



152° REGGIMENTO FANTERIA "SASSARI"
- "Sa Vida pro sa Patria" -

**MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO
DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI ADHOC**

Edizione 2020



152° REGGIMENTO FANTERIA “SASSARI”
-“Sa Vida pro sa Patria”-

ATTO DI APPROVAZIONE

Approvo il
MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI
FLUSSI DOCUMENTALI E DEGLI ARCHIVI DEL 152°
REGGIMENTO FANTERIA “SASSARI”

IL COMANDANTE DI REGGIMENTO
Col. f. t.ISSMI Giuseppe ROCCO

SOMMARIO

1.	ELENCO DI DISTRIBUZIONE.....	5
2.	ACRONIMI.....	7
3.	RIFERIMENTI NORMATIVI.....	8
4.	GLOSSARIO.....	9
5.	PRINCIPI GENERALI.....	13
5.1	Premessa.....	13
5.2	Ambito di applicazione del materiale di gestione.....	13
5.3	Area Organizzativa Omogenea.....	14
5.4	Servizio per la Gestione del Protocollo Informatico.....	14
5.5	Firma Digitale.....	14
5.6	Tutela dei Dati Personali.....	14
6.	FORMAZIONE, SOTTOSCRIZIONE, TRASMISSIONE E ARCHIVIAZIONE DEL DOCUMENTO INFORMATICO.....	15
6.1	Formazione dei documenti – Aspetti operativi.....	15
6.2	Sottoscrizione dei documenti informatici.....	15
6.3	Trasmissione del documento informatico.....	15
6.4	Archiviazione del documenti informatico.....	15
7.	LA GESTIONE DEI DOCUMENTI – ASPETTI FUNZIONALI.....	16
7.1	Principi generali.....	16
7.1.1	Orario di erogazione del servizio di protocollo.....	16
7.1.2	Documenti protocollati e documenti esclusi dalla protocollazione.....	16
7.1.3	Modalità di assegnazione dei documenti ricevuti.....	17
7.1.4	Gestione di documenti contenenti dati sensibili.....	17
7.2	La gestione del documento informatico.....	17
7.2.1	Flusso in ingresso attraverso PEI.....	18
7.2.2	Flusso in ingresso tramite PEC.....	20
7.2.3	Flusso in uscita.....	21
7.3	La gestione del documenti informatico interno.....	22
7.4	La gestione del documento analogico.....	22
7.4.1	Flusso in ingresso.....	22
7.4.2	La protocollazione dei documenti analogici.....	22
7.4.3	Flusso in uscita.....	23
7.4.4	La gestione del documento analogico interno.....	24
7.4.5	Fax e E-Message.....	24
7.4.6	Documento analogico non firmato.....	24
7.4.7	Interoperabilità con SIGE Matricola Centralizzato.....	24
7.5	Schema dei flussi in ingresso e in uscita.....	26
8.	MODALITA' DI PRODUZIONE E DI GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFOMATICO.....	28
8.1	Unicità del protocollo informatico.....	28
8.2	Registro giornaliero di protocollo.....	28
8.3	Registrazione di protocollo.....	28

8.4	Segnatura di protocollo dei documenti.....	29
8.5	Annullamento delle registrazioni di protocollo.....	29
8.6	Descrizione funzionale e operativa del sistema di protocollo informatico.....	30
9.	CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI.....	31
9.1	Il Titolare di classificazione.....	31
9.2	La classificazione dei documenti.....	31
9.3	La fascicolazione dei documenti.....	32
9.3.1	Il fascicolo unico del personale.....	32
10.	L'ARCHIVIAZIONE DEI DOCUMENTI.....	33
10.1	L'archivio dell'AOO-E20910.....	33
10.2	Archiviazione dei documenti informatici.....	33
10.3	(L'archiviazione) dei documenti analogici.....	33
11.	ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI....	34
11.1	Generalità.....	34
11.2	L'accesso la sistema.....	34
11.3	I profili di accesso.....	34
12.	IL REGISTRO DI EMERGENZA.....	36
12.1	Premessa.....	36
12.2	Attivazione del Registro di Emergenza.....	36
12.3	Attività possibili durante l'attivazione del Registrazione di Emergenza.....	36
12.4	Riattivazione del sistema informatico.....	37
13.	REGOLE GENERALI DI SCRITTURA DEI DATI ALL'INTERNO DEL SISTEMA INFORMATICO.....	38
	ELENCO DEGLI ALLEGATI.....	39

1. ELENCO DI DISTRIBUZIONE

RDS	n. 1 copia digitale
Comandante di Reggimento	n. 1 copia digitale
Capo Ufficio Maggiorità e Personale	n. 1 copia digitale
Capo Ufficio O.A.I.	n. 1 copia digitale
Capo Ufficio Logistico	n. 1 copia digitale
Capo Sezione di Coordinamento Amministrativo	n. 1 copia digitale
Comandante del I Battaglione	n. 1 copia digitale
Comandante della 1^ compagnia	n. 1 copia digitale
Comandante della 2^ compagnia	n. 1 copia digitale
Comandante della 3^ compagnia	n. 1 copia digitale
Comandante della compagnia supporto alla manovra	n. 1 copia digitale
Comandante della compagnia comando e supporto logistico	n. 1 copia digitale
Comandante alla Sede	n. 1 copia digitale
Comandante del Distaccamento del 152° Reggimento Fanteria “Sassari”	n. 1 copia digitale

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

1	
2	
3	
4	
5	
6	

2. ACRONIMI

All'interno del testo, per renderlo più snello, saranno utilizzati acronimi, abbreviazioni e sigle che di seguito vengono riportate, con il relativo significato.

Per alcune delle abbreviazioni usate, sono forniti ulteriori dettagli nel Glossario.

AOO	Area Organizzativa Omogenea
M_D E20910	Area Organizzativa Omogenea del 152° rgt.f. "Sassari"
[CAD]	D.Lgs. 7 marzo 2005, n. 82 (e successive ed eventuali varianti)
[CIRC]	Circolare AGID, n. 60 (e successive ed eventuali varianti)
[CODBCP]	D.Lgs. 22 gennaio 2004, n. 41 (e successive ed eventuali varianti)
[CODPRI]	D.Lgs. 30 giugno 2003, n. 196 (e successive ed eventuali varianti)
[DigitPa]	Ente nazionale per la digitalizzazione della Pubblica Amministrazione
[DIR]	Direttiva SMD-I-004 (e successive ed eventuali varianti)
[DPCM]	Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013 (e successive ed eventuali varianti)
DPR	Decreto del Presidente della Repubblica
[DPR]	DPR 28 dicembre 2000, n. 445 (e successive ed eventuali varianti)
D.Lgs.	Decreto Legislativo
l.	Legge
IPA	Incide delle Pubbliche Amministrazioni
PA	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

3. RIFERIMENTI NORMATIVI

Di seguito viene riportato un elenco della normativa di maggior rilevanza, cui, peraltro, si farà richiamo all'interno del testo, con le abbreviazioni indicate tra parentesi a fianco di ciascun riferimento:

i riferimenti normativi sono da intendersi comprensivi delle varianti, aggiunte e correzioni nel frattempo intervenute sul provvedimento stesso.

La normativa inerente al PI è piuttosto vasta: vengono qui riportati solo gli atti principali, rimandando ad eventuali richiami all'interno del Manuale per altre norme di dettaglio.

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 (e successive ed eventuali varianti) [DPCM]

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.

Decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 (e successive ed eventuali varianti) [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, peraltro, 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.

Circolare AGID , n. 60 (e successive ed eventuali varianti) [CIRC]

“Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni”

Decreto Legislativo 30 giugno 2003, n. 196 (e successive ed eventuali varianti) [CODPRI]

“Codice di protezione dei dati personali”, per l'attuazione, nelle Pubbliche Amministrazioni, delle disposizioni relative alla gestione delle risorse umane, con particolare riguardo ai soggetti che effettuano il trattamento.

Decreto Legislativo 22 gennaio 2004, n. 41 (e successive ed eventuali varianti) [CODBCP]

Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137.

Direttiva SMD-I-004 (e successive ed eventuali varianti) [DIR]

Il protocollo informatico della Difesa.

Decreto Legislativo 7 marzo 2005, n. 82 (e successive ed eventuali varianti) [CAD]

Codice dell'Amministrazione Digitale

Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 (e successive ed eventuali varianti)

Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata.

4. GLOSSARIO

L'applicazione della normativa inerente al Protocollo Informatico postula la necessità di introdurre una serie di termini e concetti nuovi che, nel presente paragrafo, saranno opportunamente approfonditi.

1. Area Organizzativa Omogenea (AOO)

Una AOO (art. 50 comma 4 del [DPR]), rappresenta un insieme di unità organizzative, 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. Dove, in precedenza, poteva esistere 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 (le unità organizzative) che devono utilizzare solo ed esclusivamente un unico registro di protocollo per i propri atti, 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.

2. Responsabile del Servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi (RDS)

Il RDS è l'altra novità di rilievo introdotta dalla normativa (art. 61 [DPR]). In sostanza si tratta di una figura ben diversa dal classico Capo Ufficio Posta o figure simili, da sempre presenti nell'A.D.. I suoi compiti, elencati nell'art. 61 [DPR] e nell'art. 4 [DPCM], infatti, 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 implementando nell'AOO, anche nei confronti dei cittadini/ditte/altre Pubbliche Amministrazioni.

3. Il Manuale di Gestione (Manuale)

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, costituendo, pertanto, la "carta dei servizi" dell'AOO stessa, nella quale gli interessati trovano descritte le modalità di gestione del protocollo nei suoi diversi aspetti. 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. Il Manuale deve essere predisposto dal RDS, che è garante dell'adozione ed applicazione delle procedure indicate al suo interno. Il contenuto del Manuale può essere organizzato da ciascun RDS secondo le specifiche della rispettiva AOO.

4. Titolare e relativa classificazione d'archivio

Il Titolare di archivio è uno schema generale di voci 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.

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. Per *fascicolo* si intende un insieme organico di documenti, un raggruppamento di documenti riferiti ad uno stesso procedimento/attività/materia.

Le unità archivistiche identificate nel piano di classificazione (tipicamente il fascicolo) possono essere organizzate secondo i seguenti criteri:

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

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;
- 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.

I principi su cui deve essere fondato un sistema 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 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 (l. 241/90) nel rispetto della tutela dei dati personali ([CODPRI]). Il sistema di classificazione adottato deve essere descritto all'interno del manuale.

Per ogni voce del piano di classificazione deve essere indicato:

- il tipo di fascicolo creato (fascicolo per oggetto, per procedimento, ecc.);
- il contenuto standard di ogni fascicolo (la natura dei documenti da inserire e la loro organizzazione interna);
- i criteri di ordinamento dei fascicoli (alfabetico, cronologico, ecc.);
- i termini (in numero di anni) per la tenuta del fascicolo nell'archivio corrente e per la sua conservazione nel tempo (temporanea/definitiva);
- il tipo di accesso consentito al fascicolo stesso.

Ogni voce del piano di classificazione comprende:

- un indice (codice alfanumerico, stabilito con principi di uniformità all'interno di tutta l'Amministrazione/AOO);
- la denominazione della voce (uno o più termini che definiscano 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 così classificati diventano, di fatto, irreperibili.

5. La Posta Elettronica Certificata (PEC)

La PEC, fornisce un servizio di messaggistiche 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 comprende altre funzionalità per permettere: confidenzialità, integrità, tracciabilità e storicizzazione del messaggio. La PEC è strettamente connessa all’IPA, 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 dall’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.

L’indirizzo PEC assegnato al 152° Reggimento Fanteria “Sassari” è: rgtf152@postacert.difesa.it

6. La Posta Elettronica Istituzionale (PEI)

La casella PEI è istituita da ciascuna AOO, attraverso la quale possono essere ricevuti i messaggi da protocollare. L’indirizzo PEC assegnato al 152° Reggimento Fanteria “Sassari” è: rgtf152@esercito.difesa.it

7. Amministrazioni Pubbliche

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

8. 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’AOO sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall’affare al quali di riferiscono.

Essi sono ordinati e archiviati in modo coerente e accessibile alla consultazione; l’uso degli atti può essere amministrativo, legale o storico.

L’archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, l’archivio viene suddiviso in tre sezioni: corrente, di deposito, storico.

- Archivio corrente: costituito dal complesso dei documenti relativi ad affari e a procedimenti in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse ove non c’è ancora prescrizione, in aderenza al Codice Civile, che prevede:
 - art. 2946: “salvo i casi in cui la legge dispone diversamente, i diritti si estinguono per prescrizione con il decorso di 10 anni”;
 - art. 2947: “il diritto di risarcimento del danno derivante dal fatto illecito si prescrive in 5 anni dal giorno in cui il fatto si è verificato”.
- Archivio di deposito: è il complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi. Detti documenti non risultano più necessari per il corrente svolgimento del procedimento amministrativo; verso tali documenti però, tuttavia, sussistere un interesse sporadico.
- Archivio storico: costituito da complessi di documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa effettuazione delle operazioni di scarto, alla conservazione perenne.

9. Documento informatico

Rappresentazione informatica di atti fatti o dati giuridicamente rilevanti (CAD art. 1p).

10. Documento analogico

Rappresentazione non informatica di atti fatti o dati giuridicamente rilevanti (CAD art. 1p-bis).

11. 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, lett. D [CODPRI]*).

12. Fascicolazione

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

13. 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. Nel fascicolo possono trovarsi inseriti documenti diversificati per formato, natura, contenuto giuridico, ecc., anche se non è infrequente 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 e del suo aggiornamento.

5. PRINCIPI GENERALI

5.1 Premessa

Il [DPCM] all'art. 3, comma 1, lettera c), prevede, per tutte le amministrazioni di cui all'art. 2 del decreto legislativo 30 marzo 2001, n. 165, l'adozione del manuale di gestione. Quest'ultimo, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio". In questo ambito è previsto che ogni amministrazione pubblica individui una o più AOO, all'interno delle quali sia nominato un Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (RDS).

Obiettivo del Manuale di gestione è descrivere il sistema di gestione documentale, a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna.

Il protocollo informatico costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'amministrazione.

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

Il presente documento pertanto si rivolge a tutti i dipendenti del 152° Reggimento Fanteria "Sassari".

Si ritiene utile sottolineare che il sistema di protocollo informatico non può essere concepito come un originatore asettico di numeri sequenziali, o come semplice trasposizione su un supporto elettronico del registro di protocollo cartaceo. In un sistema informativo documentale moderno, infatti, il protocollo diventa uno snodo irrinunciabile e una risorsa strategica per la corretta gestione dei documenti trattati e dei procedimenti amministrativi.

Questo Manuale, che ne descrive i principi di funzionamento, rappresenta, quindi, un elemento essenziale per la comprensione delle logiche organizzative preposte alla gestione documentale dell'AOO M_D E20910.

5.2 Ambito di applicazione del Manuale di gestione

Il presente manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma c) del [DPCM].

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi del 152° Reggimento Fanteria "Sassari".

Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficace gestione del flusso informativo e documentale interno dell'amministrazione, anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa.

Inoltre, le funzionalità del sistema in uso, aderenti alla vigente normativa, consentono di gestire la documentazione amministrativa in modalità dematerializzata, introducendo decisivi fattori di semplificazione gestionale, risparmi economici e riduzione dell'impegno complessivo necessario alla trattazione della documentazione prodotta o comunque gestita dall'AOO.

Si ritiene utile ricordare come il registro di protocollo fa fede, anche ai fini giuridici, dell'effettivo ricevimento e spedizione di un documento.

5.3 Area Organizzativa Omogenea

Per la gestione dei documenti, è stata individuata l'Area Organizzativa Omogenea (AOO) denominata: E20910 composta dall'insieme delle Unità Organizzative (UO) articolate come riportato nell'allegato 4.

Nel medesimo allegato è indicato il codice identificativo dell'AOO: M_D E20910 nell'ambito del Ministero della Difesa.

5.4 Servizio per la gestione del protocollo informatico

Nell'AOO è istituito il servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, secondo le disposizioni dell'art. 61 [DPR].

L'atto di nomina del Responsabile di tale servizio è in allegato 2.

Nello stesso atto di nomina è indicato il nominativo del Vicario.

5.5 Firma Digitale

La gestione digitale del protocollo informatico prevede l'uso della firma digitale sia per l'invio della documentazione al di fuori dell'AOO (documento informatico), sia per la digitalizzazione dei documenti cartacei in ingresso.

La figura che detiene la titolarità di firma verso destinatari esterni è il Comandante del 152° Reggimento Fanteria "Sassari", fatta eccezione per la documentazione sanitaria, che viene trasmessa dal DSS o da un suo delegato, ed i documenti prodotti da RUP e DEC.

Firmeranno digitalmente, inoltre, gli addetti alle postazioni di dematerializzazione dei documenti cartacei in ingresso (elenco nominativo in allegato 5).

I documenti informatici in uscita, oltre alla firma digitale, contengono anche la marca temporale prevista dalla normativa vigente.

5.6 Tutela dei dati personali

I dati per i quali, ai sensi del [CODPRI], è necessaria una specifica gestione sono trattati in conformità al citato decreto.

6. FORMAZIONE, SOTTOSCRIZIONE, TRASMISSIONE E ARCHIVIAZIONE DEL DOCUMENTO INFORMATICO

6.1 Formazione dei documenti – aspetti operativi

In aderenza alla normativa vigente (art. 40 [CAD]), l'AOO produce esclusivamente documenti originali informatici.

Al fine di uniformare le modalità gestionali, anche la documentazione analogica in ingresso viene dematerializzata e gestita, all'interno dei flussi di lavoro, in modalità interamente informatica.

Inoltre si evidenzia che anche i documenti cartacei in ingresso vengono dematerializzati, in modo che l'intero flusso documentale venga gestito in maniera elettronica.

Ogni documento predisposto per essere inoltrato in modo formale:

- tratta un unico argomento, indicato in maniera sintetica nello spazio riservato all'oggetto;
- è riferito ad una sola registrazione di protocollo.

Le attività di firma digitale e protocollazione dei documenti sono unificate dall'apposita interfaccia operativa del software utilizzato.

6.2 Sottoscrizione dei documenti informatici

Tutta la documentazione amministrativa in ingresso viene firmata nel formato PDF/A.

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

6.3 Trasmissione del documento informatico

Tutta la documentazione amministrativa esterna/interna viene firmata nel formato PDF/A.

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

6.4 Archiviazione del documento informatico

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

7. LA GESTIONE DEI DOCUMENTI – ASPETTI FUNZIONALI

7.1 Principi generali

I documenti vengono gestiti in relazione alla loro tipologia (documento informatico o documento analogico).

Ciascuna delle due tipologie ora descritte prevede tre metodologie di lavoro, in dipendenza del flusso del documento, che può essere:

- in ingresso;
- in uscita;
- interno all'AOO.

In linea generale, i documenti in uscita e interni all'AOO sono gestiti, secondo le regole descritte nel presente manuale e con le funzionalità previste dal sistema informatico di PI e gestione documentale, dagli utenti del citato sistema informatico.

Il flusso in ingresso viene, invece, gestito in modalità centralizzata dal Servizio per la tenuta del protocollo informatico che provvede alla protocollazione e successivo smistamento alla UO denominata “Comandante di Reggimento”, che provvederà allo smistamento alle rispettive UO di competenza.

7.1.1 Orario di erogazione del servizio di protocollazione

Ai fini della mera protocollazione va tenuto presente che i documenti in ingresso vengono protocollati dal lunedì al venerdì, con il seguente orario:

- dal lunedì al giovedì dalle 08:00 alle 16:30;
- il venerdì dalle 08:00 alle 12:00.

Ai fini della protocollazione dei documenti in entrata/uscita, il sistema è sempre operativo, ad eccezione del periodo in cui viene effettuata la stampa del registro di protocollo del giorno.

Tale attività viene effettuata attraverso l'apposizione della firma digitale da parte del RDS. Durante tale fase, per alcuni minuti potrebbe non essere accessibile il sottosistema di protocollazione.

7.1.2 Documenti protocollati e documenti esclusi dalla protocollazione

Sono oggetto di protocollazione tutti gli atti amministrativi inerenti all'attività dell'AOO.

Sono esclusi dalla registrazione di protocollo i documenti elencati nell'art. 53 [DPR]

- gazzette ufficiali;
- bollettini ufficiali e notiziari della pubblica amministrazione;
- materiali statistici;
- gli atti preparatori interni;
- giornali;
- riviste;
- libri;
- materiali pubblicitari;
- inviti a manifestazioni;
- documenti già soggetti a registrazione particolare dell'amministrazione;
- documenti soggetti a classifica di sicurezza nazionale con classifica uguale o superiore a “RISERVATO”.

7.1.3 Modalità di assegnazione dei documenti ricevuti

I documenti ricevuti dalla UO “Comandante di Reggimento” sono assegnati successivamente ai Capi delle UO interessate che provvedono alla successiva gestione interna.

L’assegnazione dei documenti pervenuti in originale informatico avviene, normalmente, entro la giornata di ricezione.

Per i documenti pervenuti in modalità analogica, deve essere tenuto in considerazione il tempo medio necessario per le attività di dematerializzazione, descritte nel paragrafo inerente alla gestione del flusso in ingresso della documentazione analogica.

Se ad una UO viene assegnato un documento non di competenza, il relativo responsabile può procedere, direttamente, alla relativa riassegnazione.

Il personale del servizio di protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta e soggetta alle operazioni di protocollazione. Tale verifica spetta al personale dell’UO interessata alla tematica che, qualora reputi necessario acquisire documenti integrativi di quelli già pervenuti, provvede a richiederli al mittente, specificando le eventuali problematiche del caso.

7.1.4 Gestione di documenti contenenti dati sensibili

Alcune tipologie documentali, per la natura degli atti coinvolti, richiedono una gestione leggermente difforme dal normale, di seguito descritta, per ciascuna tipologia.

Tali documenti vengono definiti con *documenti sensibili*.

Rientrano tra i documenti sensibili quelli appartenenti alle seguenti tipologie:

- documenti legati a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
- documenti della cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell’attività amministrativa;
- le tipologie di documenti individuate dalla normativa vigente (in particolare l’art. 24 della legge 7 luglio 1990, l’art. 8 del DPR 27 giugno 1992 n. 352 e la serie di norme collegate al [CODPRI]).

La gestione di tali documenti non differisce da tutti gli altri, ad eccezione del fatto che i dati associati e il documento stesso sono visibili soltanto al personale preventivamente autorizzato ai sensi della normativa vigente.

È fatto obbligo a tali utenti di segnalare al sistema la tipologia di documento, *clickando* nell’apposito campo *dati sensibili*. Così facendo quei documenti saranno visibili all’interno del sistema solo agli operatori parimenti abilitati a tale trattazione.

7.2 La gestione del documento informatico

L’AOO è predisposta alla ricezione e alla gestione di documenti informatici.

Per la ricezione di documenti informatici, l’AOO dispone di una casella di posta elettronica istituzionale (PEI) e di una casella di posta elettronica certificata (PEC):

- PEI: rgtf152@esercito.difesa.it
- PEC: rgtf152@postacert.difesa.it

La trattazione di documentazione amministrativa attraverso le caselle di posta elettronica comporta la necessità di adeguarsi a determinati standard per consentire l’interoperabilità dei sistemi, oltre che per rispondere al dettato normativo vigente.

Pertanto, le comunicazioni informatiche concernenti l'AOO M_D E20910, **in arrivo**, dovranno osservare le seguenti regole generali:

- il formato preferibile, per file allegati ai messaggi di posta elettronica come documenti primari, è il PDF (e PDF/A); sono accettati anche, sempre come documenti primari, i formati RFT, JPG, P7M, TXT, TIFF, TIF, XML;
- i file allegati al documento primario possono avere qualsiasi tipo di estensione e possono essere compressi nel formato ZIP;
- l'invio di allegati in un formato diverso da quelli sopra indicati comporta la restituzione al mittente del documento ricevuto;
- è preferibile l'apposizione della firma digitale ai documenti allegati al messaggio;
- le eventuali marche temporali apposte insieme alla firma digitale devono essere in formato *embedded* e non *detached* (il file firmato e la firma devono essere contenuti in un'unica busta di file);
- l'eventuale apposizione di firma digitale non valida rende non utilizzabile il file eventualmente trasmesso;
- la massima dimensione complessiva degli allegati deve essere di 30 MB; in caso di superamento di tale limite il messaggio non sarà recapitato all'AOO del sistema di posta;
- la casella postale del mittente, in caso di persone giuridiche, deve essere riferita alla persona giuridica medesima (ad esempio, la ditta ROSSI S.p.A. dovrà inviare la propria documentazione dalla casella postale rossispa@xxxxx.it e non dalla casella postale mario.rossi@rossispa.xxxxx.it);

altresì, le comunicazioni informatiche concernenti l'AOO M_D E20910, **in partenza**, dovranno osservare le seguenti regole generali:

- i formati da utilizzare per i documenti primari sono: DOC, PDF, RTF, TXT, che il sistema convertirà in automatico, al momento della firma, in PDF/A;
- i file allegati al documento primario possono essere di qualsiasi tipo di estensione (possono essere compressi nel formato ZIP);
- l'eventuale invio di documenti in formati non presenti tra quelli sopra elencati può essere effettuato previo accordo con il RDS, tramite l'UO interessata alla ricezione;
- in un singolo messaggio di posta elettronica deve essere associata la documentazione relativa ad un unico argomento (pertanto, se un mittente deve inviare cinque documenti afferenti cinque pratiche, dovrà inviare cinque mail);
- la massima dimensione complessiva degli allegati deve essere di 30 MB; in caso di superamento di tale limite il messaggio non sarà recapitato all'AOO dal sistema di posta;
- la casella postale del destinatario, in caso di persone giuridiche, deve essere riferita alla persona giuridica medesima (ed esempio, per posta indirizzata alla ditta ROSSI S.p.A. si dovrà inviare documentazione alla casella postale rossispa@xxxxx.it e non alla casella postale mario.rossi@rossispa.xxxxx.it);
- il nome degli eventuali file allegati deve essere di lunghezza moderata, non contenente spazi e caratteri speciali (lettere accentate, °, ^, virgolette, spazi);
- si suggerisce di utilizzare il carattere *_* (*underscore*) al posto di tali caratteri.

7.2.1 Flusso in ingresso tramite PEI

I messaggi in arrivo sulla casella di posta elettronica vengono inseriti in un'apposita coda.

L'operatore di protocollo, in virtù dell'abilitazione a lui concessa, accede alla predetta coda di messaggi.

I messaggi vengono presentati all'operatore in ordine di arrivo all'AOO. Se la protocollazione di un messaggio non viene completata, quello stesso messaggio sarà presentato al primo operatore che, subito dopo, accederà alla stessa coda dei messaggi.

L'operatore protocolla il messaggio, procedendo alla successiva assegnazione all'UO "Comandante di Reggimento", ovvero, nei casi dubbi, lo invia, tramite apposita funzione del sistema, sulla casella di posta funzionale dell'RDS.

I documenti che vengono sottoposti alla successiva gestione del RDS possono essere protocollati direttamente da quest'ultimo ovvero, rispediti al mittente oppure cancellati.

Nel caso in cui l'RDS decida di inviare al mittente il messaggio, il sistema mette a disposizione una casistica già predisposta di messaggi:

- a) il messaggio è corrotto o uno dei documenti non leggibile;
- b) dati non congruenti nella segnatura informatica;
- c) segnatura non conforme alla circolare AGID n. 60;
- d) mancata sottoscrizione del documento primario;
- e) destinatario errato;
- f) verifica di integrità dei documenti negativa;
- g) il documento o gli allegati dichiarati all'interno del file *segnatura.xml* non corrispondono a quanto ricevuto.

Le mail che vengono considerate *spam* non vengono protocollate e non viene spedito nessun messaggio al mittente, vengono inviate a RDS per l'eliminazione definitiva dal sistema.

Ai sensi della normativa vigente, è possibile protocollare un messaggio di posta elettronica ordinaria solo se firmato digitalmente (art. 47/1/a [CAD]).

Nel rispetto dell'art. 38 del [DPR] vengono comunque accettati e protocollati documenti informatici, nei formati indicati nel paragrafo precedente, anche privi di firma digitale, ai quali sia allegata una scansione del documento di identità del mittente. Tali documenti potranno comunque non essere accettati per la successiva trattazione dall'UO competente, se viene riscontrata qualche irregolarità. Di tale evento sarà informato il mittente attraverso apposito messaggio preparato dall'UO assegnataria per competenza.

Nel caso in cui il mittente sia una P.A., ai fini della protocollazione, anche in assenza della firma digitale, è sufficiente che siano presenti le informazioni previste dalla [CIRC] (art. 47/1/b).

In tal caso, ove richiesto dal mittente, secondo le regole della [CIRC], sarà trasmesso:

- messaggio di conferma di protocollazione, che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto;
- messaggio di notifica di eccezione, che notifica la rilevazione di un'anomalia in un messaggio ricevuto;
- messaggio di annullamento di protocollazione, che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza.

Il sistema gestisce in automatico – senza inserire i relativi messaggi in ingresso nell'AOO rispettiva coda – quei messaggi che segnalano un problema di ricezione nella casella postale ordinaria del destinatario (è il caso in cui, dall'AOO, è stato inviato un messaggio ad una casella postale ordinaria, ma quest'ultima è piena o il destinatario risulta sconosciuta al sistema di posta elettronica: in tal caso sarà recapitata alla casella PEI dell'AOO un messaggio che informa di tale evenienza).

Questi messaggi sono automaticamente inseriti quali allegati del documento che ha generato il messaggio stesso e il documento interessato viene ricollocato sulla scrivania virtuale inerente ai documenti in ingresso (nella voce *posta non consegnata*) del primo utente che predisposto il documento, per le opportune azioni del caso.

In particolare, l'addetto, dopo le necessarie verifiche può:

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

Almeno una volta al giorno viene verificata la presenza dei messaggi.

7.2.2 Flusso in ingresso tramite PEC

I messaggi in arrivo sulla casella di posta elettronica vengono inseriti in un'apposita coda.

L'operatore di protocollo, in dipendenza delle abilitazioni a lui concesse, accede alla predetta coda di messaggi.

I messaggi vengono presentati all'operatore in ordine di arrivo all'AOO.

Se la protocollazione di un messaggio non viene completata, quel messaggio sarà presentato al primo operatore che, subito dopo, accederà alla stessa coda dei messaggi.

L'operatore può protocollare il messaggio, procedendo alla successiva assegnazione all'UO "Comandante di Reggimento" ovvero, nei casi dubbi o quando ritiene che il messaggio non sia di competenza dell'AOO, può inviarlo in un apposito elenco, gestito dal RDS.

I documenti che vengono sottoposti alla successiva gestione del RDS possono essere protocollati direttamente da quest'ultimo ovvero, nei casi previsti, scartati e cancellati, senza farli entrare all'interno del sistema documentale.

Nel caso in cui siano protocollati e l'UO assegnataria riscontrasse la palese non competenza dell'AOO, sarà quest'ultima, attraverso PEC, con un messaggio protocollato, ad informare il mittente di tale evenienza. L'assegnazione di tali messaggi sarà effettuata a discrezione del RDS, secondo criteri di omogeneità di trattamento.

Le mail che vengono considerate *spam* non vengono protocollate e non viene spedito nessun messaggio al mittente, vengono inviate a RDS per l'eliminazione dal sistema.

Nel caso in cui il mittente sia una P.A., in assenza della firma digitale, è sufficiente che siano presenti le informazioni previste dalla [CIRC].

In tal caso, ove richiesto dal mittente, sarà trasmesso:

- messaggio di conferma di protocollazione, che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto;
- messaggio di notifica di eccezione, che notifica la rilevazione di un'anomalia in un messaggio ricevuto;
- messaggio di annullamento di protocollazione, che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza.

Il sistema gestisce in automatico, senza inserire i relativi messaggi nelle rispettive code le ricevute generate dal sistema di PEC.

Questi messaggi sono automaticamente inseriti quali allegati del documento che ha generato il messaggio stesso e sono visibili attraverso le normali funzioni di consultazione.

Almeno una volta al giorno viene verificata la presenza di messaggi.

7.2.3 Flusso in uscita

Come già segnalato in precedenza, tutta la documentazione amministrativa dell'AOO viene prodotta in originale in modalità informatica.

Pertanto, quando il dirigente competente ha perfezionato il relativo iter, attraverso le funzioni del sistema, provvede a firmare digitalmente e apporre la marca temporale al documento di interesse.

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.

L'utilizzo della casella postale elettronica ordinaria, piuttosto che della PEC, viene programmato 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.

Ovviamente la trasmissione per PEC è possibile solo quando il destinatario ha segnalato la propria casella di PEC dell'AOO.

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

La procedura sopra descritta è valida per tutta la documentazione prodotta dall'AOO ad eccezione dei seguenti casi:

- corrispondente privo di una qualsiasi casella di posta elettronica;
- documento primario a cui è associato un allegato analogico non dematerializzabile;
- documento primario cui è associato un allegato informatico che, per caratteristiche proprie, non può essere inviato per posta elettronica (ad esempio, dimensione eccessiva, non gestibile dai servizi di posta elettronica).

Nei casi sopraelencati, la formazione e la sottoscrizione dell'atto avvengono secondo modalità idonee alla produzione di un originale informatico che, peraltro, anche in tale formato viene archiviato. Solo la trasmissione viene effettuata con le tecnologie postali analogiche.

Ancora più in dettaglio, nel primo dei casi segnalati, il sistema informatico provvede autonomamente a trasferire il documento in questione nella lista dei documenti da materializzare, che costituirà l'elenco dei documenti da spedire attraverso i servizi postali tradizionali.

Negli altri due casi, invece, è l'operatore che deve informare il sistema che quel documento non deve essere trasmesso per posta elettronica ma, fatto confluire nella già descritta lista dei documenti da materializzare (è necessario segnalare che, nei casi in cui vi sia un allegato analogico e il documento deve essere spedito a più destinatari, alcuni dei quali in indirizzo per conoscenza, laddove questi ultimi dispongano di una casella di posta elettronica, limitatamente ad essi, il sistema procede comunque alla trasmissione del documento informatico).

Quando il documento non deve essere trasmesso per posta elettronica, il sistema informatico, una volta perfezionate le operazioni relative all'apposizione della firma digitale, all'acquisizione della marca temporale ed alla protocollazione, non ne effettua la trasmissione, ma ne processa l'inoltro in un'apposita lista di documenti da materializzare.

Possono accedere a tale lista solo gli operatori *ad hoc* abilitati, che provvedono alla stampa del documento primario e degli eventuali allegati (in caso di allegati digitali, provvedono al *download* in locale e successivo riversamento su adeguato supporto informatico).

Sulla facciata retrostante del documento così stampato, sarà apposta la seguente dicitura:

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

Sassari, gg mm aaaa

IL COMANDANTE DI REGGIMENTO

Dopo la firma di tale attestazione, il documento primario e gli eventuali allegati vengono spediti all'indirizzo postale del destinatario, attraverso il tradizionale servizio postale, secondo un processo che viene descritto nel paragrafo inerente al flusso dei documenti analogici in uscita.

Al fine di inviare correttamente un documento informatico, è necessario applicare alcune regole nella struttura del file che viene predisposto:

- utilizzare i modelli previsti, evidenziati nel par. 7.2, il sistema provvederà alla successiva conversione in formato PDF/A all'atto della firma del documento;
- nel fissare il nome del file, è preferibile non superare gli otto caratteri;
- nella denominazione del file, non si devono utilizzare caratteri speciali e/o lettere accentate (° , ^ , è, ecc.), così come non va utilizzato il segno di interpunzione “.” (il punto).

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, che potrebbero bloccare la fase di protocollazione e trasmissione del documento.

7.3 La gestione del documento informatico interno

Per documenti interni si intendono quelli scambiati tra le diverse UO afferenti alla medesima AOO. In tutti quei casi nei quali tra gli indirizzi per competenza o per conoscenza di un documento vi sia una UO interna all'AOO, tale informazione viene dichiarata all'interno del sistema informatico che provvederà ad inviare, automaticamente, quel documento sulla scrivania virtuale del dirigente competente dell'UO destinataria.

Quel documento sarà protocollato solo in uscita dalla UO mittente.

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

7.4 La gestione del documento analogico

L'indirizzo di posta cui perviene la documentazione analogica inerente all'attività dell'AOO è:

**152° REGGIMENTO FANTERIA “SASSARI”
VIA CARLO FELICE, 7
07100 SASSARI (SS)**

7.4.1 Flusso in ingresso

La corrispondenza analogica in arrivo può essere acquisita dalla AOO a mezzo posta convenzionale, previo ritiro, da parte del personale del Servizio Protocollo, presso il centro postale “Sassari 1 – Via XXV aprile, n. 12”. La posta può comunque essere consegnata anche da corrieri e servizi di recapito corrispondenza, direttamente presso

il numero civico ed accettata dal personale di servizio, **esclusivamente in orario di ufficio**. Sarà cura del personale di servizio farla recapitare celermente al protocollo.

7.4.2 La protocollazione dei documenti analogici

Le attività di protocollazione iniziano con l'apposizione manuale, sul documento in trattazione, di un codice identificativo dell'UO di competenza, al fine di facilitare le successive attività di assegnazione.

I documenti sono, quindi, scansionati massivamente, a cura di addetti abilitati alla funzione e, di seguito, valorizzati attraverso l'inserimento dei dati essenziali per la protocollazione:

- codice Amministrazione mittente, se presente;
- codice AOO mittente, se presente;
- mittente;
- oggetto;
- protocollo mittente;
- data protocollo mittente.

Se al protocollo sono associati allegati in formato analogico, ovvero allegati informatici, essi possono essere gestiti nel processo di dematerializzazione.

Se si tratta di allegati analogici cartacei, vengono inseriti nella fase di scansione massiva del documento di riferimento, con un opportuno separatore idoneo a distinguerli dal documento primario di appartenenza.

Nel secondo caso, saranno accettati allegati su supporto ottico (CD ovvero DVD) ovvero su memoria con connessione USB (rigorosamente vidimate dal Responsabile Operativo Locale per la Sicurezza ICT).

Non saranno accettati allegati informatici su supporti diversi da quelli sopra 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.

Se la dimensione dei dati contenuti nel supporto è eccessiva, il supporto viene, invece, inviato all'UO di competenza.

A questo punto il sistema chiede all'addetto di apporre la firma digitale (e la marca temporale) sul file ottenuto dal processo di scansione massiva.

Se la qualità della scansione è valida e i dati suelencati sono stati inseriti, il documento può essere firmato digitalmente e, successivamente, protocollato in ingresso e smistato all'UO di competenza.

Tutti gli addetti al servizio per la tenuta del protocollo informatico sono abilitati all'apposizione della propria firma digitale sui documenti scansionati, così come stabilito in tema di documento amministrativo informatico nel nuovo art. 23-ter del CAD.

Il documento analogico originale viene custodito all'interno dell'ufficio posta del Reggimento, ai soli fini di eventuali verifiche, con le modalità più avanti meglio descritte.

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

7.4.3 Flusso in uscita

Poiché nell'ambito dell'AOO vengono prodotti esclusivamente documento originali informatici, non avrebbe senso parlare di flusso in uscita di documenti analogici.

Tuttavia, come già esposto nel paragrafo inerente al flusso in uscita dei documenti informatici, può essere necessario procedere alla trasmissione attraverso il servizio postale tradizionale di uno o più documenti analogici. Si fa quindi rinvio al citato paragrafo, per quanto concerne le procedure di preparazione di detti documenti da parte dell'operatore incaricato.

Viene di seguito descritto, invece, il procedimento che conduce alla trasmissione vera e propria.

I documenti che devono essere trasmessi per posta ordinaria cartacea devono essere portati presso il Servizio di Protocollo, accompagnati dalla modulistica di seguito descritta per Enti Militari e Statali, Enti Privati o altro soggetto esterno:

- per via assicurata o raccomandata (anche R.R.), compilando, in duplice copia, l'apposita distinta;
- per via prioritaria, compilando, in duplice copia, l'apposita distinta.

Come disposto dalla vigente normativa in materia di trasparenza amministrativa, è fatto obbligo di compilare, in maniera leggibile ed in tutta la sua interezza, l'apposita modulistica a corredo di ciascuna tipologia di spedizione.

Inoltre, al fine di evadere tempestivamente il flusso della corrispondenza in uscita, i documenti da inviare devono essere consegnati al personale preposto non oltre le ore 10:30, per consentirne in tempo utile la spedizione presso l'Ufficio Postale.

7.4.4 La gestione del documento analogico interno

Non essendo prevista la produzione di originali analogici, non esiste la casistica inerente al documento analogico interno.

Tuttavia, i casi in cui il documento da inviare contenga allegati che, per loro natura, non possono essere dematerializzati, dovranno essere gestiti con le modalità già descritte nel paragrafo inerente al flusso in uscita dei documenti informatici.

7.4.5 Fax e E-Message

L'apparato fax viene gestito dal Centralino, che osserva i seguenti orari:

- dal lunedì al giovedì, dalle 07:30 alle 17:00;
- il venerdì, dalle 07:30 alle 12:30.

I documenti pervenuti in queste fasce orarie vengono consegnati agli addetti del Nucleo Posta. In orario non di servizio, i fax vengono ricevuti dall'Ufficiale di Picchetto all'installazione, il quale li consegnerà agli addetti al Nucleo Posta a termine del servizio.

Per quanto riguarda gli E-Message, gli stessi vengono ricevuti, in orario di servizio, dagli addetti al Nucleo Posta. In orario non di servizio, vengono ricevuti dall'Ufficiale di Picchetto all'installazione, il quale li consegnerà agli addetti al Nucleo Posta al termine del servizio.

7.4.6 Documento analogico non firmato

I documenti privi di mittente (es. esposti anonimi), sono trattati in ambito AOO direttamente dal Direttore, a cui tali documenti vengono consegnati, dopo la relativa protocollazione.

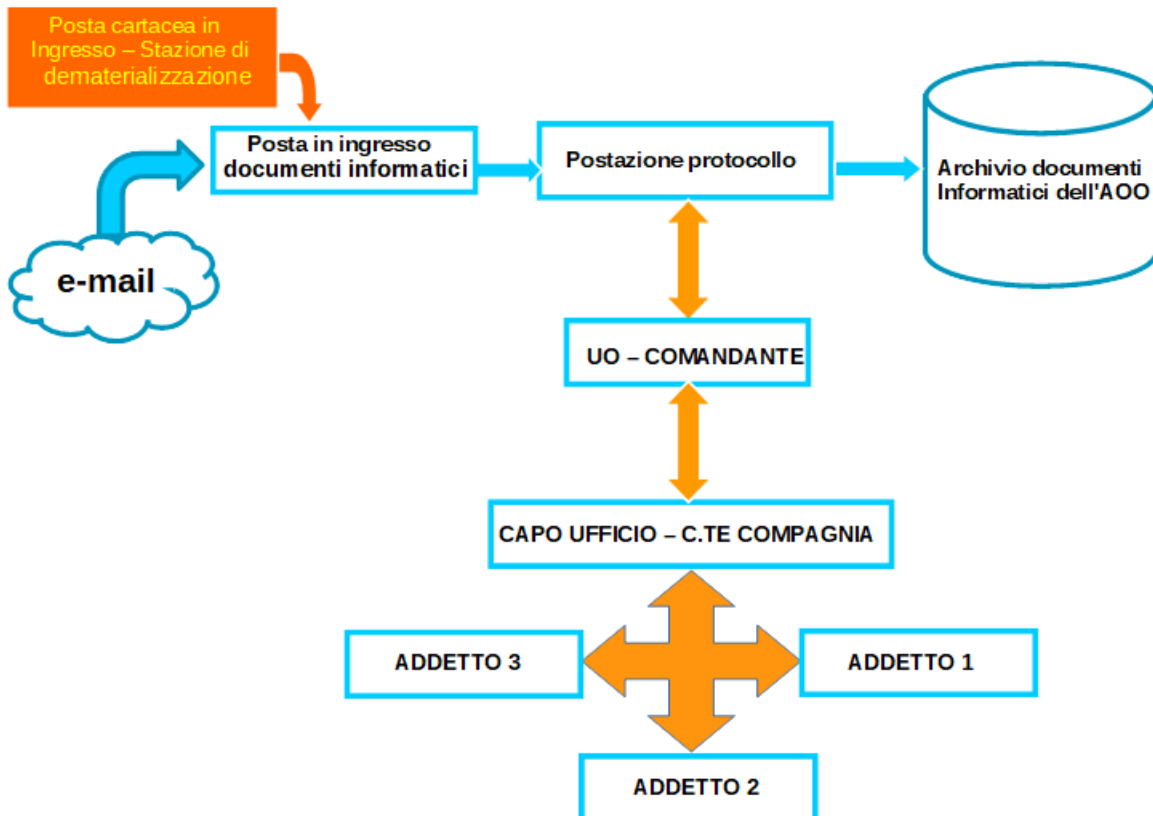
7.4.7 Interoperabilità con SIGE Matricola Centralizzato

Dal 1° settembre 2019, nel contesto del progetto di centralizzazione e dematerializzazione delle cartelle amministrative, è stato avviato il sistema "SIGE Matricola Centralizzato", interoperabile con Adhoc. Il sistema

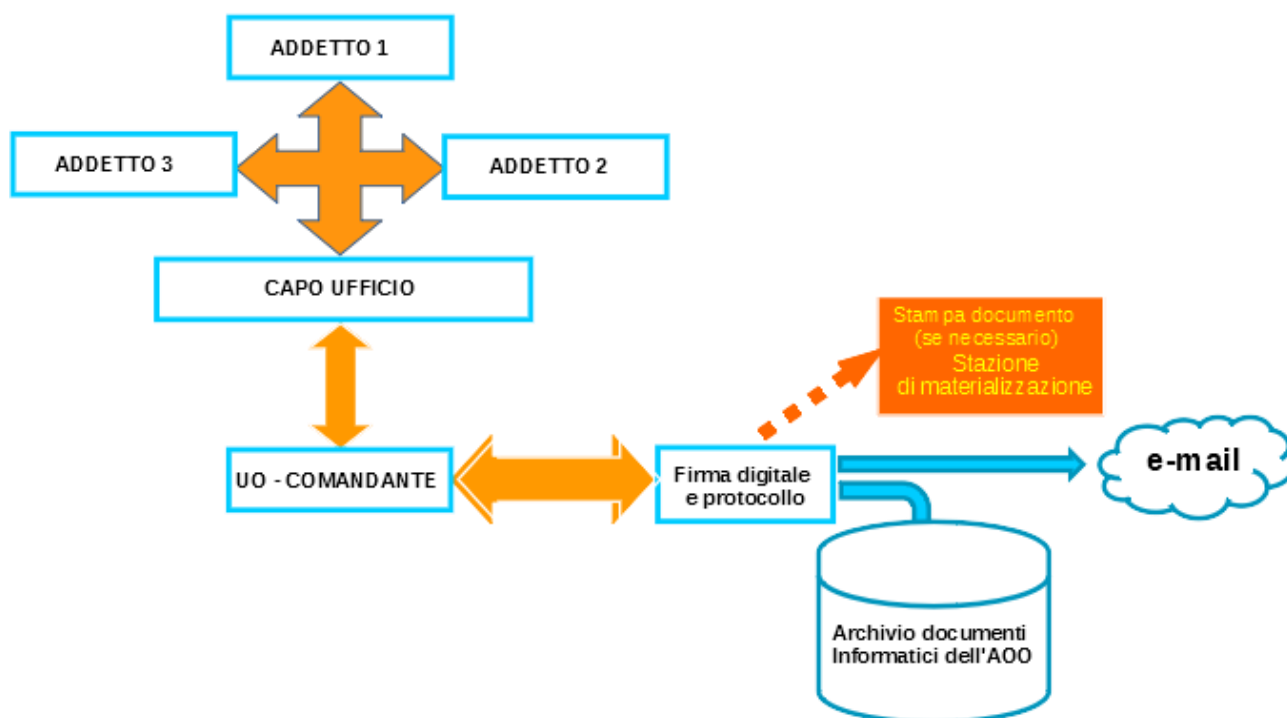
prevede che gli operatori delle sezioni competenti trasmettano alla Sezione Matricola le richieste di variazione matricolare. Una volta verificate le informazioni e valutata la significatività dei corsi, le richieste vengono inviate al Capo Ufficio Maggiorità e Personale che, firmando digitalmente, genera un protocollo (Registro RV) ed un flusso che viene inviato automaticamente, tramite il SIGE Matricola Centralizzato, al CNA, il quale valuterà la proposta e la inserirà nel D.U.M. (Documento Unico Matricolare).

7.5 Schema dei flussi in ingresso, in uscita e interno

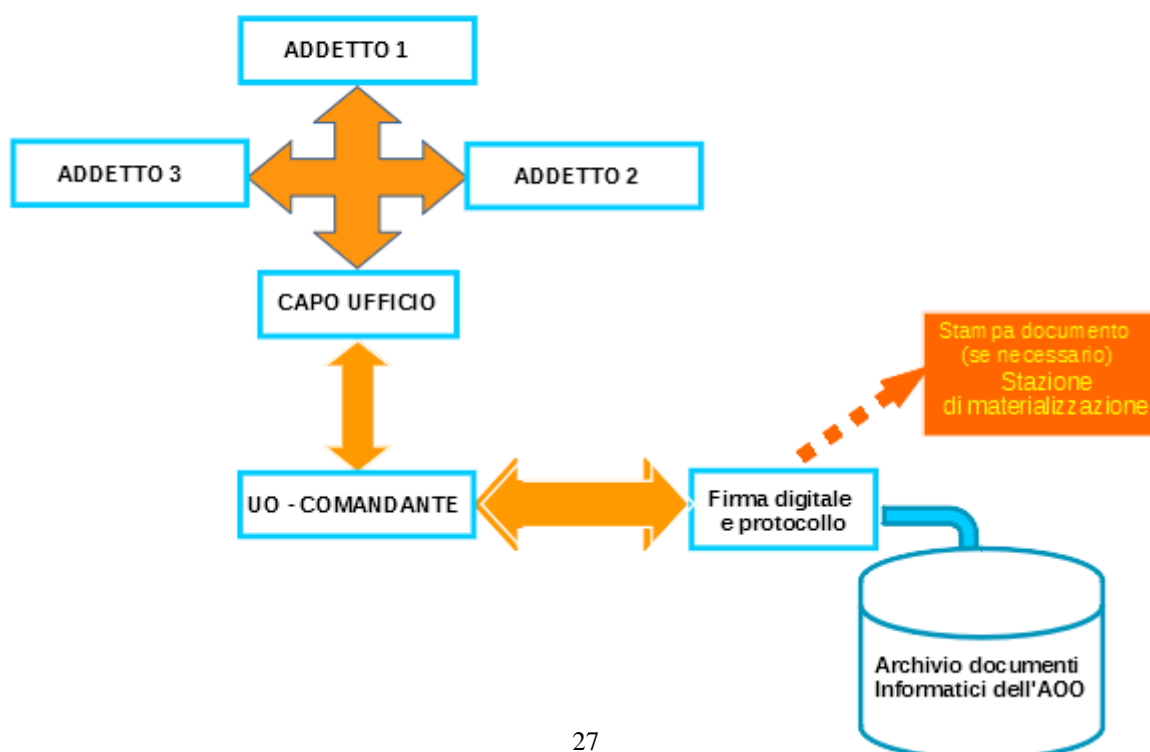
ESEMPIO DI FLUSSO IN ENTRATA



ESEMPIO DI FLUSSO IN USCITA



ESEMPIO DI FLUSSO INTERNO



8. MODALITÀ DI PRODUZIONE E DI GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

8.1 Unicità del protocollo informatico

Nell'ambito della AOO, il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica.

La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal 1° gennaio dell'anno successivo.

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

Il numero di protocollo è costituito da un numero di almeno sette cifre.

La documentazione non registrata viene considerata giuridicamente inesistente presso l'amministrazione.

Non è consentita la protocollazione di un documento già protocollato.

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

8.2 Registro giornaliero di protocollo

Ogni giorno, intorno alle 24, il sistema provvede alla generazione della stampa delle registrazioni di protocollo del giorno. Durante tale attività, della durata di pochi minuti, non sarà possibile protocollare atti in uscita e/o in entrata.

I report di stampa delle registrazioni giornaliere vengono firmati digitalmente, in modalità automatica, a cura del RDS. Ciò avviene, in genere, il giorno successivo a quello cui la protocollazione si riferisce, o il primo giorno feriale dopo quello festivo (viene editato e firmato anche il registro relativo alle giornate in cui non è stata effettuata alcuna registrazione di protocollo).

La stampa viene archiviata all'interno del sistema ed è sempre possibile effettuarne copie cartacee o digitali.

8.3 Registrazione di protocollo

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

In particolare:

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

Va tenuto presente che, nel caso in cui si tratti di un documento informatico proveniente da una P.A., dotato di file `segnatura.xml`, i relativi dati saranno utilizzati a completamento automatico delle informazioni afferenti alla registrazione di protocollo. Tali dati non saranno, peraltro, modificabili dall'operatore.

Anche il campo oggetto, per i messaggi provenienti per posta elettronica, non sarà modificabile, poiché catturato dall'oggetto della mail pervenuta all'AOO.

8.4 Segnatura di protocollo e documenti

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

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`, se conforme alle indicazioni della [CIRC].

Sui documenti in uscita, la segnatura di protocollo viene impressa sul primo foglio del documento informatico, sul lato sinistro in alto.

Al fine di garantire la validità del documento informatico così prodotto, la segnatura apposta sul documento viene firmata, in modalità automatica.

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

Il formato della segnatura di protocollo dell'AOO `M_D E20910`, conformemente alla normativa, prevede 5 dati:

- Codice dell'Amministrazione: **M_D**
- Codice dell'AOO: **E20910**
- Anno Registro: **REGxxxx**
- Numero di protocollo: **1234567**
- Data di registrazione: **gg-mm-aaaa**

Esempio di segnatura di protocollo: **M_D E20910 REG2020 1234567 01-01-2020**

8.5 Annullamento delle registrazioni di protocollo

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

È altresì possibile annullare una registrazione di protocollo per un documento erroneamente registrato (modulo richiesta annullamento protocollo, allegato 6).

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

Il sistema registra l'avvenuto annullamento, la data ed il nominativo dell'operatore che è intervenuto.

Solo il RDS è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.

L'annullamento di una registrazione di protocollo può avvenire anche su richiesta, con specifica nota, adeguatamente motivata, indirizzata al RDS.

8.6 Descrizione funzionale e operativa del sistema di protocollo informatico

Il sistema di protocollo informatico e gestione dei flussi documentali e degli archivi è quello messo a disposizione da SEGREDIFESA – V Reparto – Innovazione tecnologica per l’Area di vertice e centrale del Ministero della Difesa. L’applicativo, denominato ADHOC, è fruibile via web e localizzato presso i *server* del C4 DIFESA, che ne assicura anche l’affidabilità, la sicurezza e la ridondanza. Tutte le informazioni di dettaglio inerenti alle funzionalità presenti nel sistema informatico di PI e gestione documentale sono reperibili nel manuale utente del sistema stesso, disponibile *on-line* per ogni utente autenticato al sistema.

9. CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

9.1 Il Titolare di classificazione

I documenti ricevuti e quelli prodotti devono essere classificati e fascicolati per una corretta conservazione in archivio.

Il Titolare d'archivio adottato per tutta la F.A. è quello dell'AOO-SME che si presenta all'interno del database del sistema ADHOC come se fosse strutturato su tre livelli.

Infatti, mentre il Titolare adottato dalla Forza Armata si articola su quattro livelli ed è flessibile, permette, cioè di classificare documenti anche al secondo livello, il sistema ADHOC prevede la sola classificazione archivistica dei documenti al terzo livello. La soluzione adottata prevede l'accorpamento di terzo e quarto livello, quando presente, in un'unica voce e l'aggiunta di un terzo livello "vuoto" al secondo quando necessario.

- Le voci di 1° livello contengono 12 titoli di seguito elencati:

- 1 – organizzazione;
- 2 – pianificazione;
- 3 – programmazione;
- 4 – studi, ricerche e sviluppo progetti;
- 5 – gestione delle risorse umane;
- 6 – gestione risorse finanziarie;
- 7 – gestione risorse logistiche;
- 8 – formazione, addestramento e aggiornamento;
- 9 – impiego dello strumento operativo;
- 10 – impiego dello strumento logistico;
- 11 – controllo;
- 12 – pubblica informazione, comunicazione e stampa.

- Le voci di 2° (classe) e 3° (sottoclasse) livello.

Il secondo livello, denominato Classe, è composto da 19 titoli, mentre il terzo livello, denominato Sottoclasse, è composto da 8 titoli.

L'aggiornamento del Titolare compete esclusivamente al vertice dell'AOO-E20910, su proposta del RDS.

Ciascuna UO può chiedere integrazioni, varianti e aggiunte al Titolare, sulla base delle proprie necessità.

Dopo ogni modifica al Titolare, 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.

9.2 La classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un criterio logico, in relazione alle funzioni e alle competenze della AOO.

Essa è eseguita attraverso il Titolare di classificazione.

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

Mediante la classificazione, si assegna al documento il codice completo dell'indice di classifica (titolo, classe, sottoclasse). Inoltre, potrà essere assegnato il numero del fascicolo ed eventualmente del sottofascicolo, nonché l'UO di competenza.

L'operazione di classificazione in ingresso viene eseguita dall'addetto alla registrazione di protocollo.

9.3 La fascicolazione dei documenti

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

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

I fascicoli e i sottofascicoli sono invece gestiti direttamente dagli interessati ai relativi provvedimenti.

Il codice del fascicolo e del sottofascicolo deve essere numerico; per quanto attiene alla descrizione, occorre attenersi alle regole generali di scrittura dei dati indicati nell'apposito paragrafo.

Non devono comunque essere creati fascicoli la cui denominazione possa comportare ambiguità

gestionale (ad esempio, la descrizione "varie").

Il sistema traccia la data di creazione del fascicolo.

9.3.1 Il fasciolo unico del personale

A seguito dell'avvio, dal 1° settembre 2019, del "SIGE Matricola Centralizzato", interoperabile con Adhoc, è stato introdotto, a livello centralizzato, un fascicolo personale per ciascun militare all'interno della AOO di appartenenza e all'interno delle AOO che trattano centralmente il personale della Forza Armata.

L'identificativo del citato fascicolo è creato in modo automatico, con regole uniche e non modificabili dall'utente (Classe Leva / Prima lettera del cognome / Forza Armata / Codice Fiscale).

All'interno del fascicolo è stato creato un sottofascicolo "Documenti e Riferimenti" ad uso del processo di gestione matricolare, per la sola AOO CNA Esercito.

Nel contesto del progetto di centralizzazione e dematerializzazione delle cartelle amministrative, sono stati creati, all'interno del fascicolo personale, tutti i sottofascicoli costituenti la cartella amministrativa.

Eventuali sottofascicoli per la gestione dei procedimenti, dovranno essere creati dal RDS, nei casi previsti, come sottofascicoli del citato fascicolo personale.

10. L'ARCHIVIAZIONE DEI DOCUMENTI

10.1 L'Archivio dell'AOO-E20910

Atteso che l'AOO-E20910 produce esclusivamente originali informatici, provvedendo, altresì a dematerializzare e convalidare tutti gli atti cartacei pervenuti dall'esterno, l'universalità dei documenti originali afferenti all'AOO-E20910, a partire dalla data di avvio del servizio, sono archiviati all'interno del sistema informatico, che ne consente la gestione e ne garantisce l'accesso, in ottemperanza alle varie disposizioni di legge.

10.2 Archiviazione dei documenti informatici

I documenti informatici sono archiviati su *servers*, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo, su aree di memoria all'interno del servizio gestito dall'organizzazione informatica del C4 DIFESA. 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.

Le regole generali di archiviazione sono disponibili nel paragrafo inerente alla classificazione.

10.3 (Archiviazione) dei documenti analogici

La parola archiviazione è stata posta tra parentesi in quanto, come già spiegato nei precedenti paragrafi, l'unico archivio dell'AOO-E20910 è quello informatico. Tuttavia, è necessario considerare i documenti gestiti prima dell'entrata in esercizio del nuovo sistema e quelli che continuano a giungere all'AOO.

Per i primi, non verrà effettuato alcun inventario. Le precedenti modalità di archiviazione restano vive, fino all'eventuale esaurimento della pratica. Certamente, per i fascicoli ancora aperti, vi sarà una cesura, derivante dalla dicotomia che si viene a realizzare tra i "vecchi" documenti cartacei e i "nuovi" documenti informatici, che saranno archiviati in corrispondenti fascicoli informatici.

I documenti analogici che continuano comunque ad arrivare all'AOO-E20910 saranno smaterializzati, protocollati ed acquisiti dal sistema documentale. L'esemplare cartaceo ricevuto, sarà altresì conservato in archivio di deposito, all'interno del quale saranno predisposte apposite cartelle, una per ogni giorno di protocollazione.

11. ABILITAZIONE DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

11.1 Generalità

Il controllo degli accessi è il processo che garantisce l'impiego dei servizi del sistema informatico di protocollo, esclusivamente secondo modalità prestabilite.

Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).

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

11.2 L'accesso al sistema

L'accesso al sistema è consentito solo ed esclusivamente tramite CMD.

L'RDS, avvalendosi di un'utenza privilegiata (amministratore di sistema), assegna agli utenti diversi livelli di autorizzazione; tali utenti, una volta identificati, sono suddivisi secondo diversi profili di accesso, sulla base delle rispettive competenze.

Deve essere considerato che una singola persona fisica può ricoprire più ruoli all'interno dell'AOO.

11.3 I profili di accesso

Nell'ambito dell'AOO-E20910, la strutturazione degli accessi prevede la realizzazione di una serie di profili, sulla base della struttura ordinativa e delle rispettive competenze, tra cui, quelli principali, 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 a poche persone, sotto il diretto controllo del RDS (elenco nominativo in allegato 3);
- Protocollazione in ingresso: funzione destinata agli operatori di protocollo in ingresso dei documenti informatici e cartacei (elenco nominativo in allegato 5);
- 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 corrispondenti: si tratta di un punto di snodo fondamentale per gestione della corrispondenza. L'accesso a tale tabella deve essere centralizzato e gestito da un ristretto gruppo di utenti, che possano garantire uniformità e coerenza ai dati immessi;
- Abilitazione alla 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 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 di visibilità. Va ricordata, a questo proposito, la funzionalità, inerente alla possibilità di accedere ai documenti che contengono dati sensibili.

- Accesso alla scrivania: anche questa funzione è abilitata a tutti gli utenti, poiché su tale funzionalità si basa lo scambio della corrispondenza e le attività gestionali dei documenti in ingresso/uscita.

L'assegnazione di un profilo è decisa dal RDS, che valuta le richieste provenienti dai responsabili delle diverse UO.

Il RDS si preoccupa di mantenere costantemente aggiornati i profili associati ai vari utenti.

12. IL REGISTRO DI EMERGENZA

12.1 Premessa

La normativa (art. 63 [DPR]) disciplina, in modo piuttosto puntuale, la materia del registro di emergenza, che è stato pensato per sopperire ad eventuali malfunzionamenti del sistema informatico.

Tuttavia è necessario sottolineare come le norme risalgono al 2000, prima comunque dell'entrata in vigore del [CAD], che impone la redazione di originali informatici.

Tale regola, infatti, muta radicalmente lo scenario in cui il registro di emergenza deve agire, rendendo, inoltre, di fatto, le funzioni di protocollazione molto meno rilevanti di quanto non lo fossero nell'impianto normativo previsto dal [DPR].

Di seguito, quindi, verranno descritte le procedure previste nei casi di non funzionamento del sistema informatico, predisposte tenendo conto di quanto detto in precedenza.

12.2 Attivazione del registro di emergenza

Ogni qualvolta non fosse possibile utilizzare il sistema informatico per un periodo significativo, il RDS adotterà il registro di emergenza riportandovi la seguente dichiarazione:

APERTURA DEL REGISTRO DI EMERGENZA

Causa dell'interruzione: _____

Data di inizio interruzione: _____ ora dell'evento: _____

Numero di protocollo iniziale: _____ pagina iniziale n. _____

Timbro e firma del Responsabile del Servizio di Protocollo (RDS)

12.3 Attività possibili durante l'attivazione del registro di emergenza

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

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

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

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

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

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

12.4 Riattivazione del sistema informatico

Quando il sistema informatico riprende il suo normale funzionamento, il RDS chiude il registro di emergenza con la seguente dichiarazione:

CHIUSURA DEL REGISTRO DI EMERGENZA

Data di fine interruzione: _____ ora dell'evento: _____

Numero di protocollo finale: _____ pagina finale n.: _____

Timbro e firma del Responsabile del Servizio di Protocollo (RDS)

Dopo la riattivazione, sia i documenti in ingresso, sia i documenti in uscita, protocollati in emergenza, verranno importati all'interno del sistema con le metodologie previste.

13. REGOLE GENERALI DI SCRITTURA DEI DATI ALL'INTERNO DEL SISTEMA INFORMATICO

In tutti i sistemi informatici è di particolare importanza la qualità delle informazioni che vengono inserite al suo interno. Ancora di più rileva tale importanza 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, semplicemente, i documenti potrebbero essere difficilmente rintracciabili o, nei casi peggiori, non rintracciabili.

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

Nomi di persona	Prima il Cognome e poi il Nome. In maiuscolo solo la prima lettera. Es.: <i>Rossi Mario</i>
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. Es.: <i>Acme srl</i>
Enti/associazioni	Lettera maiuscola solo per l'iniziale della denominazione.
Ministeri	Scritti per esteso.
Enti di secondo livello	Es.: <i>Segredifesa V Reparto</i> e <i>NON V Reparto Segredifesa</i>
Sigle di enti	Senza punti. Es.: <i>ISTAT</i>
Università	Es.: <i>Università degli studi di Roma</i>
Virgolette/apici	Utilizzare, digitandolo dalla tastiera (no copia/incolla da Word) il relativo carattere.
Date	Formato numerico separatore tratti. Es.: <i>01-01-2018</i>

ELENCO DEGLI ALLEGATI

1. Messaggio avvio del sistema di gestione flussi documentali ADHOC;
2. Atto di nomina del RDS e del Vicario;
3. Atto di nomina Amministratore e Sostituto Amministratore;
4. Organigramma dell'AOO-E20910;
5. Elenco degli addetti alle postazioni di dematerializzazione autorizzati a firmare digitalmente le acquisizioni;
6. Modulo richiesta annullamento protocollo.