



MINISTERO DELLA DIFESA
TRIBUNALE MILITARE DI VERONA

**Manuale di gestione
del protocollo informatico**

Edizione 2019



MINISTERO DELLA DIFESA

TRIBUNALE MILITARE DI VERONA

ATTO DI APPROVAZIONE

Approvo il

“MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO

DEL TRIBUNALE MILITARE DI VERONA”

Verona, 01/07/2019

il Presidente del Tribunale
Vincenzo SANTORO

Sommario

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI	7
ACRONIMI E RIFERIMENTI NORMATIVI	8
GLOSSARIO	10
CAPITOLO I.....	15
1. PRINCIPI GENERALI	15
1.1 Premessa.....	15
1.2 Ambito di applicazione del Manuale di gestione/Area Organizzativa Omogenea (AOO).....	15
1.3 Servizio per la gestione del protocollo informatico.....	15
1.4 Firma digitale	16
1.5 Tutela dei dati personali	16
1.6 Entrata in vigore del Manuale	16
CAPITOLO II	17
2. FORMAZIONE TRASMISSIONE SOTTOSCRIZIONE E ARCHIVIAZIONE DEI DOCUMENTI INFORMATICI.....	17
2.1 Formazione dei documenti - aspetti operativi	17
2.2 Sottoscrizione di documenti informatici	17
2.3 Trasmissione del documento informatico.....	17
2.4 Archiviazione del documento informatico	17
CAPITOLO III	18
3. LA GESTIONE DEI DOCUMENTI – ASPETTI FUNZIONALI	18
3.1 Generalità	18
3.2 Orario di erogazione del Servizio.....	18
3.3 Documenti protocollati e documenti esclusi dalla protocollazione	18
3.4 Documento informatico.....	19
3.5 Documento informatico in ingresso su Posta Elettronica Istituzionale	20
3.6 Documento informatico in ingresso su Posta Elettronica Certificata	21
3.7 Documento informatico in uscita	22
3.8 Documento informatico interno	23
3.9 Documento analogico.....	24
3.10 Documento analogico ingresso.....	24
3.11 Documento analogico in uscita	24
3.12 Documento analogico interno.....	24
3.13 Fax.....	24
3.14 Documento analogico non firmato	24
3.15 Documenti indirizzati alle persone	24

3.16	Rubrica	25
3.17	Sistema E-MESSAGE	25
CAPITOLO IV		27
4.	MODALITÀ DI PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO	27
4.1	Premessa	27
4.2	Unicità della registrazione del protocollo informatico	27
4.3	Registro giornaliero di protocollo.....	27
4.4	Registrazione di protocollo.....	28
4.5	Segnatura di protocollo dei documenti	28
4.6	Annullamento delle registrazioni di protocollo	29
4.7	Descrizione funzionale e operativa del sistema di protocollo informatico.....	29
CAPITOLO V		30
5.	SISTEMA DI CLASSIFICAZIONE FASCICOLAZIONE DEI DOCUMENTI	30
5.1	Titolario	30
5.2	Classificazione dei documenti	30
5.3	Fascicolazione dei documenti.....	31
CAPITOLO VI		32
6.	ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI	32
6.1	Generalità	32
6.2	Accesso al sistema	32
6.3	Profili d'accesso	32
CAPITOLO VII.....		34
7.	MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA	34
7.1	Premessa	34
7.2	Attivazione del registro di emergenza	34
7.3	Attività possibili durante l'attivazione del registro di emergenza	34
7.4	Riattivazione del sistema informatico	34
CAPITOLO VIII		36
8.	REGOLE GENERALI DI SCRITTURA DEI DATI.....	36

ELENCO ALLEGATI

Allegato “A” Area Organizzativa Omogenea

Allegato “B” Nomine

Allegato “C” Fac-simile restituzione documento

Allegato “D” Fac-simile lettera/documento

Allegato “E” Personale autorizzato alla firma verso l'esterno

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

1	
2	
3	
4	
5	
6	

ACRONIMI E RIFERIMENTI NORMATIVI

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.

Inoltre, 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.

I riferimenti normativi sono da intendersi comprensivi delle varianti, aggiunte e correzioni nel frattempo intervenute sul provvedimento stesso. La normativa inerente al Protocollo Informatico (PI) è piuttosto vasta; vengono quindi riportati solo gli atti principali ed originari.

AOO	Area Organizzativa Omogenea un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
GTMIL_VR	Area Organizzativa Omogenea del Tribunale Militare di Verona
[CAD]	Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'Amministrazione digitale
[CIRC]	Circolare AIPA 7/5/2001 n. 28 Regole tecniche per l'interoperabilità dei sistemi di protocollo informatico
[CODBCP]	Decreto Legislativo n. 22 gennaio 2004 n. 41 - Codice dei beni culturali e del paesaggio, ai sensi dell'art.10 della legge 6 luglio 2002, n. 137.
[CODPRI]	Decreto Legislativo 30 giugno 2003 n. 196 "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.
AgID	Agenzia per l'Italia digitale Decreto legge n. 83/2012 Ai sensi del Decreto legge n. 83/2012, convertito in legge n. 134/2012, l'ente DigitPA (Ente nazionale per la digitalizzazione della Pubblica Amministrazione) è stato soppresso ed è stata istituita l'Agenzia per l'Italia digitale
[DIR]	Direttiva SMD-I-004 Il protocollo informatico nella Difesa.

[DPCM]	Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013, recante le “Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005” (GU n. 59 del 12-3-2014 - Suppl. Ordinario n. 20)
[DPR]	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. “Disposizioni legislative in materia di documentazione amministrativa. Con il DPR n. 445 si effettua una razionalizzazione e semplificazione della normativa inerente al Protocollo Informatico.
IPA	Indice delle Pubbliche Amministrazioni
INI-PEC	Indice degli indirizzi dei professionisti e delle imprese
PA	Pubblica Amministrazione
PEC	Posta Elettronica Certificata - Decreto del Presidente della Repubblica 11 febbraio 2005, n.68 Regolamento recante disposizioni per l'utilizzo della 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. L'art. 4, c. 1 della L. n. 241/90 e s.m.i. impone ad ogni amministrazione pubblica di determinare l'unità organizzativa responsabile della istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale.

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.

1. Area Organizzativa Omogenea (AOO)

Una AOO, (art. 50 comma 4 e dall'art. 61 **[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.

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

Il RDS è l'altra novità di rilievo introdotta dalla normativa (art. 61 **[DPR]**). In sostanza si tratta di una figura ben diversa dal classico Capo Ufficio Posta o figure simili, da sempre presenti nell'A.D.. I suoi compiti, 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.

3. Il Manuale di Gestione (Manuale)

Il Manuale, previsto dall'art. 5 del DPCM, descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del PI. In particolare, il Manuale contiene l'insieme delle regole, certificate dall'AOO, per un corretto ed efficace funzionamento del sistema di protocollo, dei procedimenti amministrativi informatici e del sistema documentale, costituendo, pertanto, la "carta dei servizi" dell'AOO stessa nella quale gli interessati trovano descritte le modalità di gestione del protocollo nei suoi diversi aspetti. Il Manuale è un documento dinamico, che deve essere aggiornato in dipendenza delle modifiche alle procedure manuali, organizzative ed informatiche applicate alla gestione del protocollo. Il Manuale deve essere predisposto dal RDS; quale garante dell'esclusiva adozione ed applicazione delle procedure indicate al suo interno siano seguite nell'ambito dell'AOO di pertinenza.

4. 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'aggregazione strutturata e univocamente

identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento.

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 gestione;
- 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;
- l'eventuale riferimento alle modalità di accesso (legge 241/90) nel rispetto della tutela dei dati personali (D.Lgs 196/2003). 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 dell'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).

Nelle voci del piano di classificazione è opportuno evitare la presenza di voci generiche, come ad esempio la denominazione “VARIE”, o simili, poiché i documenti così classificati diventano, di fatto, irreperibili. Il piano di classificazione deve essere aggiornato periodicamente (almeno ogni due anni).

5 Casella di Posta Elettronica Istituzionale [[tribmil.vr @ gm.difesa.it](mailto:tribmil.vr@gm.difesa.it)]

La casella di Posta Elettronica Istituzionale (PEI) è impiantata da ciascuna AOO. Essa è impiegata dal sistema “Adhoc” per ricevere e inviare i documenti informatici. Pertanto tutta la documentazione prodotta dalle UO è inviata dal sistema, tramite questo canale, alle AOO esterne destinatarie.

6 La Posta Elettronica Certificata (PEC) [[tribmil.vr @ postacert.difesa.it](mailto:tribmil.vr@postacert.difesa.it)]

La Posta Elettronica Certificata (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. Esso è strettamente connesso all’utilizzo della firma digitale, per l’individuazione dei soggetti intervenuti nel processo di trasmissione e ricezione del documento, del quale si hanno informazioni quali la data, l’ora, il mittente, il destinatario, l’oggetto, il contenuto e quanto altro è necessario per la trasmissione di un atto o documento informatico. 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.

La casella di posta certificata del Tribunale Militare è attiva e disponibile attraverso il sistema “Adhoc” per la ricezione (unicamente posta certificata) e l’invio di documenti informatici.

La Posta Elettronica Certificata è il sistema di comunicazione prevalente.

7. Amministrazioni Pubbliche

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

8. Archivio

L’archivio è la raccolta ordinata degli atti spediti, inviati o comunque formati dall’Amministrazione nell’esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall’Amministrazione o dalla Area Organizzativa Omogenea sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall’affare al quale si riferiscono. Essi sono ordinati e archiviati in modo coerente e accessibile alla consultazione; l’uso degli atti può essere amministrativo, legale o storico. L’archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, l’archivio viene

suddiviso in:

- **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 corrente;

- **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 (locale individuato presso la Caserma “Duca” Montorio Veronese):

- **Archivio storico**

Costituito da complessi di documenti relativi ad affari ed a procedimenti amministrativi conclusi da anni e destinati, previa l’effettuazione delle operazioni di scarto, alla conservazione perenne (Attualmente sono conservati nell’Archivio di Stato solo i fascicoli dei procedimenti penali seguiti dal Responsabile o Personale Addetto alla cancelleria e soggetti a registrazione particolare, perciò esclusi dal Protocollo Informatico).

9. 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.

10. Documento informatico

Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (CAD art. 1p).

11. Documento analogico

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

12. Dati sensibili e dati giudiziari

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.

Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all’articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale. (*art. 4 del d. lgs. 30 giugno 2003 n. 196*).

13. Fascicolazione

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

14. 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 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.

15. Unità organizzativa (UO)

Per Unità organizzativa (UO) si intende uno dei sottoinsiemi di una AOO, cioè un complesso di risorse umane e strumentali cui sono state affidate competenze omogenee nell'ambito delle quali il Capo Ufficio/Servizio è il Responsabile del Procedimento Amministrazione (RPA) nella trattazione dei documenti o procedimenti amministrativi.

CAPITOLO I

1. PRINCIPI GENERALI

1.1 Premessa

Il Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013 [DPCM], prevede per tutte le amministrazioni l'adozione del Manuale di gestione. Quest'ultimo, disciplinato dal 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, ogni Amministrazione Pubblica deve individuare una o più Aree Organizzative Omogenee, all'interno delle quali è previsto che debba essere nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Il manuale è uno strumento operativo che, per il grado di analisi che ogni Amministrazione è chiamata ad effettuare, può rappresentare un primo e significativo passo verso la certificazione di qualità del servizio.

Il manuale è rivolto pertanto a tutti coloro i quali utilizzano il protocollo informatico come strumento di lavoro per la gestione dei documenti e dei procedimenti amministrativi che sono chiamati a trattare e dei quali sono individuati come responsabili. In esso infatti, sono descritte le fasi operative del sistema per la gestione del protocollo informatico, dei flussi documentali e degli archivi, individuando per ogni azione o processo i rispettivi livelli di esecuzione, responsabilità e controllo, in una visione d'insieme – senza soluzioni di continuità – dal protocollo all'archivio storico. Inoltre si evidenzia che il citato manuale è anche lo strumento per definire i principi ed i criteri di comunicazione dei cittadini, imprese ed altre P.A. con l'AOO.

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

Questo Manuale, che ne descrive i principi di funzionamento rappresenta, quindi, un elemento essenziale per comprensione delle logiche organizzative e funzionali preposte alla gestione documentale dell'AOO: **GTMIL_VR**.

1.2 Ambito di applicazione del Manuale di gestione/Area Organizzativa Omogenea (AOO)

Il presente Manuale afferisce all'AOO del Tribunale Militare di Verona suddiviso in 8 (otto) UO (All. "A"- Atto Costitutivo).

1.3 Servizio per la gestione del protocollo informatico

Nell'AOO precedentemente individuata è istituito un servizio per la tenuta del protocollo informatico, "Adhoc" la gestione dei flussi documentali e degli archivi, l'atto di nomina del Responsabile di tale servizio è in All. "B" unitamente alla nomina del Vicario.

1.4 Firma digitale

La gestione digitale del protocollo informatico prevede l'uso della firma digitale sia per l'invio della documentazione al di fuori dell'AOO (documento informatico) sia per la digitalizzazione dei documenti cartacei in ingresso. I titolari che hanno capacità di firma sono il personale indicati dai capi delle UO.

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

1.5 Tutela dei dati personali

I dati per i quali ai sensi del D.Lgs. 30/06/2003 n. 196 è necessaria una specifica gestione sono trattati in conformità al citato decreto.

1.6 Entrata in vigore del Manuale

Le regole indicate nel presente manuale saranno applicate 2 giorni dopo la firma del Presidente del Tribunale.

CAPITOLO II

2. FORMAZIONE TRASMISSIONE SOTTOSCRIZIONE E ARCHIVIAZIONE DEI DOCUMENTI INFORMATICI

2.1 Formazione dei documenti - aspetti operativi

In aderenza alla normativa vigente (art. 40 del CAD) l'AOO formano gli originali dei propri documenti con mezzi informatici inoltre si evidenzia che anche i documenti cartacei in ingresso vengono dematerializzati in modo che l'intero flusso documentale venga gestito in maniera elettronica.

Fanno eccezione i documenti relativi ai fascicoli giudiziari per i quali l'iter di formazione ed aggiornamento è generalmente analogico. I fascicoli in ingresso non saranno attualmente dematerializzati.

Altri aspetti fondamentali di un documento sono:

- trattazione di un unico argomento indicato in maniera sintetica nello spazio riservato all'oggetto;
- riferimento ad un solo numero di registrazione di protocollo;
- possibilità di far riferimento a più fascicoli.

2.2 Sottoscrizione di documenti informatici

Tutti i documenti informatici firmati digitalmente sono gestiti dal protocollo informatico nel formato PDF/A.

Solo 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.

2.3 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 Posta Elettronica Certificata (PEC), sempreché anche il corrispondente ne disponga.

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

Il mezzo di comunicazione privilegiato è la casella di posta elettronica certificata.

2.4 Archiviazione del documento informatico

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

CAPITOLO III

3. LA GESTIONE DEI DOCUMENTI – ASPETTI FUNZIONALI

3.1 Generalità

I documenti, sia analogici, sia informatici vengono gestiti in relazione al loro formato, in ambito AOO, suddivisi nel seguente modo:

- in ingresso;
- in uscita;
- interno.

La gestione documentale in generale si basa sui principi di:

- centralità per quanto concerne la posta in ingresso, la totale corrispondenza indirizzata al Tribunale Militare viene registrata in un unico punto (Servizio di Protocollo Informatico);
- delega alle UO che hanno facoltà di trasmettere direttamente i documenti sia informatici sia analogici all'esterno dell'AOO.

I documenti in ingresso alla AOO sono assegnati direttamente ai Capi delle UO interessate (Responsabili del Procedimento Amministrativo), **entro due giorni lavorativi dalla ricezione**, i quali provvedono alla successiva gestione interna.

Inoltre 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.

3.2 Orario di erogazione del Servizio

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

- Lunedì - Venerdì dalle ore 08:30 alle ore 14:30;
- Sabato il servizio di protocollo non è attivo.

3.3 Documenti protocollati e documenti esclusi dalla protocollazione

Appare necessario evidenziare che il sistema informatico del protocollo è progettato al fine della trattazione unicamente dei documenti non classificati.

Inoltre i documenti di seguito specificati sono esclusi dalla registrazione di protocollo:

- documenti classificati;
- documenti già soggetti a registrazione particolare dell'Amministrazione;
- gazzette ufficiali;
- bollettini ufficiali P.A. notiziari P.A.;
- giornali, riviste, libri e materiali pubblicitari;
- inviti a manifestazioni che NON attivino procedimenti amministrativi;
- fogli di viaggio;
- note caratteristiche e rapporti informativi (è protocollata solo la lettera di spedizione);

- modelli 730 (è protocollata solo la lettera di spedizione);
- registro delle presenze, licenze, permessi;
- esposti anonimi;
- informazioni elettroniche superiori ai 30 mega dimensione oltre la quale il sistema non registra.
- fascicoli (è protocollata solo la lettera di spedizione).

Relativamente ai documenti “sensibili” (citato punto 12 del Glossario) sono previste particolari forme di riservatezza e di accesso controllato mediante la selezione, da parte del personale della Sezione Protocollo, di un filtro elettronico, fermo restando che l’UO competente può in qualsiasi momento filtrare il documento in trattazione.

3.4 Documento informatico

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

Per la ricezione di documenti informatici L’AOO dispone di una casella di posta elettronica istituzionale e di una casella di PEC:

- casella di Posta Elettronica Istituzionale: **tribmil.vr @ gm.difesa.it**
- casella di Posta Elettronica Certificata: **tribmil.vr @ postacert.difesa.it**

Su entrambe le caselle, nel rispetto della normativa vigente, è possibile inviare documentazione afferente l’attività dell’AOO.

La casella di posta elettronica certificata tribmil.vr@postacert.difesa.it è configurata per accettare in ingresso unicamente messaggi certificati.

Se un documento informatico viene inviato ad una casella di posta elettronica istituzionale afferente una UO, il titolare di tale caselle deve inviare un messaggio al mittente segnalando la necessità di inviare nuovamente il documento alla corretta casella postale dell’AOO secondo il testo in All. “C”.

In nessun caso è autorizzata la funzione di inoltrare verso la PEI o la PEC della AOO da parte di indirizzi interni della UO.

L’AOO accetta documenti informatici conformi ai seguenti dettami:

- Nel caso in cui il messaggio debba contenere degli allegati, il formato preferenzialmente accettato è il PDF (è obbligatorio il formato PDF/A in caso di apposizione preventiva di firma digitale);
- Sono altresì accettati i formati DOCX, XLSX (in caso di documento Excel dovrà essere allegata la stampa in formato PDF dei dati), TXT, TIFF; TIF, XML e RAR, ZIP;
- L’invio di allegati non previsti, comporta la ritrasmissione al mittente del messaggio;
- Le eventuali marche temporali apposte insieme alla firma digitale devono essere in formato embedded e non detached (il file firmato e la firma devono essere contenuti in un unico busta di file);
- È raccomandata l’apposizione della firma digitale ai documenti allegati messaggio;
- L’apposizione di una firma digitale non valida rende non utilizzabile il file eventualmente trasmesso;
- In un singolo messaggio di posta elettronica deve essere associata la documentazione relativa ad un unico argomento (pertanto se un mittente deve inviare cinque documenti afferenti cinque pratiche, dovrà inviare cinque mail);

- La massima dimensione complessiva degli allegati deve essere di 30 MB per la PEI.
- Per la PEC il limite è di 100 MB per un destinatario, 50 MB nel caso di due destinatari, ecc.;
- 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 dalla casella postale dittarossispa@xxxxx.it e non dalla casella postale mario.rossi@rossispa.xxxxx.it) poiché in tal caso risulterà il sistema risponderà ad una casella postale impropria;
- Il nome dei file allegati deve essere di lunghezza moderata, non contenere caratteri speciali (lettere accentate, caratteri speciali ad esempio ° / ^), virgolette, apici. Si suggerisce di utilizzare il carattere _ (underscore) al posto di tali caratteri.

3.5 Documento informatico in ingresso su Posta Elettronica Istituzionale

I messaggi provenienti sulle caselle di posta vengono inseriti in un'apposita coda. L'operatore di protocollo accede alla predetta coda ed i messaggi vengono presentati in ordine di arrivo all'AOO.

L'operatore può protocollare il messaggio, procedendo alla successiva assegnazione all'UO competente ovvero, nei casi dubbi, può inviare il messaggio 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, rispediti al mittente.

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 istituzionale solo se firmato digitalmente.

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 particolare, 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 i messaggi che segnalano un problema di ricezione nella casella postale istituzionale 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, per le opportune azioni del caso.

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

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

Il personale deve verificata la presenza di messaggi almeno quattro volte al giorno.

3.6 Documento informatico in ingresso su Posta Elettronica Certificata

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 non competenza dell'AOO, sarà quest'ultima, attraverso un messaggio protocollato via PEC, ad informare il mittente di tale evenienza. Per questi casi la risposta da inviare deve essere di tipo standard, secondo il testo in All. "C".

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 particolare, 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. Il personale dell'AOO deve verificata la presenza di messaggi almeno quattro volte al giorno.

3.7 Documento informatico in uscita

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

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

Il documento può essere firmato ed inoltrato anche da personale della UO non dirigente ma autorizzato dal Presidente del Tribunale (All. "E"). In questo caso è indispensabile provvedere alla creazione in "Adhoc" di un nuovo documento digitale (lettera di inoltro) al quale allegare la scansione del documento analogico firmato. Quest'ultimo sarà custodito e gestito secondo le peculiari norme.

È obbligatoria la congruenza tra gruppo firma del documento e firma digitale dello stesso.

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 aventi causa allegati presenti. L'utilizzo della casella postale elettronica PEI 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. 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, documenti ritenuti sensibili,...).

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

Nel primo caso (destinatario privo di una casella di posta elettronica) 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.

Si evidenzia che se vi sono dei destinatari a cui va inviato il documento solo per "conoscenza" a questi ultimi il sistema provvede ad inviare regolarmente la posta elettronica.

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 procedure alla successiva trasmissione.

Pertanto i documenti succitati firmati digitalmente avvenuta l'apposizione della marca temporale confluiscono invece in una apposita lista dove l'operatore originatore provvede 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) attivando la visualizzazione della segnatura e del glifo.

Il sistema in automatico non elimina la "coda di stampa" ma è compito dell'operatore dare assicurazione della avvenuta stampa premendo il pulsante di conferma a destra.

@D  C

GTML_VR 03-09-2015 Notifiche: 0 Lista Personale: 0

PROTOCOLLO / SCRIVANIA / AMMINISTRAZIONE / CONSULTAZIONE / FINE SESSIONE

[Esci](#)

6 elementi trovati.
1

Protocollo	Data prot.	Da	Oggetto	Destinatari	Nr.	Doc./All.	
0900841	02-09-2015	gtvr_capoudienze (Anna...	proc. n. RGNR 01.1999 e 691.1999 R.G.I.P. ex ...		1 - 0		  
0900845	02-09-2015	gtvr_capoudienze (Anna...	proc. n. RGNR 4.1997 e 1081.1997 R.G.I.P. ex ...		1 - 0		  



Qualora necessario apporre sul retro del documento stampato la seguente frase:

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

Verona, __/__/____

Il Responsabile dell'UO
(xxxx xxx x x xxxx x xxxxxxxxx)

Al termine, il documento primario e gli eventuali allegati vengono spediti all'indirizzo postale del corrispondente, secondo le usuali procedure analogiche. Al fine di inviare correttamente un documento informatico è necessario applicare le indicazioni di cui al paragrafo 3.4.

Qualora come allegato, venga inserito un documento informatico già firmato digitalmente, l'operatore che effettua la predisposizione deve cliccare sulla voce NO PDF, per evitare la successiva conversione in PDF/A del documento. Tale operazione oltre a non essere utile su un documento precedentemente firmato digitalmente, potrebbe generare errori nel sistema informatico idonei a bloccare la fase di protocollazione e trasmissione del documento.

3.8 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 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.

3.9 Documento analogico

L'indirizzo preposto alla ricezione della documentazione analogica dell'AOO è:

Tribunale militare di Verona - Stradone Porta Palio, 55 - 37122 VERONA (VR)

3.10 Documento analogico ingresso

La corrispondenza di tipo cartaceo che viene trattata dal Servizio di Protocollo Informatico è del tipo: posta raccomandata, assicurata, ordinaria, pacchi ed E-MESSAGE.

Tutta la posta in arrivo viene prelevata a carattere giornaliero dal personale preposto dell'Ufficio Posta. Una volta aperte le buste e controllata la titolarità del destinatario si procede secondo la procedura di protocollo (dematerializzazione e inoltrate all'UO competente).

Attualmente i fascicoli giudiziari sono esclusi dalla dematerializzazione. Solo la lettera di accompagnamento viene scansionata e protocollata.

Tutti gli originali sono consegnati alle competenti UO che provvedono all'archiviazione degli stessi.

3.11 Documento analogico in uscita

La posta ordinaria cartacea in partenza, (questa si configura come il documento informatico stampato in quanto il destinatario o non ha la casella postale elettronica o si è costretti ad inviare documenti analogici), viene portata presso l'Ufficio Posta per la successive spedizione.

3.12 Documento analogico interno

Il sistema non prevede l'origine di documenti analogici, l'eventuale documentazione cartacea segue le regole già descritte nel sottopara inerente al documento informatico in uscita.

3.13 Fax

L'Ufficio Posta dispone di un apparato fax per la ricezione di documenti.

Qualora gli originali non pervengano successivamente per posta o/e e-mail, saranno dematerializzati e soggetti a protocollazione.

In casi eccezionali o in procedura di emergenza è autorizzato l'uso del fax in trasmissione.

3.14 Documento analogico non firmato

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

3.15 Documenti indirizzati alle persone

La corrispondenza analogica indirizzata direttamente alla persona, non viene aperta dal personale dell'Ufficio Posta, ma viene consegnata all'interessato che, presa visione della documentazione, se è di interesse dell'Amministrazione, chiederà la relativa registrazione.

3.16 Rubrica

Il sistema “Adhoc” utilizza una rubrica, che contiene gli indirizzi di tutte le AOO.

La rubrica è già popolata da un numero consistente di indirizzi dell’area della Difesa e della Pubblica Amministrazione.

L’elenco per sua natura non può essere esaustivo di tutti i possibili destinatari della corrispondenza prodotta.

Il database degli indirizzi è aggiornato dal personale del RDS sulla base delle informazioni ricevute dagli utenti che ne fanno esplicita richiesta scritta fornendo i dati secondo il seguente prospetto.

Creazione Mittente/Destinatario

PULISCI | SALVA |

● Nominativo Interno * Campo Obbligatorio

● Indirizzo

● Città

● Cap

● Provincia

● Stato

● Telefono

● Fax

● Email

● Email Certificata

● Istituzionale: ☐

3.17 Sistema E-MESSAGE

La corrispondenza generata attraverso il sistema deve essere trattata come di seguito indicato.

Le UO devono, mediante le funzioni del sistema “Adhoc”:

- approntare il testo del messaggio e gli eventuali allegati in formato digitale, tenendo conto che il messaggio può essere approntato mediante il sistema E-MESSAGE e poi esportato in formato PDF, anziché essere stampato;
- inoltrare il messaggio fino al livello Responsabile della UO per la visione e l’approvazione (non deve essere spuntata la casella “Dati analogici”);
- approvare i documenti, mediante apposizione della firma digitale da parte del Responsabile della UO, contestualmente alla quale viene effettuata la registrazione di protocollo;
- il documento è inoltrato a tutti gli indirizzi indicati in sede di predisposizione.

Successivamente, le stesse UO dovranno:

- inserire nel testo del messaggio prodotto con il sistema E-MESSAGE il numero di protocollo attribuito dal sistema “Adhoc”;
- inviare il messaggio anche, laddove ritenuto necessario, tramite la postazione E-MESSAGE della UO.

I destinatari del messaggio, tra cui quelli eventualmente appartenenti alle UO del Servizio stesse, riceveranno per posta elettronica il file prodotto dal sistema “Adhoc” che, firmato digitalmente, è di per sé idoneo alla trattazione e all’archiviazione.

Qualora inviato anche via E-MESSAGE, alcuni o tutti i destinatari riceveranno il messaggio anche in formato cartaceo.

Nel caso in cui fra i destinatari compaia una lista AIG (Address Indicator Group) e l’inserimento di tutti gli indirizzi nella rubrica di “Adhoc”, o la loro selezione, risulti troppo laborioso si può provvedere a registrare il codice identificativo dell’AIG (es.: AIG 2395) nella tabella degli indirizzi, senza associare ad esso altri dati (indirizzi postale, email, ecc.).

CAPITOLO IV

4. MODALITÀ DI PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

4.1 Premessa

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

4.2 Unicità della registrazione del protocollo informatico

Nell'ambito della AOO, il registro di protocollo è unico così come la numerazione progressiva delle registrazioni di protocollo, indipendentemente dal modello organizzativo, centralizzato o distribuito delle UO, adottato dall'AOO medesima. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia l'uno gennaio dell'anno successivo. Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro. Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

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

Non è consentita la protocollazione di un documento già protocollato.

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

4.3 Registro giornaliero di protocollo

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

La stampa delle registrazioni giornaliere viene firmata digitalmente in modalità manuale/automatica. La stampa viene archiviata all'interno del sistema ed è sempre possibile effettuarne copie cartacee o digitali

4.4 Registrazione di protocollo

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

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo 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, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

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

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

4.5 Segnatura di protocollo dei documenti

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

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

Sui documenti in ingresso, se presente, vengono utilizzati dati contenuti nel file `segnatura.xml`, purché conforme alle indicazioni della [CIRC]. Il protocollo di ingresso è apposto sul margine sinistro della prima pagina del documento. Sui documenti in uscita la segnatura di protocollo viene impressa sul primo foglio del documento informatico, in alto a sinistra.

Al fine di garantire la validità del documento informatico così prodotto, la segnatura apposta sul documento viene firmata, in modalità automatica. Il file `segnatura.xml` viene allegato a tutti i documenti in uscita per posta elettronica.

Il formato della segnatura di protocollo prevede i seguenti dati:

- Codice dell'Amministrazione: `M_D`
- Codice dell'AOO: `GTMIL_VR`
- Identificativo del registro: `REGxxxx`
- Numero di protocollo: `1234567`
- Data di registrazione: `gg-mm-aaaa`

Esempio di segnatura di protocollo: **`M_D GTMIL_VR REG2019 0004013 21-05-2019`**

4.6 Annullamento delle registrazioni di protocollo

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

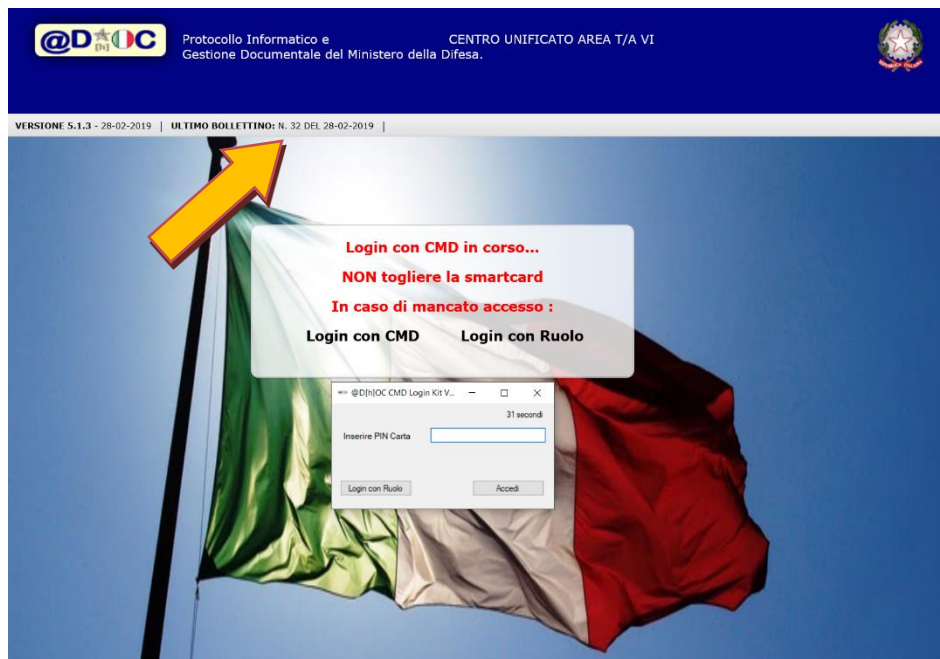
È altresì possibile annullare una registrazione di protocollo per un documento erroneamente fatto entrare nel patrimonio documentale dell'A.OO.

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

L'annullamento di una registrazione di protocollo può avvenire anche su richiesta specificando la nota ed il nominativo dell'interessato che ha indicato l'operazione, adeguatamente motivata, indirizzata al RDS.

4.7 Descrizione funzionale e operativa del sistema di protocollo informatico

Tutte le informazioni di dettaglio inerenti alle funzionalità presenti nel Sistema di Protocollo Informatico e Gestione Documentale (@DhOC) sono reperibili nella guida utente e nei bollettini disponibili sulla pagina di accesso al sistema.



CAPITOLO V

5. SISTEMA DI CLASSIFICAZIONE FASCICOLAZIONE DEI DOCUMENTI

5.1 **Titolario**

Sulla base dei riferimenti normativi e metodologici sopra esposti, è stato predisposto un *Titolario* di archivio organizzato per Titolo, Classe, Sottoclasse, Fascicolo e Sottofascicolo;

Il Titolario del GTMIL_VR presenta i caratteri di generalità e di completezza necessari per soddisfare le esigenze precipue del Tribunale Militare e del supporto.

Le voci del 1° livello

Il Titolario, è stato strutturato secondo 8 voci di 1° livello corrispondenti ad altrettante funzioni individuate:

- AMM - Amministrazione;
- GIUD - Attività Giudiziaria;
- INF - Informatizzazione uffici
- INFRA - Infrastrutture;
- MAT - Materiali;
- PER - Personale;
- PRES - Presidenza;
- TEL - Telefonia.

La struttura finale del Titolario: le voci di 2° e 5° livello

La successiva articolazione del Titolario prevede voci di livello successive (dal 2° al 5°), mediante associazione, a ciascuna delle suddette funzioni, delle rispettive sottofunzioni e/o attività e/o materie di pertinenza.

L'aggiornamento del titolario (dal 1° al 3° livello) compete esclusivamente al vertice del GTMIL_VR tramite proposta scritta da parte del responsabile dell'UO.

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.

5.2 **Classificazione dei documenti**

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

Essa è eseguita attraverso il titolario di classificazione.

Tutti i documenti ricevuti e 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 è svolta dal personale della competente UO: di norma il responsabile può inserire la voce di livello più alto, mentre l'attribuzione delle voci di dettaglio è demandata all'incaricato della trattazione della pratica.

5.3 Fascicolazione dei documenti

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

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

I fascicoli e i sottofascicoli sono invece gestiti direttamente dagli interessati ai relativi provvedimenti. In particolare, per poter classificare un documento è necessario inserirlo in un fascicolo oppure in sottofascicolo.

Il sistema consente la creazione di fascicoli e sottofascicoli. Durante la creazione di un fascicolo/sottofascicolo la visualizzazione della pagina internet DEVE essere mantenuta al 100 % di zoom.

Per tale attività gli addetti dovranno attenersi alle seguenti regole:

- il codice del fascicolo o del sottofascicolo deve essere numerico;
- la descrizione deve essere sintetica e definita.

Per quanto attiene alla descrizione occorre attenersi alle regole generali di scrittura dei dati, indicate nell'apposito paragrafo, inoltre appare opportuno evidenziare che non possono essere creati fascicoli con denominazione generica come ad es. "Varie".

Il sistema mantiene traccia della data di creazione del fascicolo.

Chi protocolla, classifica MA NON fascicola NON è in regola.

Esempio:

Codice fascicolo: anno/numero registro

Descrizione fascicolo: COGNOME Nome

Risultato: 2013/123 RGNR - ROSSI Mario

CAPITOLO VI

6. ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

6.1 Generalità

Il controllo degli accessi garantisce che l'impiego dei servizi del sistema informatico e del protocollo si svolga 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'UO di appartenenza.

6.2 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), assegna agli utenti diversi livelli di autorizzazione, tali utenti una volta identificati, sono suddivisi secondo diversi profili di accesso, sulla base delle rispettive competenze. Deve essere segnato che una singola persona fisica può ricoprire più ruoli, mantenendo, comunque la stessa password di accesso, legata, quest'ultima, alla persona fisica.

6.3 Profili d'accesso

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

Le principali profilazioni riguardano le funzioni di:

- *amministratore di sistema*: è colui il quale può accedere ai profili di configurazione di base del sistema; in genere è rilasciata a poche persone, sotto il diretto controllo del RDS;
- *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. Attualmente tutti gli utenti delle AOO sono abilitati a tale funzione.
- *accesso alla tabella dei corrispondenti (destinatari)*: l'accesso è centralizzato e gestito da un ristretto gruppo di utenti che garantiscono uniformità e coerenza ai dati immessi ;
- *abilitazione alla firma digitale degli atti*: in genere legata alla funzione di firma di documenti verso l'esterno (All. "E");

- *predisposizione di documento*: è la funzione che consente di preparare gli atti per il flusso in uscita;
- *consultazione*: in linea generale tutti gli utenti dovrebbero essere abilitati alla consultazione dell'archivio, il cui accesso è comunque legato al cono d'ombra di visibilità, determinato dalla propria posizione nell'albero gerarchico dell'AOO. In particolare, le informazioni legate al registro di protocollo sono visibili a tutti gli utenti mentre i documenti in quanto tali sono visibili solo a chi appartiene al relativo cono d'ombra. Va ricordata, a questo proposito, l'ulteriore profilazione, inerente alla possibilità di accedere ai documenti che contengono dati sensibili (tutti gli utenti sono abilitati alla consultazione);
- *accesso alla scrivania*: anche questa funzione dovrebbe essere abilitata a tutti gli utenti, poiché su tale strumento si basa lo 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 (All. "E").

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 (ad esempio per temporanee assenze dovute a corsi o licenze) sono stabiliti dal RDS.

Tale operazione per la sua importanza andando a modificare l'ordinamento delle UO, viene determinata solo ed esclusivamente previa formale richiesta da parte dei responsabili delle diverse UO. Il personale deve comunicare il delegato ed il periodo di delega (inizio/fine) per l'intero intervallo di assenza programmata.

In caso di improvviso impedimento si seguiranno le indicazioni degli ordini di servizio e/o differenti disposizioni.

CAPITOLO VII

7. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

7.1 Premessa

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

7.2 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 rilevante, 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.

7.3 Attività possibili durante l'attivazione del registro di emergenza

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

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

Per quanto riguarda la documentazione in uscita, essendo possibile solo attraverso l'apposizione della firma digitale e tramite la posta elettronica, la funzione di registrazione a protocollo 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 competenze 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.

7.4 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 a cura del RDS.

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

In particolare per i documenti in ingresso nell'oggetto dovrà essere riportato il numero del registro di emergenza in maniera che in caso di ricerca il numero di registrazione del documento informatico sia associato a quello di emergenza, es.: [**RE** xxxxxx gg-mm-aaaa].

Per i documenti in uscita, in considerazione che l'urgenza ha obbligato/costretto l'invio della corrispondenza nella modalità di emergenza, per registrare il documento senza inviarlo elettronicamente, basta indirizzarlo solo all'indirizzo anagrafico o renderlo analogico evidenziando nel campo oggetto quanto già descritto nell'ultimo capoverso.

CAPITOLO VIII

8. REGOLE GENERALI DI SCRITTURA DEI DATI

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

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

Vengono di seguito riportate poche regole, cui tutti gli utenti del sistema devono attenersi, nella redazione dei campi oggetto, 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. <i>Es.: ROSSI Mario</i>
Titoli di cortesia, nobiliari ecc.	Sempre omessi
Nomi di città	In lingua italiana, se disponibile. In maiuscolo solo la prima lettera.
Nomi di stati	In lingua italiana. In maiuscolo solo la prima lettera.
Nomi di ditte	In maiuscolo solo la prima lettera. L'eventuale forma societaria in minuscolo, senza punti di separazione. <i>Es.: Acme srl</i>
Enti/associazioni	Lettera maiuscola solo per l'iniziale della denominazione
Ministeri	Scritti per esteso. <i>Es.: Ministero della Difesa</i>
Enti di secondo livello	<i>Es.: Segredifesa V Reparto</i> NON V Reparto Segredifesa
Sigle di enti	Senza punti <i>Es.: ISTAT</i>
Date	Formato gg-mm-aaaa, numerico, separatore trattino <i>Es.: 23-10-2015</i>
Virgolette/apici	Digitare il relativo carattere dalla tastiera. NO copia/incolla da Word



TRIBUNALE MILITARE DI VERONA

- Il Presidente -

Atto di Costituzione dell'Area Organizzativa Omogenea

- VISTO l'articolo 2, comma 603 della legge 24 dicembre 2007, n. 244, che ha previsto la soppressione a far data dal 1° luglio 2008 di alcuni tribunali militari e, contestualmente ha individuato le nuove competenza del Tribunale Militare di Verona;
- CONSIDERATA la necessità di organizzare gli uffici del Tribunale Militare di Verona secondo le indicazioni contenute negli artt. 50-70 del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
- VISTO l'obbligo di istituire un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi;

DISPONE CHE

- il Tribunale Militare di Verona, sia costituito come Area Organizzativa Omogenea (AOO);
- presso questo Tribunale, siano individuate le seguenti unità organizzative responsabili delle attività di registrazione, di organizzazione e tenuta della documentazione:
 - 01 Segreteria Particolare;
 - 02 Segreteria Amministrativa, Personale, Affari Generali e Supporto;
 - 03 Cancellerie dibattimentali 1ª e 2ª Sezione;
 - 04 Cancellerie GIP / GUP;
 - 05 Recupero Crediti e Spese di Giustizia;
 - 06 Ufficio Impugnazioni;
 - 07 Ufficio Corpi di reato;
 - 08 Funzionario Delegato.

Verona, 15 maggio 2013

IL PRESIDENTE
Dott. Massimo BOCCHINI



TRIBUNALE MILITARE DI VERONA
Il Presidente

Ordine di servizio n. 5 / 2019

SERVIZIO DI PROTOCOLLO INFORMATICO E GESTIONE DOCUMENTALE

Nomina ed assegnazione dell'incarico:

Responsabile: Ten.Col. Valter BARONETTO
Vicario: App.Sc. Qual. Spec. Davide GOBBI
Addetti: Serg. Magg. Ca.Sc. Qual. Spec. Giancarlo DI GIOIA
C.M.C. Marco BELARDI
Sig. Giuseppe PALMESTON

Compiti: definire tempi, modalità e misure organizzative e tecniche finalizzate alla implementazione ed aggiornamento del servizio di protocollo Informatico;

- definire le modalità di produzione e conservazione delle operazioni di registrazione, segnatura, annullamento e modifica di protocollo informatico;
- definire le modalità di utilizzo del registro di emergenza;
- definire il sistema di classificazione delle informazioni e dei documenti e le relative modalità di aggiornamento;
- definire le modalità di utilizzo di strumenti informatici per lo scambio di documenti internamente ed esternamente all'AOO di responsabilità;
- predisporre il manuale di gestione che disciplina le procedure del sistema di gestione e di conservazione dei documenti;
- verificare la corretta applicazione del manuale di gestione e della normativa vigente da parte dei propri collaboratori.

Verona 26/06/2019



il Presidente del Tribunale
Vincenzo SANTORO

margin superiore 1,8 cm

TRIBUNALE MILITARE DI VERONA

UFFICIO

Stradone Porta Palio, 55 - 37122 tel. 045.8005319 fax 045.4931120-30
tribmil.vr @ postacert.difesa.it - tribmil.vr @ gm.difesa.it

ELIMINARE LA DATA

Allegati: n. ____ (____)

Nome Punto di Contatto
04549311__ (Sotrin 12507__)

Oggetto: Restituzione atti causa errato indirizzo

A: INDIRIZZO

37122 VERONA

^^^^^^

Si comunica che i seguenti documenti NON sono stati presi in carico da questo Tribunale Militare in quanto DESTINATI AD ALTRO ENTE:

- Lettera di prot. MD E 2528 del 6 agosto 2015
- Lettera di prot. MD E 253-355 del 6 agosto 2015

I documenti NON saranno inoltrati ad altro Ufficio/Ente.

Si invita a trasmettere nuovamente i messaggi all'indirizzo corretto:

se disponibile indicare l'ente corretto

indirizzo.mail@abcd.difesa.it

indirizzo.mail@postacert.difesa.it

IL RESPONSABILE
Grado Nome COGNOME

margin inferiore min. 4,4 cm

margin sinistro min. 2,1 cm

margin destro min. 2,1 cm

margin superiore 1,8 cm

TRIBUNALE MILITARE DI VERONA

UFFICIO

Stradone Porta Palio, 55 - 37122 tel. 045.8005319 fax 045.4931120-30
tribmil.vr @ postacert.difesa.it - tribmil.vr @ gm.difesa.it

ELIMINARE LA DATA

Allegati: n. ____ (____)

Nome Punto di Contatto
04549311__ (Sotrin 12507__)

Oggetto:

A INDIRIZZO

37122 VERONA

^^^^^^^^

Testo testo testo testo testo testo testo testo testo testo
testo testo testo testo testo testo

SALVARE IN FORMATO .docx

NON INSERIRE PROTOCOLLO E DATA NEL TESTO DEL DOCUMENTO

sarà apposta in automatico dal sistema @DhOC in alto a sinistra.

LA PARTE INFERIORE DEL DOCUMENTO È DESTINATA:

- ALLA STAMPA DELLA FIRMA DIGITALE (A SINISTRA)
- E ALL'EVENTUALE CERTIFICAZIONE TRAMITE APPOSIZIONE DEL GLIFO (A DESTRA).

IL RESPONSABILE
Grado Nome COGNOME

margin inferiore min. 4,4 cm

margin sinistro min. 2,1 cm

margin destro min. 2,1 cm

Personale Autorizzato alla firma ed invio di documenti all'esterno della AOO

MAGISTRATI

Col. CITARELLA

Ten. Col. BARONETTO

1° Lgt. LA SALA

Lgt. SIDDI

Dott.ssa MOSCATO

Dott. MOSCA

Dott.ssa ZENOBIO di FUSCO

Dott. BIAGINI

Dott.ssa GRILLO

Dott.ssa CALÒ

Sig. SICARI

Sig.ra MOTTA

App. sc. Qual. Spec. GOBBI

App. sc. RESTAINI

Staff RDS firma solo documenti in ingresso e successivamente dematerializzati