



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufaulav@geniodife.difesa.it
ufaulav@postacert.difesa.it

MINISTERO DELLA DIFESA

UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Servizio di Protocollo Informatico

MANUALE DI GESTIONE

*per la tenuta del Protocollo Informatico,
della gestione dei flussi documentali
e degli archivi*

(ai sensi dell'art. 5 D.P.C.M. 31.10.2000)

Roma

Release 1.0 del 14.06.2016	Elaborato da	Approvato da
Pag. 1 di 72	IL RESPONSABILE DEL SERVIZIO Funz.Amm.vo Dott. Antonello Buttara antonello.buttara@persociv.difesa.it	IL DIRETTORE Col.g.SPAGNA Dott. Ing. Pierluigi



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufulav@geniodife.difesa.it
ufulav@postacert.difesa.it

MINISTERO della DIFESA UFFICIO AUTONOMO LAVORI Genio Militare per il Ministero della Difesa

Copyright

Il *Manuale di gestione per la tenuta del Protocollo Informatico, della gestione dei flussi documentali e degli archivi* è pubblicato dall' Ufficio Autonomo Lavori Genio Militare per il Ministero della Difesa (di seguito denominato UFAULAV), sito in Roma in Via Firenze 35 , all'interno di Palazzo Esercito – Stato Maggiore Esercito.

Il Manuale norma e dirige il “work flow” (flusso documentale) della corrispondenza di UFAULAV ed impartisce le regole di gestione del flusso documentale e degli archivi. Il manuale è il testo di riferimento per gli “addetti ai lavori” sulla tenuta degli archivi e sulla gestione del flusso documentale.

Le norme in esso contenute rispondono a quanto previsto dal complesso Quadro Normativo Nazionale che disciplina la materia.

Questo *Manuale*, è stato redatto in osservanza alle Direttive ed alla Formazione ricevute dal Segretariato Generale della Difesa/DNA.

La classificazione adottata da UFAULAV utilizza il titolario unico quale strumento per assicurare il vincolo archivistico.

Come previsto dalla normativa (DPCM 31 ottobre 2000, art. 5, comma 3), il *Manuale* è pubblico e consultabile sul Sito Internet Istituzionale della Difesa.

Roma, 14.06.2016

Servizio di Protocollo Informatico

Manuale di Gestione

Release 1.0 del 14.06.2016

Questo documento è di proprietà della Difesa, e non può essere usato da terzi senza preventiva autorizzazione scritta

This document is Ministry of Defense property, and cannot be used by others for any purpose, without prior written consent

Pagina

2/72



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufulav@geniodife.difesa.it
ufulav@postacert.difesa.it

**MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA**

Via Firenze, 35 – 00184 Roma
Indirizzo Telegrafico: UFAULAV – ROMA
Posta elettronica istituzionale: ufulav@geniodife.difesa.it
Posta elettronica certificata: ufulav@postacert.difesa.it



ATTO DI APPROVAZIONE

Ai sensi dell'art. 12 del Decreto del Presidente della Repubblica 25 ottobre 1999, n.556 "Regolamento di attuazione della Legge 18 Febbraio 1997, n. 25"

Approvo la pubblicazione:

"Manuale di Gestione per la tenuta del Protocollo Informatico, della gestione dei flussi documentali e degli archivi dell' Ufficio Autonomo Lavori"

Edizione in data 1.4 GIU. 2016


IL CAPO UFFICIO
(Col. SPAGNA Dott. Ing. Pierluigi)

Servizio di Protocollo Informatico

Manuale di Gestione

Release 1.0 del 14.06.2016

Questo documento è di proprietà della Difesa, e non può essere usato da terzi senza preventiva autorizzazione scritta

This document is Ministry of Defense property, and cannot be used by others for any purpose, without prior written consent

Pagina

3/72



Indice

ACRONIMI.....	7
RIFERIMENTI NORMATIVI.....	8
GLOSSARIO.....	10
CAPITOLO 1 - PRINCIPI GENERALI	15
1. Introduzione	15
2. Ambito di applicazione del Manuale di Gestione	16
3. Area Organizzativa Omogenea	17
4. Servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi.	18
5. Firma Digitale	18
6. Tutela dei dati sensibili e giudiziari	18
7. Entrata in vigore del Manuale di Gestione.....	19
CAPITOLO 2 - I DOCUMENTI NELLA PUBBLICA AMMINISTRAZIONE	19
Tipologia dei documenti	19
CAPITOLO 3 - LA GESTIONE DEI DOCUMENTI – ASPETTI FUNZIONALI	21
1. Principi generali	21
2. Documenti in arrivo	21
3. Documenti in partenza	22
4. Documenti interni.....	22
5. Formazione dei documenti – aspetti operativi	23
6. Sottoscrizione di documenti informatici	24
7. Trasmissione del documento informatico	24
8. Archiviazione del documento informatico.....	24
CAPITOLO 4 – INNOVAZIONE TECNOLOGICA E PROTOCOLLO INFORMATICO	25
1. Dal documento analogico/cartaceo a quello informatico.....	25
2. La rilevanza giuridico-probatoria del Protocollo Informatico	25
3. Copie e duplicati.....	29
CAPITOLO 5 – LA CORRISPONDENZA ED IL FLUSSO DOCUMENTALE	32
1. Indicazione formale delle coordinate di ingresso/uscita della corrispondenza	32
2. Regole base per la trattazione dei documenti in arrivo.	33
3. La trattazione della corrispondenza.....	36
CAPITOLO 6 - SISTEMA DI CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI	58
1. Il Titolare Unico di Classificazione.	58
2. Archivio cartaceo di UFAULAV – Custodia dei documenti analogici	60
3. Archiviazione dei documenti informatici.....	61
CAPITOLO 7 - IL SISTEMA INFORMATICO	61
1. Il Sistema in uso per il Protocollo Informatico, per la Gestione dei Flussi Documentali e la Tenuta degli Archivi.	61
2. L'interoperabilità dei sistemi.	61
3. Descrizione funzionale e operativa del sistema di protocollo informatico	61



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufaulav@geniodife.difesa.it
ufaulav@postacert.difesa.it

4. Abilitazioni di accesso alle informazioni documentali	62
CAPITOLO 8 - IL REGISTRO DI EMERGENZA.....	64
1. Premessa.....	64
2. Attivazione del registro di emergenza.....	64
3. Attività possibili durante l'attivazione del registro di emergenza.....	64
4. Riattivazione del sistema informatico	65
CAPITOLO 9 – REGOLE GENERALI DI SCRITTURA DEI DATI ALL'INTERNO DEL SISTEMA INFORMATICO	66
ALLEGATO A - Atto costitutivo AOO.....	67
ALLEGATO B - Fac - simile lettera di UFAULAV.....	68
ALLEGATO C - Atto di nomina RDS.....	69
ALLEGATO D - Distinta per indirizzi esterni all'Amministrazione Difesa	70
ALLEGATO E - Distinta per Enti Militari	71



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufulav@geniodife.difesa.it
ufulav@postacert.difesa.it

REGISTRAZIONE DELLE 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 fornite ulteriori dettagli nel Glossario.

AOO	Area Organizzativa Omogenea
AOO-GGEN_LAV	Area Organizzativa Omogenea Di UFAULAV
UFAULAV	Ufficio Autonomo Lavori
CAD	D.Lgs. 7 marzo 2005 n. 82
CIRC	Circolare AIPA 7 maggio 2001 n. 28
COBCP	Decreto Legislativo n. 22 gennaio 2004 n. 41
CODPRI	Decreto Legislativo 30 giugno 2003 n. 196
DigitPa	Ente nazionale per la digitalizzazione della Pubblica Amministrazione
DIR	Direttiva SMD-I-004
DPCM	Decreto della Presidenza del Consiglio dei Ministri 31 ottobre 2000
DPR	Decreto del Presidente della Repubblica
DPR	DPR 30 dicembre 200 n. 445
D.Lgs	Decreto Legislativo
l.	Legge
IPA	Indice delle Pubbliche Amministrazioni
PA	Pubblica Amministrazione
PEC	Posta Elettronica Certificata
PEI	Posta Elettronica Istituzionale
PI	Protocollo Informatico
RDS	Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
RPA	Responsabile del Procedimento Amministrativo
UO	Unità Organizzativa



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufaulav@geniodife.difesa.it
ufaulav@postacert.difesa.it

RIFERIMENTI NORMATIVI

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

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

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

Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000. DPCM

Regole tecniche per il PI di cui al DPR 428/98. In attuazione ad alcune disposizioni contenute nel DPR 428/98 è stato emanato il DPCM 31 ottobre 2000, che indica, nel dettaglio, le regole tecniche per l'attuazione della normativa.

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

Disposizioni legislative in materia di documentazione amministrativa. Con il DPR n. 445 si effettua una razionalizzazione e semplificazione della normativa inerente al PI. Viene, pertanto, abrogato (art 77 DPR) il DPR 428/98, facendo salvi gli atti di legge emessi successivamente alla sua entrata in vigore (art 78 DPR n. 445). La normativa inerente al PI viene semplificata e raggruppata negli articoli dal 50 al 70 del DPR. Il DPR è il documento di riferimento principale per il PI.

Circolare AIPA 7 maggio 2001 n. 28 CIRC

Regole tecniche per l'interoperabilità dei sistemi di protocollo informatico.

Decreto Legislativo 30 giugno 2003, n. 196. CODPRI

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

Decreto Legislativo 22 gennaio 2004 n. 41. CODBCP

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

Direttiva SMD-I-004 DIR

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.



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufulav@geniodife.difesa.it
ufulav@postacert.difesa.it

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013. DPCM

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 85 del 2005.

N.B. Le disposizioni del presente Decreto sono in corso di recepimento e implementazione. saranno pienamente attuate entro i termini fissati dallo stesso.

Servizio di Protocollo Informatico

Manuale di Gestione

Release 1.0 del 14.06.2016

Questo documento è di proprietà della Difesa, e non può essere usato da terzi senza preventiva autorizzazione scritta

This document is Ministry of Defense property, and cannot be used by others for any purpose, without prior written consent

Pagina

9/72



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.

a. Area Organizzativa Omogenea (AOO)

Una AOO, (art. 50 comma 4 del DPR) rappresenta un insieme di unità organizzative facenti capo alla stessa Amministrazione che usufruiscono, in modo omogeneo e coordinato, dei servizi informatici per la gestione dei flussi documentali e, in particolare, del servizio di protocollazione. Dove, in precedenza, potevano esistere una serie di registri di protocollo, suddivisi per i diversi livelli gerarchici degli Enti, ora è necessario effettuare una *reductio ad unum* di tali registri, associando un insieme di uffici (le unità organizzative) che devono utilizzare solo ed esclusivamente un unico registro per protocollare i propri atti, con ricadute sugli aspetti pratici, funzionali e logistici. In pratica la costituzione di una AOO comporta la chiusura dei vari Uffici di Protocollo intermedi esistenti prima dell'entrata in funzione del PI.

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

Il RDS è l'altra novità di rilievo introdotta dalla normativa (art. 61 DPR). In sostanza si tratta di una figura ben diversa dal classico Capo Ufficio Posta o figure simili, da sempre presenti nell'A.D. I suoi compiti, elencati nell'art. 61 DPR e nell'art. 4 DPCM, infatti, non sono meramente burocratici, ma hanno, principalmente, una valenza di tipo legale: il RDS *garantisce* il corretto funzionamento (a norma di legge) del sistema di PI implementato nell'AOO anche nei confronti dei cittadini/ditte/altre Pubbliche Amministrazioni.

c. Il Manuale di Gestione (Manuale)

Il Manuale, previsto dall'art. 5 del DPCM, descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del PI. In particolare, il Manuale contiene l'insieme delle regole, certificate dall'AOO, per un corretto ed efficace funzionamento del sistema di protocollo, dei procedimenti amministrativi informatici e del sistema documentale, costituendo, pertanto, la "carta dei servizi" dell'AOO stessa nella quale gli interessati trovano descritte le modalità di gestione del protocollo nei suoi diversi aspetti.

Il Manuale è un documento dinamico, che deve essere aggiornato in dipendenza delle modifiche alle procedure manuali, organizzative ed informatiche applicate alla gestione del protocollo.

Il Manuale deve essere predisposto dal RDS; quale garante dell'esclusiva adozione ed applicazione delle procedure indicate al suo interno siano seguite nell'ambito dell'AOO di pertinenza. Il contenuto del Manuale può essere organizzato da ciascun RDS secondo le specifiche della rispettiva AOO.

d. Titolare e relativa classificazione d'archivio



Unitamente al Manuale, è redatto, per ciascuna AOO, anche il titolare con la relativa classificazione d'archivio.

Il titolare di archivio è uno schema generale di voci logiche rispondenti alle esigenze funzionali e articolate in modo gerarchico, al fine di identificare, partendo dal generale al particolare, l'unità di aggregazione di base dei documenti all'interno dell'archivio.

Tutti i documenti che entrano a far parte dell'archivio dell'AOO, sono soggetti a classificazione. Inoltre, uno stesso documento può essere classificato più volte in base alla molteplicità di funzioni individuate, cercando di contenerne il numero. Tale molteplicità, peraltro, comporta, in un ambiente tradizionale, la duplicazione del documento mentre, in un ambiente digitale, sono duplicate solo le informazioni di collegamento.

Classificare vuol dire attribuire a ciascun documento un indice (di classificazione) inserito in una struttura di voci (piano di classificazione) e associarlo ad una definita unità archivistica generalmente identificata come fascicolo. Per *fascicolo* si intende un raggruppamento di documenti riferiti ad uno stesso procedimento/attività/materia. Le unità archivistiche identificate dal piano di classificazione (tipicamente il fascicolo) possono essere organizzate secondo i seguenti criteri:

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

Attraverso la classificazione deve essere possibile:

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

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

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

La nuova classificazione non va applicata ad archivi già formati in precedenza secondo criteri diversi.

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

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



Il piano di classificazione deve includere:

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

Per ogni voce del piano di classificazione deve essere indicato:

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

Ogni voce del piano di classificazione comprende:

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

e. Amministrazioni Pubbliche

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

f. Archivio

L'archivio è la raccolta ordinata degli atti spediti, inviati o comunque formati dall'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'AOO sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall'affare al 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.

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

- **Archivio corrente**

Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi in



corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse ove non c'è ancora prescrizione in aderenza al Codice Civile che prevede:

- art. 2946: “salvo i casi in cui la legge dispone diversamente i diritti si estinguono per prescrizione con il decorso di 10 anni”;
- l'art. 2947: “il diritto al risarcimento del danno derivante dal fatto illecito si prescrive in 5 anni dal giorno in cui il fatto si è verificato”

- **Archivio di deposito**

È il complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi. Detti documenti non risultano più necessari per il corrente svolgimento di procedimento amministrativo; verso tali documenti può, tuttavia, sussistere un interesse sporadico.

- **Archivio storico**

Costituito da complessi di documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto, alla conservazione perenne;

g. Archiviazione elettronica

Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione (*art. 1 della Deliberazione CNIPA 19 febbraio 2004 n. 11*).

h. Casella di posta elettronica istituzionale [PEI]

La casella PEI è istituita da ciascuna AOO, attraverso la quale possono essere ricevuti i messaggi da protocollare.

i. La Posta Elettronica Certificata (PEC)

La PEC fornisce un servizio di messaggistica che sfrutta gli standard propri della posta elettronica ed assicura al mittente l'attestazione di avvenuta ricezione del messaggio ed al destinatario la garanzia dell'identità del mittente. Questo servizio comprende altre funzionalità per permettere: confidenzialità, integrità, tracciabilità e storicizzazione del messaggio.

La PEC è strettamente connessa all'IPA, ove sono pubblicati gli indirizzi di posta certificata associati alle AOO e alle funzioni organizzative previste dalle Pubbliche Amministrazioni. È necessario tenere presente che, utilizzando la PEC, viene rilasciata al mittente una ricevuta di avvenuta consegna del messaggio, contestualmente alla disponibilità del messaggio stesso nella casella di posta elettronica del destinatario, **indipendentemente dall'avvenuta lettura da parte del soggetto destinatario**. Tale ricevuta indica al mittente che il messaggio è effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario e certifica la data e l'ora dell'evento.

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

j. Documento informatico

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



k. Documento analogico

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

l. Dati Sensibili

I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (*art. 4 comma 1, lett. d CODPRI*)

m. Fascicolazione

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

n. Fascicolo

Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento/processo amministrativo, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se è non è infrequente la creazione di fascicoli formati di insieme di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc.).

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



IL MANUALE DI GESTIONE

TESTO

CAPITOLO 1 - PRINCIPI GENERALI

1. Introduzione

Tutte le pubbliche amministrazioni devono provvedere a realizzare o revisionare sistemi informativi automatizzati e finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi, come previsto dall'art. 50 del DPR 445/2000.

Tale normativa è stata ideata al fine di consentire di:

- accrescere l'efficienza delle amministrazioni attraverso l'eliminazione dei registri cartacei, la diminuzione degli uffici di protocollo e la razionalizzazione dei flussi documentali;
- migliorare la trasparenza dell'azione amministrativa, per il tramite di strumenti che rendono possibile un effettivo esercizio del diritto di accesso alla documentazione amministrativa da parte dei soggetti interessati.

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

In quest'ottica, ciascuna amministrazione:

- definisce un adeguato piano di sviluppo dei sistemi informativi automatizzati;



- individua le proprie Aree Organizzative Omogenee (AOO) e le relative Unità Organizzative Responsabili (UO);
- istituisce i servizi per la gestione informatica dei documenti, dei flussi documentali e degli archivi;
- nomina il Responsabile del Servizio per la tenuta del Protocollo Informatico, della gestione dei flussi documentali e degli archivi e suo Vicario;
- redige e adotta il manuale di gestione del protocollo informatico;
- introduce un sistema informatico per la gestione documentale.

2. Ambito di applicazione del Manuale di Gestione

Il presente manuale disciplina la gestione del sistema per la tenuta del protocollo informatico e dei flussi documentali dell' Ufficio Autonomo Lavori del Genio Militare per il Ministero della Difesa.

Il protocollo informatico è strumento del sistema di gestione dei flussi documentali. Attraverso l'integrazione con le procedure di gestione dei provvedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti, realizza condizioni operative per il miglioramento del flusso informativo e documentale all'interno dell'Ente, anche ai fini dello snellimento e della trasparenza dell'azione amministrativa. Il protocollo ha validità giuridica dell'effettivo ricevimento e spedizione di un documento.

Alla tenuta del protocollo informatico di UFAULAV è preposto apposito "Servizio di Protocollo Informatico", adiacente all'Ufficio del Capo Ufficio, che tra l'altro svolge anche un ruolo di coordinamento e di indirizzo nei confronti delle sezioni dell'ente, al fine di garantire uniformità nell'attività di gestione del flusso documentale e di archiviazione.

L'introduzione del "Protocollo Informatico" ha un impatto concreto nella gestione dei flussi documentali e degli archivi, eliminando di fatto i vecchi microsistemi di classificazione "locali", adottati all'interno delle singole sezioni (ove presenti), a favore di un sistema "unico" di fascicolazione (titolario unico) per UFAULAV.

L'ufficio dovrà gradualmente migrare verso una gestione informatizzata degli archivi, rispettando il vincolo archivistico mediante un "work-flow" dei documenti strutturato all'interno del titolario unico. In pratica, in un sistema strutturato di gestione e tenuta dei documenti, ciò che conta non è il documento in quanto tale, ma l'insieme delle relazioni che quel documento ha con tutti gli altri



(cioè l'intero archivio) e, più in particolare, con quelli che riguardano un medesimo procedimento amministrativo.

Il protocollo informatico in sé, infatti, non può essere concepito solo come un dispensatore asettico di numeri sequenziali, né può essere progettato come semplice trasposizione su un supporto elettronico del registro di protocollo cartaceo. In un sistema informativo documentale moderno, il protocollo deve diventare uno snodo irrinunciabile e una risorsa strategica per il buon andamento dei documenti trattati e dei procedimenti amministrativi. Per raggiungere questi obiettivi, devono essere garantiti l'interoperabilità, la trasparenza e il controllo dell'azione amministrativa attraverso i documenti che ogni Pubblica Amministrazione produce durante la propria attività pratica o l'esercizio delle proprie funzioni.

Proprio a questo fine è orientato l'insieme delle norme recentemente approvate in materia di gestione documentale e fra loro riunificate nel Testo Unico sulla documentazione amministrativa. La parte relativa al protocollo informatico ha come strategia di base la trasformazione del sistema documentario in un sistema informativo specializzato e altamente qualificato.

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

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

Questo manuale è pertanto rivolto a tutti coloro che lo utilizzano 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.

Le normative in vigore impongono anche la creazione di un archivio cartaceo.

3. Area Organizzativa Omogenea

L'Area Organizzativa Omogenea (AOO) denominata UFAULAV – Ufficio Autonomo Lavori è composta dall'insieme della UO articolate come riportato nell'atto costitutivo a pag.67 del seguente manuale. Alla predetta AOO è assegnato il codice identificativo univoco nell'ambito del Ministero della Difesa "GGEN_LAV". L'AOO GGEN_LAV è costituita a sua volta da UO – Unità Organizzative, un complesso di risorse umane e strumentali cui sono state affidate competenze omogenee che sostanzialmente ricalcano la struttura ordinativa e nell'ambito delle quali i dipendenti assumono la responsabilità nella trattazione di documenti o procedimenti amministrativi.



Il sistema è aperto alla creazione di Gruppi di Lavoro e/o Strutture di Progetto in base a specifiche esigenze all'interno dell'AOO GGEN_LAV.

4. Servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi.

E' il servizio al quale sono attribuite le funzioni di coordinamento relative alla gestione documentale, ossia tutte quelle attività finalizzate alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi.

A capo di tale Servizio è preposto un dirigente o un funzionario dotato di specifica preparazione professionale tecnico-archivistica.

Il Responsabile del Servizio (RDS) per la tenuta del Protocollo Informatico, della Gestione dei Flussi Documentali e degli Archivi di UFAULAV assume il ruolo di coordinatore delle attività di classificazione e fascicolazione, con particolare riferimento alla gestione degli archivi informatici, ed al flusso documentale degli atti amministrativi. Il RDS si avvale della collaborazione di un Vicario.

Il Software adottato è quello istituzionale fornito dal Segretariato Generale della Difesa (SGD).

5. Firma Digitale

La gestione digitale del protocollo informatico prevede l'uso della firma digitale. Il personale della Difesa è dotato di Smart-Card Difesa (CMD) con un certificato di firma rilasciato da Ministero della Difesa – PKI di Firma Qualificata. La firma elettronica utilizza un algoritmo “sha256RSA”. I riferimenti sono disponibili all'URL: www.pki.difesa.it/firmadigitale.pdf

La firma digitale è impiegata per la protocollazione ed invio (contestuali) degli originali informatici, nonché per la certificazione delle copie informatiche di originali cartacei.

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

6. Tutela dei dati sensibili e giudiziari

La tutela dei dati per i quali è necessaria una specifica gestione, è assicurata dagli strumenti elettronici adottati con il software del Protocollo Informatico in uso. In particolare, il software del Protocollo Informatico assicura l'adozione delle misure minime di sicurezza e gestione dei dati personali nei termini di legge previsti (comma a, b, c, d, e, f, h dell'art. 34 del CODPRI).



7. Entrata in vigore del Manuale di Gestione

Le regole indicate nella presente versione, “Release 1.0” del 14.06.2016, del presente manuale decorrono dal 7° giorno dalla firma del Capo Ufficio. Il Manuale in vigore è sempre l’originale informatico pubblicato sul sito istituzionale della Difesa.

CAPITOLO 2 - I DOCUMENTI NELLA PUBBLICA AMMINISTRAZIONE

Tipologia dei documenti

1. Il documento amministrativo

Per documento amministrativo si intende ogni rappresentazione grafica, fotocinematografica, informatica o di qualsiasi altra specie del contenuto di atti, fatti o cose giuridicamente rilevanti, anche interni, prodotti e acquisiti ai fini dell’attività amministrativa, così come prevede l’art. 22 comma 2 della legge 7 agosto 1990, n. 241 nonché del Decreto Legislativo 30/07/1999 n. 281.

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

2. Il documento informatico

Per documento informatico si intende qualsiasi supporto informatico contenente dati o informazioni aventi efficacia probatoria, cioè la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, così come previsto dall’art. 3 della legge 23 dicembre 1993, n. 547. Esso si configura come un documento digitale sottoscritto con firma digitale.

Secondo le norme del testo unico, il documento informatico, per essere considerato tale deve soddisfare il requisito legale della forma scritta. Perché tale affermazione sia vera, il documento informatico è tale solo se sottoscritto con firma digitale.

Pertanto, tutti i documenti provenienti dall’esterno sono considerati legalmente validi se soddisfano i requisiti di cui al precedente capoverso.



Ai sensi dell'art. 53, comma 5 del DPR 445/2000 i documenti interni informatici all'AOO, devono essere protocollati. Il software in uso prevede che la protocollazione avvenga con l'apposizione della firma digitale.

Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni, inviati/ricevuti all'interno o all'esterno, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

Per la formazione e la gestione di documenti informatici per i quali non è prevista la sottoscrizione, l'Amministrazione utilizza, per economia di gestione e di uniformità formale, ovvero per necessità di rendere, all'occorrenza, validi a tutti gli effetti di legge anche i documenti in questione, le stesse tecnologie e procedure utilizzate per i documenti che rispondono ai requisiti minimi di legge sopra richiamati.

3. Il documento analogico

Per documento analogico si intende un documento amministrativo "formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale".

Un documento analogico/cartaceo può essere prodotto con strumenti analogici, quali lettera scritta a mano o a macchina, o con strumenti informatici quale lettera prodotta tramite un sistema di videoscrittura o "text editor" e poi stampata. In quest'ultimo caso come originale si considera quello cartaceo stampato su carta intestata dotato di firma autografa. Questo originale è analogico.

Un originale è un documento nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali comprendente tutti gli elementi di garanzia e di informazione del mittente e destinatario.

Una minuta è invece un originale del documento conservato "agli atti", cioè nel fascicolo relativo al procedimento amministrativo trattato.

Un documento analogico può essere convertito in documento informatico tramite opportune procedure di scannerizzazione, purché al termine della procedura l'operatore apponga la propria firma (digitale) che attesti la veridicità tra l'originale e la copia informatica. In tal



caso, mediante l'apposizione della firma digitale, il documento informatico diventa copia informatica dell'originale analogico.

CAPITOLO 3 - LA GESTIONE DEI DOCUMENTI – ASPETTI FUNZIONALI

1. Principi generali

I documenti, analogici e informatici, vengono gestiti in relazione al loro formato, e sono suddivisi nel seguente modo:

- in ingresso;
- in uscita;
- interno.

La gestione documentale in generale si basa sui principi di:

- **centralizzazione della posta in ingresso e flusso discendente. La totale corrispondenza indirizzata a UFAULAV entra e viene registrata attraverso un unico punto dal Servizio per la tenuta del protocollo informatico che provvede alla protocollazione e successivo inoltro al Capo Ufficio;**
- **delega al Capo del Servizio Amministrativo che ha facoltà, previa autorizzazione, di trasmettere direttamente i documenti sia informatici sia analogici all'esterno dell'AOO.**

Il controllo della completezza formale e sostanziale della documentazione pervenuta e soggetta alle operazioni di registrazione spetta al personale dell'UO interessata alla tematica che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente, specificando le eventuali problematiche del caso.

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

2. Documenti in arrivo

Per documenti in ingresso si intendono i documenti che hanno rilevanza giuridico-probatoria, comunque acquisiti dall'AOO nell'esercizio delle proprie funzioni.



Il Servizio di Protocollo Informatico di questa AOO potrà accettare solo la corrispondenza inviata secondo quanto previsto all'interno del presente Manuale.

In caso contrario la corrispondenza non sarà accettata e restituita al mittente.

3. Documenti in partenza

Per documenti in partenza si intendono quei documenti a rilevanza giuridico-probatoria, prodotti dal personale autorizzato di UFAULAV nell'esercizio delle funzioni, incarichi e deleghe attribuite ed indirizzati ad enti esterni alla Direzione stessa.

4. Documenti interni

Per documenti interni si intendono quelli scambiati tra le diverse UO afferenti alla medesima AOO ad eccezione degli Appunti e delle Note.

In tutti quei casi nei quali tra gli indirizzi per competenza o per conoscenza di un documento vi sia una UO interna all'AOO, tale informazione viene esplicitamente dichiarata all'interno del sistema informatico che provvederà ad inviare, automaticamente, quel documento sulla scrivania virtuale di competenza dell'UO destinataria.

Quel documento sarà protocollato solo in uscita dalla UO mittente.

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

I documenti interni si distinguono in:

- a) documenti di preminente carattere informativo;
- b) documenti di preminente carattere giuridico-probatorio.

I documenti interni di preminente carattere informativo sono memorie informali, appunti, messaggi, brevi comunicazioni di rilevanza meramente informativa scambiate tra Sezioni/Uffici. L'invio di tali documenti può essere fatto in copia (i documenti ricevuti in copia non necessitano di fascicolazione).

I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti dal personale nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi, e, come tali, devono essere protocollati secondo le disposizioni previste.



Il Protocollo Informatico prevede che la fascicolazione dei documenti interni sia affidata ad un RPA delle UO, incaricato di individuare il fascicolo relativo al procedimento amministrativo. Tale fascicolazione deve essere eseguita obbligatoriamente nella fase di predisposizione del documento.

Nella fase di registrazione dell'atto (segnatura) il sistema impegna un numero di protocollo progressivo di Direzione (nessuna differenza fra documento in partenza interno ed esterno).

5. **Formazione dei documenti – aspetti operativi**

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

a. Documenti in partenza.

Un documento originato per essere inoltrato in modo formale deve avere i seguenti requisiti:

- trattare un unico argomento indicato in maniera sintetica nello spazio riservato all'oggetto;
- avere ad una sola registrazione di protocollo.

b. Documenti in ingresso.

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

Il documento cartaceo in arrivo è riprodotto digitalmente mediante scansione ed assunto a protocollo con il software di protocollo informatico in uso a UFAULAV.

L'operatore che effettua la scansione dovrà:

- Firmare digitalmente la copia informatica. In tal modo attesta che la copia informatica è esattamente fedele all'originale cartaceo custodito agli atti dell'ente;
- Inviare al Capo Ufficio, a mezzo del protocollo informatico, la copia informatica riportante la propria firma digitale;
- Custodire presso l'archivio l'originale cartaceo, disponibile a chi ne abbia titolo alla visione ed uso secondo quando previsto dalla normativa in vigore.

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



6. Sottoscrizione di documenti informatici

Tutta la documentazione amministrativa confluyente all'interno del sistema di PI e gestione documentale viene firmata nel formato PDF/A.

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

7. Trasmissione del documento informatico

Nei casi previsti dalla legge per i quali si renda necessario disporre di una ricevuta di ricezione della corrispondenza inviata, viene utilizzata la casella di PEC, sempreché anche il corrispondente ne disponga.

Parimenti si utilizzerà la casella di PEC ogni qualvolta che il corrispondente ne richieda esplicitamente l'impiego.

Negli altri casi il veicolo privilegiato di comunicazione è la casella di PEI.

8. Archiviazione del documento informatico

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



CAPITOLO 4 – INNOVAZIONE TECNOLOGICA E PROTOCOLLO INFORMATICO

1. Dal documento analogico/cartaceo a quello informatico.

In aderenza alla normativa vigente (art. 40 del CAD) UFAULAV produce esclusivamente documenti originali informatici, mediante il software di Protocollo Informatico in uso. Tali originali informatici potranno essere riprodotti in copia analogica ove strettamente necessario e/o su richiesta degli Organismi, Enti, Dipartimenti, etc. che, per esplicita richiesta, non accettano originali informatici, bensì trattano solo copie analogiche.

I documenti analogici in ingresso vengono dematerializzati ed inseriti nel protocollo informatico, in modo che l'intero flusso documentale venga gestito in maniera elettronica.

I documenti gestiti sono classificati come documenti in arrivo, documenti in partenza e documenti interni.

2. La rilevanza giuridico-probatoria del Protocollo Informatico

a. Documenti da protocollare

Sono soggetti a protocollazione tutti quei documenti utilizzati ai fini dell'attività amministrativa ovvero quei documenti che possono avere una rilevanza giuridico-probatoria e comunque nel pieno rispetto dell'art. 1 comma "a" e "b" del D.P.R. 28 dicembre 2000 n. 445.

b. La registrazione dei documenti e la segnatura di protocollo (ex. Art. 55 DPR 445/2000). Unicità del protocollo informatico, modalità di produzione delle registrazioni.

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

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

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

Il numero di protocollo è costituito da sette cifre numeriche.



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

Non è consentita la protocollazione di un documento già protocollato. Tutti gli atti protocollati sono elencati nel registro di protocollo.

Il registro di protocollo è un atto pubblico originario che certifica l'effettiva ricezione e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

c. Elementi obbligatori per la registrazione di protocollo. Linee guida per l'inserimento dei dati.

Ogni documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi deve essere protocollato.

Il sistema, per ciascuna registrazione di protocollo, prevede l'inserimento dei dati previsti all'art. 53 DPR con le caratteristiche riportate di seguito:

- **numero di protocollo del documento**: è generato automaticamente dal sistema e registrato in forma non modificabile;
- **data di registrazione di protocollo**: è assegnata automaticamente dal sistema e registrata in forma non modificabile;
- **mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti**: sono registrati in forma non modificabile e reperiti nella tabella dei corrispondenti del sistema informatico;
- **oggetto del documento**: per i documenti informatici, è registrato automaticamente. Per i documenti analogici che vengono scansionati è registrato manualmente in forma non modificabile secondo regole generali di codifica;
- **data e protocollo del documento ricevuto**: inseriti automaticamente dal sistema al momento della protocollazione;
- **l'impronta del documento informatico**: calcolata automaticamente dal sistema con l'algoritmo SHA-256.



I documenti informatici provenienti da una P.A. sono dotati di file “*segnatura.xml*”. Tali dati sono caricati dal sistema automaticamente, senza possibilità di modifica da parte dell’operatore.

Anche il campo oggetto per i messaggi provenienti per posta elettronica non è modificabile perché importato automaticamente dall’oggetto della mail pervenuta all’AOO.

d. Protocollo differito

UFAULAV non attua il protocollo differito nel normale esercizio. Tuttavia, potrebbe eccezionalmente verificarsi che, o a causa di un temporaneo ed eccezionale carico di lavoro o a causa di motivazioni non dipendenti dalla volontà del Servizio di Protocollo Informatico, non sia possibile protocollare la corrispondenza in entrata nella medesima giornata lavorativa. Per tale mancata registrazione di protocollo può venire meno un diritto di terzi. In tal caso, il responsabile del servizio di protocollo, chiede l’autorizzazione al Direttore per impiegare il protocollo differito con motivato provvedimento.

Il protocollo differito consiste nel differimento dei termini di registrazione di uno o più procedimenti amministrativi. Nel provvedimento con il quale vengono individuati i documenti da ammettere alla registrazione differita, saranno inserite le cause che hanno prodotto la protocollazione differita e la data entro il quale tale procedimento deve assolutamente essere assunto a protocollo.

Il protocollo differito si applica solo ai documenti in arrivo, per tipologie omogenee ed in casi del tutto eccezionali autorizzati di volta in volta dal Direttore dell’Ente.

L’autorizzazione è chiesta dal Capo Servizio Protocollo Informatico e concessa dal Direttore. L’autorizzazione concessa è mantenuta agli atti.

e. La segnatura di protocollo

La segnatura di protocollo è l’apposizione al documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo. La segnatura di protocollo assicura l’univocità di un documento in modo inequivocabile.

La registrazione e la segnatura sono contestuali ed hanno natura di atto pubblico.

I documenti informatici in ingresso prodotti dalla PA pervengono con il file di segnatura associato. Per tutti gli altri documenti privi di segnatura e che devono essere assunti a protocollo, il software in uso consente la generazione ed apposizione al documento di una segnatura. Non è possibile protocollare un documento privo di segnatura.



Sui documenti in uscita la segnatura di protocollo viene apposta al momento della firma digitale del documento.

Il file “*segnatura.xml*” è allegato a tutti i documenti in uscita via PEI.

Il formato della segnatura di protocollo dell’AOO-GGEN, conformemente alla normativa, prevede 4 dati:

- Codice dell’Amministrazione: **M_D**
- Codice dell’AOO: **GGEN_LAV**
- Numero di protocollo: **1234567**
- Data di registrazione: **gg-mm-aaaa**
- Esempio di segnatura di protocollo: **M_D GGEN_LAV 1234567 01-01-2016**

f. Annullamento di una registrazione di protocollo

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

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

È altresì possibile annullare una registrazione di protocollo per un documento erroneamente entrato nel patrimonio documentale dell’AOO.

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

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

Le richieste di annullamento devono essere inviate al RDS con lo strumento del protocollo informatico; tali richieste devono contenere il numero di protocollo da annullare, i motivi dell’annullamento e, se il documento è stato successivamente protocollato correttamente,



l'indicazione del nuovo numero di protocollo attribuito al documento. L'annullamento di un documento informatico è effettuato mediante l'uso del software di protocollo informatico.

Qualora il documento informatico annullato esista anche in formato cartaceo, il documento è da considerarsi annullato solo attraverso l'apposizione della dicitura a stampa/timbro «annullato», che deve essere effettuata in maniera tale da consentire la lettura delle informazioni registrate in precedenza e da non alterare le informazioni registrate negli elementi obbligatori del protocollo.

g. Il registro giornaliero di protocollo

Al fine di tutelare l'integrità e la regolarità delle registrazioni, quotidianamente è effettuata la firma digitale del registro giornaliero.

Il registro di protocollo è gestito dal software del protocollo informatico e custodito all'interno del server sito presso il Centro elaborazione dati unificato dell'area T.A. di Via Marsala.

3. Copie e duplicati

Il Codice dell'amministrazione digitale (CAD) modificato dal d.lgs. 235/2010, introduce le definizioni di copie e duplicati informatici che sono utilizzate per disciplinare la complessa questione della copia di un documento su un medium differente da quello originale (copia informatica di documento cartaceo e copia cartacea di documento informatico), nonché quella della copia informatica di un documento informatico.

Al riguardo, il Codice per la PA digitale riporta che "*Con decreto del Presidente del Consiglio dei Ministri possono essere individuate 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 sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.*"

Per la trattazione specifica della materia, ampia e quanto mai in continua evoluzione, si rimanda sempre e comunque alle norme di legge in vigore. Quanto di seguito citato si riferisce alle norme in vigore alla data della pubblicazione del presente Manuale.

a. La “copia informatica di documento analogico” (art. 22 CAD).



E' definita come il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto. Si tratta, per esempio, del documento “.pdf” che risulta dalla scansione di un documento analogico.

Il CAD implica la possibilità del rilascio, da parte di pubblico ufficiale autorizzato, di copie autentiche o di copie conformi di un documento originale cartaceo su supporto informatico elaborate con software che acquisisce "per immagine", a condizione che il relativo file sia formato secondo le specifiche previste, con la stessa efficacia probatoria garantita dal codice civile secondo le regole ordinarie.

L'art. 22, comma 1 del citato CAD, dispone che le copie informatiche di documenti analogici, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno la medesima efficacia probatoria degli originali se ad esse è apposta o associata, da parte di colui che le spedisce o rilascia, una firma digitale o altra firma elettronica qualificata.

Sempre l'art. 22, nei comma 2 e comma 3, dispone che le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la medesima efficacia probatoria degli originali se:

- **la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71, o ancora se**
- **sono formate nel rispetto delle regole tecniche di cui all'articolo 71 e se la loro conformità all'originale non è espressamente disconosciuta. Questo significa che, in difetto di autenticazione da parte di pubblico ufficiale, le semplici copie informatiche di documento cartaceo sono reputate conformi all'originale, salva la possibilità di disconoscimento da parte di chi vi fosse interessato.**

Nell'AOO-GGEN_LAV il rilascio di tale copia è normalmente eseguito dal Servizio di Protocollo Informatico nella fase di protocollazione degli originali cartacei in ingresso.

Il software in uso per il protocollo informatico obbliga l'operatore ad attenersi a quanto previsto dall'art. 22 comma 1 del CAD, mediante apposizione della propria personale firma digitale alla scansione dell'originale analogico.

Il IV comma dell'art. 22 prosegue disponendo che "Le copie formate ai sensi dei commi 1, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti per legge, sia pure con l'eccezione di quanto stabilito al V comma.

b. La “copia informatica di documento informatico” (art. 23 bis - CAD).



E' definita come il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari. Si tratta, per esempio, del documento “.pdf” che risulta dalla effettuazione di una copia, cioè dalla registrazione in un diverso formato, di un documento “.doc”.

c. Il “duplicato informatico” (art. 23 bis - CAD).

E' definito come il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario. Si tratta, per esempio, della duplicazione di un documento “.doc” in un altro documento “.doc”.

L'art. 23-bis, relativo ai duplicati e copie informatiche di documenti informatici rimanda sostanzialmente alle regole tecniche, affermando che:

- ***i duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche di cui all'articolo 71;***
- ***le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratti se la loro conformità all'originale, in tutti le componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta.***

Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

d. Copie analogiche di documenti informatici (art. 23 CAD).

Le copie analogiche di documenti informatici devono soddisfare i seguenti requisiti:

- 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. L'AOO-GGEN_LAV produce tali copie.
- se manca la dichiarazione di conformità, 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.

Pertanto, all'interno dell'AOO-GGEN_LAV la copia conforme cartacea di un originale informatico è prodotta come descritto nel Capitolo 5 del Manuale.

e. Copie analogiche di documenti analogici.

Nulla di variato rispetto a quanto già in vigore per le copie conforme cartacee di originali analogici. La copia conforme cartacea di un originale cartaceo è un atto o un documento che ne riproduce un altro, la cui fedele corrispondenza all'originale è attestata dalla dichiarazione formale di un pubblico ufficiale per legge autorizzato a tali funzioni. L'attestazione di conformità non certifica la genuinità del documento originale, ma solo la fedele corrispondenza di esso alla copia.

CAPITOLO 5 – LA CORRISPONDENZA ED IL FLUSSO DOCUMENTALE

1. Indicazione formale delle coordinate di ingresso/uscita della corrispondenza

a. L'indirizzo postale per la corrispondenza cartacea (tradizionale) di UFAULAV è:

MINISTERO DELLA DIFESA – UFFICIO AUTONOMO LAVORI – GENIO MILITARE PER IL MINISTERO DELLA DIFESA – Via Firenze, n. 35 – 00184 ROMA.

Il personale della Segreteria è autorizzato al ritiro della corrispondenza secondo gli orari di apertura consentiti dall'Ufficio Postale sito in Via Firenze, n.36 e di seguito riportati:

- Dal Lunedì al Giovedì dalle ore 10,00 alle ore 14,00
- Venerdì, dalle ore 10,00 alle ore 12,00.

Tali orari non sono rispettati per il ritiro della documentazione afferente le Procedure di Gara, in quanto le offerte di appalto che pervengono all'Ufficio Postale, previo avviso telefonico degli impiegati preposti alla distribuzione della posta, vengono ritirati dal Lunedì al Giovedì dalle ore 08,00 alle ore 16,30 ed il Venerdì dalle ore 08.00 alle ore 14.00.

Ai fini della mera protocollazione dei documenti in entrata (informatici ed analogici), il personale del Servizio Protocollo Informatico, addetto alla ricezione e protocollazione della posta di UFAULAV osserva il seguente orario lavorativo:

- Lunedì e Martedì : ore 08,00 – 17:30;
- Mercoledì e Giovedì: ore 08.00 – 16,30;



- Venerdì: ore 08,00 – 14,00.

b. Gli indirizzi di corrispondenza elettronica di UFAULAV sono i seguenti:

- ufulav@postacert.difesa.it – indirizzo di Posta Elettronica Certificata PEC – tutte le comunicazioni sono ricevute con il software del Protocollo Informatico, hanno carattere di ufficialità e vengono assunte a protocollo. La PEC assicura inoltre la certezza di trasmissione, ricezione e distribuzione delle ricevute di trasmissione con data ed ora altrettanto certi.
- ufulav@geniodife.difesa.it – indirizzo di Posta Elettronica Istituzionale PEI – tutte le comunicazioni sono ricevute con il software del Protocollo Informatico, hanno carattere di ufficialità e vengono assunte a protocollo.

2. Regole base per la trattazione dei documenti in arrivo.

a. La protocollazione dei documenti analogici

I documenti pervenuti vengono protocollati secondo quanto già specificato.

Se gli allegati sono su supporto informatico (CD – DVD - USB), gli stessi saranno inseriti nel sistema durante il processo di protocollazione da parte degli operatori del servizio di protocollo.

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

In ogni caso i supporti informatici non vengono riconsegnati al mittente ma rimangono associati al documento cartaceo originario.

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

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

Il documento analogico originale viene custodito in un apposito archivio presso l'AOO ai soli fini di eventuali verifiche, con le modalità più avanti descritte.

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

Il Servizio di Protocollo Informatico di questa AOO potrà accettare solo la corrispondenza di competenza ossia solo quella riportante l'indicazione formale delle coordinate in ingresso/uscita citate al precedente paragrafo, ad esclusione di quella indirizzata "ad personam" ossia diretta al personale in servizio a UFAULAV. In caso contrario la corrispondenza non potrà essere accettata e sarà restituita al mittente.



Ai sensi del D.M. n. 55/2013 UFAULAV può accettare solo fatture in formato elettronico recapitate attraverso il Sistema di Interscambio. Pertanto, a tali documenti, pervenuti a mezzo posta elettronica ovvero in formato cartaceo, non possono essere assunti a protocollo e saranno restituiti al mittente in quanto improcedibili.

La corrispondenza personale (“ad personam”) non può essere aperta, né protocollata, ma deve essere consegnata al destinatario che ne valuterà il contenuto, nel caso dovesse riguardare l’istituzione, provvederà a farla protocollare.

b. Documenti esclusi dalla protocollazione

I documenti di seguito specificati sono esclusi dalla registrazione di protocollo, a meno che gli stessi non siano inviati/trasmessi in forma di allegato a specifica lettera di trasmissione con segnatura di protocollo:

- note di ricezione circolari;
- note di ricezione altre disposizioni;
- materiali statistici;
- giornali;
- riviste;
- libri;
- materiali pubblicitari;
- inviti a manifestazioni che non attivino procedimenti amministrativi;
- documenti già soggetti a registrazione particolare dell’Amministrazione;
- fogli di viaggio;
- note caratteristiche;
- rapporti informativi;
- registro delle presenze;
- modelli 730;
- esposti anonimi;
- informazioni elettroniche superiori ai 30 mega dimensione oltre la quale il sistema non registra.



c. Gestione di documenti contenenti dati sensibili e giudiziari

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

Tali documenti vengono definiti come *documenti sensibili*.

Rientrano tra i documenti sensibili quelli appartenenti alle seguenti tipologie:

- certificati (richiesti da questo Ufficio all'atto di aggiudicazione di lavori in seguito a gara di appalto) rilasciati dai vari Tribunali relativi a Casellario Giudiziale, insussistenza di procedimenti per le misure di prevenzione, certificato in cui risulti che la ditta non si trovi in stato di liquidazione, di fallimento, di concordato o di amministrazione controllata;
- certificato dell'Agenzia delle Entrate in cui risulti l'inesistenza di violazioni definitivamente accertate rispetto agli obblighi relativi al pagamento di imposte e tasse della ditta;
- certificati medici;
- documenti legati a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
- documenti della cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- le tipologie di documenti individuate dalla normativa vigente (in particolare l'art. 24 della legge 7 luglio 1990; Art. 8 del DPR 27 giugno 1992 n. 352 e la serie di norme collegate al CODPRI

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

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

Per quanto attiene alla successiva gestione informatica, rientrano nella casistica dei documenti sensibili anche quei documenti con la classifica di sicurezza nazionale NCC (non classificato controllato).



3. La trattazione della corrispondenza.

a. Corrispondenza cartacea.

La corrispondenza cartacea indirizzata a UFAULAV deve necessariamente transitare per l'Ufficio Postale di RAMDIFE. Eventuali corrieri dovranno consegnare a mano la posta all'Ufficio Postale di RAMDIFE oppure al personale addetto alla Segreteria di UFAULAV, comprese le notifiche che prevedono il riconoscimento formale di un addetto alla ricezione e le offerte di appalto.

Il personale operante per il Servizio di Protocollo Informatico è preposto al prelevamento (anche la speciale spedizione registrata) presso l'Ufficio Postale di RAMDIFE ed è regolarmente autorizzato al trattamento dei dati personali.

Tutti i documenti analogici ricevuti sono protocollati come precedentemente specificato. La firma digitale dell'operatore attesta la conformità all'originale cartaceo. L'originale cartaceo viene conservato presso l'archivio.

Per i documenti pervenuti in modalità analogica, deve essere tenuto in considerazione il tempo medio necessario per le attività di de-materializzazione.

Il software del protocollo informatico assicura la **contemporaneità** fra la protocollazione e la segnatura di protocollo.

Si precisa che il software per la gestione del protocollo informatico consente di effettuare la chiusura del Registro di Protocollo alle ore 24,00 di ogni giorno e la riapertura dello stesso alle ore 00,01 del giorno successivo, apponendo automaticamente la firma dell'RDS.

I. Buste e plichi spediti a mezzo posta raccomandata A/R.

L'Ufficio riceve posta raccomandata presso l'Ufficio Postale di RAMDIFE secondo i sistemi tradizionali. Tuttavia a tale sistema deve essere preferito il flusso elettronico con Posta elettronica Certificata (PEC) ove attuabile (mittente e destinatario dispongono di casella di PEC attiva e funzionante - art. 48 del CAD), in virtù dell'implementazione del Protocollo Informatico nella PA.

Il contenuto delle buste giunte sarà scansionato nella sua totalità (se il documento è nei formati previsti per la scansione) ovvero sarà scansionata la lettera di trasmissione, unitamente alla cartolina indicante la data di ricezione e la firma dell'addetto della Segreteria di UFAULAV. La cartolina sarà successivamente riconsegnata all'Ufficio Postale.



II. Buste e plichi contenenti documenti classificati.

Tale corrispondenza può essere veicolata solo con i mezzi tradizionali cartacei, in osservanza delle norme in vigore per la trattazione dei documenti classificati.

III. Buste e plichi contenenti documenti di carattere privato per il personale impiegato come da tabelle organiche.

La posta per l'Ufficio, indirizzata a Dirigente e/o funzionario e/o impiegato presso UFAULAV, dovrà riportare l'indicazione del Grado/Qualifica, Cognome e Nome e la dicitura completa del /Ufficio/Sezione ove il destinatario opera.

IV. Buste chiuse contenenti documentazione amministrativa.

Tutte le buste chiuse indirizzate all'Ufficio saranno aperte, tranne che non riportino chiaramente diciture e/o scritte che consentano visivamente di ricondurle a specifici casi (es: Procedure di gara e/o contratti coperti da segreto, documenti classificati, etc...). L'apertura della busta nasce dall'esigenza di permettere quanto previsto dall'art. 55 dell'ex DPR 445/2000 (segnatura di protocollo) e cioè mediante l'associazione in maniera univoca e non modificabile del documento in essa contenuto e riconducibile a quel numero di protocollo.

Le buste chiuse che dovessero erroneamente pervenire direttamente a Uffici/Sezioni senza che sia stata effettuata la registrazione e segnatura del procedimento amministrativo in esse contenuto dovranno essere immediatamente consegnate al Servizio di Protocollo Informatico per quanto previsto a norma di legge, pena la nullità dell'assunzione al protocollo ufficiale dell'Ufficio del procedimento amministrativo stesso.

V. Fogli che non possono essere convertiti in copia elettronica con gli strumenti informatici in possesso della Direzione.

Si fa riferimento a tutti quei formati dei fogli superiori al formato A3 (disciplinati dalle "PRINCIPALI NORME PER LA RAPPRESENTAZIONE DEL DISEGNO TECNICO" di seguito riportata in tabella), che non possono essere fisicamente scansionati e trasformati/riprodotti in formato elettronico con gli strumenti informatici di cui l'Ufficio è dotato; si considerano come tali anche i formati multipli superiori al A4.

PRINCIPALI NORME DI DISEGNO TECNICO



ARGOMENTO	Norme UNI	Norme ISO
<u>Principi generali:</u>		
. Fogli	UNI EN ISO 5457:02	5457:99
. Tipi di linee	UNI EN ISO 128-20:02 UNI ISO 128-24:06	128-20:96; 128-24:99
. Scale	UNI EN ISO 5455:98	5455:79
. Riquadro iscrizioni	UNI EN ISO 7200:2007	7200:04
. Scritte	UNI EN ISO 3098-0/5:00	3098-0/6:97,00
<u>Rappresentazione:</u>		
. Metodi di rappresentazione	UNI EN ISO 5456-1/3:01	5456-1/3:96
. Convenzioni particolari	UNI ISO 128-30,34:06	128-30,34:01
. Sezioni	UNI ISO 128-40,44,50:06	128-40,44,50:01
<u>Quotatura</u>	UNI 3973,3974,3975:89	129-1:04

In particolare, i progetti riprodotti con riferimento alle norme di disegno tecnico sopra riportate, e pervenuti all' Ufficio in formato cartaceo, potranno essere associati ad uno specifico numero di protocollo in entrata solo se accompagnati da lettera di trasmissione in formato A4. La lettera di trasmissione sarà "smaterializzata" ed inserita nel Protocollo Informatico; i disegni tecnici non potranno essere smaterializzati, bensì potranno essere ritirati direttamente dal RPA come documenti cartacei. Tuttavia tale procedura non consente di associare in forma univoca uno specifico documento ad uno specifico numero di protocollo, annullando di fatto quelle reciproche relazioni tra i documenti che sono alla base di un archivio. Pertanto tale procedura deve essere abbandonata, pena la conseguente perdita del vincolo archivistico che si fonda sulle caratteristiche peculiari di "naturalità" ed "originalità".

La nuova procedura da porre in essere, in ottemperanza alle norme del CAD in vigore, obbliga questa Direzione a riconoscere come validi solo quei progetti che perverranno in formato elettronico, associabili nella loro interezza ad un numero di protocollo univoco e gestibili a mezzo di scrivanie virtuali. I formati elettronici accettati sono quelli citati nel presente Manuale.



VI. Documento analogico non firmato

I documenti privi di mittente (es. esposti anonimi), sono trattati, in ambito AOO-
GGEN_LAV, direttamente dal Capo Ufficio.

VII. Fogli privi di protocollo/data.

Qualora pervenga un documento cartaceo privo di protocollo e data, in quanto tale non deve essere protocollato, bensì sottoposto all'attenzione del RDS e successivamente del Capo Ufficio per le decisioni del caso. Sempre che il mittente sia identificato, in via generale va fatto presente al mittente che il documento va perfezionato.

Se il documento perviene a mezzo posta elettronica direttamente al Protocollo Informatico, sarà necessario verificare se si tratti di "spamming" per le ragioni più diffuse (a scopo pubblicitario o per offerte commerciali, truffe, etc.). Di tali messaggi l'Ufficio non terrà conto.

Se invece si tratta di posta di cui è stato casualmente omessa la protocollazione e la datazione, sarà generata una segnatura dal software di protocollo informatico.

VIII. Fogli/lettere non firmate, prive di timbri e/o apposizioni che consentano di identificarne la provenienza /bontà dell'Ente/Società/Impresa/Azienda/ Associazione/Privato originante l'atto.

Un documento di cui non si riesce a identificarne la bontà, sarà comunque sottoposto all'attenzione del RDS per le decisioni del caso.

Se in qualche modo è possibile risalire al mittente, tale sarà avvertito che il documento andrà perfezionato.

IX. Buste che pervengono all'Ufficio Postale di RAMDIFE lacere, bagnate, ovvero con dati identificativi (mittente, data di spedizione, affrancature, etc.) non leggibili.

Tutta la documentazione cartacea ordinaria indirizzata a UFAULAV e ritirata dall'Ufficio Postale di RAMDIFE con buste/plichi laceri, bagnati o rotti sarà comunque trattata ma di ciò sarà informato il RPA che ne dovrà informare il mittente al fine di controllare che il documento sia pervenuto completo ed esatto.

Se trattasi invece di buste/plichi riconducibili a bandi di gara o documenti classificati, tali saranno consegnati al RPA che adotterà i provvedimenti ritenuti utili al caso, in ottemperanza al regolamento di gara o alle normative in vigore.



In ogni caso viene sempre comunque avvertito il mittente circa le condizioni in cui la busta/il plico è stato recapitato all'Ufficio Postale di RAMDIFE.

X. Errata ricezione di documenti cartacei e altri casi.

Nel caso in cui pervengano all'Ufficio documenti erroneamente indirizzati, questi vengono rinviati all'ufficio postale se dall'indirizzo riportato sulla busta o bensì sul procedimento è possibile stabilire a quale Ente erano destinati. Sulla busta viene apposta la dicitura: *“Corrispondenza pervenuta per errore - non di competenza di questo Ufficio Autonomo Lavori, inviare a....”*.

Nella circostanza in cui venga erroneamente aperta una lettera destinata ad altra Amministrazione, questa viene richiusa e rispedita al destinatario scrivendo sulla busta la dicitura *“Aperta e richiusa dall'Ufficio Autonomo Lavori per individuare il destinatario”*.

Nel caso in cui venga erroneamente protocollato un documento non indirizzato all'Ufficio, il RDS provvede all'annullamento del protocollo, o alla protocollazione in uscita indicando come oggetto *“protocollato per errore, inviato a ..”*.

Il documento oggetto della rettifica viene inviato al destinatario con la dicitura *“protocollato per errore”*.

XI. Rilascio di ricevute attestanti la ricezione di documenti cartacei

Il personale operante presso la Segreteria è tenuto a rilasciare ricevute per la consegna delle offerte delle gare di appalto. La semplice apposizione del timbro datario di UFAULAV sulla copia non ha alcun valore giuridico e non comporta alcuna responsabilità del personale della Segreteria in merito alla ricezione ed all'assegnazione del documento.

La notifica di atti pubblici indirizzati all'Ufficio viene effettuata a carico dell'operatore che consegna a mano il documento cartaceo presso la Segreteria di UFAULAV.

b. FAX

Il Servizio di Tenuta del PI dispone di apparato fax. In aderenza alle norme vigenti non saranno accettati documenti trasmessi a mezzo fax provenienti dalla Pubblica Amministrazione. L'eventuale trasmissione di documentazione attraverso tale strumento, riservata esclusivamente ai soggetti diversi dalla Pubblica Amministrazione, può essere effettuata verso il fax dell'Ufficio di competenza tenendo presente che:



- Il fax registrato è trattato con le stesse modalità descritte nel sottoparagrafo inerente al documento analogico in ingresso;
- il mittente che invia il documento via fax, in aderenza alla normativa vigente “art. 45 del CAD”, non deve inviare anche la copia del documento originale con altri mezzi; ciò per evitare che uno stesso documento possa avere due numeri di protocollo diversi;

Tutti i FAX saranno trattati al pari dei documenti cartacei, solo se ammessa la ragionevole certezza del mittente. In tal caso infatti, tali documenti soddisfano il requisito della forma scritta e, pertanto, trattati al pari dei documenti cartacei. I FAX saranno protocollati nella stessa data di arrivo/consegna al Servizio di Protocollo Informatico.

Qualora non sia possibile accertare la fonte di provenienza, su di esso o sulla sua fotocopione dovrà essere apposta la dicitura “documento ricevuto via FAX di cui non è possibile accertare la provenienza”; per la registrazione e segnatura di tale documento si dovrà necessariamente attendere l’arrivo dell’originale cartaceo.

E’ possibile inviare via FAX i documenti informatici in partenza mediante la loro materializzazione. Il RPA appone sul frontespizio del FAX la dicitura “Il presente documento, composto di n. xx pagine, inviato via telefax, non sarà/sarà seguito dall’originale”.

Il documento materializzato da inviare via FAX deve riportare la segnatura del protocollo **FAX seguito dall’originale.**

Ogni documento deve essere individuato da un solo numero di protocollo, indipendentemente dal supporto di trasmissione.

Tutti i documenti anticipati via FAX (di cui segue sempre l’originale) saranno protocollati una sola volta. Pertanto sull’originale dovrà essere apposta la dicitura “anticipato via fax in data xx/xx/xx”. Il personale del Servizio di Protocollo Informatico protocolla la posta secondo l’ordine cui è ricevuta. Pertanto, se omessa la dicitura prevista, il documento potrebbe essere protocollato più di una volta (anche se il software in uso è in grado di riconoscere una segnatura già presente all’interno del database), perdendo di fatto la rilevanza giuridico-probatoria del procedimento amministrativo nonché la sua univocità.

Il RPA, sulla scorta delle comunicazioni ricevute per le vie brevi dal mittente del FAX (informazioni necessarie ad accertare la provenienza del FAX stesso), deve comunque comunicare al Servizio di Protocollo Informatico che tale FAX sarà seguito dall’originale (il documento che segue deve riportare la dicitura “già anticipato via FAX” a cura del mittente); sarà cura del RPA accertare che si tratti del medesimo documento; qualora vi



fosse qualche correzione, anche minima, si tratterebbe di un documento diverso e quindi andrà registrato con un nuovo numero di protocollo.

I numeri di fax convenzionali riconosciuti come validi ed ufficiali ai quali la Direzione riceve la corrispondenza sono:

- +39 06 4884679 (Segreteria).

A decorrere dalla data di pubblicazione del presente Manuale di Gestione, si assicura la protocollazione di tutti i documenti ricevuti al numero sopra riportato. Tuttavia, sempre a decorrere dalla data di pubblicazione del presente Manuale di Gestione, il fax già abilitato potrà essere utilizzato come mezzo utile per la ricezione della posta purchè il destinatario sia in grado di accertare ed assicurare la veridicità del documento inviato dal mittente e recapiti l'intero contenuto del fax al personale del Servizio di Protocollo Informatico per la successiva scansione e protocollazione.

c. Corrispondenza elettronica.

E' la corrispondenza ricevuta con il software del Servizio di Protocollo Informatico a mezzo delle caselle di posta certificata ed istituzionale.

I. Smistamento della corrispondenza elettronica in arrivo.

Tutta la corrispondenza elettronica in entrata è processata con il software di Protocollo Informatico ed inoltrata al Capo Ufficio.

La trattazione di documentazione amministrativa veicolata con i sistemi di posta elettronica comporta la necessità di adeguarsi a determinati standard per consentire l'interoperabilità dei sistemi oltre che per rispondere al dettato normativo vigente.

Pertanto le comunicazioni informatiche indirizzate all'AOO-GGEN_LAV, dovranno osservare le seguenti regole generali:

- il formato preferito per file allegati ai messaggi di posta elettronica è quello definito dallo standard ISO 19005-1 che definisce "un formato di file basato su PDF, conosciuto come PDF/A". Tale formato fornisce un meccanismo di rappresentazione dei documenti elettronici preservandone l'aspetto visivo nel tempo, indipendentemente dagli strumenti e dai sistemi utilizzati per la creazione, la memorizzazione e il rendering dei file. Il PDF è molto diffuso in tutto il mondo, sia nel settore pubblico che privato, ed è un formato di archiviazione già accettato in innumerevoli mercati. Lo standard PDF/A garantisce la riproducibilità a lungo termine.
- Sono anche accettati i formati: JPG, P7M, TXT, TIFF, TIF, XML;



- I file di progetto con estensione DWG, che sono file che interessano il “*core business*” dell’Ufficio sono anch’essi accettati solo se preventivamente concordati fra mittente e destinatario. Tali file, comunque, non possiedono la caratteristica richiamata dallo standard ISO 19005-1 in quanto consentono, fra l’altro, la modifica delle informazioni in esso contenute nel tempo;
- L’invio/ricezione di altri formati, differenti da quelli sopra citati, (es. file di progetto non prodotti con AUTOCAD, computi metrici, fogli di calcolo, bilanci e resoconti finanziari prodotti con software specifici, etc.) potranno essere di volta in volta concordati fra il mittente ed il destinatario affinché gli stessi possano essere “processati” dagli aventi titolo senza disservizi. Si consiglia l’uso di protocolli di accordo standard per l’inoltro/ricezione di quegli allegati che possono essere modificati (esempio cifratura, firma digitale, etc.), al fine di preservarne il contenuto e proteggerli da terzi;
- I file allegati al documento primario possono essere nei formati supportati dall’UO interessata e compressi nei formati ZIP o RAR;
- L’oggetto della mail con cui viene inviato il documento non deve superare i 256 caratteri, altrimenti il software del protocollo informatico non consente la protocollazione e il RDS sarà costretto a rispedire al mittente tale documento con preghiera di ridefinire la quantità di caratteri costituenti il campo “oggetto” della mail. Si sottolinea che gli spazi inseriti con la barra spaziatrice da tastiera concorrono alla formazione dei 256 caratteri. Tale regola è applicata dal sistema sia in fase di ricezione (PEI o PEC) che in fase di predisposizione (invio all’esterno);
- L’invio di allegati non previsti, comporta la mancata accettazione del messaggio da parte dell’Ufficio e la restituzione al mittente. Le eventuali marche temporali apposte insieme alla firma digitale devono essere in formato “embedded” e “non detached” (il file firmato e la firma devono essere contenuti in un unico busta di file);
- L’apposizione di firma digitale non valida rende non utilizzabile il file eventualmente trasmesso;
- La firma digitale di tutti i documenti allegati al messaggio è auspicabile;
- In un singolo messaggio di posta elettronica deve essere associata la documentazione relativa ad un unico argomento (pertanto se un mittente deve inviare cinque documenti afferenti cinque pratiche, dovrà inviare cinque mail perché le stesse dovranno avere cinque protocolli differenti cambiando l’oggetto del procedimento);



- La massima dimensione complessiva degli allegati non deve essere superiore ai 30 MB (compresa la lettera di invio); in caso di superamento di tale limite il messaggio non sarà recapitato all'AOO dal sistema di posta e respinto al mittente. Allegati di dimensione superiore potranno essere inviati solo su supporto informatico (CD – DVD – USB) Sono esclusi tutti gli altri dispositivi non espressamente citati nel presente Manuale;
- La casella postale del mittente, in caso di persone giuridiche, deve essere riferita alla persona giuridica medesima (ad esempio, la ditta ROSSI Spa dovrà inviare la propria documentazione da una casella postale istituzionale (es.:rossispa@xxxxx.it e non dalla casella postale mario.rossi@rossispa.xxxxx.it);
- Il nome degli eventuali file allegati deve essere di lunghezza moderata (comunque non superare i 256 caratteri, inclusi gli spazi inseriti con la barra spaziatrice), non contenere spazi e caratteri speciali (lettere accentate, caratteri speciali come “”,”^”, virgolette, apici, etc.). Si suggerisce di utilizzare il carattere _ (underscore) al posto di tali caratteri. Tale regola si applica sia al flusso in entrata (a mezzo PEI o PEC) che al flusso in uscita (nella maschera di predisposizione).

Esempi di file validi:

- ✓ *richiesta_di_risarcimento.pdf;*
- ✓ *foto_di_citta.jpg,*

mentre non vanno bene nomi come *questo è il 1° documento.pdf* oppure *si.transmette.domanda.pdf* o ancora *questa è la mia domanda per entrare a far parte dell'esercito.pdf*.

I mittenti interessati ad inviare file che debbano essere trattati/aggiornati/modificati elettronicamente (cioè tutti quei formati differenti dal PDF/A, XML, TIFF), dovranno:

- Inviare la copia valida per gli aspetti giuridico-probatori nei formati sopra citati;
- Aggiungere alla stessa corrispondenza elettronica un ulteriore allegato nel formato “lavorabile/modificabile” (es: *.rtf, *.doc, *.xls, *.cad, etc.), che non sarà trasformato in formato pdf e contestualmente non sarà firmato digitalmente dal programma (apposizione del flag “no pdf” sulla maschera di predisposizione);

Il personale dell'Ufficio che risponde al mittente con la situazione aggiornata invierà la corrispondenza elettronica allegando:



- Una copia valida per gli aspetti giuridico-probatori in un formato “non modificabile”;
- Una copia “lavorabile/modificabile” (es: *.rtf, *.doc, *.xls, *.cad, etc.) che non sarà trasformato in formato pdf e contestualmente non sarà firmato digitalmente dal programma (apposizione del flag “no pdf” sulla maschera di predisposizione) e che pertanto permetterà la lavorazione/modifica da parte dell’utente destinatario della corrispondenza.

II. Flusso in ingresso dei documenti informatici con casella PEI

I messaggi provenienti sulle caselle di posta vengono inseriti in un’apposita coda temporale.

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

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

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

L’operatore può protocollare il messaggio, procedendo alla successiva assegnazione all’UO competente ovvero, nei casi dubbi o quando il messaggio è palesemente non di competenza dell’AOO, può inviarlo in un apposito elenco, gestito dal RDS.

I documenti che vengono sottoposti alla successiva gestione del RDS possono essere protocollati direttamente da quest’ultimo ovvero, rispediti al mittente perché erroneamente consegnati oppure perché incompleti o illeggibile, oppure cancellati nel caso in cui il documento sia già pervenuto.

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

- il messaggio è corrotto o uno dei documenti non leggibile;
- dati non congruenti nella segnatura informatica;
- segnatura non conforme alla circolare AIPA/CR/28 7 maggio 2001;
- mancata sottoscrizione del documento primario;
- destinatario errato;
- verifica di integrità dei documenti negativa;



- il documento o gli allegati dichiarati all'interno del file "segnatura.xml" non corrispondono a quanto ricevuto.

Oltre ai casi suindicati il RDS può inviare il messaggio al mittente per un qualunque motivo a sua discrezione e, in tal caso, segnalerà il motivo nel messaggio di trasmissione.

Le mail che vengono considerate SPAM non vengono protocollate e non viene spedito nessun messaggio al mittente.

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

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

Nel caso in cui il mittente sia una P.A., in assenza della firma digitale, è sufficiente che sia presente in allegato il file "segnatura.xml", informazioni previste dalla CIRC..

In quest'ultimo caso, ove richiesto dal mittente, sarà trasmesso:

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

III. Flusso in ingresso dei documenti informatici con casella PEC

L'impiego della PEC è disciplinato da specifiche norme in materia.

La PEC viene impiegata per la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna. Quindi, la trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta. La data e l'ora di trasmissione e di ricezione di



un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.

Per i privati che intendono utilizzare il servizio di posta elettronica certificata, il solo indirizzo valido, ad ogni effetto giuridico, è quello espressamente dichiarato ai fini di ciascun procedimento con le pubbliche amministrazioni o di ogni singolo rapporto intrattenuto tra privati o tra questi e le pubbliche amministrazioni. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma.

La validità della trasmissione e ricezione del messaggio di posta elettronica certificata è attestata rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata, devono avvalersi di gestori opportunamente riconosciuti.

Per tutti i messaggi recapitati e inviati, il mittente riceve due ricevute dai gestori di PEC:

- La Ricevuta di Accettazione, che attesta la data e l'ora dell'invio della mail e contiene in allegato i dati di certificazione rilasciati dal gestore PEC;
- La Ricevuta di Consegna che attesta la consegna del messaggio nella casella di PEC del destinatario. Attenzione però che tale ricevuta non garantisce l'avvenuta lettura.

Le ricevute della PEC, rilasciate via e-mail, sono gestite dal software di protocollo informatico in uso “@d[h]oc”.

I messaggi provenienti sulle caselle di PEC vengono inseriti in un'apposita coda.

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

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

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

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

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



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

Le mail che vengono considerate SPAM non vengono protocollate e non viene spedito nessun messaggio al mittente.

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

In quest'ultimo caso, ove richiesto dal mittente, sarà trasmesso:

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

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

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

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

IV. Corrispondenza elettronica ricevuta su supporti informatici rimovibili.

L'Ufficio può ricevere documenti su CD - DVD – USB (allegati a documenti cartacei) solo nei formati riconosciuti come validi e se firmati digitalmente (art. 47 comma 2 del CAD). Tali documenti saranno importati all'interno del sistema mediante il software di Protocollo Informatico e assunti a protocollo in formato digitale, purché fornito nei formati elettronici che l'Ufficio considera come validi/leggibili (i documenti cartacei scansionati e il materiale elettronico contenuto nei CD - DVD – USB associato al file scansionato). Non saranno assunti a protocollo con il software del Protocollo Informatico i “documenti classificati” spediti da ditte esterne (es. gare di appalto coperte da segreto) o da altri Enti militari, ma tali saranno protocollati sul registro dei documenti classificati posto in apposita Area Riservata di UFAULAV e trattati secondo la normativa in vigore. Inoltre



L'Ufficio si riserva la facoltà di acquisire documenti ricevuti con supporti rimovibili chiavette USB, purché il mittente sia univocamente identificabile mediante informazioni contenute all'interno del supporto stesso; tali informazioni devono essere chiaramente decodificabili e interpretabili dall'Ufficio stesso con gli strumenti a sua disposizione.

V. Corrispondenza elettronica ricevuta con sistemi di “AMHS” o “Message Handling”, stazioni di messaggistica, etc.

Tutta la corrispondenza ricevuta con i sistemi di messaggistica in uso per la Difesa sarà stampata e successivamente smaterializzata con il software di Protocollo Informatico. Il Protocollo Informatico non tiene in considerazione il codice di priorità della messaggistica (per la trasparenza degli atti la corrispondenza è protocollata per ordine di arrivo e non per priorità), pertanto gli “ordini” pervenuti a mezzo messaggio saranno processati secondo la priorità assegnata dal sistema di messaggistica e successivamente assunti a protocollo.

Proprio per tale specifica peculiarità del sistema di messaggistica, in cui la priorità riveste maggiore importanza dell'ordine di arrivo, non è possibile interfacciarlo in modo automatico con il Protocollo Informatico. E' auspicabile e quanto mai necessario inviare tutte le comunicazioni a mezzo PEI o PEC piuttosto che con sistemi di messaggistica. Infatti, in tale modo, si garantisce immediata trattazione della documentazione pervenuta (al pari del codice “O”), in quanto la documentazione è processata immediatamente al momento della ricezione. Inoltre, il sistema di messaggistica AMHS non gestisce l'invio di allegati e pertanto la ricezione è incompleta.

VI. Corrispondenza elettronica ricevuta/trattata on-line con sistemi informatici in uso alla Difesa (SIV, SICOGE, etc.) e/o alla Pubblica Amministrazione.

Sono previsti dei protocolli di intercomunicazione fra i diversi software in uso nella Difesa e/o nella PA per la protocollazione automatica contestuale e contemporanea della documentazione elettronica prodotta con sistemi “on-line”. Tali protocolli non sono disponibili alla data di pubblicazione del presente Manuale e saranno pertanto trattati in epoche successive.

VII. Documenti informatici corrotti (non leggibili).

Sono tutti quei documenti informatici che risultano non leggibili dalle postazioni in uso nella Difesa non per problemi di compatibilità software ma per problemi di “rotture/alterazioni dei codici binari”. L'Ufficio, per tramite del software di



Protocollo Informatico, contatta i mittenti facendo esplicita richiesta di re-inviare la documentazione corrotta pervenuta.

4. Assegnazione dei documenti in arrivo.

Come già premesso, tutta la corrispondenza in arrivo, sia cartacea che elettronica, viene trattata esclusivamente con il software del Protocollo Informatico (tranne che nei casi particolari già citati).

Il personale del servizio di Protocollo non è tenuto a controllare la completezza sostanziale della documentazione pervenuta. Tale verifica spetta al personale dell'UO interessata alla tematica (ovvero al relativo RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti provvede a richiederli al mittente, specificando le eventuali problematiche del caso. Il personale del Servizio di Protocollo Informatico si accerta solo della completezza formale dei documenti in arrivo (es: il numero degli allegati citati nel documento primario corrisponde a quanto effettivamente ricevuto, il mittente è chiaramente identificabile, la data del procedimento è veritiera, etc.).

Modifica delle assegnazioni dei documenti.

Se a una UO viene assegnato un documento non di competenza, il relativo responsabile può, procedere, direttamente, alla relativa riassegnazione tramite ulteriore invio per competenza.

Nel caso che la competenza sia esterna all'AOO l'assegnatario temporaneo provvederà ad informare il mittente in modo formale, tramite documento trasmesso attraverso il sistema di protocollo, indicando, se noto, anche l'Ufficio competente.

La modifica dell'assegnazione di un RPA può essere fatta solo dal Capo dell'UO che l'ha precedentemente assegnata.

5. Documento informatico in uscita.

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

Pertanto, quando il dirigente/funziionario competente ha perfezionato il relativo iter, attraverso le funzioni del sistema, provvede a firmare digitalmente. L'inserimento della firma digitale appone anche la marca temporale al documento di interesse e contestualmente:

- protocolla il documento;
- lo invia per e-mail, e lo inserisce nei documenti da stampare con il previsto l'allegato analogico.



Il sistema informatico, sulla base delle informazioni inserite nella fase di predisposizione di quel documento, provvede ad inviare, per posta elettronica, il documento primario e tutti gli eventuali allegati presenti.

La dimensione massima del messaggio che può essere inviato con il Protocollo Informatico è di 30 MB. Ciò comporta che, in fase di predisposizione, potranno essere inseriti documenti la cui sommatoria non superi il valore di 30 MB. Occorre tenere presente che nei 30 MB il sistema include il file segnatura-xml. Pertanto, se viene superato tale limite, il sistema non consente la firma digitale al dirigente preposto, non protocolla e non invia il documento.

L'utilizzo della casella postale elettronica ordinaria, piuttosto che della PEC, viene programmato dall'operatore che ha predisposto la pratica e può essere modificato da tutti coloro i quali hanno titolo a farlo fino alla firma del documento stesso.

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

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

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

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

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

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

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



Quando il documento non deve essere trasmesso per posta elettronica, il sistema informatico, completa le operazioni di firma digitale, apposizione della marca temporale e protocollazione del documento senza procedere alla successiva trasmissione.

I documenti così lavorati confluiscono invece in una apposita lista di documenti da materializzare.

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

Sul documento così stampato sarà apposto, sul retro, la seguente frase:

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

Roma, xx xx xxxx

IL CAPO UFFICIO

(xxxx xxx x x x xxxx x xxxxxxxxx)

Il Servizio di Protocollo Informatico ha distribuito una serie di timbri per apporre la frase sopra citata.

La firma deve essere apposta esclusivamente dal RPA, dopo essersi accertato che il documento sia stato stampato correttamente, sia completo di tutti gli allegati previsti e siano state stampate per l'inoltro tutte le copie necessarie.

Dopo la firma di tale attestazione il documento primario e gli eventuali allegati vengono spediti all'indirizzo postale del corrispondente, attraverso il tradizionale servizio postale.

Tale copia cartacea deve riportare tutti i dati di segnatura previsti dalle normative vigenti.

a. Predisposizione di un documento.

Al fine di inviare correttamente un documento informatico è necessario applicare le seguenti regole nella struttura del file che viene predisposto (maschera predisposizione del protocollo informatico):

- nella preparazione del documento primario, utilizzare il modello nel formato RTF all'uopo predisposto. Il modello è stato pubblicato sul sito ufficiale di UFAULAV (facsimile della lettera in formato RTF in Allegato "E"). Nel *nome_file* non utilizzare caratteri speciali e/o



lettere accentate (°,’,^, è, ecc). Il sistema di protocollo informatico provvede in automatico alla trasformazione dell’originale in formato PDF/A all’atto della firma del documento;

- nell’oggetto occorre riscrivere (non si può utilizzare copia/incolla di Microsoft) l’oggetto del documento primario, senza utilizzare caratteri speciali e/o lettere accentate (°,’,^, è, ecc). Tale accorgimento faciliterà la gestione dei documenti archiviati specialmente nella consultazione;
- nel fissare il nome del file è bene non superare gli otto caratteri;
- nella classificazione, seguire le regole descritte nel presente Manuale;
- nel selezionare i destinatari, controllare sempre l’indirizzo inserito in rubrica (cliccando sull’indirizzo stesso al momento dell’inserimento);
- ricordarsi di inserire il flag “Allegati analogici” e/o “Dati sensibili”;
- quando si inserisce un documento, se tale non deve essere firmato digitalmente e non deve essere trasformato in PDF/A, oppure si tratta di un documento informatico già firmato digitalmente, occorre spuntare il “No PDF”. Tale operazione oltre a non essere utile su un documento già firmato in precedenza, potrebbe generare errori nel sistema informatico idonei a bloccare la fase di protocollazione e trasmissione del documento.

b. Posta non consegnata.

Il sistema gestisce in automatico, i messaggi che segnalano un problema di ricezione nella casella postale ordinaria del destinatario (ad esempio, destinatario sconosciuto, casella postale del destinatario piena). Questi messaggi sono automaticamente inseriti quali allegati del documento che ha generato il messaggio stesso e il documento interessato viene ricollocato sulla scrivania virtuale (posta non consegnata) inerente ai documenti in ingresso del primo utente che ha predisposto il documento.

In questi casi, l’utente che trova nella posta non consegnata un messaggio, dopo le opportune verifiche (controllo degli indirizzi, completezza della pratica, etc., può:

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



E' indispensabile verificare costantemente la presenza di messaggi nella "Posta non consegnata".

6. Documento informatico interno

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

In tutti quei casi nei quali tra gli indirizzi per competenza o per conoscenza di un documento vi sia una UO interna all'AOO, tale informazione viene esplicitamente dichiarata all'interno del sistema informatico che provvederà ad inviare, automaticamente, quel documento sulla scrivania virtuale del dirigente competente dell'UO destinataria.

Quel documento sarà protocollato (*non inviato per e-mail*) solo in uscita dalla UO mittente.

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

7. La firma dei documenti.

Occorre richiamare l'importanza dei dirigenti e funzionari con **potere di firma** di procedimenti amministrativi.

Il Capo Ufficio di UFAULAV, nell'esercizio delle proprie funzioni, delega il il funzionario alla firma di documentazione amministrativa e tecnica, secondo le attribuzioni relative alla posizione organica ricoperta.

UFAULAV produce solo originali informatici firmati a mezzo di carta multi servizi della Difesa (CMD) con il protocollo informatico. La firma di ciascun documento è tracciata in maniera indelebile e non modificabile dal sistema.

Appare utile sottolineare che, al fine di tutelare la trasparenza nella trattazione dei procedimenti amministrativi (DPR 445/2000), il Capo Ufficio può disporre il controllo circa l'uso del potere di firma da parte del personale preposto.

8. La MINUTA del documento in partenza.

Prima dell'uso del protocollo informatico, i RPA che producevano i documenti apponevano la firma sulla minuta che veniva custodita agli atti. Il protocollo informatico non genera una "minuta", bensì mantiene traccia di tutte le operazioni svolte su un procedimento. Pertanto la "tradizionale minuta" è di fatto sostituita dal registro delle attività sempre disponibile per ciascun documento sia sulla scrivania di colui che è stato inserito nel "flusso documentale" sia in consultazione.

Nel caso in cui si renda necessaria la materializzazione del documento, l'unico originale da cui trarre copia cartacea è il documento informatico nel sistema di protocollo. La copia materializzata,



proprio perché viene materializzata e rimane copia (cartacea), anche se autenticata conforme all'originale.

9. Inoltro di documenti analogici in partenza.

Poiché nell'ambito dell'AOO vengono prodotti esclusivamente documenti originali informatici che sono inoltrati automaticamente dal sistema di protocollo informatico, non avrebbe senso parlare di flusso in uscita di documenti analogici.

Tuttavia, come già ampiamente spiegato nei paragrafi precedenti, può essere necessario procedere alla trasmissione di documenti attraverso il servizio postale tradizionale.

Le procedure di preparazione dell'atto da parte dell'operatore incaricato sono state già descritte nel citato paragrafo inerente al flusso in uscita del documento informatico.

I documenti che devono essere trasmessi per posta ordinaria cartacea devono essere portati presso l'Ufficio Postale.

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

10. Duplicazione dei documenti

Se si è in presenza di un documento informatico, la duplicazione dello stesso può essere eseguita dallo stesso titolare che lo ha firmato digitalmente, mediante copia firmata digitalmente.

Se invece trattasi di duplicazione di un originale cartaceo in formato elettronico, la trasformazione del documento avviene con i sistemi di digitalizzazione del documento in dotazione all'Ufficio e l'attestazione che la copia informatica è conforme all'originale cartaceo è firmata digitalmente da colui che effettua la scansione ed appone la propria firma digitale al termine del procedimento.

Invece, se occorre duplicare un documento informatico in formato cartaceo, occorre materializzare il documento stesso a firma autografa di colui che ha firmato digitalmente il documento informatico originale, con apposizione del timbro già descritto precedentemente.

11. Obblighi di conservazione dei documenti.

I procedimenti amministrativi sono disponibili nell'archivio elettronico di UFAULAV per i periodi stabiliti dalle norme di legge in vigore.



Il Ministero della Difesa si fa carico del mantenimento e dell'accessibilità di tali archivi elettronici mediante opportune procedure di tutela degli archivi e garantisce la disponibilità e l'accessibilità degli stessi che sono memorizzati all'interno del Server di Protocollo Informatico.

12. La gestione del documento analogico interno.

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

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

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

In tutti quei casi nei quali tra gli indirizzi per competenza o per conoscenza di un documento vi sia una UO interna all'AOO, tale informazione viene esplicitamente dichiarata all'interno del sistema informatico che provvederà ad inviare, automaticamente, quel documento sulla scrivania virtuale del Capo Sezione competente dell'UO destinataria.

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

13. Particolari casistiche dei documenti analogici.

a. Documento analogico non firmato

I documenti privi di mittente (es. esposti anonimi), a seguito di disposizioni interne, sono trattati in ambito AOO direttamente dal Capo Ufficio.

b. Documenti indirizzati alle persone

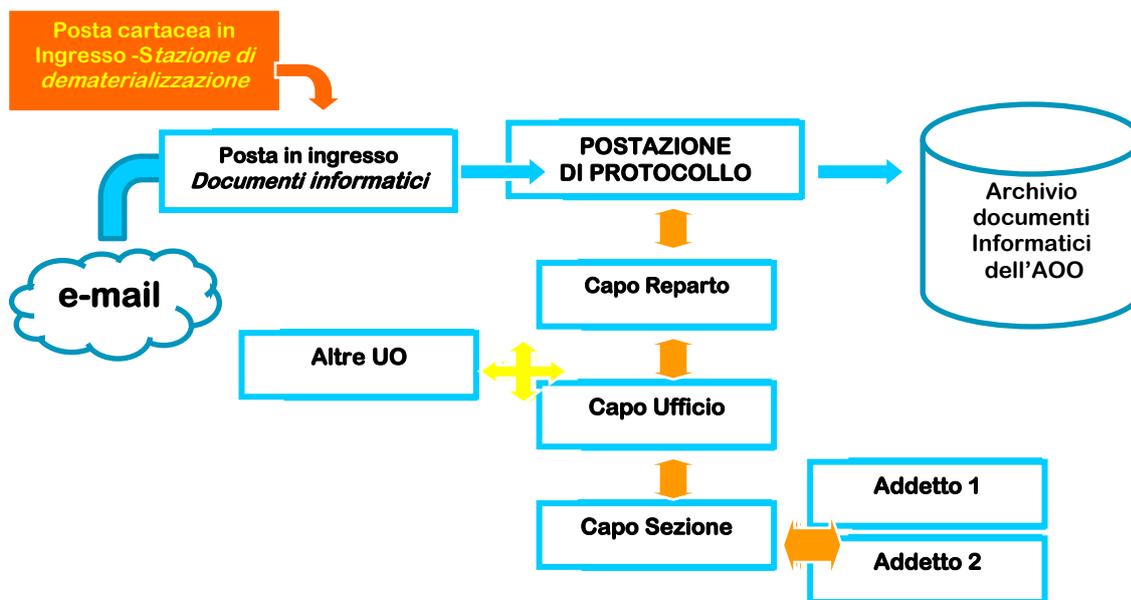
La corrispondenza analogica indirizzata direttamente alla persona, non viene aperta dal personale del Servizio di protocollo, ma viene consegnata all'interessato o al Capo della Sezione di appartenenza. A riguardo si evidenzia che la posta privata indirizzata al personale deve giungere presso l'AOO-UFAULAV solo ed esclusivamente per motivi straordinari.



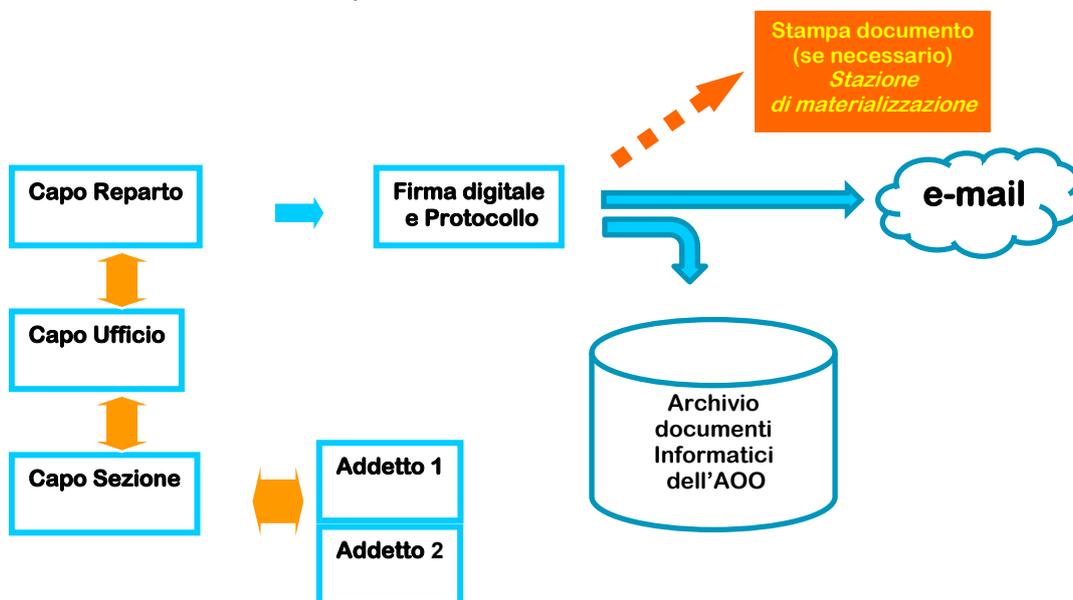
14. Workflow del flusso documentale – Riepilogo finale.

Descrizione grafica del flusso documentale

Esempio di flusso di ingresso



Esempio di flusso di uscita





CAPITOLO 6 - SISTEMA DI CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

1. Il Titolario Unico di Classificazione.

a. Principi generali.

Per **archivio** si intende un complesso ordinato e sistematico di atti, scritture e documenti prodotti e/o acquisiti da un soggetto pubblico o privato (ente, istituzione, famiglia o individuo nel normale esercizio delle proprie funzioni), durante lo svolgimento della propria attività, e custoditi in funzione del loro valore di attestazione e di tutela di un determinato interesse. Fra tali atti, scritture, documenti esiste un legame logico: il **vincolo archivistico**.

Il vincolo archivistico è il legame che collega un documento agli altri del fascicolo e/o della serie e lo rende, in virtù di questo collegamento, significativo. Per sancire in maniera incontrovertibile il vincolo archivistico, tutti i documenti d'archivio vengono classificati, vale a dire suddivisi e raggruppati secondo le voci di un quadro, appositamente predisposto, chiamato **titolario**.

Un titolare è, quindi, lo strumento che dà forma all'archivio al momento della sua nascita. Si archivia gerarchicamente in voci generali, chiamate titoli, categorie o classi, che corrispondono a raggruppamenti di competenze/funzioni.

Ad ogni titolo, classe e sottoclasse è attribuito un codice numerico, che sarà riportato anche sui singoli documenti di archivio che compongono la serie (codice di classificazione). La funzione del codice è quella di riassumere la definizione e, soprattutto, eliminare eventuali equivoci nell'attribuzione di un documento a una partizione del titolare piuttosto che ad un'altra: le combinazioni di codici, infatti, non sono espresse, come invece le definizioni, a interpretazioni soggettive da parte degli addetti al protocollo/archivio.

Il titolare tratta tutti gli argomenti dell'organizzazione.

b. Descrizione.

Il titolare di archivio di UFAULAV è:

- frutto di un complesso coordinamento interno dell'ufficio fra tutte le Sezioni;
- discendente da un preciso modello funzionale che si riferisce alle competenze ed attività assegnate ad UFAULAV;

Il titolare di classificazione di archivio di UFAULAV si riferisce alle competenze delle UO, è sempre aggiornabile, pubblico e disponibile sul sito istituzionale di UFAULAV.



L'aggiornamento del titolario compete esclusivamente al vertice dell'AOO-GGEN_LAV, effettuato dal RDS o suo Vicario.

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

Il titolario non è retroattivo non si applica, cioè, ai documenti protocollati prima della sua introduzione.

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

c. **Struttura**

Il titolario dell'AOO-UFAULAV presenta i caratteri di generalità e di completezza necessari per soddisfare le esigenze di classificazione delle varie sezioni.

In particolare, nel modello di classificazione dei documenti è evidenziata la gestione delle infrastrutture della Difesa di competenza di UFAULAV e tutte le attività giuridiche/tecniche/contrattuali ad esse connesse.

d. **Classificazione dei documenti**

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo uno schema logico, in relazione alle funzioni e alle competenze della AOO.

Essa è eseguita attraverso il titolario di classificazione.

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

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

Le operazioni di classificazione dei documenti in entrata può essere fatta dall'addetto alla protocollazione ovvero dal responsabile del procedimento che archivia la pratica. Invece, per i documenti in uscita, la fascicolazione deve essere obbligatoriamente eseguita in fase di predisposizione. E' comunque possibile modificare il fascicolo al quale quel documento si riferisce finché non è protocollato e firmato. Con la procedura di firma il protocollo informatico "congela" tutte le informazioni inserite nel documento, inclusa la classe di fascicolo/sottofascicolo assegnata.



e. Fascicolazione dei documenti

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

Il sistema prevede i primi tre livelli del titolare (titolo, classe e sottoclasse), non modificabili, gestiti dal RDS.

I fascicoli e i sottofascicoli sono “aperti”, cioè gestibili e modificabili dagli aventi causa (normalmente gli RPA).

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

Il sistema di protocollo informatico in uso permette la modifica in qualsiasi momento del codice e della descrizione dei fascicoli e sottofascicoli creati.

E' buona norma non modificare i codici e le descrizioni dei fascicoli creati precedentemente. Qualora tale operazione si rendesse indispensabile, è necessario coordinarsi con il RDS e/o suo Vicario per definire tale operazione.

Per tale attività gli addetti dovranno attenersi alle seguenti regole:

- il codice del fascicolo o del sottofascicolo deve essere numerico;

Ogni Sezione/Ufficio può organizzare regole di fascicolazione riferite alle regole generali inserite nel presente Manuale. L'obiettivo è sempre la salvaguardia del vincolo archivistico. Una corretta fascicolazione, ben organizzata, consente una ottimizzazione sia di impiego delle risorse sia di struttura dell'archivio e, soprattutto, agevola e velocizza le operazioni di ricerca dei procedimenti.

Le varie Sezioni/Uffici possono definire dei codici convenzionali per la creazione di fascicoli e sottofascicoli.

Il sistema mantiene traccia dei dati inseriti nella fase di creazione del fascicolo.

2. Archivio cartaceo di UFAULAV – Custodia dei documenti analogici

Sulla base della normativa vigente, l'AOO-GGEN_LAV (UFAULAV) è dotato di due archivi, uno generale ed uno relativo alla documentazione amministrativa delle gare e prevede una organizzazione archivistica così articolata:

- Archivio temporaneo – documenti protocollati nel corrente anno mantenuti presso i locali delle varie Sezioni/Uffici. Una volta trascorso il tempo occorrente alla completa definizione delle varie pratiche, i documenti vengono trasferiti nell'archivio in base all'ordine cronologico di arrivo;



- archivio di deposito: vi sono conservati tutti i documenti relativi all'Ufficio a partire dall'anno 1999.

3. Archiviazione dei documenti informatici

Il sistema è conforme alle norme vigenti, ciascun documento è dotato di firma digitale, di marca temporale, di hash in formato SHA-256 e delle informazioni di registrazione ad esso associate. Ogni giorno viene anche, prodotto, il registro giornaliero delle registrazioni di protocollo, firmato digitalmente dal RDS o suo Vicario.

CAPITOLO 7 - IL SISTEMA INFORMATICO

1. Il Sistema in uso per il Protocollo Informatico, per la Gestione dei Flussi Documentali e la Tenuta degli Archivi.

Il software adottato dall'Ufficio per il Protocollo Informatico, denominato “@d[h]oc”, è quello già adottato in ambito Area Tecnico Amministrativa della Difesa, in particolare pilotato dal Segretariato Generale e degli Armamenti della Difesa/DNA.

2. L'interoperabilità dei sistemi.

Si prevede una interoperabilità fra diversi sistemi informatici della Difesa, la quale non è ancora attiva.

3. Descrizione funzionale e operativa del sistema di protocollo informatico

Tutte le informazioni di dettaglio inerenti alle funzionalità presenti nel sistema informatico di PI e gestione documentale sono reperibili richiedendo la guida dalla pagina di accesso al sistema. Tali informazioni sono sempre aggiornate e si riferiscono in particolare a:

- *login* – come si accede al sistema;
- *protocollo* – Le funzioni di protocollazione;
- *scrivania* – funzioni di scrivania in ingresso ed in uscita.

Il sistema è costantemente aggiornato in base alle necessità ed al fine di implementarne/migliorarne le funzionalità. Per ogni aggiornamento sono rilasciati:

- bollettino per gli utenti ove si descrivono le modifica apportate;



- pubblicazione periodica di informazione per gli utenti.

Sul sito istituzionale di UFAULAV, il menù principale “Protocollo Informatico” riporta diverse informazioni circa l’uso del protocollo informatico presso l’Ufficio, incluso il titolario di fascicolazione ed una versione in formato PDF del presente Manuale.

4. Abilitazioni di accesso alle informazioni documentali

a. Generalità

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

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

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

b. Accesso al sistema

Per poter accedere al sistema ad ogni utente è assegnata una credenziale composta da:

- una componente pubblica che permette l’identificazione dell’utente da parte del sistema (user_Id);
- una componente riservata di autenticazione (password);
- una autorizzazione di accesso (profilo), al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie a svolgere le attività di competenza dell’ufficio a cui appartiene.

L’RDS, avvalendosi di una utenza privilegiata (amministratore di sistema), predispone l’organigramma dell’Ente, configurando tutte le figure professionali previste dalla struttura organica. Ogni posizione organica corrisponde ad una serie di profili (Capo Ufficio, Capo Sezione, Addetto di Sezione, Addetto di Segreteria, etc.). Successivamente, ogni utente viene configurato nel sistema (componente pubblica e privata) e ad esso associato un ruolo con un profilo ben preciso.

Appare utile sottolineare che una singola persona fisica può ricoprire più ruoli. Ruoli differenti sono sempre gestiti con la stessa chiave privata.



c. Profili d'accesso

Nell'ambito della AOO-GGEN_LAV la strutturazione degli accessi prevede una realizzazione di una serie di profili sulla base della struttura ordinativa e delle rispettive competenze.

I principali profili di accesso riguardano le funzioni di:

- amministratore di sistema: è colui il quale può accedere ai profili di configurazione di base del sistema; è di competenza del RDS, del Vicario e loro addetti;
- protocollazione in ingresso: funzione destinata agli operatori di protocollo in ingresso dei documenti informatici e cartacei;
- lista dei documenti da materializzare: è l'elenco all'interno del quale confluiscono i documenti che per le proprie caratteristiche non possono essere inviati per posta elettronica. Tale configurazione è predisposta "ad hoc" sulla base dell'organizzazione lavorativa di ciascuna UO. E' modificabile nel tempo e normalmente viene concessa a livello apicale dell'UO preposta;
- accesso alla tabella dei mittenti/destinatari: si tratta di un punto di snodo fondamentale per la gestione della corrispondenza. L'accesso a tale tabella è centralizzato e gestito solo dal personale del Servizio di Protocollo Informatico che con coerenza e senza duplicazione inserisce gli indirizzi necessari;
- abilitazione alla firma digitale degli atti: tutti coloro che per funzione, incarico hanno l'attribuzione alla firma digitale degli atti. Alla firma digitale è legata la possibilità di protocollare e trasmettere tutti i documenti verso l'esterno per quanto concerne la spedizione in uscita, la materializzazione e dematerializzazione di documenti analogici o la trasmissione di allegati non digitalizzabili;
- predisposizione di documento: è la funzione che consente di preparare gli atti per il flusso in uscita. Normalmente concessa a tutti gli operatori;
- consultazione: è la funzione che consente la ricerca di tutti i documenti contenuti nella banca dati dell'AOO-GGEN_LAV. Tale ricerca è legata alla possibilità di visualizzare un documento in base alla competenza di gestione di un procedimento (comunemente chiamato "cono d'ombra di visibilità"). In particolare, le informazioni legate al registro di protocollo sono visibili a tutti gli utenti mentre i documenti in quanto tali sono visibili solo a chi appartiene al relativo cono d'ombra;
- dati sensibili: è la funzione che consente di accedere ai documenti che contengono dati sensibili;



- accesso alla scrivania: anche questa funzione è abilitata a tutti gli utenti poiché si basa sullo scambio della corrispondenza e le attività gestionali dei documenti in ingresso/uscita;
- trasmissione degli atti: attivata per gli utenti con poteri di firma stabiliti in ambito UO.

I profili ora delineati non vanno considerati esaustivi delle molteplici possibilità fornite dal sistema informatico e, inoltre, è possibile anche creare profili ex-novo che contengano un mix di quelli ora elencati.

L'assegnazione dei profili ed il loro aggiornamento sono normalmente gestiti dal RDS. Per l'attribuzione della trasmissione degli atti, si fa riferimento a quanto già menzionato nei precedenti paragrafi.

CAPITOLO 8 - IL REGISTRO DI EMERGENZA

1. Premessa.

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

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

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

2. Attivazione del registro di emergenza

Ogni qualvolta, per motivi accidentali o programmati, non fosse possibile utilizzare il sistema informatico per le attività di protocollazione per un periodo di tempo significativo, il RDS emette una dichiarazione, che sarà mantenuta agli atti, nella quale indica, con esattezza, la data e l'ora di inizio del non funzionamento e il relativo motivo.

3. Attività possibili durante l'attivazione del registro di emergenza

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



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

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

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

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

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

4. Riattivazione del sistema informatico

Quando il sistema informatico riprende il suo normale funzionamento, il RDS produce una ulteriore dichiarazione, con l'esatta indicazione della data e dell'ora della ripresa del servizio.

Tutte le dichiarazioni del RDS di attivazione e chiusura del registro di emergenza sono conservate agli atti a cura del RDS.

Dopo la riattivazione i documenti in ingresso protocollati in emergenza, verranno immessi all'interno del sistema mediante acquisizione come da documentazione cartacea. Nella scansione dei documenti in ingresso, la prima pagina del documento sarà anticipata da una pagina bianca riportante la dicitura "**NOTE ATTP**". Tale dicitura richiama e rammenta agli utenti la precedente operazione di protocollazione con il registro di emergenza.

Parimenti si riprodurranno, a cura delle UO di competenza, i documenti protocollati in emergenza in uscita, con l'accortezza di farli confluire all'interno della lista dei documenti da materializzare. 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 verrà trascritto a cura degli operatori che si occuperanno della nuova produzione nel sistema informatico nei campi previsti (Note/decretazioni).



CAPITOLO 9 – REGOLE GENERALI DI SCRITTURA DEI DATI ALL'INTERNO DEL SISTEMA INFORMATICO

In tutti i sistemi informatici è di particolare importanza la qualità delle informazioni inserite. Il Protocollo Informatico rivoluziona la metodologia di lavoro, diffondendo di fatto nuove convenzioni nella trattazione dei procedimenti amministrativi e del flusso documentale.

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

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

Nomi di persona	Prima il Cognome e poi il Nome. In maiuscolo solo la prima lettera. Esempio: <i>Rossi Mario</i>
Titoli di cortesia, nobiliari ecc.	Sempre omessi
Nomi di città	In lingua italiana, se disponibile
Nomi di stati	In lingua italiana
Nomi di ditte	Lettera maiuscola solo nella prima lettera. L'eventuale forma societaria in minuscolo, senza punti di separazione. Esempio: <i>Acme srl</i>
Enti/associazioni	Lettera maiuscola solo per l'iniziale della denominazione
Ministeri	Scritti per esteso Esempio: <i>Ministero della difesa</i>
Enti di secondo livello	Esempio: <i>Segredifesa V Reparto</i> e non <i>V Reparto Segredifesa</i>
Sigle di enti	Senza punti: Esempio: <i>ISTAT</i>
Università	Esempio: <i>Università degli studi di Roma</i>
Virgolette/apici	Utilizzare, digitandolo dalla tastiera (no copia/incolla da Word) il relativo carattere
Date	Formato numerico, separatore trattino: esempio: <i>01-01-2012</i>



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufulav@geniodife.difesa.it
ufulav@postacert.difesa.it

ALLEGATO A
ATTO COSTITUTIVO AOO

Allo stato attuale, le UO che afferiscono alla AOO GGEN_LAV, sono le seguenti:

1. CAPO UFF. – Capo Ufficio di UFAULAV
2. RDS – Responsabile del Protocollo Informatico
3. ADDRDSA,ADDRDSB,ADDRDSC,ADDRDSD – Vicario ed addetti del servizio di protocollo
4. 1^SEZIONE LAVORI
5. 2^SEZIONE LAVORI
6. 3^SEZIONE LAVORI
7. SEZIONE PERSONALE
8. SEGRETERIA
9. SERVIZIO AMMINISTRATIVO
10. SUB CONSEGNETARIO
11. GESTIONE FINANZIARIA
12. UFFICIO ACQUISTI
13. UFFICIALE ROGANTE
14. SERVIZIO PREVENZIONE E PROTEZIONE
15. GESTIONE RETE LAN



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufulav@geniodife.difesa.it
ufulav@postacert.difesa.it

ATTO DI NOMINA RDS

ALLEGATO C



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Servizio Amministrativo
Via Firenze, 35 - 00184 Roma
Indirizzo Telegrafico: UFAULAV - ROMA

OGGETTO: Nomina Responsabile del Servizio del protocollo informatico

Ordine del Giorno n. 1 del 02.01.2015

Visto l'art. 61 del DPR 445/2000 in materia di documentazione digitale della Pubblica Amministrazione;

Visto l'ODG n. 86 del 02.12.2013 che prevede la costituzione dell' AOO UFAULAV:

NOMINO

In sostituzione del Cap. com. Massimiliano STELLA, il Funz. Amm.vo Dott. Antonello Buttara quale Responsabile del protocollo informatico, della gestione dei flussi documentati e degli archivi.

IL CAPO UFFICIO
Col. g. SPAGNA / Dott. Ing. Pierluigi



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufulav@geniodife.difesa.it
ufulav@postacert.difesa.it

ALLEGATO D

DISTINTA PER INDIRIZZI ESTERNI ALL'AMMINISTRAZIONE DIFESA

MITTENTE: UFFICIO AUTONOMO LAVORI G.M. PER M.D.

DISTINTA PER
INDIRIZZI ESTERNI ALL'AMMINISTRAZIONE DIFESA
(ex ENTI PRIVATI e NOMINATIVI)
(presentate per la spedizione nell'Agenzia di Roma 13)

1. La corrispondenza estera va distinta separata dalla italiana;
2. Le assicurate per l'estero con busta telata pesante;
3. Barrare la casella che interessa;
4. Non vanno apportate correzioni e vanno compilate in ogni loro parte.

Assicurate
(5 copie)

Prioritaria
(2 copie)

Pacchi
(2 copie)

Raccomandate
(5 copie)

Raccomandate R.R.
(5 copie)

Numero d'ordine	PROTOCOLLO	DESTINATARIO	LOCALITA'	N° CODICE A BARRE (a cura Nucleo Posta)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				

Dichiaro sotto la mia responsabilità che i plichi indicati nel presente elenco vengono inoltrati per motivi di servizio
E pertanto con oneri a carico dell'A.D.

Roma, li

IL CAPO UFFICIO
Col. g. SPAGNA Dott. Ing. Pierluigi



MINISTERO DELLA DIFESA
UFFICIO AUTONOMO LAVORI
GENIO MILITARE PER IL MINISTERO DELLA DIFESA
Via Firenze , 35 - 00184 ROMA
ufulav@geniodife.difesa.it
ufulav@postacert.difesa.it

Elenco del personale preposto alle attività previste dall'art. 23 ter/3 del CAD

- ❖ Funz. Amm.vo Dott. Antonello Buttara;
- ❖ Vicario Serg. Magg. Pasquale Riccardi;
- ❖ Ass. Amm.vo Patrizia Cau;
- ❖ Ass. Amm.vo Giusy Pace;
- ❖ Ass. Amm.vo Sandro Della Ciana.

N.B.

Il presente Manuale è disponibile sulla rete INTERNET, pubblicato sul sito della DIFESA