso, sulla base delle rispettive competenze. È possibile assegnare più ruoli allo stesso utente.

c. Profili di accesso

La strutturazione degli accessi prevede una realizzazione di una serie di profili sulla base della struttura ordinativa e delle rispettive competenze.

Le principali profilazioni riguardano le funzioni di:

- amministratore di sistema: è colui il quale può accedere ai profili di configurazione di base del sistema; in genere, è rilasciata ad un numero limitato di utenti;
- protocollazione in ingresso: funzione destinata agli operatori di protocollo in ingresso dei documenti informatici e cartacei;
- lista dei documenti da materializzare: è l'elenco all'interno del quale confluiscono i documenti che per le proprie caratteristiche non possono essere inviati per posta elettronica. In linea generale, è consigliabile avere un utente con questo profilo in ciascuna UO;
- accesso alla tabella dei mittenti e destinatari: si tratta di un punto di snodo fondamentale per la gestione della corrispondenza. L'accesso a tale tabella deve garantire uniformità e

coerenza ai dati immessi;

- abilitazione alla trasmissione/firma digitale degli atti: in genere legata alla funzione di firma di documenti verso l'esterno;
- predisposizione di documento: è la funzione che consente di preparare gli atti per il flusso in uscita;
- consultazione: in linea generale, tutti gli utenti dovrebbero essere abilitati alla consultazione dell'archivio, il cui accesso è comunque legato al cono d'ombra di visibilità determinato dalla propria posizione nell'albero gerarchico dell'AOO. In particolare, le informazioni legate al registro di protocollo sono visibili a tutti gli utenti mentre i documenti in quanto tali sono visibili solo a chi appartiene al relativo cono d'ombra. Va ricordata, a questo proposito, l'ulteriore profilazione, inerente alla possibilità di accedere ai documenti che contengono dati sensibili;
- accesso alla scrivania: funzione abilitata a tutti gli utenti con la quale si realizzano gli scambi della corrispondenza e le attività gestionali dei documenti in ingresso/uscita. Deve essere controllata con continuità per evitare la giacenza di documentazione senza porre in essere gli adempimenti previsti. In caso di assenza del titolare è necessario attivare la delega su di un altro utente/collaboratore. Particolare importanza assumono le scrivanie ai vertici delle UO o delle varie articolazioni contraddistinte dalla spunta di "capo" in quanto ricevono i documenti in ingresso;
- abilitazioni di accesso ai fascicoli: si tratta di funzioni che consentono l'apertura dei fascicoli nonché l'assegnazione delle specifiche abilitazioni tramite la creazione o associazione dei relativi template. I profili ora delineati non vanno considerati esaustivi delle molteplici possibilità fornite dal sistema in quanto è possibile anche creare profili che contengano un mix di quelli elencati. L'assegnazione dei profili e il loro aggiornamento sono stabiliti dall'RDS sulla base delle effettive esigenze, formalizzate con apposite richieste dai responsabili delle diverse UO. Allo scopo di agevolare l'assolvimento dei compiti connessi alla protocollazione e gestione documentale può essere necessario individuare, all'interno dell'AOO, una o più figure definendo il contesto organizzativo (UO) e la tipologia delle attività che le stesse potranno esercitare, la cui nomina deve essere effettuata con atto formale dell'Ente di appartenenza (Ordine di servizio, Decreto, Ordine del Giorno, Atto Dispositivo, ecc.). Tali figure, pur non avendo una dipendenza organica diretta dall'RDS, svolgeranno alcune funzioni, definite con apposite normative interne, per garantire il buon andamento della gestione documentale nelle strutture più articolate e complesse. L'RDS dovrà, comunque, esercitare la vigilanza sull'osservanza delle disposizioni in questione rimanendone responsabile.

7. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

a. Attivazione

L'RDS autorizza lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su registri di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema. Tale autorizzazione consiste in un provvedimento, riportante la causa, la data e l'ora di inizio dell'interruzione del funzionamento del sistema ADHOC.

In caso di utilizzo di apposito software, la protocollazione deve avvenire solo presso specifiche postazioni di lavoro sulle quali è stato preventivamente installato, consentendo all'AOO di proseguire le attività di protocollazione.

L'elenco delle postazioni su cui è installato il Registro di emergenza deve essere a conoscenza del personale dell'AOO e deve essere riportato sul Manuale dell'AOO. L'RDS assicura che

presso ciascuna postazione siano sempre disponibili le indicazioni aggiornate per gli utenti interessati.

b. Svolgimento delle attività

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

In presenza di un documento analogico in arrivo da protocollare immediatamente, si procederà al suo inserimento nel registro di emergenza, provvedendo alla consegna del medesimo all'UO di competenza.

Per quanto riguarda la documentazione in uscita la funzione di registrazione a protocollo non sarà possibile. In caso di urgenza, l'UO dovrà procedere con metodologie alternative e consegnare il documento all'RDS, per la protocollazione di emergenza e la successiva trasmissione tramite canali analogici.

Appare evidente che non è conveniente procedere con tali modalità ed è opportuno ridurre al minimo indispensabile l'accesso a tali funzioni. Si sottolinea che in caso di blocco del sistema risulta inibito anche l'accesso all'archivio informatico e alle funzioni di ricerca in generale.

c. **Riattivazione del sistema informatico**

Alla ripresa del normale funzionamento del sistema ADHOC, l'RDS produce una ulteriore dichiarazione, con l'esatta indicazione della data e dell'ora della ripresa del servizio.

Tutte le dichiarazioni di attivazione e chiusura del registro di emergenza sono conservate a cura dell'RDS. Dopo la riattivazione sia i documenti in ingresso sia i documenti in uscita protocollati in emergenza, dovranno essere inseriti nel sistema ADHOC con le procedure previste.

In particolare, nell'oggetto si dovrà riportare il numero del registro di emergenza (RE xxxxxx gg-mm-aaaa) per consentire la ricerca del numero di registrazione di emergenza tramite il campo "oggetto".

8. CARATTERISTICHE SPECIFICHE DELL'AOO DELLA BMIS

a. Premessa

Il presente paragrafo riporta le caratteristiche dell'AOO della BMIS nonché le scelte organizzative e le disposizioni relative alla gestione dei flussi documentali valide nell'ambito della stessa, cosi come previsto nell'Allegato "A" del Manuale di gestione del Protocollo Informatico del COI.

b. Unità Organizzative responsabili dei documenti

L'AOO della BMIS (codice AOO: S89307) comprende le seguenti UO responsabili per l'organizzazione e la tenuta dei documenti gestiti:

- Comandante;
- CAG;
- Cellula J1;
- Cellula J4;
- Cellula J6;

- Cellula J6_CC;
- Cellula J8;
- CIMIC;
- CISP;
- COFS;
- CSCI;
- CSMGT;
- FP;
- JMED;
- JMOU;
- LEGAD;
- LNO MIADIT
- LNOHN-FAF;
- LNO USA;
- MP;
- PCN;
- RSPP;
- Segreteria Comando.

c. Caselle di posta elettronica ed indirizzo postale

Le caselle di posta elettronica istituzionali dell'AOO della BMIS adibite alla ricezione/trasmissione di documenti sono:

- casella di posta elettronica istituzionale (PEI): ***bmis.gibuti@smd.difesa.it***
- casella di posta elettronica certificata (PEC): ***bmis.gibuti@postacert.difesa.it***

Per la posta in ingresso, nel rispetto della garanzia di sicurezza e di quanto riportato sul "Manuale", la casella PEC della BMIS può ricevere e-mail solo da paritetiche caselle di posta elettronica certificata.

Per la posta in uscita, l'indirizzo PEC di destinazione è quello preimpostato sul sistema documentale ADHOC della BMIS per la trasmissione dei documenti.

L'indirizzo postale dell'AOO della BMIS presso il quale potrà essere recapitata la corrispondenza analogica, in originale o in copia autentica (plichi e pacchi a mezzo servizio postale, sia per la posta ordinaria, sia per le raccomandate e le assicurate), è il seguente:

BASE MILITARE ITALIANA DI SUPPORTO

Località Nagad – Djibouti (Ville), DJIBOUTI (AFRICA)

d. Unità Organizzativa responsabile della gestione del protocollo e del sistema documentale, con relativi orari

Il servizio di protocollo informatico e della gestione documentale nell'AOO della BMIS è attualmente organizzato nel seguente modo:

RDS: compito assegnato al Capo Cellula J6 (UO: Cellula J6);

Vicario: compito assegnato al Segretario del Comandante (UO: Segreteria);

Amministratore: compito assegnato al Custode Cifra (UO: Cellula J6).

La UO Segreteria è di massima il punto di protocollo in ingresso della BMIS.

Le varie Cellule/Nuclei della BMIS, qualora in possesso di eventuale documentazione cartacea indirizzata alla Base, in qualunque maniera ad esse pervenuta, devono provvedere alla consegna di tale documentazione al Segretario del Comandante (vicario) per la relativa registrazione a protocollo.

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

L'Ufficio assicura la protocollazione in ricezione di tutta la corrispondenza ricevuta dalle 08:00 alle 18:00, dalla domenica al venerdì. In considerazione della prontezza operativa della Base, sia gli orari sia i giorni sono da considerarsi suscettibili di variazione.

Il Segretario del Comandante (vicario) è autorizzato all'apertura di buste e plichi NON CLASSIFICATI.

I documenti "RISERVATI" non sono oggetto di protocollazione sul sistema ADHOC e devono essere consegnati al PCN.

e. Servizio di scambio posta

I punti di scambio posta per la BMIS sono i seguenti:

- Segreteria Comando per la posta NON CLASSIFICATA;
- PCN per la posta CLASSIFICATA.

f. Titolario

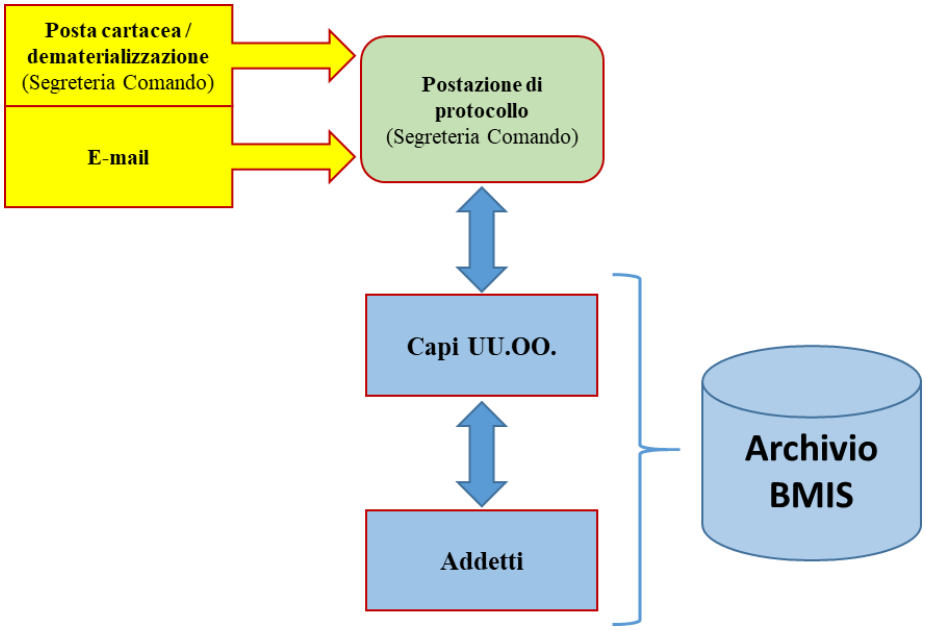
Il "Titolario di archivio" utilizzato dalla BMIS è quello dello Stato Maggiore Difesa (SMD – I – 006) .

g. Postazione del registro di emergenza

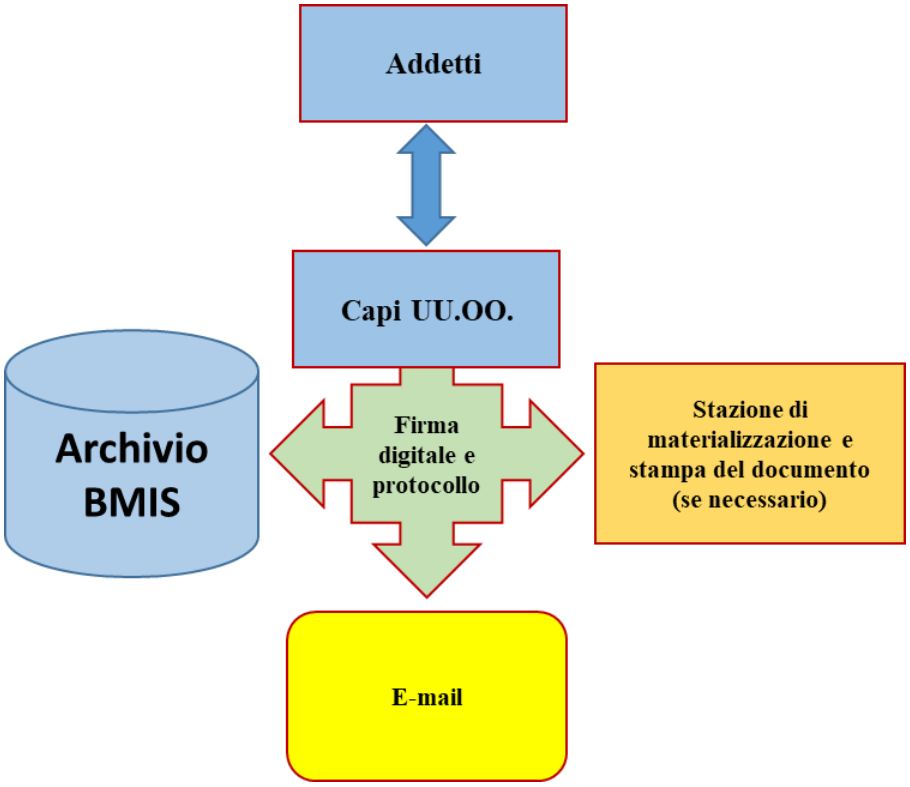
Per la protocollazione d'emergenza è stata approntata una postazione in locale "Sala Briefing" che verrà attivata all'occorrenza su disposizioni dell'RDS (nome macchina BMIS095W).

SCHEMI DI FLUSSO IN ENTRATA ED USCITA DEI DOCUMENTI DELLA BMIS

Flusso in ingresso



Flusso in uscita



Allegato "B"

REGOLE GENERALI DI SCRITTURA DEI DATI

In tutti i sistemi informatici è di particolare importanza la qualità delle informazioni che vengono inserite al suo interno soprattutto in un sistema diffuso e invasivo come quello di PI e gestione documentale.

È facilmente intuibile, infatti, come, in assenza di regole comuni e coerenti, non sarà possibile ottenere tutti i benefici attesi dal sistema, in quanto i documenti potrebbero essere difficilmente rintracciabili o, nei casi peggiori, non rintracciabili!

Vengono di seguito riportate poche regole, a cui tutti gli utenti del sistema devono attenersi, nella redazione dei campi "Oggetto", dei nomi dei fascicoli e, in generale, ogni qualvolta sia necessario digitare una qualunque descrizione.

Nomi di persona prima il cognome e poi il nome.

In maiuscolo solo la prima lettera, esempio: Rossi Mario.

Titoli di cortesia, nobiliari ecc., sempre omessi.

Nomi di città in lingua italiana, se disponibile.

Nomi di stati in lingua italiana.

Nomi di ditte, lettera maiuscola solo nella prima lettera.

L'eventuale forma societaria in minuscolo, senza punti di separazione, esempio: Acme srl.

Enti/associazioni, lettera maiuscola solo per l'iniziale della denominazione.

Ministeri scritti per esteso, esempio: Ministero della Difesa

Enti di secondo livello, esempio: Stato Maggiore Difesa V Reparto e NON V Reparto SMD

Sigle di Enti, senza punti, esempio: ISTAT

Università, esempio: Università degli studi di Roma

Virgolette/apici, digitare dalla tastiera (no copia/incolla da Word) il relativo carattere.

Caratteri speciali non si devono utilizzare, esempio: *, ', ^, ecc....

Date in formato numerico gg-mm-aaaa con separatore trattino esempio: 01-01-2012.

Allegato "C"

NOMINA DEGLI INCARICATI ALLA DEMATERIALIZZAZIONE

_____

ORDINE DI SERVIZIO

OGGETTO: Attestazioni di conformità agli originali analogici delle copie su supporto informatico mediante l'utilizzo della firma digitale.

PREMESSO CHE:

è necessario assicurare la dematerializzazione dei documenti cartacei pervenuti presso la Base Militare Italiana di Supporto a Gibuti, tramite i servizi postali o corrieri abilitati e che alle predette attività deve provvedere il personale in forza al:

- Sezione, Nucleo

VISTO: il D.P.R. n. 445 del 28/12/2000, "Testo Unico delle Disposizioni Legislative e regolamentari in materia di documentazione amministrativa", circa la gestione dei flussi documentali e dei procedimenti amministrativi delle P.A.;

VISTO: l'articolo 23 ter, comma 3, del CAD di cui al D.Lgs. n. 82 del 7/3/2005 e successive modificazioni e integrazioni, circa le copie su supporto informatico di documenti analogici ed il valore giuridico della conformità all'originale delle copie informatiche realizzate dai delegati;

il seguente personale:

Grado, Cognome, Nome,

è delegato alle attestazioni di conformità all'originale analogico della copia su supporto informatico mediante l'utilizzo della firma digitale.

Firma

_____

IL TITOLARIO O PIANO DI CLASSIFICAZIONE

I principi su cui deve essere fondato un sistema o piano di classificazione dei documenti devono essere coerenti e funzionali:

- i documenti devono essere accorpati al fine di soddisfare le esigenze di lavoro di chi produce i documenti e svolge le attività amministrative;
- si deve evitare sia l'eccessiva frammentazione delle pratiche, sia l'eccessivo accorpamento;
- l'articolazione e la struttura del sistema deve essere semplice e di facile comprensione da parte dell'utilizzatore.

Il sistema non deve articolarsi su più di tre livelli, in generale essi sono:

- livello per funzioni in materia (ad esempio, bilancio, concorsi ed assunzioni, ecc.);
- livello per macro-attività per ciascuna funzione (ad esempio, programmazione di spesa, assestamento di bilancio, consuntivo di bilancio, ecc.);
- livello per ulteriore specializzazione delle attività o delle materie (ad esempio, verifica contabile, ecc.).

Il piano di classificazione deve includere:

- la definizione dei criteri di formazione e ordinamento dei fascicoli per ogni voce del piano;
- il collegamento delle voci finali del piano con le informazioni relative ai tempi e alle modalità di conservazione (piano di conservazione dei documenti; art. 68 [DPR]);
- l'eventuale riferimento alle modalità di accesso (legge 241/90) nel rispetto della tutela dei dati personali [CODPRI]. Il sistema di classificazione adottato deve essere descritto all'interno del Manuale.

Ogni voce del piano di classificazione comprende:

- un indice (codice alfanumerico, stabilito con principi di uniformità all'interno di tutta l'AOO);
- la denominazione della voce (uno o più termini che definiscono in modo sintetico la funzione o l'attività);
- la descrizione della voce (una o più proposizioni in grado di descrivere la funzione o la materia considerata in modo comprensibile anche da utenti esterni).

Nelle voci del piano di classificazione è opportuno evitare la presenza di voci generiche, come ad esempio la denominazione "VARIE", o simili, poiché i documenti cosi classificati diventano, di fatto, irreperibili. Il Titolario deve essere aggiornato periodicamente (almeno ogni due anni) significando che, comunque, una nuova classificazione non va applicata ad archivi già formati in precedenza, secondo criteri diversi.