MINISTERO DELLA DIFESA

STATO MAGGIORE DELLA MARINA

1° REGGIMENTO SAN MARCO

Manuale di gestione per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi nelle AOO di terra

Edizione GIUGNO 2023

MINISTERO DELLA DIFESA

STATO MAGGIORE DELLA MARINA

1° REGGIMENTO SAN MARCO

ATTO DI APPROVAZIONE

Approvo il

"MANUALE DI GESTIONE PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI DEL 1° REGGIMENTO SAN MARCO" (M1RGTSMA)

Brindisi,

IL COMANDANTE
(C.V. Ferruccio FERRELI)
(*Firmato digitalmente*)

Firmato Digitalmente da/Signed by:
FERRUCCIO FERRELI

In Data/On Date:
sabato 18 ottobre 2025 09:51:08

SOMMARIO

ELENCO DI DISTRIBUZIONE

DIRAMAZIONE INTERNA

DIRAMAZIONE ESTERNA

SEGRETARIATO GENERALE DELLA DIFESA – Referente Unico per il Protocollo Informatico della Difesa

STATO MAGGIORE DELLA MARINA – Reparto C4S - Ufficio Informatica Gestionale

REGISTRAZIONE DELLA AGGIUNTE E VARIANTI

1	
2	
3	
4	
5	
6	

ACRONIMI

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

AD	Amministrazione Difesa
AGID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
AOO – M1RGTSMA	1° Reggimento "San Marco".
[CAD]	Codice dell'Amministrazione Digitale (D.lgs. 7 marzo 2005 n. 82)
[CODBCP]	Decreto legislativo 22 gennaio 2004 n. 41
[GDPR]	Decreto legislativo 30 giugno 2003 n. 196
[DIR]	Direttiva SMD-I-004
[DPCM]	Decreto della Presidenza del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
[DPR]	DPR 30 dicembre 2000 n. 445
D.lgs.	Decreto legislativo
INCC	Informazioni non classificate controllate
IPA	Indice delle Pubbliche Amministrazioni
l.	Legge
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
RDC	Responsabile della Conservazione Sostitutiva interno all'AOO.
RPA	Responsabile del Procedimento Amministrativo
UO	Unità Organizzativa
UOR	Unità Organizzativa Responsabile (del Protocollo Informatico)
LG	Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici. Ed. Maggio '21.

RIFERIMENTI NORMATIVI

La normativa inerente al Protocollo Informatico è piuttosto vasta. Di seguito viene riportato un elenco degli atti normativi di maggior rilevanza a cui si farà riferimento all'interno del testo. I riferimenti normativi sono da intendersi comprensivi delle varianti, aggiunte e correzioni nel frattempo intervenute sul provvedimento stesso.
In Marina è il Servizio Documentale Navale che gestisce il processo di gestione archiviazione e conservazione dei documenti informatici dei Comandi/Enti della F.A. individuati come Aree Organizzative Omogenee (AOO). Il Servizio Documentale Navale è tutt'ora regolato internamente dal SUPPLEMENTO alla SMM 18- UEU ed. 2012 – "*Norme particolari per la corrispondenza d'ufficio con l'impiego del Sistema Documentale*".

Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 [DPR]

"Disposizioni legislative in materia di documentazione amministrativa" (T.U.D.A.). Il DPR è il documento di riferimento principale per il PI. Con esso si effettua una razionalizzazione della normativa inerente al PI che viene semplificata e raggruppata negli articoli da 50 a 70. All'art. 77 viene abrogato il DPR 428/98, mentre all'art. 78 co. 1 lett. f viene, comunque, mantenuto in vigore il DPCM 31ottobre 2000.

Ex Decreto Legislativo 30 giugno 2003, n. 196 "*General Data Protection Regulation*" [GDPR]

Il regolamento UE 679/2016 (c.d. GDPR), è il codice relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

Decreto Legislativo 22 gennaio 2004, n.41 [CODBCP]

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

Direttiva SMD-I-004 Ed. 2004 [DIR]

Pubblicazione edita dallo Stato Maggiore della Difesa: "Il protocollo informatico nella Difesa".

Decreto legislativo 7 marzo 2005, n.82 [CAD]

"Codice dell'Amministrazione digitale".

Decreto del Presidente della Repubblica 11 febbraio 2005, n.68

"Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della L. 16 gennaio 2003, n. 3".

Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici. Ed. Maggio 2021 [LG]

Entrate in vigore 1 gennaio 2022 le [LG] aggiornano le attuali regole tecniche concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici, come previsto dall'articolo 71 del CAD[1] incorporano in un unico documento le regole tecniche e le circolari in materia, addivenendo ad un "unicum" normativo che disciplini gli ambiti sopracitati, nel rispetto della disciplina in materia di Beni culturali.

Variante 1 alla "Direttiva sulla gestione delle *Informazioni Non Classificate Controllate*" emanata da Marina OCS in data 2 agosto 2017

[1] L'art. 71, comma 1, del CAD prevede che "L'AGID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice".

Direttiva riguardante la trattazione delle I.N.C.C. nel settore C.I.S. (*Communication and Information System*), ossia su reti informatiche attraverso l'impiego del sistema documentale e di posta elettronica, e che indica al paragrafo 5 in particolare modalità di gestione di detta documentazione all'interno del Sistema Documentale.

GLOSSARIO

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

Amministrazioni Pubbliche

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

Archivio

L'archivio è la raccolta ordinata e sistematica degli atti e dei documenti ricevuti o comunque formati dall'AOO 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 quale si riferiscono (cd. Vincolo archivistico). Essi sono ordinati e archiviati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico.

Archiviazione elettronica

È il processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici univocamente identificati mediante un codice di riferimento.

Area Organizzativa Omogenea (AOO)

Una AOO (art. 50 co. 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 Protocollo. Dove, in precedenza, potevano esistere una serie di registri di protocollo, suddivisi per i diversi Reparti / Uffici, 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 per protocollare i propri atti, con ricadute sugli aspetti pratici, funzionali e logistici (art. 3 co. 1 lett. d del [DPCM]). In pratica la costituzione di una AOO comporta la chiusura dei vari Uffici di Protocollo intermedi esistenti prima dell'entrata in funzione del PI. Successivamente all'atto di costituzione di una AOO le vengono assegnati 3 codici identificativi: il *codice IPA* che identifica l'amministrazione, il *codice interno dell'AOO* che identifica l'AOO all'interno della Amministrazione di appartenenza ed infine il *codice univoco AOO*, un codice alfanumerico che identifica l'AOO a livello nazionale ed è pubblicato sul portale IPA.

Documento informatico

Il documento elettronico contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (Codice della Amministrazione Digitale - art. 1 lett. p). Per documento informatico si intende qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.

Documento analogico

È la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti (Codice dell'Amministrazione Digitale art. 1 lett. p-bis).

Fascicolazione

La fascicolazione è l'operazione di associazione logica di un documento informatico ad una aggregazione documentale informatica chiamata "fascicolo".

Fascicolo

Il fascicolo è l'insieme ordinato di documenti, che possono fare riferimento ad uno stesso affare / procedimento / processo amministrativo, o ad una stessa materia, o ad una stessa tipologia di documenti; si forma nel corso delle attività amministrative, allo scopo di riunire, a fini decisionali o informativi, tutti i documenti utili allo svolgimento di tali attività. Esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti.

Il Manuale di Gestione

Ai sensi del paragrafo 3.5 delle [LG], il Manuale di gestione documentale descrive il Sistema di gestione informatica dei documenti e fornisce le istruzioni per la corretta conduzione del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi all'interno della AOO. 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. Esso deve essere predisposto dal RDS rispettando le specificità della rispettiva AOO e costituisce lo strumento che garantisce l'esclusiva adozione ed applicazione delle procedure indicate al suo interno.

Informazioni di Identificazione Personale (ex dati sensibili)

L'articolo 9 del [GDPR] sancisce un generale divieto di trattare dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute (anche la semplice ferita ad una mano) o alla vita sessuale o all'orientamento sessuale della persona. All'interno del josh© ogni qualvolta viene formato un documento, contenente dati soggetti a trattamento speciale, esso deve essere categorizzato come "documento privato" e opportunamente evidenziato (procedura al paragrafo 2.4).

La Posta Elettronica Istituzionale (PEI)

La casella P.E.I. viene assegnata in Marina a ciascun Ente/AOO, è un servizio della Forza Armata che consente l'invio e la ricezione di messaggi di posta elettronica utilizzando la piattaforma del servizio posta elettronica non classificata e costituisce un mezzo attraverso il quale possono essere ricevuti messaggi da protocollare.

La Posta Elettronica Certificata (PEC)

La PEC fornisce un servizio di messaggistica che sfrutta gli standard propri del servizio di 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 anche altre funzionalità che garantiscono al fruitore integrità, tracciabilità e storicizzazione del messaggio. La PEC delle PPAA è strettamente connessa all'IPA ove sono pubblicati gli indirizzi di posta elettronica certificata associati alle AOO oltre a tutte le informazioni di sintesi relative agli Enti. 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 del destinatario e certifica la data e l'ora dell'evento.

Il dominio di PEC per la Difesa è: @postacert.difesa.it.

Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi (RDS) ed il Vicario

a. Il RDS è l'altra novità di rilievo introdotta dalla normativa. I suoi compiti, ai sensi della normativa vigente, non sono invero meramente burocratici, ma hanno, principalmente, una valenza di tipo legale. Infatti, il RDS garantisce il corretto funzionamento, a norma di legge, del sistema di PI implementato nell'AOO, anche nei confronti dei cittadini, delle ditte, e delle altre Pubbliche Amministrazioni.
b. Il "Capo Servizio per la tenuta del protocollo informatico" si identifica nella figura del RDS e viene nominato dal proprio Titolare dell'Ente con atto formale **(Allegato A)**, in sua vece, interviene il "Vice Capo Servizio per la tenuta del protocollo informatico" che si identifica nella figura del Vicario. In caso di assenza di entrambe le figure dovrà essere redatto un Ordine di Servizio con il quale il Titolare della AOO nomina provvisoriamente un RDS

Sistema di protocollo informatico e gestione documentale della Marina

La Marina Militare Italiana utilizza la piattaforma "josh©" e tutti suoi applicativi, per i quali la Ditta proprietaria, IT Consult Srl, fornisce l'assistenza sistemistica e applicativa. Gli applicativi attualmente installati *lato client* dalla Marina sono i seguenti: josh Infosign©, josh Infojam© e josh Scanner©, che interagiscono con le applicazioni *lato server* josh© e josh Protocol©.

Task

Il termine indica, all'interno del sistema josh© una "attività informatica" che consente all'operatore di effettuare alcuni tipi di operazione sul documento ad esso associato.

Titolario e relativa classificazione d'archivio

L'Amministrazione Difesa ha redatto un modello di classificazione d'archivio per la documentazione, denominato "Titolario", tale modello è distribuito dallo Stato Maggiore Marina a tutte le AOO, con il divieto di modificarlo. Il Titolario d'archivio è uno schema generale di voci logiche rispondenti alle esigenze funzionali dell'Amministrazione Difesa ed 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 indicatore di classificazione inserito in una struttura di voci (piano di classificazione).

Unità Organizzativa (UO)

Per UO s'intende uno dei sottoinsiemi di una AOO, cioè un complesso di risorse umane e strumentali a cui sono state affidate competenze omogenee per la trattazione dei documenti o dei procedimenti amministrativi.

CAPITOLO 1

PRINCIPI GENERALI

1.1. Premessa

In linea con la normativa vigente, l'Amministrazione adotta il Manuale di Gestione, disciplinato al paragrafo 3.5 delle [LG].
In questo ambito, l'Amministrazione individua i confini delle proprie AOO, all'interno delle quali è previsto che debba essere nominato un Responsabile del Servizio per la tenuta del protocollo informatico della gestione dei flussi documentali e degli archivi.
Il Manuale è rivolto, pertanto, a tutti coloro i quali utilizzano il protocollo informatico come strumento di lavoro per la gestione dei documenti e dei procedimenti amministrativi che sono chiamati a trattare e dei quali sono individuati come responsabili. Esso descrive gli aspetti operativi e funzionali del Sistema per la gestione del protocollo informatico, dei flussi documentali e degli archivi.
Questo Manuale, che ne descrive i principi di funzionamento rappresenta, quindi, un elemento essenziale per la comprensione delle logiche organizzative e funzionali preposte alla gestione documentale dell'**AOO-M1RGTSMA**. Per sua natura il contenuto del presente manuale viene certificato dal RDS ogni anno e comunque aggiornato a fronte di varianti normative eventualmente entrate in vigore.

1.2. Ambito di applicazione del Manuale di Gestione

Il presente manuale si applica ai processi di gestione del protocollo informatico, dei flussi documentali e degli archivi, legati ai procedimenti amministrativi di competenza del **1° Reggimento San Marco**.

1.3. Area Organizzativa Omogenea del 1° Reggimento "San Marco"

Il presente Manuale afferisce all'AOO del 1° Reggimento San Marco, composta dall'insieme delle Unità Organizzative articolate come riportato in **Allegato B**. All'atto della creazione della AOO le vengono assegnati 3 codici identificativi: il *codice IPA* che identifica l'amministrazione [M_D], il *codice interno dell'AOO* [**M1RGTSMA**][2] ed il *codice univoco AOO* riportato sul portale IPA [**AA7FFC3**], a titolo informativo, si fa presente che da qui in poi ogni riferimento del presente manuale al "codice AOO" sarà fatto intendendo il "codice interno dell'AOO".

1.4. 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, supportato dal Sistema Informatico denominato "josh©" che consente la gestione del protocollo informatico non classificato della FA, in accordo con la normativa vigente. A capo di tale Servizio è preposto un Responsabile del Servizio, "*il quale deve essere un dirigente o funzionario, dovranno essere indicati per tale ruolo Ufficiali con il grado minimo di Capitano (o equivalente) oppure, in alternativa dipendenti civili almeno della categoria C1*"[3]. L'atto di nomina del Responsabile del Servizio e del suo Vicario è riportato in **allegato A**.

1.5. Firma Digitale della documentazione afferenti all'AOO

Premesso che, in armonia con le attuali disposizioni di legge in materia, la Firma Digitale identifica univocamente il firmatario di un documento, e se associata ad una Marca Temporale, si ottiene anche un riferimento temporale legalmente opponibile a terzi, all'interno della AOO l'applicazione della firma digitale è prevista per i casi sottoelencati:

- Trasmissione della documentazione al di fuori dell'AOO;
- Dematerializzazione di documenti originali cartacei in ingresso/uscita ai fini della protocollazione;

[2] Il Codice Interno AOO è assegnato e comunicato a ciascuna AOO dall'Organismo sovraordinato (SMD, SGD, SME, SMM e SMA e Carabinieri), in accordo con la vigente normativa.
[3] Le norme citate sono la direttiva SMD-I-004 e l'art. 61 comma 2 del [DPR].

- Corretto funzionamento di alcuni processi interni del Sistema.

1.6. Tutela dei dati personali

I dati per i quali, ai sensi del [GDPR], è necessaria una specifica gestione sono trattati in conformità al citato decreto, attraverso l'apposizione di un *flag* nell'apposito spazio previsto dal Sistema per i *dati sensibili* (cfr. voce di Glossario e successivo paragrafo 2.4).

CAPITOLO 2

LA GESTIONE DEI DOCUMENTI

2.1. Generalità

In Marina l'automatizzazione della gestione dei documenti e del protocollo informatico avviene tramite la piattaforma "josh".
I documenti, analogici e informatici, vengono gestiti in relazione al loro formato e sono suddivisi, in dipendenza del flusso, nel seguente modo:
- in ingresso;
- in uscita;

2.2. Erogazione del servizio di protocollazione

Ai fini della mera protocollazione/registrazione va tenuto presente che i documenti in ingresso, informatici ed analogici, **vengono protocollati dal lunedì al sabato, per tutta la giornata lavorativa, fino al "cessa lavori".**

2.3. Documenti esclusi dalla protocollazione

Il sistema informatico di protocollo è progettato per trattare esclusivamente documenti ***non classificati***.

La posta classificata erroneamente pervenuta alla Segreteria Comando, che detiene la tenuta del servizio di protocollo, dovrà essere consegnata al PCN.

Sono oggetto di protocollazione tutti gli atti amministrativi inerenti all'attività dell'AOO. Sono esclusi dalla registrazione nel protocollo informatico i documenti ricevuti/spediti tramite il servizio di *Message Handling*, quelli elencati nell'art. 53 co. 5 del [DPR] e comunque quelli elencati qui sotto:

- gazzette ufficiali;
- bollettini ufficiali e notiziari della pubblica amministrazione;
- le note di ricezione delle circolari e altre disposizioni;
- materiali statistici;
- gli atti preparatori interni;
- giornali, riviste e/o libri;
- materiali pubblicitari;
- inviti a manifestazioni che non attivino procedimenti amministrativi;
- tutti i documenti già soggetti a registrazione particolare dell'Amministrazione, quali i documenti soggetti a classifica di sicurezza nazionale;
- fogli di viaggio;
- note caratteristiche;
- rapporti informativi;
- registro delle presenze;
- modelli 730;
- licenze permessi;
- esposti anonimi.

2.4. Gestione di documenti contenenti dati sensibili ed equiparati

Per talune tipologie di documenti è richiesta una gestione differente da quella ordinaria. In primo luogo, si rappresenta che rientrano tra tali documenti quelli appartenenti alle seguenti tipologie:

- documenti contenenti dati sensibili e dati personali di cui al GDPR;
- documenti di carattere e di indirizzo politico che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa.

All'interno del Sistema Documentale è garantita l'esclusiva visione e gestione dei documenti solamente a chi ha i diritti per farlo, ai sensi della normativa vigente, ed è fatto obbligo, pertanto, a tali utenti di cliccare ("*flaggare*"), nella fase di predisposizione del protocollo, nell'apposito campo "documento privato", affinché venga messa in evidenza la peculiarità dei documenti trattati. Così facendo quei documenti saranno visibili all'interno del sistema solo dalla catena di assegnazione del documento stesso (oltre che dai responsabili privacy).

Nell'approcciarsi alla trattazione dei documenti succitati è bene tenere presente i seguenti suggerimenti:

- i responsabili privacy devono essere condivisi con il RDS prima di emettere l'OdG, che si preoccuperà di proporre personale adeguato prendendo in considerazione la peculiarità dell'incarico; deve inoltre essere valutato l'aspetto riguardante il numero degli utenti che si devono/possono eleggere come "responsabili privacy" perché, sebbene *flaggare* un documento come privato significhi limitarne la visibilità, questo particolare permesso consente la visibilità di tutti i documenti soggetti a privacy.
- il protocollista che *flagga* il documento come "privato" deve porre attenzione all'assegnazione: il documento *flaggato* deve essere assegnato ad un solo operatore[4] perché assegnandolo al singolo anziché alla UO destinataria del documento, significa dargli la possibilità di vederne l'anteprima (ai fini dell'eventuale successivo smistamento) limitando allo stesso tempo la visibilità degli altri membri della UO.

2.5. Formazione dei documenti informatici

Il documento informatico deve essere formato nelle modalità previste ai punti a), b), c) e d) dell'art. 2.1.1 delle [LG]. Dovranno, altresì, essere garantite immodificabilità e integrità attraverso l'utilizzo della firma digitale, la memorizzazione nelle banche dati del Sistema Documentale adottato e il versamento nei sistemi di conservazione. Il documento, per essere trasmesso, prima dell'apposizione della firma digitale, dovrà essere trasformato nel formato standard PDF/A, profilo particolarmente adatto alla creazione di documenti per i quali deve essere garantita la leggibilità in caso di archiviazione e conservazione a lungo termine.

[4] Ad esempio un membro della segreteria della UO destinataria.

2.6. Trasmissione e ricezione dei documenti informatici

Le comunicazioni tra PPAA avvengono obbligatoriamente tramite PEC in armonia con la normativa vigente.

Il Gestore del Servizio PEC per la MM è INFOCERT, su tale cassetta non si può ricevere posta ordinaria e questa opzione non è configurabile dagli utenti utilizzatori e non deve essere configurata dagli Amministratori.

2.7. La gestione del documento informatico in entrata

Per la ricezione di documenti informatici l'AOO dispone di una casella di posta elettronica istituzionale e di una casella di posta elettronica certificata:

- PEI: **rgtsanmarco1@marina.difesa.it**;
- PEC: **rgtsanmarco1@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, in ingresso le comunicazioni informatiche indirizzate **all'AOO M1RGTSMA**, dovranno osservare le seguenti regole generali:

- il formato preferibilmente accettato per file allegati ai messaggi di posta elettronica, è il PDF e PDF/A;
- sono accettati tutti i formati riconosciuti dalla normativa (Allegato 2 delle LG) e i file allegati al documento primario possono essere compressi nei formati ZIP o RAR;
- l'oggetto della mail con cui viene inviato il documento non deve ragionevolmente superare i 255 caratteri;
- la dimensione massima complessiva della corrispondenza in ingresso comprensiva degli allegati in entrata, tramite PEC, non deve superare i 100 MB ovvero 9 MB tramite PEI;
- qualora si abbia la necessità di far registrare a protocollo un documento informatico pervenuto da un mittente esterno all'AOO ad una casella di posta elettronica ordinaria interna ad una UO (Posta Elettronica Funzionale (PEF) della UO o posta personale di un membro della UO), è raccomandabile richiedere un reinvio sui canali ufficiali dell'AOO (PEI o PEC).
- i documenti pervenuti devono essere sempre trattati ad eccezione di quelli appartenenti alla tipologia trattata al precedente paragrafo 2.3;
- nel caso di contenuti "sospetti" (ad es. presenza di allegati eseguibili o di link che possono rimandare a file eseguibili di programmi veicolanti virus), si avvisa il RDS e si attendono disposizioni in merito all'eventuale eliminazione (l'RDS deve segnalare il caso a chi di competenza, ad es. Ufficio informatica, PCN ecc.).
- i documenti pervenuti, privi anche solo di uno degli allegati citati nella lettera di accompagnamento, si trattano come descritto al successivo paragrafo 2.8 (punto "a").
- nel caso uno o più documenti informatici vengano consegnati su supporto informatico e si decida che devono essere registrati a protocollo, si deve procedere alla "*protocollazione web*" (cfr. Manuale di Sistema).

2.8. Flusso in ingresso tramite PEI/PEC

I messaggi inviati alle caselle di posta elettronica istituzionale o certificata vengono inseriti in un'apposita coda. Il protocollista, in dipendenza delle abilitazioni a lui concesse, accede alla predetta coda di messaggi. I messaggi possono essere visualizzati dall'operatore in ordine di arrivo all'AOO. Se la protocollazione di un messaggio non viene completata, quel messaggio potrà essere trattato da un altro operatore che accede alla medesima coda di messaggi. L'operatore, quindi, procede alla protocollazione del messaggio, provvedendo ad una pre-decretazione verso l'UO competente, in seguito il messaggio segue un flusso interno che può passare da varie assegnazioni (processi di smistamento) fino alla presa in carico dell'utente finale. Quando il messaggio è palesemente non di competenza dell'AOO, con contenuti illeggibili (ad es. file allegati corrotti) o negli altri casi dubbi, il protocollista agirà con le seguenti modalità:

a) Sposta la mail nel contenitore delle "email elaborate" del mail manager, con lo stato "*documenti da non protocollare*" con una nota esplicativa (per futura memoria). La mail non ancora protocollata dovrà essere re inoltrata al mittente (senza protocollo) con l'apposita funzione ed eventuali note esplicative[5].
b) Nel caso, invece, fosse stata già protocollata in arrivo, verrà restituita al mittente dal protocollista, tramite la funzione "Protocollazione email in uscita". Il protocollista "collegherà" con un'altra funzione apposita[6] i due protocolli in questione, in ingresso e in uscita.

Le mail ricevute che rientrano nella categoria del cosiddetto "SPAM", vengono scartate direttamente dalla cassetta Exchange che le sposta all'interno della casella "posta indesiderata". È consigliabile che il Responsabile si preoccupi quotidianamente di verificare la presenza di eventuali mail che possano voler essere protocollate all'interno della casella di "posta indesiderata" del Gestore (Infocert/Exchange MM); nell'eventualità che si decida di protocollare un messaggio, si può effettuare "manualmente" lo spostamento dello stesso nella casella "posta in arrivo" e di conseguenza consentire le operazioni di protocollazione come di consueto.

2.9. Modalità di assegnazione dei documenti ricevuti

I documenti ricevuti vengono, in fase di protocollazione, dirottati (decretati o pre-assegnati) verso delle "macro aree" di smistamento dove la "pre-assegnazione", può essere confermata o perfezionata.

Se a una UO viene assegnato un documento non di competenza:

- **nel caso il responsabile della UO abbia chiaro chi è l'assegnatario, può direttamente effettuare lo smistamento;**
- **nel caso il responsabile della UO NON abbia chiaro a chi assegnare, può restituirlo al mittente e, così, a ritroso, fino a tornare alla segreteria che ha protocollato in origine il documento in ingresso, che provvede ad una nuova decretazione;**
- **in casi estremamente particolari, non contemplati nei precedenti, interviene RDS.**

2.10. Flusso in uscita del documento informatico

La trasmissione della documentazione deve essere effettuata utilizzando gli strumenti dell'applicativo josh e possono essere impiegati i canali PEI o PEC. In merito, premesso che il metodo più consono per le comunicazioni tra PPAA è quello che prevede l'utilizzo della PEC e che, comunque, la modalità di trasmissione-ricezione deve essere PEC *to* PEC (o alternativamente PEI *to* PEI), è necessario evidenziare il caso particolare della comunicazione tra Pubblica Amministrazione e Soggetti Terzi. Laddove il destinatario non sia una PA e non abbia una casella di PEC attiva, si può provvedere in due modi:

- inviare una PEI (se il destinatario ha comunicato l'indirizzo e se non è necessario avere una ricevuta di avvenuto recapito - es: destinatari per conoscenza o trasmissione di documenti puramente informativi);
- materializzare la documentazione informatica ed inviare una Raccomandata A/R (modalità trattata più avanti assieme alle "fasi del processo di approvazione").

Di tutti gli utenti, all'interno di un'AOO, che hanno accesso al Sistema Documentale **il Titolare dell'AOO** delega i Dirigenti e/o i Funzionari alla firma di documentazione amministrativa e tecnica, secondo le

[5] Ad oggi il "tasto" inoltra è disponibile solo sulle UUNN, pertanto la mail può essere reinoltrata al mittente soltanto via Outlook o web mail.
[6] Il protocollista utilizza l'apposita funzione che si trova nel corredo dei dati di protocollo durante la registrazione.

attribuzioni relative alla posizione organica ricoperta. Tale delega si concretizza con l'apposita configurazione sul profilo dell'interessato di un "Timbro".[7]

Tutti i documenti principali che vengono protocollati in uscita all'interno del Sistema vengono firmati previa trasformazione nel formato PDF/A (si effettua mediante l'utilizzo della busta crittografica PAdES). Gli allegati che per loro natura (o per il loro utilizzo) non possono o non devono essere convertiti in tale formato sono conservati nel loro formato originale.

Il flusso dei documenti in uscita prevede, con l'ausilio dello strumento informatico, l'esecuzione di alcune azioni che, nel loro insieme, sono denominate "Processo di Approvazione". Esse si articolano nelle seguenti fasi[8]:

1. **Elaborazione** del documento da parte dell'operatore: composizione e caricamento della lettera di trasmissione[9] e degli eventuali allegati, previa compilazione di tutti i metadati a corredo.
2. **Approvazione**[10], con eventuale *coordinamento*, da parte degli utenti della catena gerarchica sovraordinata a chi ha preparato il documento. Le fasi di approvazione prevedono la possibilità di restituzione del documento verso l'approvatore precedente fino al redattore ed in tutte queste fasi il documento può essere ancora modificato.
3. **Firma** (singola o massiva) del titolare del procedimento amministrativo o suo delegato;
4. **Registrazione** del protocollo come da normativa vigente (LG AgID);
5. **Apposizione del Sigillo Elettronico** come da normativa vigente (LG AgID);
6. **Spedizione**:
   a. Per posta elettronica;
   b. Per posta ordinaria (*task* di "Spedizione Documenti");
7. **Riconciliazione** di eventuali ricevute PEC.

L'andamento del flusso di un particolare documento può essere monitorato, in ogni fase, da ciascun utente che abbia preso parte all'iter del Processo di Approvazione.
In caso di spedizione via PEC di un documento, le relative ricevute di accettazione e consegna prodotte sono automaticamente ricongiunte al documento spedito, all'interno del Registro di Protocollo.
In particolare:

- **la ricevuta di accettazione** attesta la data e l'ora in cui il server PEC del mittente, dopo un controllo formale, accetta il messaggio e lo spedisce al server PEC del destinatario;
- **la ricevuta di consegna** attesta il giorno e l'ora in cui il messaggio viene recapitato nella casella di PEC del destinatario.

Se si verifica una delle seguenti situazioni:

- ✓ presenza di un destinatario privo di una qualsiasi casella di posta elettronica;
- ✓ documento primario a cui è associato un allegato analogico non dematerializzabile;
- ✓ documento primario a cui è associato un allegato informatico che, per caratteristiche proprie, non può essere inviato per via telematica, come ad esempio, un documento informatico la cui dimensione sia eccessiva e non gestibile dai servizi di posta elettronica;

procedere nel seguente modo: durante la fase di predisposizione del documento, al momento della selezione del destinatario, dovrà essere optata la modalità di invio di tipo "altro". In questo caso, la fase di "Spedizione" sarà di tipo 6.b, ovvero, il Sistema predisporrà il documento per la "spedizione per posta ordinaria". La lettera di trasmissione, registrata a protocollo (ma non inviata per posta elettronica), deve essere stampata, si deve

[7] E' prerogativa dell'RDS disporre la configurazione del timbro affinché sia successivamente effettuata da un Gestore tecnico dell'AOO.
[8] Gli step 4, 5, 6.a e 7 sono automatismi dell'applicazione.
[9] Sulla base dei modelli disponibili all'interno dell'applicazione.
[10] Le eventuali note di approvazione o coordinamento rimangono tracciate nel sistema.

apporre un'attestazione che è copia del documento originale[11] conservato nel sistema documentale, e inserita nel plico insieme agli allegati, pronta per essere spedita, tramite **l'Ufficio Postale della Brigata Marina San Marco**, tramite raccomandata A/R. A tale scopo, si suggerisce di apporre, sul retro della lettera (documento principale), la seguente frase:

> *Si attesta che il presente documento è copia del documento informatico originale firmato digitalmente composto complessivamente da n. ___ pagine. L'originale citato è disponibile presso l'archivio del **1° Reggimento San Marco** previa richiesta ufficiale di accesso agli atti.*
>
> ***Brindisi il, xx xx xxxx*** *FIRMA*

In questo caso il flusso informatico si conclude al completamento della Attività (task "Spedizione Documenti").

Al fine di inviare correttamente un documento informatico è necessario attenersi ad alcune regole relative alla preparazione del file che deve essere allegato in fase di predisposizione:

- utilizzare il modello nel formato ".DOCX" predisposto per tale scopo e scaricabile tramite la procedura SW (il facsimile è disponibile in **allegato C**). Il sistema provvederà in automatico alla successiva conversione in formato PDF/A prima della firma del documento;
- nella denominazione dei file non si devono utilizzare caratteri speciali e/o lettere accentate (°,',^, ') o punti (.); si suggerisce, eventualmente, di utilizzare il carattere _ (*underscore*) al posto di tali caratteri;
- nel fissare il nome del file è buona norma non superare i 64 caratteri.

Se uno o più allegati al documento necessitano anch'essi di firma digitale, questa andrà apposta all'esterno della procedura SW, tramite le applicazioni messe a disposizione dalla M.M. (Kit Firma o josh InfoSign).
Eventuali allegati saranno, pertanto, caricati nella procedura (fase di predisposizione) già firmati digitalmente.

2.11. La gestione del documento informatico interno

Per documenti informatici interni si intendono quelli scambiati tra le diverse UO afferenti alla medesima AOO. In tutti quei casi, quindi, nei quali tra gli indirizzi dei destinatari a cui inviare della documentazione, per competenza o per conoscenza, vi sia una UO interna all'AOO, il sistema informatico provvederà ad inviare quel documento sulla scrivania virtuale del responsabile competente dell'UO destinataria. In questo caso non viene inviata una mail, bensì viene generato un task di tipo "Estensione di copia in uscita" indirizzato al responsabile della UO, che potrà gestirlo prendendolo in carico o smistandolo a un subalterno.

2.12. *Trattazione di procedimenti in coordinamento tra varie UO interne*

La trattazione di procedimenti in coordinamento nel Sistema avviene puntualmente tra soggetti: il soggetto che predispone il documento e avvia il processo di approvazione provvede, prima di passare il documento in approvazione al superiore gerarchico, ad inviare tramite il pulsante "coordinamento" la documentazione in visione al soggetto a cui si chiede un parere di coordinamento, il quale potrà inserire note di coordinamento e/o aggiungere documenti di coordinamento (ma non modificare la documentazione che viene spedita), al termine, può far proseguire il documento verso un'ulteriore UO coinvolta o restituirlo; il Sistema prevede che la procedura corretta di restituzione sia fatta a ritroso *step by step* fino alla UO pilota che, raccogliendo tutti i commenti e/o note, produrrà il documento finale per la firma del Dirigente preposto all'inoltro.

---

[11] Ai sensi dell'Art. 23 del C.A.D. Comma 1: "*Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato*". Comma 2: "*Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico*".

2.13. *La "minuta" per i documenti informatici*

Prima dell'uso del protocollo informatico, la minuta dei documenti prodotti dal **1° Reggimento San Marco** veniva firmata e custodita agli atti. Adesso il documento che parte viene duplicato ed il concetto di minuta perde di significato.
Pertanto, la tradizionale minuta è di fatto sostituita dal documento che rimane all'interno del sistema archiviata.

2.14. Corrispondenza elettronica ricevuta con il sistema di "Message Handling"

Tutta la messaggistica non classificata ricevuta/in uscita attraverso l'apposita postazione MCCIS di Message Handling, non viene e non deve essere trattata dal Sistema Documentale.

2.15. La Gestione del documento analogico

In prima istanza, si sottolinea che al flusso di documentazione analogica deve essere preferito il flusso elettronico con Posta Elettronica Certificata (PEC) o Posta Elettronica Istituzionale (PEI), ove attuabile, in virtù dell'implementazione del Protocollo Informatico nella PA. Ciò premesso, l'indirizzo preposto alla ricezione della documentazione analogica inerente all'attività dell'AOO è:

1° Reggimento San Marco
Via Provinciale per San Vito dei Normanni 47
72100 Brindisi

2.15.1. Flusso in ingresso analogico

La corrispondenza analogica in arrivo viene acquisita dalle AOO a **mezzo posta convenzionale esclusivamente previo consegna da parte del personale dell'Ufficio Posatale della Brigata al personale della Segreteria Comando dell'AOO.**

2.15.2. Le raccomandate /assicurate

La corrispondenza ricevuta con posta raccomandata/assicurata viene recapitata dal personale (Procaccia) dell'Ufficio Postale della Brigata Marina San Marco presso la Segreteria Comando del 1°Reggimento San Marco due volte a settimana (ritiro mercoledì e consegna giovedì). Il personale della Segreteria Comando prende in carico la posta unitamente ad una copia della distinta, che verrà controfirmata dal personale addetto del Protocollo Informatico, previa verifica di rispondenza con quanto consegnato. Il contenuto delle buste giunte a mezzo raccomandata / assicurata sarà scansionato nella sua totalità, se il documento è nei formati previsti per la scansione, protocollato e smistato alla UO competente alla trattazione. Se non fosse possibile procedere alla dematerializzazione della corrispondenza pervenuta, sarà scansionata solo la lettera di trasmissione ai fini dell'apposizione del protocollo e successivamente verrà consegnata l'intera documentazione in formato cartaceo alla UO competente. E' opportuno che la cartolina A/R restituita a seguito di una spedizione (di ritorno) venga scansionata ed annessa al protocollo; in caso invece di ricezione della corrispondenza A/R, la firma analogica sulla cartolina A/R viene apposta dall'Ufficio Postale. Se tra le raccomandate vi fossero documenti indirizzati direttamente agli appartenenti ai Reparti /Uffici dell'AOO, tali raccomandate non saranno aperte, ma verranno ritirate dagli addetti delle varie UO preposti al ritiro della corrispondenza analogica presso [nome dell'UO Responsabile della tenuta del PI], per la successiva consegna al destinatario o, se questi non fosse presente, al capo della segreteria dell'UO dove il destinatario presta servizio.

2.15.3. Buste chiuse contenenti particolari tipologie di documentazione amministrativa

Tutte le buste chiuse indirizzate all'AOO saranno aperte, fatta eccezione per i casi in cui siano riportate chiaramente diciture e/o scritte che consentano visivamente di ricondurle a specifiche fattispecie, quali ad esempio procedure di gara e/o contratti coperti da segreto, documenti classificati, etc.. Per quanto riguarda le procedure di gara, il personale addetto al Servizio di protocollo informatico provvederà alla consegna del plico chiuso e sigillato ad un responsabile della UO competente al ritiro. Per ciò che attiene, invece, alla documentazione classificata, il personale addetto al Servizio di protocollo informatico provvederà alla consegna dell'incartamento presso il PCN per la successiva apertura e trattazione a cura del personale preposto.

2.15.4. La posta ordinaria

Il ritiro della posta ordinaria avviene, sempre con cadenza bisettimanale, a cura del Servizio Procaccia della Brigata marina San Marco. Tale tipologia di corrispondenza non è accompagnata da distinta di dettaglio. Il personale addetto al Servizio di protocollo informatico provvederà alla successiva apertura e protocollazione tramite scansione del documento.
L'eventuale corrispondenza ordinaria diretta al personale dell'AOO non sarà aperta e verrà inoltrata all'UO di competenza, priva di protocollo, per la consegna all'interessato.

2.15.5. La protocollazione dei documenti analogici

L'attività di protocollazione dei documenti analogici inizia con la generazione del codice a barre tramite josh scanner, che richiede l'inserimento di "Mittente" e "Oggetto", seguita dall'apposizione dell'etichetta sul documento originale, sulla quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:
- **codice identificativo dell'amministrazione;**
- **codice identificativo dell'AOO;**
- **codice identificativo del Registro dell'anno in corso;**
- **data e numero di protocollo del documento.**

L'operazione di acquisizione dell'immagine dei documenti cartacei viene effettuata solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche l'etichetta/*barcode* sul documento.
Al termine di queste azioni il protocollista deve perfezionare la registrazione inserendo i metadati di seguito elencati:
- **Titolario (obbligatorio);**
- **Fascicolo (opzionale);**
- **Assegnatario principale (obbligatorio);**
- **Assegnatari per competenza e conoscenza (opzionali);**
- **Protocollo mittente (opzionale);**
- **Data protocollo mittente (opzionale).**

Al documento analogico principale possono essere associati allegati analogici i quali vengono inseriti nella fase di scansione del documento. Possono, altresì, essere associati al documento primario allegati su supporto ottico (CD ovvero DVD) ovvero su memoria con connessione USB, i quali vengono annessi al documento principale scansionato e protocollato ed inviati all'UO di competenza.

Al termine della scansione, se la qualità della scansione è valida e i dati sopra elencati sono stati inseriti, il documento viene firmato digitalmente dall'operatore, protocollato in ingresso e smistato all'UO di competenza. Si evidenzia che tutti gli addetti al servizio per la tenuta del protocollo informatico sono abilitati all'apposizione della propria firma digitale sui documenti scansionati.

In merito alla tematica trattata, nei casi in cui un documento analogico debba essere trasferito all'interno del Sistema Documentale, si evidenzia che: in accordo con le disposizioni dell'Art. 23ter, comma 3, del C.A.D.[12], laddove si presentasse la necessità giuridica di avere una "copia conforme all'originale", i Titolari delle AOO di F.A. sono tenuti ad emanare apposito OdG per la nomina di personale delegato a certificare la conformità dei documenti scansionati.

[12] Art. 23ter comma 3 del CAD: " *Le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle ((Linee guida)); in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico*".

2.15.6. Flusso in uscita analogico

Come già segnalato in precedenza, nell'ambito dell'AOO vengono prodotti di massima documenti originali in modalità informatica. Tuttavia, come già ampiamente indicato nei paragrafi precedenti inerenti al flusso in uscita dei documenti informatici, può essere necessario procedere alla trasmissione attraverso il servizio postale tradizionale di uno o più documenti. Le procedure di preparazione di tali atti da parte dell'operatore incaricato sono state già descritte nel precedente paragrafo "2.10", al quale esplicitamente si rimanda. Pertanto, i documenti così prodotti, che devono essere, quindi, trasmessi per posta ordinaria cartacea, **vengono portati, già imbustati e pronti per la partenza, presso la segreteria Comando, dove si provvederà al successivo inoltro.** È fatto obbligo di compilare in maniera leggibile ed in tutta la sua interezza l'apposita modulistica a corredo di ciascuna tipologia di spedizione.

2.15.7. La gestione del documento analogico interno

Nei casi in cui il documento da inviare ad una UO interna contenga allegati che per la loro natura non possono essere dematerializzati, **la specifica causa che ne ha reso impossibile la dematerializzazione deve essere riportata nelle note del protocollo informatico.**

2.15.8. Fax

Ai sensi dell'art. 47 co. 2 lett. "c" del CAD non è prevista la comunicazione via fax tra PPAA. L'eventuale trasmissione di documentazione attraverso tale strumento per cittadini o ditte può essere effettuata verso i fax delle UO di competenza tenendo presente che:

- il documento così trasmesso viene trattato dal UOR completo della dichiarazione di accertamento della fonte di provenienza a cura del responsabile della UO interessata;
- il fax è trattato con le stesse modalità descritte nel paragrafo inerente alla protocollazione dei documenti analogici;
- le eventuali istanze trasmesse via fax devono essere accompagnate da una fotocopia del documento d'identità del mittente (art. 38 D.P.R. 445/2000).

All'interno della Amministrazione non è previsto l'utilizzo della modalità "via telefax" per la trasmissione di documenti informatici.

2.16. Annullamento delle registrazioni di protocollo

Quando si presenta la necessità di annullare una registrazione di protocollo è bene ricordare che le informazioni relative alla stessa rimangono memorizzate nel registro informatico del protocollo. Il Sistema Documentale prevede che per effettuare l'annullamento, la compilazione di due campi obbligatori in cui vengano riportate in uno la motivazione e nell'altro il provvedimento autorizzativo dell'annullamento.
Solo il RDS è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo agli addetti del Servizio di Protocollo Informatico: il sistema registra l'avvenuto annullamento, la data, l'ora ed il nominativo dell'operatore che è intervenuto.
L'annullamento di una registrazione di protocollo può avvenire anche su richiesta dei Capi Uffici / Reparti interessati, con specifica nota adeguatamente motivata ed indirizzata al RDS.

CAPITOLO 3

SISTEMA DI CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

3.1. Il Titolario di classificazione

Sulla base dei riferimenti normativi e metodologici sopra esposti, l'Amministrazione Difesa ha predisposto un Titolario di archivio discendente da un preciso modello funzionale. Ogni AOO di Marina adotta il Titolario della Difesa per soddisfare le esigenze di classificazione delle UO dipendenti ed in esso è evidenziata la gestione di tutte le attività giuridiche, amministrative, tecniche e contrattuali connesse alle attività istituzionali dell'AOO nella loro globalità. Il piano di classificazione dell'Amministrazione è articolato su tre livelli, che

non possono essere liberamente modificati dall'AOO. Il primo livello del Titolario, una volta recepite le specificità degli argomenti / temi /materie trattati dall'Amministrazione è stato strutturato in 18 voci. La successiva articolazione del secondo e del terzo livello del Titolario è avvenuta mediante l'associazione, a ciascuna delle suddette voci di primo livello, delle rispettive attività e/o materie di pertinenza ad esse connesse, individuate mediante un'attività che ha interessato, sotto forma di colloqui, riscontri, attività di analisi e razionalizzazione i Reparti dello Stato Maggiore Difesa. Il Titolario non è retroattivo, non si applica, cioè, ai documenti protocollati prima della sua introduzione. Una versione del Titolario è riportata in **allegato D**.

3.2. La classificazione dei documenti

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO. Essa è eseguita attraverso il Titolario di classificazione. Tutti i documenti ricevuti e originati dalle UO sono classificati in base al sopra citato Titolario. Classificare un documento significa dunque associare al documento un indice di classificazione, possibilmente di livello 3 (titolo, classe, sottoclasse). L'operazione di classificazione dei documenti in entrata deve essere preordinata da un addetto alla protocollazione ovvero dal responsabile del procedimento.

3.3. La fascicolazione dei documenti

La fascicolazione è l'operazione di associazione logica di un documento informatico ad una aggregazione documentale informatica chiamata "fascicolo". All'interno di un fascicolo vengono inseriti tipicamente documenti che hanno in comune le stesse finalità. I fascicoli e i sottofascicoli, sono creati dagli utenti e sono, quindi, gestiti direttamente dagli interessati ai relativi procedimenti; l'RDS provvede ad effettuare un monitoraggio, eventualmente disponendo in proposito, al fine di evitare il proliferare dei fascicoli in maniera non controllata. Nel procedere alla creazione dei fascicoli e dei sottofascicoli, l'operatore, all'interno del "codice titolo" e della "descrizione titolo", dovrà utilizzare degli elementi identificativi del documento archiviato utili agli utenti per una futura ricerca dello stesso. È sconsigliato creare fascicoli la cui denominazione possa comportare ambiguità gestionale (ad esempio, la descrizione *varie*).
Per i documenti in uscita, è consigliabile eseguire la fascicolazione già in fase di predisposizione, ma rimane comunque possibile modificare il fascicolo al quale quel documento si riferisce anche in un secondo momento (eventualmente dopo la protocollazione).

CAPITOLO 4

ARCHIVIAZIONE DEI DOCUMENTI

4.1. L'Archiviazione dei documenti analogici

In linea con le disposizioni della normativa vigente[13], ogni AOO è tenuta ad effettuare la gestione dell'archiviazione/conservazione della documentazione analogica, all'interno del quale i responsabili dei procedimenti amministrativi sono tenuti ad esplicitare le modalità con cui intendono archiviare/conservare (ponendo attenzione alle tempistiche previste dalla legge) i documenti analogici all'interno dei propri fascicoli.

I fascicoli analogici chiusi sono soggetti alle precedenti modalità di archiviazione con cui sono stati iniziati fino all'eventuale esaurimento della pratica. I fascicoli analogici che, ancora aperti, subiscono il passaggio a digitale, non devono essere né buttati né alimentati da copie stampe di documenti già dematerializzati, ma: la parte analogica del fascicolo ormai divenuto "misto" deve essere conservati dalla UO che lo ha in carico sino ad esaurimento della pratica, dopodiché seguirà le modalità di versamento già illustrate. La parte digitale del fascicolo, invece, seguirà le modalità di archiviazione indicate nel successivo paragrafo 4.2. Infine, i fascicoli digitali contenenti copia elettronica di documenti analogici che per vari motivi sono stati già stati versati nell'archivio di deposito o storico, dovranno essere anch'essi chiusi in modo da impedire che siano

[13] DPR 445 (art. 68) e Linee guida AgID (cap. 4 e seguenti).

ulteriormente alimentati. In merito a quanto appena detto, l'RDS provvede, nel merito delle proprie competenze, alla creazione di un "piano di versamento" (coordinandosi eventualmente con il proprio titolare dell'Ente) richiedendo i contributi a tutte le UO interessando ciascun responsabile di procedura amministrativa i quali dovranno, per i propri documenti ed in accordo con le disposizioni di legge, redigere una parte del piano di versamento contenente le indicazioni utili all'archiviazione/conservazione della documentazione di propria competenza.

4.2. Archiviazione dei documenti informatici

L'AOO produce, attualmente, come più volte chiarito, prevalentemente originali informatici, i quali a partire dalla data di avvio del servizio di PI, sono archiviati all'interno del sistema informatico, che ne consente la gestione e ne garantisce l'accesso ottemperando alle norme di legge previste. I documenti informatici sono archiviati su supporti di memorizzazione, in modo non modificabile e contestualmente alle operazioni di registrazione e segnatura di protocollo, e sono gestiti dai Centri di telecomunicazione della Marina Militare che erogano il servizio. Periodicamente una copia dei documenti viene riversata nel Centro di Elaborazione Dati (CELD) del proprio Maritele di riferimento (per gli Enti a terra) mentre per le UUNN il Maritele è quello di Roma, previa procedura di sottoscrizione con firma digitale e marca temporale da parte degli RDC.

4.3. Processi di Archiviazione e di Consolidamento dei documenti informatici

Il Sistema Documentale consta di due processi funzionali alla corretta gestione della documentazione predisposta all'archiviazione:

- Il processo di archiviazione viene avviato dal Sistema ad intervalli periodici regolari, posto all'attenzione del RDS il quale appone (o delega il suo Vicario) la firma digitale (nei formati previsti e con l'ausilio dello strumento informatico josh InfoJam) sul Registro di Protocollo e sul relativo file di "Errata Corrige";
- Il processo di consolidamento dell'archivio di conservazione digitale, si realizza con l'apposizione sullo stesso della firma digitale, nei formati previsti, parte del RDC (o suo Vicario). In particolare l'RDC, sottoscrive l'elenco delle impronte informatiche dei documenti presenti all'interno dell'archivio in parola garantendone, attraverso l'uso della firma elettronica e della marca temporale, l'immutabilità nel tempo.

CAPITOLO 5

ABILITAZIONI DI ACCESSO AL SISTEMA DOCUMENTALE E PROFILAZIONI

5.1. Generalità

Il controllo degli accessi è il processo che garantisce l'impiego dei servizi del Sistema informatico di protocollo esclusivamente secondo modalità prestabilite. Gli utenti del servizio di protocollo informatico dell'AOO, in base ai rispettivi ruoli e competenze, hanno profilazioni di accesso differenziate in funzione delle tipologie di operazioni da eseguire.

5.2. Accesso al sistema

Potenzialmente ogni utente che abbia già ricevuto le proprie credenziali di accesso in Dominio MM, può essere autorizzato ad accedere al Sistema da un amministratore dell'AOO, tramite le operazioni di profilazione indicate nei prossimi paragrafi. Di massima è sufficiente essere preso in forza nell'AOO per avere il diritto di accedere al Sistema. Le principali profilazioni per una AOO riguardano gli incarichi di:

5.2.1. Responsabile del Servizio di Protocollo (e suo vicario):

Il Responsabile del Servizio (RDS) è nominato con Ordine del Giorno (ODG) del Comandante del 1° Reggimento San Marco (**allegato A**) assieme al suo Vicario (che coadiuva l'RDS nei casi di vacanza, assenza o impedimento). I compiti[14] principali dell'RDS sono:

- Adegua e pubblica il presente Manuale di Gestione;

[14] I compiti del RDS sono riportati in modo esaustivo nelle Linee Guida al paragrafo 3.4.

- Attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- Garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni dell'art. 53 del D.P.R. nr. 445 del 28 dicembre 2000[15];
- Predispone tempi, modalità e misure organizzative e tecniche finalizzate alla eliminazione dei protocolli diversi dal PI.
- Autorizza le operazioni di annullamento delle informazioni relative alle registrazioni di protocollo (di cui all'articolo 54 del TUDA) in armonia con le disposizioni di Maristat in merito ad annullamento ed oscuramento delle stesse;
- Garantisce la corretta produzione e la conservazione del Registro di protocollo;
- Cura che le funzionalità del Sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile[16].
- Garantisce, attraverso il monitoraggio, il buon funzionamento degli strumenti e dell'organizzazione dell'attività di registrazione di protocollo, incluse le funzionalità di accesso e le attività di gestione degli archivi, accordandosi eventualmente con gli Enti tecnici di FA preposti.
- è responsabile del buon andamento dei flussi documentali.
- Vigila sull'osservanza delle disposizioni della normativa vigente da parte del personale autorizzato o incaricato.
- Provvede alla produzione e conservazione di un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito.

5.2.2. Responsabile del consolidamento dell'archivio:

Il suo compito principale, nell'ambito M.M., ha carattere di garanzia rispetto alla validità della documentazione contenuta nell'archivio elettronico. In particolare, attraverso l'ausilio di strumenti informatici, convalida la corrispondenza esistente tra il documento cartaceo esistente presso il Comando/Ente ed il corrispondente documento elettronico. Nel caso di documenti formati direttamente per via elettronica, garantisce attraverso l'uso della firma elettronica e della marca temporale, l'immutabilità del documento nel tempo. Provvede al consolidamento dell'archivio di conservazione sostitutiva, è un processo che avviene in successione alla firma del registro di protocollo da parte del responsabile del servizio. Ulteriori dettagli su questa figura sono esplicitati nel supplemento alla SMM 18/UEU (Ed. 2012).

5.2.3. Gestore tecnico del sistema:

Il Gestore Tecnico del sistema/Amministratore di AOO del **1° Reggimento San Marco**, viene nominato con ODG del **Titolare** e dispone di strumenti di amministrazione del Sistema che gli consentono di effettuare alcune operazioni che non possono essere effettuate da tutti gli utenti. Il Gestore Tecnico supporta l'RDS nelle attività sistemistiche e coordina le attività relative alle installazioni HW/SW. Rappresenta, inoltre, il punto di contatto dell'AOO con il Maritele di competenza per quanto concerne problematiche relative alla funzionalità e all'efficienza del sistema. In particolare è l'unico che ha l'abilitazione alla modifica della matrice dei permessi della AOO (ma MARISTAT ha imposto un divieto a tale azione).

5.2.4. Supervisore di AOO:

Il Supervisore di AOO è un profilo che è colui che visualizza tutti i documenti protocollati, ma non ha nessuna azione su di essi.

[15] "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa – T.U.D.A."
[16] In Marina MARISTAT ha stabilito che si debbano seguire le seguenti direttive in caso di blocco delle attività di protocollo: 1) Prendere atto dell'anomalia/guasto che ha generato il blocco; 2)Contattare prontamente l'ente tecnico (di F.A.) preposto ed informare dell'evento richiedendo i tempi di riparazione dell'anomalia/guasto; 3)Procedere se necessario all'attivazione del registro delle emergenze (para/capitolo successivo).

5.2.5. Responsabile Privacy

Il responsabile Privacy è colui che ha diritto di gestire documenti riservati soggetti al GDPR. In particolare il Responsabile della privacy può inserire o rimuovere da un documento il cosiddetto *flag* "Documento Privato". Il permesso "responsabile privacy" è assegnato con Ordine del Giorno per la nomina dell'incarico privacy nel servizio documentale ed abilitato sul Sistema Documentale con l'ordine del Giorno per l'assegnazione di Permessi e Ruoli all'interno dell'AOO. Il Responsabile del Servizio (RDS) controlla le azioni dell'amministratore AOO.

5.2.6. Protocollista:

Il Protocollista (*record manager*) è la persona che ha l'autorizzazione ad eseguire la registrazione a protocollo dei documenti, sia in arrivo sia in partenza, da/verso interlocutori esterni o scambiati tra uffici dell'AOO se interni. Nel caso dei documenti in arrivo, l'Operatore, nell'effettuare le operazioni di registrazione, attribuisce al documento una classificazione di primo livello **e inoltra il documento verso la Compagnia/Plotone/Sezone di Smistamento competente, che a sua volta lo inoltra verso la UOR destinataria. Il completamento della classificazione fino al terzo livello e la fascicolazione sono assicurati dal Responsabile del Procedimento Amministrativo (RPA).** Nel caso dei documenti in partenza, è chi elabora e predispone per la firma il documento che, su indicazione dell'RPA competente, provvede alla classificazione di terzo livello e alla fascicolazione del documento.

5.2.7. Utente con delega di firma (invio documenti all'esterno dell'AOO)

L'Utente con Delega di firma è un Utente a cui il Titolare dell'AOO ha delegato la possibilità di sottoscrivere la corrispondenza in partenza tramite firma digitale qualificata. Agli Utenti con delega di firma vengono associati uno più "gruppi firma digitali" (più comunemente chiamati "timbri"). Le deleghe di firma devono essere sancite con O.d.G. in cui sono specificati gli incarichi degli Utenti.

5.2.8. Utente

Quando viene inserito un utente nel Sistema, l'inserimento in una UO (richiesto obbligatoriamente dal Sistema) lo rende possibile "assegnatario" di documenti dell'AOO, di conseguenza l'utente può visualizzare tutti e soli i documenti che gli vengono assegnati.

I profili/permessi sopra elencati non vanno considerati esaustivi delle molteplici possibilità fornite dal Sistema. L'assegnazione del profilo o dei permessi agli utenti è gestita dagli amministratori di AOO/Sistema, così come l'eventuale aggiornamento dello stesso, previa formale richiesta da parte dei responsabili delle diverse UO. Il RDS monitora e censisce regolarmente i profili associati ai vari utenti al fine di mantenerli aggiornati (o eventualmente eliminarli). Maggiori dettagli su profili/ruoli/permessi e funzionalità sono riportati sul manuale operativo del Sistema.

CAPITOLO 6

MODALITA' DI UTILIZZO DEL REGISTRO DI EMERGENZA

6.1. Premessa

La normativa disciplina la materia del registro di emergenza, che è stato concepito per sopperire ad eventuali malfunzionamenti del sistema informatico. Di seguito, quindi, verranno descritte le procedure previste nei casi di interruzione delle funzionalità dell'utilizzo del sistema informatico.

6.2. Attivazione del registro di emergenza

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico, ogni evento deve essere registrato su un supporto alternativo, denominato Registro di Emergenza (RE). Su questo registro devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora del ripristino

della piena funzionalità del Sistema, eventuali annotazioni ritenute rilevanti dal responsabile del servizio di protocollo informatico e il provvedimento autorizzativo dell'RDS che giustifica l'utilizzo del registro di emergenza. Nel concreto, si tratta di utilizzare il registro di emergenza da una o più postazioni definite dal RDS, che identifica ognuno dei registri con un numero cardinale sequenziale di due cifre, preceduto dalla sigla "RE"; ad esempio, RE01, RE02, ecc. Prima di autorizzare l'avvio della procedura, il responsabile del servizio di protocollo informatico deve impostare prima e verificare poi la correttezza di data e ora sui rispettivi registri di emergenza, verificandone successivamente la correttezza. Nel caso di un completo malfunzionamento delle infrastrutture hardware, per assicurare il funzionamento del servizio di protocollo è necessario ricorrere a procedure manuali attraverso l'uso di registri cartacei su cui riportare gli stessi dati previsti nel registro di emergenza. Ciascun registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il 1° gennaio e termina il 31 dicembre di ogni anno. Il responsabile del servizio di protocollo informatico dovrà annotare nel protocollo unico i periodi di attivazione del registro di emergenza. Una volta ripristinata la piena funzionalità del Sistema, il responsabile del protocollo informatico provvede alla chiusura dei registri di emergenza, annotando su ciascuno il numero delle registrazioni effettuate e la data e l'ora di chiusura. Egli poi provvede senza ritardo alla connessione del registro di emergenza con il protocollo unico, inserendo le registrazioni effettuate utilizzando l'apposita funzione di recupero "riga per riga". Verificato lo "scarico" delle registrazioni, autorizza il ripristino del protocollo unico. Il registro di emergenza viene sostanzialmente a configurarsi come un repertorio del protocollo unico: ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo senza soluzione di continuità la numerazione del protocollo unico raggiunta al momento dell'interruzione del servizio. A tale registrazione sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza. I documenti annotati nel registro di emergenza e trasferiti nel protocollo unico recheranno, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo unico. L'efficacia della registrazione è dunque garantita dal numero attribuito dal registro di emergenza e a quel numero deve farsi riferimento per l'avvio dei termini del procedimento amministrativo; l'efficienza, invece, verrà garantita dall'unicità della catena documentale e dalla normalizzazione dei dati gestionali, comprese la classificazione e la fascicolazione archivistica.

6.3. Riattivazione del sistema informatico

Quando il sistema informatico riprende il suo normale funzionamento, il RDS produce una dichiarazione sul registro d'emergenza, nella quale riporta la data e l'ora del ripristino delle funzionalità del sistema. Dopo la riattivazione del sistema i documenti in ingresso protocollati in emergenza, verranno importati all'interno del sistema di PI seguendo la procedura prevista nel manuale operativo. Parimenti, i documenti usciti che erano stati conservati in minuta dalle UO di competenza, dovranno essere importati all'interno del sistema di PI seguendo la procedura prevista nel manuale operativo. Tale azione consentirà di disporre del nuovo numero di protocollo senza la necessità di ritrasmettere il documento stesso. Il numero di protocollo assegnato ai documenti con il registro di emergenza in uscita, verrà trascritto automaticamente[17] dal sistema nell'apposito spazio dedicato.

[17] L'automatismo avviene qualora si utilizzi, per il registro d'emergenza, il previsto file "Excel": Affinché la procedura vada a buon fine occorre seguire le seguenti regole:

- il Registro di Emergenza deve essere un file Excel e chiamarsi obbligatoriamente "*registro_emergenza.xslx*" la struttura di questo file Excel deve essere analoga all'esempio allegato al manuale operativo: *josh Protocol_SUM_Appendice_registro_emergenza.xslx* (stesse colonne e nello stesso ordine);
- i dati contenuti devono essere validi per la AOO corrente;
- la cartella può contenere i file che rappresentano i protocolli da importare (con il nome indicato nel file Excel stesso).

ELENCO DEGLI ALLEGATI

A. Atto di nomina del RDS e del Vicario.

B. Elenco delle Unità Organizzative (UO) dell'AOO di MARISTAT.

C. Facsimile Lettera in uscita.

D. Titolario di classificazione dell'AOO.