



Manuale di Gestione del Protocollo Informatico

(art. 5 del D.P.C.M. in data 3 dicembre 2013)

Area Organizzativa Omogenea:
“Comando Supporti Enti di Vertice”
(identificativo: M_D ARM090)

Edizione 2025

ATTO DI APPROVAZIONE.....	4
REGISTRAZIONE DELLE AGGIUNTE E VARIANTI	5
ELENCO DI DISTRIBUZIONE.....	6
ACRONIMI.....	7
1 AMBITO DI APPLICAZIONE DEL MANUALE E DEFINIZIONI.....	8
1.1 INTRODUZIONE.....	8
1.1.1 Aree Organizzative Omogenee (AOO)	8
1.1.2 Unità Organizzative (UO)	9
1.1.3 Responsabile del Servizio	9
1.1.4 Protocollo Unico ed abolizione dei protocolli interni	10
2 LE TIPOLOGIE DOCUMENTARIE	11
2.1 IL DOCUMENTO AMMINISTRATIVO.....	11
2.2 IL DOCUMENTO ANALOGICO.....	11
2.3 IL DOCUMENTO ELETTRONICO.....	11
2.4 IL DOCUMENTO INFORMATICO	11
2.5 TIPOLOGIE DOCUMENTARIE	12
2.5.1 Documenti in entrata.....	12
2.5.2 Documenti in uscita.....	13
2.5.3 Documenti interni.....	13
2.5.4 Documenti a trattazione particolare	13
3 I FLUSSI DOCUMENTALI.....	14
3.1 DESCRIZIONE DEL FLUSSO DOCUMENTALE	14
3.2 FLUSSO DOCUMENTALE IN ENTRATA.....	15
3.3 FLUSSO DOCUMENTALE IN USCITA	15
3.4 FLUSSO DOCUMENTI INFORMATICI TRA AOO	16
4 REGISTRAZIONE DEI DOCUMENTI: REGOLE E MODALITA'	18
4.1 IL PROTOCOLLO.....	18
4.1.1 Protocollo documenti cartacei in entrata all'AOO	19
4.1.2 Copia autentica di documenti cartacei in uscita	20
4.1.3 Protocollo in ingresso di telefax	20
4.1.4 Protocollo di documenti già registrati.....	20
4.2 POSTA ELETTRONICA ISTITUZIONALE E PEC.....	20
4.3 FATTURE ELETTRONICHE	21
4.4 TIPOLOGIE PARTICOLARI DI DOCUMENTI	22

4.4.1	<i>Documentazione Classificata</i>	22
4.4.2	<i>Lettere anonime pervenute o senza firma</i>	22
4.4.3	<i>Lettere I.N.C.C. (Informazione non Classificata Controllata)</i>	23
4.5	ANNULLAMENTO DI UNA REGISTRAZIONE	23
4.6	DOCUMENTI DA PROTOCOLLARE	23
4.7	DOCUMENTI DA NON PROTOCOLLARE	23
4.8	PRIVACY E PROTEZIONE DEI DATI PERSONALI	234
4.9	REGISTRO DI PROTOCOLLO	234
5	ARCHIVIAZIONE	26
5.1	L'ARCHIVIO	26
5.2	L'ARCHIVIO CORRENTE	26
5.2.1	<i>Piano di classificazione</i>	26
5.2.2	<i>I fascicoli</i>	27
5.2.3	<i>La pratica e la cartella elettronica</i>	28
5.3	L'ARCHIVIO DI DEPOSITO	28
6	SICUREZZA	29
6.1	PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI	29
6.1.1	<i>Accesso al sistema</i>	29
6.2	ABILITAZIONI DI ACCESSO	29
6.2.1	<i>Responsabile del protocollo informatico</i>	30
6.2.2	<i>Operatore di protocollo del CRS</i>	30
6.3	GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO	30
6.4	REGISTRO DI EMERGENZA	31
7	DISPOSIZIONI FINALI	33
7.1	MODALITÀ DI COMUNICAZIONE DEL MANUALE	33
7.2	MODALITÀ DI AGGIORNAMENTO DEL MANUALE	33
8	RIFERIMENTI NORMATIVI	34
9	GLOSSARIO	35



COMANDO SUPPORTI ENTI DI VERTICE

ATTO DI APPROVAZIONE

Approvo il presente

“MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL
COMANDO SUPPORTI ENTI DI VERTICE”

redatto in conformità alle “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici”.

Roma li, _____

IL COMANDANTE f.f.
(Col. A.A.r.a.n. Antonio PELLEGRINO)

Documento informatico firmato digitalmente ai sensi del D. Lgs n.82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa.

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

Nr.	DATA DELLA VARIAZIONE	VARIAZIONE (Riportare il paragrafo del manuale oggetto dell'aggiunta/variante; indicare gli estremi di protocollo della comunicazione di aggiunta/variante)	PERSONALE CHE EFFETTUA LA VARIAZIONE (Data e Firma leggibili)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			

ELENCO DI DISTRIBUZIONE**DIRAMAZIONE INTERNA**

	COPIE N°
UFFICIO COMANDO	1
REPARTO SERVIZI GENERALI	1
UFFICIO ALLOGGI DELLA CAPITALE	1
SEZIONE OBIETTIVI ED ATTIVITA'	1
S. L.C.P.P. E PROTEZIONE TUTELA AMBIENTALE	1
ORGANO PERIFERICO DI SICUREZZA	1
SEZIONE PUMASS	1
INFERMERIA DI CORPO	1
CENTRO LOGISTICO SPORTIVO AM ROMA URBE	1
CENTRO LOGISTICO CASTEL DI DECIMA	1
PRESIDENTE SOTT.LI, GRADUATI E MIL. TRUPPA	1
SEZIONE COMUNICAZIONE ISTITUZIONALE	1
CONSULENTE GIURIDICIO	1

DIRAMAZIONE ESTERNA

COMANDO AERONAUTICA MILITARE ROMA	1
-----------------------------------	---

ACRONIMI

AOO: Area Organizzativa Omogenea;

CAD: Codice Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82, e successive integrazioni);

COMSEV: Comando Supporti Enti di Vertice;

COMAER: Comando Aeronautica Militare Roma;

CRS: Centro Ricezione e Smistamento;

LLGG: Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

DPR: Decreto del Presidente della Repubblica del 28 dicembre 2000 n.445;

GDPR: Regolamento Generale sulla Protezione dei Dati;

IPA: Indice delle Pubbliche Amministrazioni;

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;

SdP: Servizio per la tenuta del Protocollo informatico, della gestione, dei flussi documentali e degli archivi;

UO: Unità Organizzativa.

1 AMBITO DI APPLICAZIONE DEL MANUALE E DEFINIZIONI

1.1 Introduzione

L'introduzione del protocollo informatico presso le pubbliche amministrazioni è stata stabilita con **D.P.R. n. 445 del 28 Dicembre 2000**: "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa". Con tale sistema, il protocollo non è più concepito come una collezione di sistemi autonomi e indipendenti in prevalenza di tipo cartaceo ma si è trasformato in un sistema informativo unico informatizzato, specializzato ed altamente qualificato che rappresenta un vero e proprio sistema di gestione documentale che segue il documento in tutte le sue fasi di gestione: dall'acquisizione fino alla fascicolazione, diventando una risorsa strategica per il buon andamento e la trasparenza dei procedimenti amministrativi.

Il presente documento, viene redatto alla luce della recente costituzione dell'AOO (Area Organizzativa Omogenea) del COMSEV contrassegnata dall'identificativo M_D ARM090 (codice univoco di AOO: AVJIVLC), a seguito della separazione dello stesso dall'A.O.O. del COMAER (M_D ARM024) di cui era parte. Per AOO s'intende un insieme di Unità Organizzative di un'amministrazione che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. In particolare, ciascuna AOO mette a disposizione delle Unità Organizzative (UO) dipendenti il servizio di protocollo dei documenti in entrata ed in uscita, utilizzando un'unica sequenza numerica propria dell'AOO stessa ed il servizio per la gestione documentale elettronica.

Le LLGG prevedono che con l'entrata in vigore del protocollo informatico le pubbliche amministrazioni, ciascuna nel rispetto del proprio ordinamento, perseguano alcuni obiettivi di adeguamento organizzativo e funzionale:

- individuazione delle Aree Organizzative Omogenee;
- nomina del responsabile del servizio (RdS) per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi;
- nomina del/i Vicari/o Responsabile/i del Servizio per la tenuta del Protocollo Informatico, con il compito di intervenire in assenza del RdS;
- tempi, modalità e misure organizzative e tecniche finalizzate alla eliminazione dei protocolli interni;
- redazione di un Manuale costantemente aggiornato per la gestione del protocollo informatico.

In tale ottica, la Forza Armata si è dotata di un sistema software per la gestione del protocollo informatico denominato SIDPAM-2.

1.1.1 Aree Organizzative Omogenee (AOO)

L'individuazione delle AOO¹ in ambito Forza Armata è stata effettuata dallo Stato Maggiore A.M., in base ai criteri definiti dalla direttiva SMA-ORD-040, la quale, tra l'altro, elenca i relativi codici identificativi attribuiti agli elementi di organizzazione della F.A..

Il Comando Supporti Enti di Vertice è, pertanto, identificato quale AOO mentre le UO rappresentano i Gruppi/Servizi/Uffici che lo compongono.

¹ Prevista dal DPR n. 445 del 28 Dicembre 2000.

Ogni AOO mette a disposizione un complesso di risorse umane e strumentali che assicura il “Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi” cui sono affidate la gestione ed il funzionamento del sistema di gestione informatica documentale².

Il codice AOO attribuito al COMSEV, **M_D ARM090**, è così interpretabile: M_D sta per Ministero Difesa , A per Aeronautica Militare , RM rappresenta la provincia dove il Comando opera, ovvero Roma e 090 il numero ordinario identificativo assegnato tra gli Enti operanti nella predetta provincia. Detto codice identificativo è univoco nell’ambito della Forza Armata.

1.1.2 Unità Organizzative (UO)

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

Le Unità Organizzative di 1° livello dell’AOO – M_D ARM090 sono:

- 1) Ufficio Comando;
- 2) Organo periferico di sicurezza;
- 3) Consulente Giuridico;
- 4) Sezione Comunicazione Istituzionale;
- 5) Sezione Obiettivi ed Attività;
- 6) Servizio Locale Comprensoriale Prevenzione e Protezione e Tutela ambientale;
- 7) Presidente dei Sottufficiali, Graduati e Mil. di Truppa;
- 8) Sezione Rappresentanza Umana/Promozione Umana Sociale e Sportiva/Benessere e Sport;
- 9) Reparto Servizi Generali;
- 10) Ufficio Alloggi della Capitale;
- 11) Infermeria di Corpo;
- 12) Centro Logistico Sportivo AM della Capitale;
- 13) Centro Logistico Castel di Decima.

Ciascuna delle articolazioni componenti le predette UO di 1° livello, costituiranno UO di livello successivo.

1.1.3 Responsabile del Servizio

Nell’ambito di ciascuna AOO è individuata la figura del Responsabile del Servizio del Protocollo Informatico (RdS) che rappresenta il garante delle operazioni di registrazione, di protocollo, di organizzazione e tenuta dei documenti originali all’interno dell’AOO stessa fino al momento della loro presa in carico da parte del Responsabile della Conservazione³. Egli è la figura dirigenziale responsabile di tutte le operazioni di registrazione, di protocollo, di organizzazione e tenuta dei documenti all’interno della AOO stessa. Garantisce il corretto funzionamento, a norma di legge, del sistema di PI implementato nell’AOO anche nei confronti dei cittadini/ditte/altre PA. È nominato con Atto Dispositivo del Comandante del COMSEV, unitamente ad un vicario che lo sostituisce in caso di assenza.

² Art. 52 del DPR 445/2000.

³ LLGG.

Al Responsabile del Servizio sono devolute le seguenti funzioni⁴:

- presiedere alle attività del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi alle dipendenze della stessa AOO;
- predisporre il Manuale di Gestione del Protocollo Informatico;
- attribuire il livello di autorizzazioni per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e modifica delle informazioni;
- garantire la regolarità delle operazioni di registrazione e segnatura del protocollo;
- garantire la corretta produzione e la conservazione del registro giornaliero di protocollo;
- curare che le funzionalità del sistema, in caso di guasti o anomalie, possano essere ripristinate entro le 24 ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- disporre per la corretta esecuzione delle operazioni di salvataggio dei dati⁵ garantendone l'integrità ed il backup. Per tale attività si avvale delle procedure automatizzate previste dal sistema, implementate e gestite dal Centro unico di Backup e Business Continuità del Reparto Sistemi Informativi Automatizzati di Roma (ReSIA);
- conservare in caso di registrazione di protocollo manuale, in luoghi sicuri le copie dei Registri di Protocollo di emergenza;
- autorizzare le operazioni di annullamento di un protocollo;
- vigilare sull'osservanza delle disposizioni da parte del personale incaricato.

1.1.4 Protocollo Unico

Ai sensi delle LLGG, con l'entrata in vigore del Protocollo Informatico, è cessata ogni altra numerazione di protocollo interna agli Enti ad esclusione di quella generata dal predetto sistema che rappresenta il sistema unico di protocollazione centralizzato, in ingresso in uscita e per le comunicazioni interne (tramite interoperabilità o acquisita "manualmente").

Le operazioni di protocollazione/gestione della posta in ingresso sono devolute alla Sezione Coordinamento Generale dell'Ufficio Comando che assume con il Nucleo Archivio e Protocollo, le funzioni di CRS ossia di Centro di ricezione e smistamento della posta presso il COMSEV. La protocollazione in uscita è, invece, decentrata, presso tutte le UO presso le quali sono presenti i titolari abilitati alla firma (su delega del Comandante) dei documenti in uscita tramite apposizione della firma digitale.

Un documento sottoscritto con firma digitale, formato secondo le prescrizioni del Codice dell'Amministrazione Digitale (CAD):

- si presume riconducibile al titolare, salvo prova contraria fornita dal medesimo;
- fa piena prova ai sensi dell'art. 2702 del Codice Civile (fino a querela di falso della provenienza delle dichiarazioni da parte di chi ha sottoscritto il documento);
- soddisfa il requisito legale della forma scritta (art. 20 del CAD).

⁴ Art. 61 del DPR 445/2000.

⁵ Art. 61 e 62 del DPR 445/2000.

2 LE TIPOLOGIE DOCUMENTARIE

2.1 Il documento amministrativo

Per documento amministrativo si intende ogni rappresentazione grafica, foto-cinematografica, informatica o di qualsiasi altra natura contenente atti, fatti o cose giuridicamente rilevanti, anche interni, prodotti e acquisiti ai fini dell'attività amministrativa⁶. Un documento amministrativo è quindi una rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa⁷.

2.2 Il documento analogico

Il documento analogico è un supporto fisico di informazioni che può presentarsi in diverse forme. Esiste in forma tangibile (es. formato cartaceo) e richiede generalmente processi di scansione o digitalizzazione per essere convertiti in formati elettronici. La digitalizzazione dei documenti analogici consente di preservarli nel contesto del panorama informatico odierno, permettendo l'archiviazione, la ricerca e la condivisione più efficace delle informazioni. Inoltre, la digitalizzazione facilita la creazione di sistemi di gestione documentale più strutturati ed accessibili, integrando abilità di ricerca e recupero delle informazioni. È importante notare che l'acquisizione di dati da documenti analogici richiede, a volte, strumenti specifici per garantire l'accuratezza e l'integrità delle informazioni durante la transizione verso un formato digitale. In alcuni contesti, può essere necessario mantenere i documenti in formato fisico per questioni legali o normative (ad esempio, contratti firmati, relazioni ufficiali o archivi storici), ma la digitalizzazione rimane un passo fondamentale per migliorare l'efficienza e i costi di gestione.

2.3 Il documento elettronico

In linea generale, il documento elettronico è un documento (file) creato, trasmesso o archiviato su supporto informatico, indipendentemente dal fatto che abbia o meno rilevanza giuridica (es: un'email, un file di testo, una foto digitale ecc.). Un aspetto fondamentale è la sua capacità di essere facilmente accessibile, modificabile e condivisibile. Essi possono essere soggetti a normative specifiche come la firma elettronica che ne garantisce l'autenticità e integrità.

2.4 Il documento informatico

Un documento informatico è il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati **giuridicamente rilevanti**⁸, idonea a produrre effetti legali. La distinzione principale tra documento elettronico e documento informatico risiede nel fatto che, mentre tutti i documenti informatici sono elettronici, non tutti i documenti elettronici possiedono valore legale o giuridico. Per esempio, una email o file word privi di firme o senza le caratteristiche necessarie per attestare la loro autenticità e integrità non sarebbero considerati documenti informatici validi in senso legale. Perciò, il documento informatico è creato, gestito ed archiviato in formato elettronico e la sua validità è garantita attraverso l'uso di firme elettroniche che ne conferiscono autenticità e integrità, secondo le normative vigenti (es: fattura elettronica, atto amministrativo firmato

⁶ Art. 22 comma 2 L. n. 241 del 7 Agosto 1990.

⁷ Art. 1 del DPR n. 445 del 28 Dicembre 2000.

⁸ Art. 1 lett. p) CAD.

digitalmente, un contratto con firma elettronica qualificata). La sua valenza probatoria dipende dalla conformità della sua sottoscrizione a norme legali e dal tipo di firma elettronica utilizzata. Al documento informatico non sottoscritto viene riconosciuta la mera efficacia probatoria attribuita dal nostro ordinamento giuridico alle riproduzioni meccaniche⁹. Il documento informatico sprovvisto di qualsivoglia tipologia di firma elettronica, quindi, forma piena prova dei fatti e delle cose rappresentate, solo se colui contro il quale è prodotto non ne disconosce la conformità ai fatti o alle cose medesime. Una differente disciplina ed una maggiore valenza probatoria è, invece, prevista nei casi in cui il documento informatico risulti sottoscritto con firma elettronica (semplice) o con firma elettronica qualificata¹⁰. Per essere considerato valido, un documento informatico deve rispettare i principi stabiliti dal CAD e dalle normative correlate, tra cui:

- **autenticità:** garantita tramite firma elettronica, sigillo elettronico o altri strumenti di identificazione (certezza dell'identità dell'autore e la provenienza del documento stesso);
- **integrità:** il documento non deve essere alterato dopo la sua creazione (immodificabilità);
- **affidabilità:** il documento deve essere prodotto e gestito attraverso sistemi e processi che ne assicurino la validità, assicurando che rappresenti una fonte veritiera e completa delle informazioni a cui si riferisce;
- **leggibilità:** il documento deve essere accessibile e leggibile nel tempo (indipendentemente dai sw o hw utilizzati al momento della sua creazione).

2.5 Tipologie documentarie

I sistemi documentali e nello specifico quello utilizzato presso il Comando Supporti Enti di Vertice, (in uso presso tutta Forza Armata), consente la gestione e la protocollazione di tutti i documenti che possiedono i requisiti minimi e sufficienti, richiesti per i documenti amministrativi e/o informatici. Le tipologie di documenti - in entrata, in uscita e interni - trattati dall'AOO - M_D ARM090 sono di massima:

- Lettera, Messaggio, Telegramma, Telefax, Appunto, Nota, Nota Esplicativa, Promemoria, Verbale di Riunione, Resoconto Sommario di Riunione, Modulo Inoltro Documento, Modulo di Coordinamento, Ordine del giorno, Atto Dispositivo, Disposizione Permanente, Ordine d'Operazioni.

Il Sistema di Gestione Documentale NON è abilitato alla trattazione di documenti classificati ma solo documenti non classificati e documenti contenenti Informazioni non Classificate Controllate (INCC). Per quanto attiene i documenti che contengono dati sensibili¹¹ dovrà essere valutata, di volta in volta, la modalità di acquisizione e smistamento a cura degli operatori del settore, in coordinamento con il responsabile e/o vicario del CRS. Il sistema consente di limitare la visione di alcune tipologie di documenti solo a coloro che sono abilitati alla loro visione, in ragione del proprio incarico/ruolo.

2.5.1 Documenti in entrata

Per documenti in entrata si intendono quelli acquisiti dall'AOO nell'esercizio delle proprie funzioni. I documenti in entrata giungono presso la Sezione Coordinamento Generale dell'Ufficio Comando del COMSEV

- tramite posta ordinaria con invio presso l'indirizzo: Viale dell'Università 4 – Roma 00185;

⁹ Art. 23 del Codice dell'Amministrazione Digitale (D.lgs n. 82 del 7 Marzo 2005) e Art. 2712 c.c..

¹⁰ Art. 20 CAD

¹¹ D.Lgs 196 del 2003 e GDPR

- tramite il meccanismo automatico d'interoperabilità del Sistema di Protocollo Informatico che integra PEI: comsev.prot@aeronautica.difesa.it e PEC: comsev@postacert.difesa.it;
- tramite telefax;
- tramite PEI o PEC con importazione manuale, quando non processati automaticamente dal sistema.

La consultazione delle citate caselle di P.E.I. e P.E.C. sono effettuate, giornalmente, dal personale preposto della Sezione Coordinamento Generale.

2.5.2 Documenti in uscita

Per documenti in uscita s'intendono quelli che hanno rilevanza giuridico-probatoria, prodotti dal personale di una UO nell'esercizio delle proprie funzioni e sottoscritti dal Responsabile dell'AOO ovvero dal Comandante o da altro Ufficiale delegato. Essi sono diretti/spediti, informaticamente o cartaceamente, ad altre A.O.O. di altre o della stessa amministrazione o a privati (persone fisiche o giuridiche). Il mezzo di trasmissione principale per la trasmissione dei documenti destinati ad Enti di F.A. è il sistema di Protocollo Informatico ossia l'interoperabilità. La fascicolazione dei documenti in partenza è di competenza del Responsabile del Procedimento Amministrativo, mentre il protocollo viene effettuato dagli utenti abilitati di ogni unità organizzativa (UO).

2.5.3 Documenti interni

I documenti interni sono scambiati tra le UO (Gruppi, Uffici ecc.) facenti capo alla medesima AOO e, se richiesto, possono essere protocollati in caso di necessità. Quando non protocollati, i documenti interni sono comunque identificati da un univoco numerico progressivo, detto ID (identificatore), che è differente dal numero di protocollo. Lo stesso potrà essere utilizzato come riferimento per individuare il documento all'interno del sistema. Di massima, mentre l'ID è una chiave univoca utilizzata all'interno di un sistema informatico, una sorta di contatore, il numero di protocollo ha una funzione specifica nel contesto di registrazione e gestione documentale ufficiale.

2.5.4 Documenti a trattazione particolare

I documenti che contengono "dati sensibili", "dati personali", "dati particolari", "dati giudiziari" dovranno essere "etichettati" sul sistema di gestione del protocollo informatico di FA tramite l'apposito campo. Oltre a queste tipologie di documenti, ne sarà prevista una specifica per i "dati particolari/giudiziari" relativamente a quei documenti che possono contenere sia dati giudiziari sia dati personali di natura particolare.

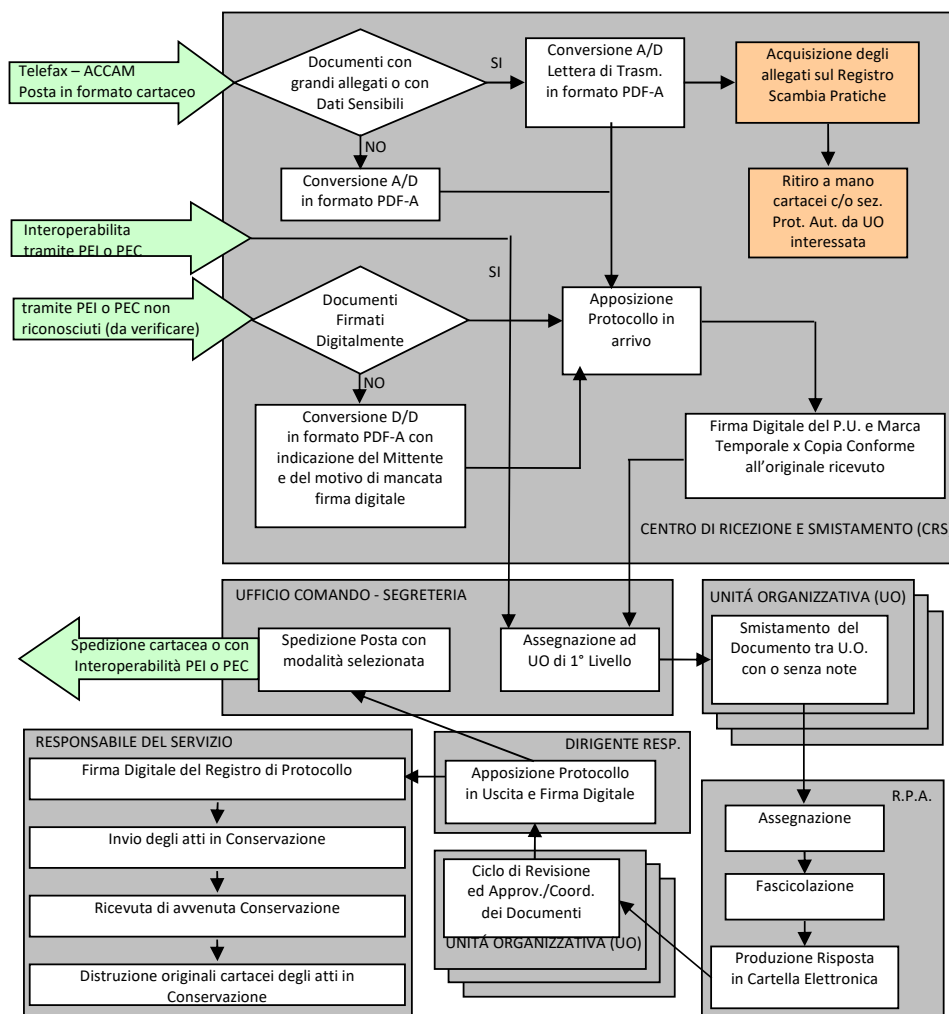
Per tutti questi documenti, una volta etichettati, l'accesso sarà consentito solo agli utenti il cui profilo prevede l'autorizzazione alla trattazione di tale tipologia di informazioni e che siano nella catena di smistamento (conoscenza, trasmissione o competenza), per quelli in arrivo, o inseriti nella catena di approvazione e firma per la pratica dei documenti in uscita. Tuttavia l'accesso sarà possibile solo con l'utilizzo della CMD e l'inserimento del PIN carta.

I documenti in entrata, contenenti dati personali, sensibili e giudiziari, non pervenuti tramite il sistema di protocollo della FA o comunque non correttamente marcati dall'originatore, verranno etichettati con una delle tipologie previste dal personale della Sezione Coordinamento Generale, prima dello smistamento all'UO competente.

3 I FLUSSI DOCUMENTALI

3.1 Descrizione del flusso documentale

La descrizione del flusso di lavorazione dei documenti è rappresentata nel diagramma sottostante:



Legenda:

- A/D => Analogico/Digitale
- D/D => Digitale/Digitale

3.2 Flusso documentale in entrata

Il CRS (Nucleo Archivio e Protocollo) protocolla tutta la documentazione non classificata in arrivo presso l'A.O.O. sia in formato cartaceo che elettronico, che soddisfi i criteri di autenticità, inalterabilità e dei quali sia certa la provenienza¹².

I documenti vengono smistati all'UO di competenza, il cui Capo provvede all'individuazione del Responsabile del Procedimento Amministrativo (RPA) ossia colui che lavorerà il documento; quest'ultimo è incaricato delle operazioni di fascicolazione, vale a dire della corretta creazione e gestione del fascicolo relativo alla pratica o al procedimento amministrativo. La fascicolazione rappresenta l'ultimo passo della vita del documento: l'archiviazione. L'RPA è sempre una persona fisica.

Il sistema di protocollo attualmente in uso (SIDPAM-2) obbliga l'assegnazione “per competenza” ad almeno una UO per ciascun documento in ingresso. L'assegnazione “per competenza” sul sistema documentale, tuttavia, potrebbe esulare dalla corrispondenza con gli indirizzi “per competenza” riportati sul documento. Ciò comporta che nel caso in cui il documento sia stato inviato dal mittente solo per conoscenza, sarà comunque smistato all'UO competente “per competenza”, non significando la necessità di dover effettuare delle azioni ma solo l'esigenza di garantire la classificazione e la fascicolazione del documento stesso.

Le pratiche erroneamente smistate all'interno della AOO, dovranno essere rifiutate e restituite al CRS che provvederà al conseguente corretto re-instradamento verso l'UO competente. Quelle assegnate ad un'UO perché oggetto di esplicito indirizzamento nella comunicazione ma che per la materia trattata rientrano nelle competenze di una collaterale UO interna alla AOO, dovranno essere rifiutate e restituite all'Ufficio Comando con indicazione della corretta UO.

I documenti non rientranti nell'area di competenza della AOO dovranno essere oggetto di formale restituzione a cura delle UO eventualmente indicate esplicitamente nell'indirizzo dal mittente.

Le UO curano il recapito dei documenti non classificati da protocollare, eventualmente ricevuti direttamente al di fuori dell'interoperabilità, presso la Sezione Coordinamento dell'Ufficio Comando.

I documenti IN ARRIVO indirizzati al Comandante del COMSEV di tipo “Esclusivo per il Titolare” (EPT) (in plico o altra forma che esula dalla trasmissione sul sistema documentale) vengono registrati dalla Segreteria di Sicurezza su apposito registro, con una numerazione progressiva. Sul sistema documentale arriverà dal mittente, un documento privo dei contenuti coperti da riservatezza che richiama ad un inoltro dello stesso in formato cartaceo o tramite altro mezzo di trasmissione diverso dal SIDPAM-2. L'operatore del CRS smisterà il documento pervenuto sul documentale, alla Segreteria di Sicurezza.

3.3 Flusso documentale in uscita

I documenti in uscita dalle UO, destinati all'esterno dell'AOO, per il cui contenuto ne sia ammessa l'acquisizione nel sistema documentale, sono acquisiti obbligatoriamente con il Protocollo Informatico.

¹² Art. 45 e 47 CAD.

I documenti in uscita dalle UO che contengono informazioni o della tipologia come di seguito specificato, dovranno essere spediti in forma cartacea :

- dati sensibili¹³ (personali, giudiziari, particolari, etc.) SOLO SE INDIRIZZATI ALL'ESTERNO DELLA FA non dotate di PEC (alle AOO della FA dovranno essere inviati in formato elettronico dopo averli correttamente etichettati come “documenti a trattazione particolare”);
- documenti di natura tale da non poter essere acquisiti a sistema (allegati che in forma digitale eccedono la dimensione massima ammessa dal sistema). In tal caso la lettera di trasmissione va comunque acquisita a protocollo, ma deve essere impostata nel sistema l'opzione che indica la spedizione cartacea del documento, in modo da evitare che il documento incompleto (privo di allegati) possa essere acquisito automaticamente a protocollo dal sistema documentale del destinatario (dando origine ad una decorrenza legale);
- destinati a privati che non abbiano comunicato la volontà di ricevere comunicazioni tramite PEC¹⁴;
- destinati ad AOO dell'A.D. o di altre amministrazioni che non siano ancora conformi alle regole di interoperabilità del protocollo informatico ai sensi del DPR 445/2000 e che non siano dotate di PEC.
- documenti assunti a Registro di Protocollo Informatico, destinati a professionisti¹⁵ e/o aziende¹⁶, non possono essere spediti in forma cartacea.

In tali casi le UO competenti dovranno consegnare la propria corrispondenza alla Sezione Coordinamento Generale, in plichi chiusi, recanti le indicazioni del mittente, del destinatario e del protocollo il quale provvederà a svolgere le ulteriori azioni di competenza, ovvero a consegnare la documentazione in parola presso il Nucleo Postale del COMSEV.

Per i documenti “Esclusivo per il Titolare” in uscita, non classificati, a mente di quanto previsto dalla direttiva SMA-RGS-007, l'acquisizione del numero di protocollo dovrà avvenire mediante l'uso del sistema documentale utilizzando un foglio in bianco con l'intestazione del mittente avendo come oggetto “esclusivo per il titolare” o “esclusivo per...” (senza mettere grado cognome e nome) e l'“Ente/Reparto destinatario”. Al centro del foglio sarà riportata la dicitura “seguirà documento cartaceo per l'Ente/Reparto destinatario” tramite una delle sottoelencate modalità:

- “Servizio Corriere Abilitato”;
- “Centro Comunicazioni Classificato”;
- “Sistema classificato nazionale”;
- “Sistema EDC”.

3.4 Flusso documenti informatici tra AOO

La trasmissione di un documento informatico tra due AOO:

- presso l'AOO mittente viene predisposto il documento da inviare, inserendo l'oggetto, il titolario ed il/i destinatario/i nonché il riferimento alla pratica in trattazione;

¹³ Regolamento UE n. 2016/679 (GDPR) e Paragrafo 5.6.2.12 della Direttiva SMD-I-004.

¹⁴ Art. 6 del Codice dell'Amministrazione Digitale (D.lgs n. 82 del 7 Marzo 2005).

¹⁵ D.L. n. 179 del 18 Ottobre 2012 e decreto MISE 19 Marzo 2013.

¹⁶ Art. 5-bis del Codice dell'Amministrazione Digitale (D.lgs n. 82 del 7 Marzo 2005).

- presso l'AOO mittente il documento viene inserito in una cartella elettronica di lavoro (nel sistema di Protocollo Informatico) che segue il processo di lavorazione/approvazione passando attraverso le UO della catena gerarchica;
- se il documento deve essere assunto a Registro di Protocollo, il RPA abilitato dell'AOO mittente approva il documento e ne richiede l'assunzione a protocollo. Il documento viene convertito dal sistema in formato PDF, includendo al suo interno la segnatura di protocollo in uscita;
- presso l'AOO mittente, il RPA firma digitalmente¹⁷ il documento. Il sistema forma il messaggio di posta elettronica contenente il documento informatico da inviare, compone ed allega al messaggio il file di segnatura;
- il sistema di posta elettronica dell'AOO mittente trasmette il documento al sistema dell'AOO ricevente all'indirizzo di posta elettronica da quest'ultima dichiarato presso l'IPA;
- il documento è protocollato in entrata dal sistema ricevente. La registrazione è effettuata automaticamente utilizzando le informazioni provenienti dall'AOO mittente e contenute nella segnatura informatica;
- il documento informatico, contenuto nel messaggio di posta elettronica, è smistato all'UO destinataria a cura del personale per lo svolgimento del procedimento amministrativo di competenza.

¹⁷ Art. 20 del Codice dell'Amministrazione Digitale (D.lgs n. 82 del 7 Marzo 2005).

4 REGISTRAZIONE DEI DOCUMENTI: REGOLE E MODALITA'

4.1 Il protocollo

La registrazione di protocollo serve ad annotare la data e l'ora in cui si è svolta l'operazione di registrazione del documento nelle forme e con i contenuti con cui lo stesso è pervenuto. In particolare sono annotati:

- numero di protocollo del mittente;
- data di registrazione di protocollo;
- mittente per il documento in entrata;
- destinatario per il documento in uscita;
- oggetto del documento;
- data e protocollo del documento ricevuto (se disponibili);
- impronta del documento se trasmesso per via telematica;
- numero degli allegati.

L'insieme di tali elementi è denominato “*Registrazione di protocollo*” ed è memorizzata nel Registro di Protocollo giornaliero del sistema, in modo non modificabile, mediante l'apposizione della firma digitale e della marca temporale al registro a cura del RdS.

La *segnatura di protocollo*¹⁸ è l'apposizione o l'associazione all'originale del documento, in forma permanente NON modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo unico ed univoco inequivocabile. La segnatura di protocollo viene apposta al documento dal sistema, *prima dell'apposizione della firma digitale (al fine di rendere immediatamente rintracciabile il documento)* e l'annotazione dell'impronta del documento nel registro di protocollo ne sancisce la non modificabilità prevista dalle norme.

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

E' possibile **annullare**¹⁹, nei casi previsti, una registrazione di protocollo (descrizione sulle modalità è riportata al par. 4.6).

Qualora siano riscontrate delle difformità tra il contenuto effettivo del documento ed i metadati presenti nel sistema è possibile **modificare**²⁰, in modo controllato, solo oggetto e mittente/destinatario purché non generati automaticamente dal sistema. In caso di modifica il Responsabile del Servizio dovrà provvedere all'aggiornamento del Registro di Protocollo, avendo cura di conservare agli atti la precedente versione.

Nei due paragrafi successivi sono fornite indicazioni sulle modalità di protocollazione dei documenti in entrata e in uscita.

¹⁸ Art. 55 comma 1 del DPR n. 445 del 28 Dicembre 2000 e LLGG.

¹⁹ Art. 54 comma 1 del DPR n. 445 del 28 Dicembre 2000.

²⁰ DPR n. 445 del 28 Dicembre 2000.

4.1.1 Protocollo documenti cartacei in entrata all'AOO

I documenti in ingresso sono protocollati esclusivamente presso la Sez. Coord. Generale dell'Ufficio Comando.

Le attività di “acquisizione”, “completamento” e “classificazione” dei documenti pervenuti in formato analogico (cartaceo) prevedono la seguente procedura a cura dei Pubblici Ufficiali²¹ all'uopo nominati:

- inserire il documento nello scanner;
- acquisire il documento attraverso lo scanner con una risoluzione idonea a renderlo correttamente leggibile;
- verificare che la qualità del documento acquisito sia idonea ad attestarne la sua conformità al documento originale;
- per ogni documento accettato, indicare il mittente (persona fisica, giuridica, altro soggetto) ed il numero di protocollo mittente, la data di emissione, l'oggetto del documento e l'UO di primo livello destinataria. *(il Sistema impedisce di procedere con la registrazione di protocollo, qualora si ometta di specificare i precedenti campi obbligatori);*
- dopo aver digitato i campi obbligatori suddetti ed aver accettato il documento prodotto, il Sistema genera automaticamente un numero di protocollo con la data corrente e tutte le informazioni di completamento precedentemente inserite dall'operatore;
- il sistema crea una copia del documento in formato PDF, contenente la segnatura di protocollo associata al documento in arrivo;
- apporre alla copia per immagine del documento analogico la firma digitale per attestare la sua conformità al documento analogico;
- estrarre il documento analogico dallo scanner e apporre l'etichetta autoadesiva con la segnatura di protocollo prodotta dal sistema. Qualora la stampante di “bar-code” sia temporaneamente non disponibile, l'operatore del protocollo riporta manualmente la segnatura sul documento. *(Tale ultima procedura verrà meno con l'attivazione del processo di conservazione).*

La copia digitale di documento analogico prodotta con la procedura suddetta ha la stessa efficacia probatoria del documento originale da cui sono tratte²² e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo le eccezioni di legge (individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione, la loro conformità all'originale deve essere autenticata da un notaio da da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico)²³. Al momento dell'attivazione del processo di Conservazione sarà possibile procedere alla distruzione dei documenti analogici che non siano originali unici.

Il Sistema invia, quindi, automaticamente il documento al responsabile dell'UO di primo livello indicata dall'operatore.

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

- Codice dell'amministrazione (M_D);
- Codice della AOO (ARM 090);

²¹ Art. 22 del Codice dell'Amministrazione Digitale (D.lgs n. 82 del 7 Marzo 2005).

²² Art. 22 comma 4 del Codice dell'Amministrazione Digitale (D.lgs n. 82 del 7 Marzo 2005).

²³ DPCM 21 marzo 2013.

- Codice del Registro (REG)
- Numero progressivo di protocollo (7 cifre). La numerazione è rinnovata ogni anno solare;
- Data di protocollazione (gg-mm-aaaa).

Un esempio di segnatura di protocollo in entrata è:

M_D ARM090 REG2025 0004321 15-05-2025

4.1.2 Copia autentica di documenti cartacei in uscita

Qualora sia necessario produrre una copia cartacea di un documento digitale inserito e protocollato a sistema sarà necessario ricorrere all'ausilio di un Pubblico Ufficiale all'uopo nominato²⁴, che dovrà attuare la seguente procedura: il documento protocollato e firmato a sistema viene stampato e sul retro di ogni sua pagina viene apposta mediante timbro la dicitura prevista per le copie conformi all'originale.

4.1.3 Protocollo in ingresso di TELEFAX

Il documento pervenuto in forma cartacea attraverso telefax deve sempre rispondere al requisito di leggibilità e di chiarezza riguardo la fonte di provenienza; qualora il supporto cartaceo non ne assicuri la corretta conservazione nel tempo, lo stesso dovrà essere fotocopiato.

L'utilizzo del telefax soddisfa il requisito della forma scritta e, pertanto, il documento di norma non sarà seguito dalla successiva trasmissione in originale.

Il documento ricevuto via telefax può essere conservato senza l'acquisizione dell'originale, con l'apposizione della dicitura "documento ricevuto via telefax".

La procedura per la sua trasformazione in formato digitale è analoga a quella per la protocollazione dei documenti cartacei in entrata all'AOO.

Ogni documento deve essere individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione. L'uso del fax non è consentito tra le PP.AA (art.47 comma 2 lettera c) CAD).

4.1.4 Protocollo di documenti già registrati

Prima di effettuare una registrazione di protocollo, il motore di ricerca del Sistema Documentale segnala all'operatore la presenza di altri documenti registrati nello stesso anno con la stessa anagrafica e stesso numero di protocollo. Il Sistema consente la visualizzazione del documento precedentemente acquisito via scanner e protocollato.

4.2 Posta elettronica istituzionale (PEI) e PEC.

Tutti i messaggi di Posta Elettronica pervenuti alle caselle di posta istituzionali dichiarate all'IPA (tramite PEC o firmati elettronicamente) devono essere protocollati (sia il corpo dell'E-mail che uno o più file ad essa allegati).

²⁴ Art. 23 del Codice dell'Amministrazione Digitale (D.lgs n. 82 del 7 Marzo 2005).

*Se l'eventuale segnatura di protocollo rispetta lo standard XML il messaggio, sia esso PEI o PEC, viene **automaticamente** migrato nel Sistema di Protocollo informatico e protocollato dal sistema, in caso contrario sarà necessario ricorrere ad una procedura manuale. Nel caso in cui alcuni documenti, pur essendo autentici, siano pervenuti privi di firma digitale (ad esempio tramite la casella di PEC, che autentica il mittente) o in formato non ammesso a sistema l'operatore all'uopo incaricato in qualità di Pubblico Ufficiale dovrà provvedere ad effettuare una conversione da documento digitale "semplice" a documento digitale²⁵ inserito a sistema con l'apposizione della sua firma digitale per dare efficacia probatoria al documento ricevuto. La copia originale informatico del messaggio ricevuto dovrà essere custodita a cura del Responsabile del Servizio fino al momento dell'invio in conservazione.*

Verranno protocollati solo i messaggi ricevuti presso la casella di posta elettronica istituzionale principale dell'Ufficio Comando significando che qualora il messaggio di posta elettronica sia pervenuto ad una casella diversa ed abbia i requisiti necessari per la protocollazione, lo stesso dovrà essere re-indirizzato al predetto indirizzo e, per conoscenza, al mittente.

Ai sensi della normativa vigente, è possibile protocollare un messaggio di posta elettronica ordinaria solo se firmato digitalmente.

Nel rispetto dell'art. 38 del DPR (i documenti informatici non firmati digitalmente possono essere accettati a condizione che sia garantita l'autenticità del mittente), vengono comunque accettati e protocollati quei documenti informatici inviati tramite una casella di posta non certificata e 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 tramite apposita comunicazione a cura dell'UO assegnataria per competenza.

Nel caso in cui il mittente sia una P.A., in assenza della firma digitale, è sufficiente che sia presente in allegato il file *segnatura.xml* con le informazioni previste dall'All. 6 alle LLGG.

A far data dal 1 dicembre 2021, è stata impedita la ricezione di email provenienti da indirizzi di posta elettronica ordinaria sulle PEC dell'A.D., giusto quanto disposto dal SMD VI Reparto (fgl M_D SSMD REG2021 0189827 del 18.10.2021, inoltrato dallo SMA in data 26.10.2021, con il foglio M_D ARM001 REG2021 0104062).

4.3 Fatture elettroniche.

Il Decreto Ministeriale n. 55 del 3 aprile 2013, entrato in vigore il 6 giugno 2013, ha fissato la decorrenza degli obblighi di utilizzo della fatturazione elettronica nei rapporti economici con la Pubblica Amministrazione ai sensi della Legge 244/2007, art. 1 commi da 209 a 214.

In ottemperanza a tale disposizione, questa Amministrazione, a decorrere dal 6 giugno 2014, non accetta fatture che non siano trasmesse in forma elettronica "Formato delle fatture elettroniche" del citato DM n. 55/2013.

Inoltre ai sensi dell'art. 25 del Decreto Legge n. 66/2014, al fine di garantire l'effettiva tracciabilità dei pagamenti da parte delle pubbliche amministrazioni, le fatture elettroniche emesse verso le PA devono riportare:

²⁵ Art. 23-bis del Codice dell'Amministrazione Digitale (D.lgs n. 82 del 7 Marzo 2005).

- Il codice identificativo di gara (CIG), tranne i casi di esclusione dall'obbligo di tracciabilità di cui alla Legge n. 136 del 13 agosto 2010;
- Il codice unico di progetto (CUP), in caso di fatture relative a opere pubbliche.

Il formato della fattura elettronica non è ancora importabile nel sistema quindi l'operatore per poter protocollare tali fatture dovrà:

- aprire la posta certificata istituzionale (comsev@postacert.difesa.it);
- scaricare le fatture pervenute in formato xlm/p7m e salvarle in locale.

Successivamente, con il software “kit di firma” il documento viene decrittato e salvato nuovamente in locale in formato pdf tale da poterla acquisire a sistema nella “sezione documenti in entrata” e smistarla all'UO competente per le operazioni propedeutiche alla liquidazione. Tale operazione richiede da parte dell'operatore una scrupolosa attenzione nell'acquisizione e controllo della stessa fattura, compilando tutti i campi previsti dal sistema

Al riguardo, è in fase di sperimentazione l'acquisizione automatica di suddette tipologie di fatture, attraverso il sistema di interoperabilità.

4.4 Tipologie particolari di documenti

Qui di seguito vengono fornite alcune indicazioni pratiche riguardo ai comportamenti operativi da adottare di fronte ad alcune situazioni che accadono di frequente presso gli uffici di protocollo:

4.4.1 Documentazione classificata

La documentazione classificata non deve essere trattata, né in ingresso né in uscita, né scambiata internamente al Reparto tramite il sistema di Protocollo Informatico ma deve essere gestita e protocollata esclusivamente dalla Segreteria di Sicurezza del COMSEV. Pertanto alla stessa non viene attribuito alcun numero di protocollo generato dal sistema. Per la stessa sarà usata la seguente stringa: **M_D ARM090/numero/SIC**, laddove il numero è generato con un sistema di numerazione progressivo in uso presso la citata Segreteria di Sicurezza e l'acronimo “SIC” farà intendere che trattasi di documentazione classificata a numerazione differente da quella generata dal SIDPAM-2.

4.4.2 Lettere anonime o senza firma

I documenti anonimi/apocrifi, comunque pervenuti, sono protocollati conservandone in copia la busta e vengono trattati anche nel rispetto delle procedure relative alla custodia dei documenti contenenti dati personali, giudiziari e sensibili.

Gli stessi, con l'eventuale documentazione annessa, sono archiviati e conservati dal Comandante.

Nell'assunzione sul sistema di protocollo informatico, tali documenti non dovranno essere acquisiti integralmente sul sistema, ma solo inserendo dei dati di riferimento (metadati) indicando, nel campo “mittente”, la dicitura: “MITTENTE SCONOSCIUTO O ANONIMO”. Successivamente il documento sarà smistato al responsabile della UO competente utilizzando preferibilmente le procedure di trasmissione della posta “Esclusivo per il titolare” (e.p.t.).

4.4.3 Lettere I.N.C.C. (Informazione non Classificata Controllata)

L'utilizzo dell'attribuzione limitativa "Informazioni non Classificate Controllate (I.N.C.C.)" è intesa per quelle informazioni non gravate da vincolo di segretezza (es. aspetti/procedimenti disciplinari, pubblicazioni/direttive di natura esclusivamente amministrativo/procedurale, riferimenti anagrafici a familiari del personale o qualifiche, abilitazioni e corsi di specializzazione ecc), ma tali da richiedere le misure di protezione minime (D.P.C.M. 6 novembre 2015). La trattazione di tale tipologia di documentazione può essere effettuata come un normale documento "non classificato" da attuarsi comunque nel rispetto del c.d. principio "need to know". Nel sistema il documento dovrà essere "etichettato" come contenente "dati particolari". Nel caso di creazione di fascicoli contenenti documentazione INCC/NU, questi dovranno essere chiusi appena sia venuta meno l'esigenza di accedere ai documenti in essi contenuti significando che, una volta chiusi, tali fascicoli potranno essere riaperti solo mediante richiesta formale al personale dotato di privilegio di gestione dell'archivio di deposito, secondo le linee di indirizzo fornite dal Reparto Generale Sicurezza.

A completamento, si evidenzia che la documentazione dell'Amministrazione A.M. priva di qualsiasi forma di vincolo amministrativo di segretezza, inclusa l'I.N.C.C., rientra nella sua interezza nel quadro generale del patrimonio informativo dell'A.M. ovvero nella cosiddetta "area delle informazioni non classificate" (direttiva SMA RGS-024 edizione 2015) per la quale la normativa vigente definisce specifiche modalità di gestione e divulgazione, chiare responsabilità individuali e correlate possibili conseguenze di natura penale e/o civile (M_D ARM001 0036130 31-03-2017).

4.5 Annullamento di una registrazione

L'annullamento di una registrazione di protocollo²⁶, è prerogativa del capo dell'A.O.O. ovvero del delegato Responsabile del Servizio o suo vicario. I motivi che determinano l'annullamento di un numero di protocollo devono essere indicati nell'apposito campo del registro di protocollo. Sia i documenti annullati che le informazioni connesse saranno ancora visibili solo attraverso il registro che riporterà la dicitura "Annullato".

4.6 Documenti da protocollare

I documenti da protocollare sono:

- in entrata: a mente di quanto previsto dal DPR 445/2000 art. 53 comma 5, sono oggetto di registrazione obbligatoria tutti i documenti ricevuti e spediti dall'amministrazione così come tutti i documenti informatici, ad esclusione di quelli elencati nel successivo punto 4.7;
- in uscita: tutti i documenti.

4.7 Documenti da non protocollare

Di seguito sono riportati i documenti esclusi dalla registrazione di protocollo²⁷:

- gazzette ufficiali;
- notiziari P.A.;
- note di ricezione documenti;

²⁶ LLGG

²⁷ DPR 445/2000

- atti preparatori interni;
- giornali, riviste, libri;
- inviti a manifestazioni, cartoline;
- certificati medici (riportanti la diagnosi della malattia);
- biglietti d’auguri;
- lettere personali e corrispondenza “e.p.t.” (esclusivo per il titolare);
- provvedimenti medico-legali (da valutare di volta in volta);

e tutti i documenti già soggetti a registrazioni particolari dell’Amministrazione già menzionati.

4.8 Privacy e protezione dei dati personali

La trattazione dei documenti contenenti dati **personali, sensibili e giudiziari** deve avvenire nel rispetto della legge²⁸. Con l’entrata in vigore del nuovo GDPR è stato nominato il Data Protection Officer per il Ministero della Difesa che dovrà emanare le disposizioni per la protezione dei citati dati. In tale ambito, per la FA è stato nominato quale Referente del Responsabile della Protezione dei dati personali dell’A.D. il Referente dell’A.M. per la prevenzione della Corruzione e della Trasparenza.

Su indicazione del citato Referente per la FA, i documenti contenenti dati personali, dati sensibili (cioè quelli idonei a rivelare: l’origine razziale ed etnica, le convinzioni religiose, filosofiche od altro, le opinioni politiche, l’adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale) e dati giudiziari dovranno essere “etichettati” sul sistema di protocollo informatico (come descritto in precedenza). Qualora ciò non sia possibile, questi documenti non dovranno essere acquisiti all’interno del sistema automatizzato di gestione documentale e si dovrà provvedere alla registrazione della sola lettera di trasmissione o del solo protocollo del documento, avendo cura di inoltrare lo stesso, secondo i tradizionali sistemi di gestione della posta, in busta chiusa recante l’apposita dicitura:

<< La pratica, completa di tutta la documentazione prevista, contiene dati da trattare ai sensi del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio e del Decreto Legislativo n. 196/2003 “Codice in materia di protezione dei dati personali” >>

4.9 Registro di protocollo

La registrazione di protocollo è un atto pubblico che consente di verificare l’effettivo ricevimento o spedizione di un documento.

Ciascuna registrazione di protocollo è riportata nel registro di protocollo.

Al fine di tutelare l’integrità e la regolarità delle registrazioni, il Responsabile del Servizio provvede quotidianamente alla firma digitale con marca temporale del registro giornaliero di protocollo.

Entro il mese di gennaio o entro il termine del proprio mandato, il Responsabile del Servizio di protocollo provvede alla firma digitale con marca temporale del registro di protocollo dell’anno precedente o del periodo di mandato concluso e, verificata la congruità delle registrazioni, provvede all’archiviazione dei documenti del registro giornaliero di protocollo dell’anno precedente.

²⁸ Regolamento UE n. 2016/679 – “Regolamento Generale sulla Protezione dei Dati (GDPR - General Data Protection Regulation), in vigore dal 25 maggio 2018.

Il Sistema consente di visualizzare un estratto del registro di protocollo inserendo gli estremi. L'operatore di protocollo inserisce la data inizio e di fine del periodo temporale di interesse.

5 ARCHIVIAZIONE

5.1 L'archivio

L'*archivio*, è definito come il complesso dei documenti prodotti e acquisiti dal soggetto produttore nell'esercizio delle sue funzioni. Esso si distingue in:

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

I documenti si distinguono in:

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

5.2 L'archivio corrente

E' costituito dall'insieme dei documenti appartenenti a fascicoli aperti ed agli affari correnti. Tutto l'archivio corrente è gestito attraverso il Sistema informatico che ne garantisce la corretta memorizzazione e archiviazione, assicurandone nel contempo l'accessibilità e la consultabilità.

5.2.1 Piano di classificazione

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

A tale scopo ciascun documento deve essere classificato.

La normativa vigente²⁹ stabilisce che la classificazione d'archivio deve adottare principi di coerenza funzionale nell'ambito di ciascuna AOO e presentare modalità di articolazione uniformi per tutta l'amministrazione.

L'applicazione di un piano di classificazione o titolario di archivio, che si presenta come un sistema integrato di informazioni sui documenti basato sul loro ordinamento funzionale, costituisce un presupposto indispensabile per la realizzazione e lo sviluppo della gestione informatica dei flussi documentali.

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

²⁹ DPR n. 445/2000 art. 50 e le LLGG

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

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

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

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

Presso il COMSEV viene adottato il titolario d'archivio in uso presso la Forza Armata, redatto dallo SMA - 1° Reparto e denominato "SMA - 3 - Titolarlo d'archivio A.M".

5.2.2 I fascicoli

Il fascicolo è l'insieme ordinato di documenti, relativi ad uno stesso procedimento amministrativo, a una stessa materia, a una stessa tipologia, che si forma nel corso dell'attività amministrativa allo scopo di riunire tutti i documenti utili per il procedimento stesso. La fascicolazione consiste nell'inserimento fisico (se cartaceo) o logico (se informatico) di un documento all'interno di un'unità archivistica denominata fascicolo, al fine di mantenere vivo il vincolo archivistico che lega fra loro i documenti afferenti ad una medesima trattazione.

I fascicoli possono essere organizzati:

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

La sigla che identifica il fascicolo è desunta dalle varie articolazioni del Titolario d'archivio e risulta così strutturata: "L.nn.nn.nn-n" dove la "L" rappresenta la lettera relativa all'argomento principale trattato nel titolario, le 3 "nn" successive indicano l'eventuale 2°, 3° e 4° sottolivello del titolario mentre l'ultima "n" è il progressivo che individua il fascicolo stesso.

Per esempio: **M.01.01.01-1** = fascicolo n° 1 della classifica di Titolario d'Archivio M.01.01.01, corrispondente alla voce "*autobus*"

I fascicoli possono essere "*aperti*" se il relativo procedimento amministrativo è in essere, "*chiusi*" se il procedimento è concluso.

Se un documento fa parte di più fascicoli lo stesso può essere inserito in tutti i fascicoli di cui fa parte attraverso l'operazione di classificazione del documento in un altro fascicolo.

E' necessario indicare sempre dove è conservato il documento cartaceo originale.

I documenti, una volta classificati e inseriti in un fascicolo, possono essere ancora: "copiati" in altro fascicolo - "spostati" in altro fascicolo - "trasmessi" ad un altro utente .

Al fine di gestire i fascicoli cosiddetti **“ibridi”** (contenenti cioè documenti cartacei e documenti informatizzati dopo l'adozione della nuova modalità di gestione), colui che sta gestendo la pratica ha l'obbligo di inserire all'interno del fascicolo "cartaceo" un espresso richiamo alla posizione informatica del documento non presente. Viceversa, avrà cura di inserire nel sistema di gestione informatica dei documenti, il richiamo al documento cartaceo non presente in forma digitale.

5.2.3 La pratica e la cartella elettronica

Tutti i documenti in uscita dall'AOO seguono un processo amministrativo che ne determina la formazione. Il processo amministrativo è contenuto in una pratica, ovvero in un insieme di documenti organicamente raggruppati, strutturati e formati per una specifica finalità. La pratica viene creata da chi crea e forma il documento e viene presentata alla firma del RDP con l'aspetto di una cartella elettronica, ovvero di una rappresentazione grafica a video dei documenti che replica la tradizionale rappresentazione della pratica all'interno della cartella cartacea.

Tutti i documenti inviati dall'AOO a decorrere dall'entrata in servizio del nuovo sistema documentale SiDPAM-2 sono collegati ad una pratica e, quindi, ad una cartella elettronica, che può essere ricercata e visualizzata mediante l'impiego di idonee funzionalità rese disponibili dal sistema.

Ciascuna pratica è contenuta all'interno del fascicolo di cui fa parte.

5.3 L'archivio di deposito

L'archivio di deposito è costituito dai documenti relativi a fascicoli conclusi. Esso consente solo operazioni di consultazione e mantiene i documenti per il numero di anni previsti dalla normativa vigente. Tutte le disposizioni in merito alla conservazione dei documenti dovranno essere emanate dal Responsabile per la Conservazione dei documenti per il Ministero Difesa, nominato con apposito atto.

Il sistema documentale SiDPAM-2 trasferisce automaticamente i fascicoli in archivio di deposito quando l'ultimo documento in esso inserito abbia superato il numero di anni previsto per la tenuta in archivio corrente. Il numero di anni viene stabilito dal Responsabile del Servizio e comunicato all'Amministratore centrale del sistema (ReSIA), che provvede a pianificare e controllare l'esecuzione delle procedure previste per l'archiviazione.

Il trasferimento viene attuato rispettando l'organizzazione che i fascicoli avevano nell'archivio corrente.

6 SICUREZZA

6.1 Piano di sicurezza dei documenti informatici

I documenti informatici, così come descritti nei precedenti paragrafi, sono oggetto di un apposito piano di sicurezza³⁰. La redazione di tale piano è demandata al Reparto Sistemi Informativi Automatizzati di Roma (ReSIA), quale Ente deputato alla gestione Tecnica del sistema SIDPAM-2 per l'intera FA.

6.1.1 Accesso al sistema

L'accesso di un utente al sistema SIDPAM-2 avviene per mezzo di un processo di autenticazione che funziona mediante piattaforma Windows che consente l'utilizzo della postazione di lavoro. Questo è verificato in tempo reale su un apposito sistema di autenticazione (*domain controller*) fornendo le proprie credenziali (*user name* e *password*). Se le credenziali sono corrette, si apre una sessione tra il client dell'utente ed il server applicativo comunicando a quest'ultimo solamente il codice d'accesso. In tal modo l'applicativo non viene a conoscere la parola-chiave. Il sistema di gestione documentale controlla inoltre che non venga utilizzato lo stesso codice di accesso (*user name*) contemporaneamente da due postazioni di lavoro.

La sicurezza per l'accesso ai documenti è garantita prendendo in considerazione:

- i privilegi di consultazione assegnati all'utente;
- consultazione ristretta all'ufficio di appartenenza;
- consultazione estesa agli uffici sottostanti nella gerarchia;
- consultazione estesa agli uffici di pari livello aventi lo stesso superiore gerarchico;
- consultazione estesa a tutta la AOO.

Il sistema offre un insieme di funzioni per la sicurezza che consentono di registrare le seguenti informazioni:

- accessi al sistema effettuate da un dato operatore;
- operazioni effettuate su un dato documento;
- operatore che ha effettuato una certa operazione;
- operazioni effettuate nell'ambito di una data sessione.

Il sistema consente inoltre la riconfigurazione del modello sicurezza attraverso:

- Creazione e cancellazione di utenti;
- Configurazione dei diritti di utenti;
- Configurazione dei diritti di accesso ad un documento;
- Configurazione dei diritti di accesso ai fascicoli;
- Configurazione dei diritti di accesso attraverso le voci di titolare.

6.2 Abilitazioni di accesso³¹

Gli utenti dell'AOO accedono al Sistema, dopo essere stati posizionati nella struttura della stessa in funzione del proprio incarico. Il Dirigente Responsabile dell'AOO per il tramite del RdS, eventualmente con il supporto del Resia, provvede a tale operazione ed attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra le abilitazioni per:

³⁰ LLGG.

³¹ LLGG.

- la consultazione delle informazioni;
- l'inserimento e modifica delle informazioni;
- la concessione del livello di accesso alle informazioni, attraverso una serie di parametri previsti dal software.

Ciò avviene su richiesta del Capo dell'Articolazione dove il militare è inserito in base all'incarico che svolge.

6.2.1 Responsabile del protocollo informatico

E' la persona che ha la possibilità di effettuare operazioni straordinarie, sui vari livelli di competenza, sul SIDPAM2, come ad esempio, il ripristino del sistema in caso di interruzioni, il monitoraggio delle operazioni effettuate, la predisposizione delle autorizzazioni di accesso al sistema e la gestione delle varie operazioni previste dal modulo di Amministrazione.

Nell'ambito del sistema documentale di cui si è dotata l'A.M. le funzionalità, ad esempio per il Backup dei dati e dell'applicazione sono centralizzate per tutta l'A.M. e sono attestate presso il Reparto Sistemi Informativi Automatizzati (ReSIA) sito in ROMA - Via Appia Pignatelli, 123.

Il Responsabile del protocollo informatico può delegare le suddette funzionalità ad una persona individuata dal ReSIA ed effettua periodici controlli sul corretto svolgimento delle stesse.

6.2.2 Operatore di protocollo del CRS

È l'operatore, militare o dip. civile dell'AD, autorizzato ad eseguire la registrazione dei documenti, sia in entrata che in uscita, che è stato nominato quale "Pubblico Ufficiale" per la conversione dei documenti cartacei (analogici) in formato digitale. Tale tipologia di personale viene, di norma, individuato nell'ambito dell'Ufficio Comando.

6.3 Gestione delle registrazioni di protocollo

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

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

- nome dell'utente che ha eseguito l'operazione;
- data e ora;
- valore precedente dei campi soggetti a modifica,

permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione.

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

Dopo le ore 24.00 di ciascuna giornata, qualora i documenti protocollati siano stati tutti firmati digitalmente, la procedura consente di produrre e archiviare il Registro di protocollo.

6.4 Registro di emergenza³²

Ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica, ogni evento deve essere registrato manualmente su un registro denominato “*Registro di emergenza*”. Lo stesso viene utilizzato su autorizzazione/disposizione del RdS e per documentazione di urgente protocollazione in ingresso o spedizione.

Sul registro è riportata la causa, la data e l’ora di inizio dell’interruzione, la data e l’ora del ripristino della funzionalità del sistema, nonché eventuali annotazioni ritenute rilevanti dal responsabile del protocollo informatico.

Qualora il malfunzionamento della procedura di protocollo informatico si prolunghi per oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile del protocollo informatico può autorizzare l’uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro sono riportati gli estremi del provvedimento di autorizzazione.

Per ogni giornata di registrazione manuale è riportato il numero totale di operazioni registrate manualmente.

La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l’identificazione univoca dei documenti registrati nell’ambito dell’AOO.

Le informazioni relative ai documenti protocollati manualmente sono inserite nel sistema informatico subito dopo il ripristino delle funzionalità del sistema, ad opera del personale operatore del CRS. A ciascun documento registrato manualmente viene attribuito un numero di protocollo del sistema informatico. Deve essere comunque mantenuta la correlazione con il numero di protocollo utilizzato in emergenza.

Una volta ripristinata la piena funzionalità del sistema, il responsabile del protocollo informatico provvede alla chiusura del registro di emergenza, annotando il numero delle registrazioni effettuate e la data e ora di chiusura.

Concretamente, il servizio di protocollo in condizioni di emergenza verrà gestito nel seguente modo:

- la Sezione Coordinamento Generale ha in uso il registro di emergenza che viene utilizzato per la corrispondenza sia in ingresso che in uscita;
- il personale delle Segreterie delle UO che hanno necessità di protocollare in emergenza un documento si recheranno presso la citata articolazione ovvero interagiscono con la stessa, per ottenere la numerazione da apporre sul documento.
- per ogni documento da protocollare manualmente, l’utente inserisce i seguenti dati: data, ora, oggetto, mittente o destinatario;
- il registro di emergenza si rinnova ogni anno solare, con inizio il 1° gennaio e termine il 31 dicembre dello stesso anno.

Le operazioni di protocollazione in emergenza sia in ingresso che in partenza sono effettuate dal personale preposto della Sezione Coordinamento Generale dell’Ufficio Comando. Sul documento in arrivo / uscita dovrà essere utilizzata la seguente stringa:

³² DPR n. 445 del 28 dicembre 2000 all’art. 63, comma 1

MD_ARM090/RE/(7 cifre)

Una volta ripristinata la piena funzionalità del sistema, il personale preposto della Sez. Coord. Generale provvede alla compilazione del Registro ed alla chiusura della giornata

Al ripristino del SIDPAM-2 le informazioni relative ai documenti protocollati manualmente, in emergenza, sono inserite nel sistema informatico, tramite l'apposita funzione, dal personale della Sezione sopracitata, subito dopo il ripristino delle funzionalità del sistema, tramite l'apposita opzione del software. A ciascun documento registrato manualmente viene attribuito un numero di protocollo del sistema informatico. Deve essere comunque mantenuta la correlazione con il numero di protocollo utilizzato in emergenza.

7 DISPOSIZIONI FINALI

7.1 Modalità di comunicazione del manuale

Il presente documento viene adottato con atto deliberativo del Comandante del Comando Supporti Enti di Vertice ed è soggetto a pubblicazione sul sito dedicato alle AOO della Difesa (<http://www.difesa.it/protocollo>).

7.2 Modalità di aggiornamento del manuale

Il Responsabile del Servizio di Protocollo ha il compito di garantire la corretta applicazione delle regole contenute nel manuale di gestione nonché di curarne l'aggiornamento, in relazione alle eventuali esigenze di ordine organizzativo e normativo.

8 RIFERIMENTI NORMATIVI

- ❑ **Legge 241 del 7 agosto 1990** – Nuove norme in materia di procedimento amministrativo e di diritto d’accesso ai documenti amministrativi;
- ❑ **DPR 352 del 27 giugno 1992** -- Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
- ❑ **Legge 191/1998** – L’art. 4 regola il telelavoro nelle pubbliche amministrazioni;
- ❑ **DL 368/98** – Istituzione del Ministero per i beni e le attività culturali a norma dell’art. 11 della legge 15 marzo 1997, n. 59;
- ❑ **DL 281/99** – Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica;
- ❑ **Decreto del Presidente della Repubblica del 26 dicembre 2000 n. 445**. Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- ❑ **Direttiva SMD-I-004 del 2004** – Il Protocollo Informatico nella Difesa.
- ❑ **Codice dell’Amministrazione Digitale (CAD)**. Decreto Legislativo 7 marzo 2005 n.82 e successive modifiche. Questo decreto è la norma fondamentale che regola l’uso delle tecnologie informatiche nell’ambito della pubblica amministrazione
- ❑ **Decreto Legislativo 10 agosto 2018, n. 101** – “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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 (regolamento generale sulla protezione dei dati)”.
- ❑ **D.Lgs 42/2004** “Codice dei beni culturali e del paesaggio”.
- ❑ **DPCM 22 febbraio 2013** “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”.
- ❑ **Circolare Agenzia Italia Digitale (AgID)** “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici” ed. Maggio 2021.

9 GLOSSARIO

Definizioni

<i>Termine</i>	<i>Acron.</i>	<i>Definizione</i>
Area Organizzativa Omogenea	AOO	Struttura amministrativa individuata da settori che, per tipologia di mandato istituzionale, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato. In particolare, ciascuna AOO mette a disposizione delle unità organizzative clienti il servizio di protocollo dei documenti in entrata ed in uscita, utilizzando un'unica sequenza numerica propria alla AOO stessa.
Assegnazione di un documento		Individuazione di un responsabile del procedimento amministrativo (v.) cui affidare un documento in gestione, ai sensi degli artt. 5 e 6 della legge 7 agosto 1990, n. 241.
Casella di posta elettronica istituzionale	PEI	La PEI è la e-mail istituita da ciascuna AOO attraverso la quale vengono ricevuti i messaggi da protocollare. E' la casella utilizzata per lo scambio dei documenti, sia in entrata che in uscita, con le altre AOO della P.A. attraverso i rispettivi sistemi di PI.
Casella di Posta Elettronica Certificata	PEC	La PEC fornisce un servizio di messaggistica che sfrutta gli standard propri della posta elettronica, assicurando al mittente l'attestazione di avvenuta ricezione del messaggio e al destinatario la garanzia dell'identità del mittente. La PEC istituzionale è strettamente connessa all'Indice delle Pubbliche Amministrazioni (IPA), ove sono pubblicati gli indirizzi di posta certificata associati alle AOO e alle funzioni organizzative previste dalle Pubbliche Amministrazioni.
Classificazione dei documenti		La classificazione d'archivio consiste in un'attività di organizzazione fisica e logica di tutti i documenti correnti, protocollati e non (spediti, ricevuti, interni), di un soggetto produttore secondo uno schema articolato di voci che identificano le funzioni, attività, materie specifiche del soggetto. Il sistema di classificazione dei documenti è definito nel "piano di classificazione" (o Titolario).
Digitalizzazione		Trasposizione numerica delle immagini relative ad una pagina di un documento. È anche detta "scannerizzazione", "scansione", "acquisizione immagine".
Dato anonimo		Dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
Dati personali		Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Dati particolari		Qualunque dato personale, genetico o biometrico relativo allo stato di salute, o comunque idoneo 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 l'orientamento sessuale (art. 9 del GDPR).
Dati giudiziari		I dati personali idonei a rivelare provvedimenti di cui all'art. 10 del GDPR, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
Direzioni Centrali		Hanno responsabilità globali sulle intere fasi del processo e del ciclo operativo, con i fini d'omogeneizzazione della funzionalità e delle procedure sull'intero territorio nazionale.

Termine	Acron.	Definizione
Documenti da protocollare		Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione.
Documento amministrativo		Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.
Documenti a trattazione particolare		Rientrano in questa categoria i documenti che contengono dati personali, dati particolari e dati giudiziari.
Documento Informatico		Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Documento elettronico		Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento analogico		Rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Fascicolo		Il "fascicolo" è l'insieme ordinato di documenti, relativi ad uno stesso procedimento amministrativo/materia/tipologia, che si forma nel corso dell'attività amministrativa, allo scopo di riunire tutti i documenti utili per il procedimento stesso.
Gestione dei Documenti		L'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato; essa è effettuata mediante sistemi informativi automatizzati.
Manuale di gestione		Previsto dal DPCM del 3 dicembre 2013, il Manuale di gestione descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la gestione dei documenti per la tenuta del protocollo informatico.
Procedimento amministrativo		Modello di processo istituzionalmente eseguito da una amministrazione (e.g. ecc.). NOTA: con il termine procedimento si intendono in senso allargato non solo i procedimenti ai sensi della legge 241, ma più in generale qualsiasi tipo di modello di processo amministrativo.
Protocollo		Fase del processo di gestione documentale che certifica provenienza/destinazione e data certa di acquisizione/trasmissione del documento, mediante la sua identificazione univoca nell'ambito di una sequenza numerica collegata con l'indicazione temporale.

Termine	Acron.	Definizione
Registrazione di protocollo		La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni: a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile; b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile; c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile; d) oggetto del documento, registrato in forma non modificabile; e) data e protocollo del documento ricevuto, se disponibili; f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.
Registro di emergenza		Supporto alternativo su cui vengono riportate manualmente le registrazioni di protocollo nel caso di malfunzionamenti che rendano impossibile l'utilizzo della normale procedura automatica.
Responsabile del Procedimento Amministrativo	RPA	Persona responsabile delle operazioni di registrazione, di protocollo, di organizzazione e tenuta dei documenti all'interno di una UO (v.).
Responsabile del Servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi - (art. 61 DPR)	RdS	È la figura dirigenziale responsabile legalmente di tutte le operazioni di registrazione, di protocollo, di organizzazione e tenuta dei documenti all'interno della AOO stessa. Garantisce il corretto funzionamento, a norma di legge, del sistema di PI implementato nell'AOO anche nei confronti dei cittadini/ditte/altre PA.
Segnatura di protocollo		L'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile degli elementi di identificazione riguardanti il documento stesso. Ciò per consentire di individuare in modo inequivocabile ciascun documento.
Sistema di gestione informatica dei documenti		L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti.
Titolario di archivio		Il piano di classificazione, o "titolario d'archivio", consiste in uno schema generale di voci logiche, stabilite in modo uniforme ed articolate tendenzialmente in modo gerarchico, che identificano l'unità archivistica, ovvero l'unità di aggregazione di base dei documenti all'interno dell'archivio (fascicolo); all'interno dell'unità archivistica, i documenti sono ordinati tipicamente per data di acquisizione.
Ufficio Postale		Svolge il compito di smistamento generale della posta generica in arrivo ed uscita.
Unità Organizzativa	UO	Sottoinsieme di una AOO (v.), cioè un complesso di risorse umane e strumentali cui sono affidate competenze omogenee nella trattazione di procedimenti amministrativi.