

Manuale di gestione del protocollo informatico, dei documenti e dell'archivio

Data approvazione modifiche	Modifiche apportate:

Titolo	Manuale di gestione del protocollo informatico, dei documenti e dell'archivio
Redattori del documento	Direttore Logistico Gestionale Vice Dirigente Elisabetta Carta
Stato del documento	Concluso
N. versione documento	1.0.0
Data di preparazione	20 Febbraio 2025
Data di revisione	
Data di approvazione	20 Febbraio 2025

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

1	DISPOSIZIONI GENERALI	6
1.1	Premessa	6
1.2	Ambito di applicazione del manuale.....	9
1.3	Organizzazione del Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile ai fini dell'adozione del protocollo informatico	9
1.3.1	Aree Organizzative Omogenee (AOO), Unità Organizzative (UOP), Responsabile del Procedimento Amministrativo.....	10
1.3.2	Servizio per la gestione informatica del protocollo	11
1.4	Accreditamento dell'amministrazione/AOO all'IPA	12
2.	LE TIPOLOGIE DOCUMENTARIE	13
2.1	Il documento amministrativo	13
2.1.1	Il documento informatico.....	13
2.1.2	Versione analogica di un documento informatico	13
2.1.3	Il documento analogico	13
2.1.4	Copia informatica di un documento analogico.....	14
2.1.5	Copia per immagine su supporto informatico di un documento analogico	14
2.2	Le tipologie operative di documenti	14
2.2.1	Documento ricevuto	14
2.2.2	Documento inviato	15
2.2.3	Documenti interni.....	16
3.	FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI.....	16
3.1	Requisiti degli strumenti informatici di scambio.....	17

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

3.2	Firma digitale e verifica delle firme con il Prodotto di Protocollo Informatico.....	18
4.	MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO.....	18
4.1	Unicità del protocollo informatico.....	19
4.2	Registro giornaliero di protocollo.....	20
4.3	Registrazione di protocollo	20
4.3.1	Registrazione dei documenti informatici	21
4.3.2	Registrazione dei documenti analogici	21
4.4	Elementi obbligatori delle registrazioni di protocollo.....	22
4.5	Segnatura di protocollo dei documenti	22
4.5.1	Segnatura dei documenti informatici.....	22
4.5.2	Uso della posta elettronica certificata	24
4.5.3	Segnatura dei documenti cartacei	25
4.6	Annullamento parziale delle registrazioni di protocollo	25
4.7	Annullamento di un protocollo (del registro ufficiale di corrispondenza)	26
4.8	Protocollazione di documenti riservati e livelli di riservatezza	26
4.8.1	documenti riservati.....	26
4.8.2	Livelli di riservatezza	28
4.9	Casi particolari di registrazioni di protocollo	30
4.10	Documenti oggetto di protocollazione obbligatoria ed esclusi dalla registrazione di protocollo.....	36
4.11	Registri di protocollo	37
4.12	Registro Ufficiale AOO COM-CA.....	37

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

4.13	Registro Ordini del Giorno.....	37
4.14	Registro delle Disposizioni di Servizio.....	38
4.15	Registro Atti Interni (Verbali e Decreti interni)	38
4.16	Registro interno atti contabili	38
4.17	Disposizioni finali in merito alle abilitazioni sui singoli Registri.....	38
5.	ORGANIZZAZIONE E GESTIONE DELL'ARCHIVIO CORRENTE SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE.	39
5.1	Generalità.....	39
5.2	Misure di protezione e conservazione degli archivi pubblici	39
5.3	Titolario	40
5.3.1	Classificazione dei documenti.....	41
5.4	Fascicolazione dei documenti	41
5.4.1	Apertura e chiusura del fascicolo	41
5.4.2	Processo di assegnazione dei documenti ad un fascicolo.....	42
6.	DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI.....	42
6.1	Flusso dei documenti ricevuti dalla AOO	43
6.1.1	Documenti in arrivo.....	43
6.1.2	Documenti in uscita.....	44
6.1.3	Assegnazione dei documenti.....	44
6.1.4	Presa in carico dei documenti	45
6.1.5	Classificazione ed archiviazione	46
7.	ACCESSO AL SISTEMA DI PROTOCOLLO INFORMATICO	47

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

7.1	Abilitazioni di accesso al sistema	47
7.2	Profili di accesso	48
8.	Piano di sicurezza	48
8.1	Obiettivo del Piano di Sicurezza	49
8.2	Generalità.....	49
8.3	Formazione dei documenti – aspetti di sicurezza	50
8.4	Gestione dei documenti informatici.....	51
8.5	Componente fisica della sicurezza.....	51
8.6	Custodia e archiviazione dei dati.....	52
8.7	Misure logiche di sicurezza.....	52
8.8	Norme di comportamento per la sicurezza informatica	53
8.9	Infrastruttura di rete.....	53
8.10	Criteri e procedure per il salvataggio e il ripristino dei dati (di competenza delle Strutture Centrali)	53
8.11	Trasmissione e interscambio dei documenti informatici.....	54
8.11.1	All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico).....	54
8.11.2	All'interno della AOO.....	55
8.12	Accesso al PdP da parte degli utenti interni alla AOO.....	55
8.12.1	Utenti esterni alla AOO – Altre AOO/Amministrazioni.....	56
8.12.2	Utenti esterni alla AOO – Privati	56
9.	MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA	57
9.1	Il registro di emergenza	57
9.2	Modalità di apertura del registro di emergenza	57

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

9.3	Modalità di utilizzo del registro di emergenza	61
9.4	Modalità di chiusura e recupero del registro di emergenza	61

1 DISPOSIZIONI GENERALI

1.1 Premessa

Ai sensi del decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000 (TUDA), le amministrazioni individuano una o più Aree Organizzative Omogenee, ai fini della gestione unica o coordinata dei documenti, assicurando criteri uniformi di classificazione e archiviazione.

In questo contesto ogni AOO nomina un responsabile della gestione documentale (RGD).

Il Dpcm del 3 Dicembre 2013 recante “*Regole tecniche per il protocollo informatico*” adottato ai sensi dell’art. 71 del D.Lgs 82/2005 – Codice dell’Amministrazione Digitale (CAD), obbliga le Pubbliche Amministrazioni di cui all’art. 2 comma 2 del CAD ad adottare il manuale di gestione del protocollo informatico, dei documenti e dell’archivio su proposta del RGD.

Il manuale succitato, in attuazione della normativa vigente, descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Tra i requisiti richiesti al sistema di gestione informatica documentale vi sono la garanzia di sicurezza e l’integrità del sistema, la corretta e puntuale registrazione del protocollo dei documenti in entrata e in uscita, consentire il reperimento delle informazioni riguardanti i documenti registrati nonché i collegamenti tra di essi ed il provvedimento finale, consentire, in condizioni di sicurezza, l’accesso degli interessati alle informazioni del sistema nel rispetto delle disposizioni in materia di riservatezza dei dati personali, garantire la corretta organizzazione del sistema di classificazione di archivio informatico (art. 53 TUDA).

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'amministrazione.

Il software per la protocollazione e gestione documentale adottato dal Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile è denominato "VIGILI@", sviluppato dalla società Dedagroup S.p.A.

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 ed archiviazione dei documenti.

Il presente documento pertanto, si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

Esso disciplina:

- relativamente agli aspetti organizzativi:
- le modalità di utilizzo degli strumenti informatici per la formazione dei documenti e per lo scambio degli stessi all'interno e all'esterno dell'AOO (Comando dei Vigili del Fuoco di Cagliari).
- l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno del fascicolo;
- l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro degli stessi verso aree organizzative omogenee del Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile o verso altre amministrazioni;
- i criteri e le modalità per il rilascio delle abilitazioni di accesso al sistema di gestione informatica dei documenti.

relativamente ai formati dei documenti:

- l'individuazione dei formati utilizzati per la formazione del documento informatico;
- la descrizione di eventuali ulteriori formati utilizzati in relazione a specifici contesti operativi.

relativamente al protocollo informatico e alle registrazioni particolari:

- le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di protocollazione;

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

- la descrizione delle modalità di utilizzo del sistema di protocollo informatico dei Vigili del Fuoco – VIGILI@;
- le modalità di utilizzo del registro di emergenza;
- l'elenco dei documenti esclusi dalla registrazione di protocollo;
- descrizione del registro Ufficiale, del registro degli Ordini del Giorno, del registro delle Disposizioni di Servizio e del registro degli Atti Esterni (Decreti).

relativamente alle azioni di classificazione e selezione:

- il piano di classificazione adottato dal Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile con nota DCAFFGEN 22343 del 10.12.2018 (Allegato 1).

relativamente alla formazione delle aggregazioni documentali, alla organizzazione dei documenti, dei fascicoli e delle serie informatiche:

- le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni documentali informatiche (nota DCAFFGEN 22343 del 10.12.2018- Allegato 1);
- la definizione della struttura dell'archivio e dei fascicoli all'interno di Vigilia;
- l'individuazione dei soggetti abilitati alla creazione e gestione dei fascicoli all'interno di ogni Ufficio del Comando;

relativamente alle misure di sicurezza e protezione dei dati personali adottate:

- le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali;
- gestione dei livelli di riservatezza previsti dall'applicativo VIGILI@.

1.2 Ambito di applicazione del manuale

Il presente manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma 1 lettera c), del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, del succitato decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 e delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate dall'AGID nel maggio 2021.

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'Area Organizzativa Omogenea (A.O.O. del Comando dei Vigili de Fuoco di Cagliari).

L'entrata in vigore del protocollo unico, inizialmente con l'applicativo FOLIUM, è avvenuto in data 15/09/2008, ed ha implicato la cessazione di fatto e di diritto della gestione separata del protocollo riservato e dei protocolli di settore o di ufficio e di tutti gli altri sistemi di registrazione da protocollare dei documenti diversi dal protocollo unico.

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

La protocollazione di un documento in ingresso ha effetto, anche giuridico, sull'effettivo ricevimento.

1.3 Organizzazione del Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile ai fini dell'adozione del protocollo informatico

In ottemperanza all'art. 50 del DPR 445/2000, sono state individuate delle Aree Organizzative Omogenee (AOO) e delle Unità Organizzative (UO), secondo l'organizzazione del Dipartimento in ogni componente ufficialmente riconosciuta.

Il DM 179 del 26/06/2024 del Ministro dell'Interno ha individuato le seguenti AOO:

- Uffici di Diretta Collaborazione con il Capo Dipartimento e con il Vice Capo Vicario Capo del Corpo Nazionale (n. 2);
- Direzioni Centrali (n. 10);
- Ufficio Centrale Ispettivo (n. 1);
- Direzioni Regionali ed Interregionali (n. 18);
- Comandi Provinciali (n. 103).

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

1.3.1 Aree Organizzative Omogenee (AOO), Unità Organizzative (UOP), Responsabile del Procedimento Amministrativo

Per quanto riguarda le definizioni, si riportano, di seguito, gli acronimi utilizzati più frequentemente:

- AOO - Area Organizzativa Omogenea (Comando dei Vigili del Fuoco di Cagliari);
- MdG - Manuale di Gestione del protocollo informatico e gestione documentale e degli archivi;
- RPA - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi, o tecnici, o informatici, relativi ad un affare;
- RGD - Responsabile della Gestione Documentale;
- PdP - Prodotto di Protocollo informatico – l'applicativo denominato "VIGILIA", sviluppato o acquisito dall'amministrazione/AOO per implementare il servizio di protocollo informatico;
- UOP - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo; Su VIGILIA hanno il ruolo di "operatore".
- UU - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali. Su Vigilia hanno il ruolo di "utente".

Per Area Organizzativa Omogenea si intende una struttura amministrativa dotata di propri organi di governo, gestione e controllo, o comunque dotata di autonomia organizzativa e contabile.

È individuata da settori che, per tipologia di mandato istituzionale, di obiettivi perseguiti, di funzione amministrativa e attività svolta, presentano esigenze di gestione unitaria e coordinata della documentazione.

All'interno della AOO deve essere adottato il protocollo unico, secondo il quale è stabilita un'unica sequenza numerica di protocollazione per tutti i documenti in entrata ed in uscita di tutte le UOP che compongono l'Area Organizzativa Omogenea.

L'Unità Organizzativa (UOP) è l'ufficio (sezione, servizio, nucleo, ripartizione, etc.) dell'Area Organizzativa Omogenea che ne utilizza i servizi messi a disposizione per la gestione dei documenti.

L'Unità Organizzativa è lo strumento attraverso il quale si articola in livelli gerarchici la struttura di un'Area Organizzativa Omogenea.

Pertanto:

- costituisce un elemento terminale della struttura dell'AOO;
- è ulteriormente suddivisibile in ulteriori Unità Organizzative gerarchicamente dipendenti;

Per ciascuno dei procedimenti di competenza della U.O.P., è associato, se necessario, il responsabile del procedimento amministrativo (RPA), figura prevista dall'art. 4 della legge 7 agosto 1990, n. 241.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Il Responsabile del Procedimento Amministrativo è il dipendente responsabile dell'istruttoria e di ogni altro adempimento inerente il singolo procedimento; cura l'iter per l'adozione del provvedimento finale (L. 241/1990).

Un procedimento amministrativo è composto da una o più procedure amministrative collegate.

1.3.2 Servizio per la gestione informatica del protocollo

Nell'AOO alla quale fa riferimento il presente MdG, è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi ai sensi dell'articolo 61 del TUDA.

Alla guida del suddetto servizio è posto il Responsabile della gestione documentale (di seguito RGD), un dirigente ovvero un funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente, individuato nel Direttore Vice Dirigente Logistico Gestionale Elisabetta Carta.

È compito del servizio:

- predisporre lo schema del manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del manuale sulla Intranet e sul sito istituzionale del Comando dei Vigili del Fuoco di Cagliari;
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, e, più in generale, dei protocolli diversi dal protocollo informatico;
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici. Considerato che per il Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile, dal quale dipende il Comando dei Vigili del Fuoco di Cagliari, la conservazione dei documenti informatici viene effettuata su infrastruttura hardware centralizzata sita presso il CED Dipartimentale, il piano di sicurezza per la conservazione è predisposto dal RSP della Direzione Centrale per l'innovazione Tecnologica, la digitalizzazione e per i beni e le Risorse Logistiche e Strumentali ;
- definire i ruoli applicativi da associare agli addetti dell'AOO per l'utilizzo dell'applicativo per il protocollo informatico, richiedendone l'abilitazione all'Amministratore Informatico di AOO;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- verificare la produzione di documenti digitali secondo gli standard definiti dalla normativa vigente;

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

- verificare periodicamente la corretta produzione del registro giornaliero di protocollo su VIGILI@ e la sua conservazione su supporto informatico non riscrivibile, a cura del responsabile della conservazione delle copie, qualora nominato;
- garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali e le attività di gestione degli archivi;
- aprire e chiudere il registro di protocollazione di emergenza, curandone la conservazione dei dati in attesa del riversamento nell'applicativo di protocollo informatico dopo il ripristino del sistema. Funzioni normalmente di competenza del RGD della AOO demandante all'applicativo ed al Responsabile del servizio di protocollo informatico della Direzione Centrale per l'innovazione Tecnologica, la digitalizzazione e per i beni e le Risorse Logistiche e Strumentali.
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard previsti dalla normativa vigente;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- garantire il buon funzionamento degli strumenti e il rispetto delle procedure stabilite dalla normativa vigente, incluse le eventuali funzionalità di accesso dall'esterno.

1.4 Accreditamento dell'amministrazione/AOO all'IPA

L'amministrazione (Dipartimento dei Vigili del Fuoco, del Soccorso pubblico e della Difesa Civile), nell'ambito degli adempimenti previsti, ha provveduto all'accreditamento presso l'indice delle pubbliche amministrazioni (IPA) tenuto e reso pubblico dal DigitPA, raggiungibile all'indirizzo: <http://www.digitpa.gov.it>.

CARATTERIZZAZIONE DELL' AREA ORGANIZZATIVA OMOGENEA

Denominazione dell'Area Organizzativa Omogenea	Comando dei Vigili del Fuoco di Cagliari
Codice Identificativo assegnato alla AOO	m_it.COM-CA
Responsabile dell'Area Organizzativa Omogenea	Dirigente Superiore Ing. Luca Manselli
Responsabile della Gestione Documentale	Direttore Logistico Gestionale Vice Dirigente Elisabetta Carta
Casella di posta elettronica certificata dell'AOO	com.cagliari@cert.vigilfuoco.it
Casella di posta elettronica ordinaria dell'AOO	comando.cagliari@vigilfuoco.it
Indirizzo completo della sede principale	Via le Marconi n. 300, CAP 09131 - CAGLIARI
Data di istituzione della AOO	15/09/2008

Sul sito internet istituzionale del Comando del Comando di Cagliari è consultabile l'organigramma che descrive la struttura organizzativa dell'AOO.

2. LE TIPOLOGIE DOCUMENTARIE

2.1 Il documento amministrativo

Ai sensi dell'art 1 comma 1 del D.P.R. 445 del 2000 e *ss.mm.ii.*, per documento amministrativo si intende ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa. Il documento amministrativo, in termini tecnologici, è classificabile in:

- Informatico (rappresentazione informatica di atti fatti giuridicamente rilevanti - art 1 comma 1 lettera b) del D.P.R. 445 del 2000 *ss.mm.ii.*;
- Analogico (rappresentazione non informatica di fatti, atti e dati giuridicamente rilevanti - art 1. comma 1, lettera p-bis del D.P.R. 445 del 2000 *ss.mm.ii.*, (come ad esempio un documento su supporto cartaceo).

Secondo quanto previsto dal decreto legislativo n.82/2005 e *ss.mm.ii.* (CAD) *le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le linee guida (sulla formazione, gestione e conservazione dei documenti informatici dell'AGID n.d.r..)"*

2.1.1 Il documento informatico

Il Codice dell'Amministrazione Digitale definisce il documento informatico come ogni "*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".

L'aggettivo informatico qualifica il documento in base al fatto che sia scritto (memorizzato) su un supporto informatico (e non su carta o su altro supporto analogico, per esempio su pergamena o su pellicola).

2.1.2 Versione analogica di un documento informatico

Per versione analogica di un documento informatico si intende una copia, di norma cartacea, di un documento amministrativo prodotto in origine su supporto informatico.

2.1.3 Il documento analogico

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Nell'attività amministrativa di norma il documento analogico è un documento formato su supporto cartaceo prodotto con strumenti analogici (es. documento scritto a mano o a macchina da scrivere) o con strumenti informatici (es. documento prodotto con un sistema di videoscrittura e stampato).

È considerato originale analogico il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali e sostanziali, comprendente tutti gli elementi di garanzia e di informazione, del mittente e del destinatario e dotato di firma autografa.

2.1.4 Copia informatica di un documento analogico

La copia informatica di documento analogico è costituita da un documento informatico che ha solo il contenuto identico (e non la forma) a quello del documento analogico da cui è tratto (CAD, art. 1, c. 1, lett. i-bis). È il caso della copia che risulta da una scansione con programma OCR finalizzata al recupero del testo e non della formattazione

2.1.5 Copia per immagine su supporto informatico di un documento analogico

La copia per immagine su supporto informatico di documento analogico è costituita da un documento informatico che ha contenuto e forma identici a quelli del documento analogico da cui è tratto (CAD, art. 1, c. 1, lett. i-ter). È il caso della copia che risulta da una scansione in pdf di un documento analogico.

2.2 Le tipologie operative di documenti

Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in:

- Ricevuto
- Inviato
- Interno formale
- Interno informale

2.2.1 Documento ricevuto

Sono tutti i documenti ricevuti dall'Unità Organizzativa, a qualunque titolo e con qualsiasi mezzo. Essi possono essere sia documenti analogici, sia documenti informatici.

La corrispondenza in ingresso può essere acquisita dalla AOO con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Un documento informatico può essere recapitato:

- A mezzo posta elettronica convenzionale o certificata,
- Su supporto removibile consegnato direttamente alla UO o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

- A mezzo posta convenzionale o corriere;
- A mezzo posta raccomandata;
- Telegramma
- Con consegna a mano diretta da parte dell'interessato o persona delegata.

L'operazione di protocollazione dei documenti in arrivo può essere effettuata in modalità centralizzata dal personale dell'ufficio protocollo dell'AOO, o dall'UO, se destinataria diretta dei documenti (es. documenti contabili o istanze del personale). In entrambi i casi l'ufficio che effettua la protocollazione provvede a registrare (se necessario a scansionandolo), classificare e smistare il documento. La fascicolazione invece è sempre affidata all'ufficio destinatario.

Il sistema deve consentire la produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con operazione di registrazione di protocollo nell'arco di uno stesso giorno.

2.2.2 Documento inviato

Si intendono i documenti prodotti nell'esercizio delle proprie funzioni dal personale in servizio presso la AOO e diretti all'esterno (ad altra AOO della stessa amministrazione VF o ad enti esterni) o all'interno, quando ne è richiesta una notifica formale.

La registrazione di protocollo di tali documenti è eseguita dal singolo Responsabile del Procedimento (o suo delegato) cui il documento afferisce, oppure in casi particolari dall'Ufficio Segreteria in orario d'ufficio e dalla Sala Operativa H24.

I documenti informatici, compresi gli eventuali allegati, anche essi digitali, sono inviati, di norma, per mezzo della posta elettronica certificata se la dimensione del documento non supera la dimensione massima dei messaggi (30Mb è il limite stabilito da VIGILI@, da dividersi per il numero dei destinatari).

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

In caso la dimensione del documento non consentisse la spedizione attraverso VIGILI@, allora questo verrà riversato su supporto digitale rimovibile non modificabile e trasmesso al destinatario con altri mezzi.

2.2.3 Documenti interni

Di intendono i documenti scambiati all'interno della stessa AOO. Essi si distinguono in :

- Documenti di preminente carattere informale
- Documenti di preminente carattere giuridico probatorio

Per i primi non esiste l'obbligo della protocollazione (appunti, brevi comunicazioni di rilevanza meramente informativa).

I secondi, invece, possono essere registrati nell'apposito registro denominato "Atti esterni" che contiene documenti interni al Comando di preminente carattere giuridico - probatorio, redatti dal personale nell'esercizio delle proprie funzioni al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative.

I documenti indirizzati al singolo dipendente aventi carattere giuridico probatorio, vengono registrati nel registro ufficiale e inviati all'indirizzo mail istituzionale, all'indirizzo e-mail cert istituzionale @cert.vigilfuoco.it e alla PEC personale, se conosciuta.

Tali documenti possono sempre essere assegnati al dipendente attraverso il sistema di gestione documentale.

3. FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa (art 40 del CAD come modificato dal D.Lgs 179 del 2016); ogni documento, creato per essere inoltrato all'esterno o all'interno in modo formale, tratta un unico argomento, indicato in maniera sintetica ma esaustiva, a cura dell'autore, nello spazio riservato all'oggetto.

Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso la denominazione, il logo dell'amministrazione e l'indirizzo di casella di posta elettronica istituzionale. Ulteriori informazioni aggiuntive utili sono il numero di telefono e l'indicazione del numero di allegati (se presenti).

Le firme necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione:

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

- in caso di documento cartaceo, sigla autografa dell'istruttore e sottoscrizione autografa del responsabile del procedimento amministrativo e/o del responsabile del provvedimento finale;
- in caso di documento digitale, sottoscrizione ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente da parte dell'istruttore del documento e sottoscrizione digitale del responsabile del procedimento amministrativo e/o del responsabile del provvedimento finale.

I documenti informatici prodotti dall'amministrazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità.

3.1 Requisiti degli strumenti informatici di scambio

Scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi è garantire sia l'interoperabilità sia i requisiti minimi di sicurezza di seguito richiamati:

- L'integrità dei messaggi
- Il non ripudio dei messaggi
- La riservatezza dei messaggi
- L'automazione dei processi di protocollazione e smistamento dei messaggi all'interno delle AOO
- L'interconnessione tra AOO, ovvero l'interconnessione tra le UO di una stessa AOO nel caso di documenti interni formali
- La certificazione dell'avvenuto inoltro e ricezione
- L'interoperabilità dei sistemi informativi pubblici

3.2 Firma digitale e verifica delle firme con il Prodotto di Protocollo Informatico

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 3.1 è la firma digitale, un particolare tipo di firma elettronica avanzata, basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. Le chiavi devono essere certificate, in particolare la certificazione di una chiave pubblica da parte di una autorità di certificazione garantisce la corrispondenza della chiave con il soggetto che la espone.

La firma digitale è utilizzata per sottoscrivere documenti o qualsiasi altro file digitale con valenza giuridico - probatoria.

In VIGILI@ sono previste funzioni di verifica della firma digitale apposta sui documenti in ingresso e sugli eventuali allegati. Tale funzione è disponibile prima della protocollazione in ingresso per un'eventuale verifica preventiva. VIGILI@, al momento dell'acquisizione e presentazione del documento all'operatore di protocollo, esegue comunque automaticamente la verifica della firma e ne visualizza il certificato. I dati del certificato vengono salvati, insieme al documento protocollato, all'interno di VIGILI@, per eventuali successive attività di verifica.

4. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

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

Il Comando dei Vigili del Fuoco di Cagliari è dotato di tre caselle di posta elettronica istituzionale, gestite direttamente all'interno di Vigilia:

- **com.cagliari@cert.vigilfuoco.it** per comunicazioni di natura tecnica e amministrativocontabile (in orario d'ufficio);
- **com.salaop.cagliari@cert.vigilfuoco.it** per comunicazioni inerenti il soccorso pubblico (H24);
- **com.prev.cagliari@cert.vigilfuoco.it** per comunicazioni concernenti la prevenzione incendi e l'attività ricompresa nelle competenze dei Comitati Tecnici Regionali di cui ai Decreti Legislativi n. 139/06 e n. 105/15.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

L'AOO è inoltre dotata di un ulteriore casella di posta elettronica al di fuori di Vigilia avente il seguente indirizzo: **comando.cagliari@vigilfuoco.it**.

Il Comandante, se lo ritiene opportuno, può disporre l'istituzione di ulteriore casella d'appoggio [@vigilfuoco.it](mailto:comando.cagliari@vigilfuoco.it)

4.1 Unicità del protocollo informatico

Nell'ambito dell'AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica 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 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. 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 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 che non è stata registrata presso una UO viene considerata giuridicamente inesistente presso l'amministrazione.

Non è consentita la protocollazione di un documento già protocollato.

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

Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

4.2 Registro giornaliero di protocollo

Il programma Vigilia, genera automaticamente, alla fine di ogni giornata, il registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Il file PDF viene inviato automaticamente alla casella e-mail prescelta (di norma del responsabile della gestione documentale o, se nominato, del responsabile della conservazione dei dati per la successiva archiviazione).

4.3 Registrazione di protocollo

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo valide per tutti i tipi di documenti trattati dal Comando di Cagliari (ricevuti, trasmessi, verso l'esterno o interni formali, informatici ed analogici).

Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori. Tale registrazione è eseguita in un'unica operazione. L'inserimento di informazioni oltre ai dati minimali in più fasi successive è possibile.

L'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma non modificabile, determina l'automatico e contestuale annullamento della intera registrazione di protocollo. Delle altre informazioni, registrate in forma non modificabile, l'annullamento anche di un solo campo, che si rendesse necessario per correggere errori intercorsi in sede di immissione di dati, comporta la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica; così analogamente per lo stesso campo, od ogni altro, che dovesse poi risultare errato. La modifica dei dati minimali viene tracciata e segnata come modifica.

Ciascuna registrazione di protocollo contiene i seguenti dati obbligatori ai sensi dell'art. 53 del TUDA:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente che ha prodotto il documento, registrato in forma non modificabile;
- il destinatario del documento, registrato in forma non modificabile;
- l'oggetto del documento, registrato in forma non modificabile;

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Come previsto dalla normativa in materia di tutela dei dati personali, gli addetti al protocollo adottano tutti gli accorgimenti necessari per la tutela dei dati sensibili e giudiziari non inserendoli nel campo "oggetto" del registro di protocollo.

Le registrazioni di protocollo, in armonia con la normativa vigente, prevede elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili. Tali dati facoltativi sono descritti nei paragrafi seguenti.

4.3.1 Registrazione dei documenti informatici

I documenti informatici sono, preferibilmente, ricevuti e trasmessi in modo formale tramite casella di posta elettronica certificata istituzionale dell'amministrazione. La registrazione di protocollo di un documento informatico in ingresso sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma. La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più dei file ad esso allegati.

I documenti giunti via posta elettronica che non siano conformi agli standard indicati dalla normativa, ovvero non siano dotati di firma digitale o non inviati tramite casella di posta elettronica certificata che ne attesti la provenienza certa, sono da protocollarsi con le stesse modalità degli altri, lasciando al responsabile del procedimento amministrativo la valutazione di ammissibilità e valenza.

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

I documenti ricevuti agli indirizzi di posta elettronica non certificata di ogni Ufficio del Comando vengono protocollati in ingresso dagli addetti dello stesso ufficio.

Per quanto concerne le note in uscita, anch'esse vengono protocollate e spedite dagli operatori degli uffici competenti oppure dallo stesso RPA o dall'Ufficio Segreteria o dalla Sala Operativa.

4.3.2 Registrazione dei documenti analogici

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza, (il servizio postale pubblico e/o privato o con consegna diretta alla UO).

La registrazione di protocollo di un documento analogico cartaceo ricevuto viene sempre eseguita, per tutte le tipologie di documento soggetti a protocollazione obbligatoria, in quanto l'AOO ha la funzione di registrare l'avvenuta

ricezione. Nel caso di corrispondenza in uscita, verso l'esterno o interna formale, l'UO esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali.

Le buste si allegano al documento in arrivo in caso di rilevanza della parte relativa ai timbri postali (es. raccomandate, consegna tramite corriere, ecc.).

Le registrazioni in ingresso e in uscita dei documenti analogici vengono eseguite dagli Uffici di competenza.

4.4 Elementi obbligatori delle registrazioni di protocollo

Di seguito vengono riportati gli elementi obbligatori finalizzati alla conservazione e gestione della documentazione che ogni addetto al protocollo deve inserire in VIGILIA:

- data documento, data ricezione o spedizione;
- protocollo mittente;
- firmatario;
- collegamento a documenti precedenti;
- classificazione: obbligatoria da parte di ogni ufficio assegnatario dopo che viene protocollata in ingresso da parte della segreteria;
- indicazione del livello di riservatezza se diverso da quello standard applicato dal sistema di protocollazione.

4.5 Segnatura di protocollo dei documenti

Ai sensi dell'art 55 del TUDA, 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 al documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione del documento. Essa consente di individuare ciascun documento in modo inequivocabile.

4.5.1 Segnatura dei documenti informatici

I dati della segnatura di protocollo di un documento informatico sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell' Extensible Markup Language (XML). In caso di spedizione di

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

e-mail da casella certificata verso altra casella certificata, le informazioni incluse nella segnatrice generata da Vigili© sono quelle di seguito elencate:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea mittente;
- data e numero di protocollo del documento; indirizzo telematico del mittente;
- denominazione dell'amministrazione mittente (compreso indirizzo postale);
- indirizzo telematico destinatario;
- denominazione destinatario;
- oggetto del documento riportato nell'applicativo VIGILIA;
- nome assegnato al documento da VIGILIA;
- eventuale indice di classificazione; controllo di avvenuta ricezione (si/no);
- nome dei file degli eventuali allegati.

In caso di spedizione dalla casella e-mail certificata verso casella di posta elettronica normale, non viene generato il file segnatrice.xml. I dati di riconoscimento del protocollo vengono inseriti nel file datichert.xml generato dal server di pec utilizzato, contenente i seguenti dati comunicati da VIGILIA:

- indirizzo e-mail mittente;
- indirizzo e-mail destinatario;
- oggetto contenente il numero di protocollo e la data.

La struttura ed i contenuti del file di segnatrice di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti. Il destinatario che riceve il documento informatico può utilizzare le informazioni contenute nel file segnatrice.xml per automatizzare le operazioni di registrazione di protocollo del documento ricevuto. Per preservare l'integrità dei documenti informatici firmati digitalmente, Vigilia effettua una copia sulla quale applica il "timbro" di segnatrice, lasciando l'originale integro all'interno del gestore documentale.

4.5.2 Uso della posta elettronica certificata

Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo.

Per l'invio di e-mail tramite la casella di posta elettronica certificata istituzionale si deve:

- Redigere il documento informatico
- Firmare il documento con firma digitale
- Acquisire il documento, ed eventuali allegati, con il programma VIGILIA
- Inserire in Vigilia i dati del destinatario (almeno denominazione e casella di posta elettronica)
- Scegliere il mezzo di spedizione:
 - E-mail (se si tratta di un destinatario, pubblico o privato, con *posta non certificata*)
 - E-mail interna dipartimento (se si tratta di un destinatario all'interno del dipartimento con posta certificata quindi con estensione *@cert.vigilfuoco.it*)
 - E-mail ad altra amministrazione (se si tratta di un destinatario, pubblico o privato, all'esterno del dipartimento/di altra amministrazione con posta certificata)
- Protocollo il documento. Vigilia automaticamente assegnerà il numero di protocollo in uscita e invierà il documento firmato digitalmente.

L'utilizzo della posta elettronica certificata (PEC) consente di:

- Conoscere in modo inequivocabile la data e l'ora di trasmissione
- Garantire l'avvenuta consegna all'indirizzo di posta elettronica del destinatario, ricevendo le notifiche relative all'invio e ricezione del messaggio qualora l'invio sia effettuato verso altro indirizzo PEC
- Interoperare e cooperare, dal punto di vista applicativo, con altre AOO appartenenti alla stessa e ad altre amministrazioni che utilizzano un prodotto di protocollo informatico conforme agli standard di interoperabilità.

Le notifiche di sistema, come ad esempio la "ricevuta di accettazione" (da parte del server di pec del mittente) e la "ricevuta di avvenuta consegna" (da parte del server di pec del destinatario) vengono associate automaticamente da Vigilia al documento protocollato.

Le UOP dovranno verificare attentamente il corretto invio e l'avvenuta ricezione ed accettazione del documento da parte del destinatario.

Qualora al servizio di protocollo provenissero documenti analogici indirizzati ad altri essi andranno restituiti senza procedere alla protocollazione.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Qualora l'errata ricezione riguardi documenti digitali sulla casella PEC, le UOP dovranno rispedire il messaggio al mittente con la dicitura "messaggio pervenuto per errore – non di competenza di questa AOO".

4.5.3 Segnatura dei documenti cartacei

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un "segno" grafico sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- codice identificativo e denominazione dell'amministrazione, codice identificativo e denominazione dell'AOO;
- data e numero di protocollo del documento;
- modalità di registrazione (ingresso/uscita);
- eventuale indice di classificazione.

Il "segno" grafico, contenente i suindicati elementi di norma è realizzato direttamente dall'applicativo sul documento. L'applicativo adottato dal Dipartimento consente anche la stampa del timbro di protocollo su etichetta autoadesiva da apporre sul documento.

L'operazione di segnatura dei documenti in partenza viene effettuata dall'Ufficio competente – o dal RPA cioè chi ha redatto la nota in questione.

L'operazione di acquisizione dell'immagine dei documenti cartacei (scansione) viene eseguita contemporaneamente alle operazioni registrazione. Nel caso di documento e/o allegati sia di formato non idoneo ad essere acquisito dagli scanner in uso all'amministrazione, viene effettuata la protocollazione con i dati minimali, indicando nelle note di VIGILI@, il numero esatto di pagine costituenti il documento e gli allegati e la segnatura di protocollo va messa su ogni allegato.

4.6 Annullamento parziale delle registrazioni di protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrate in forma non modificabile (Oggetto e Mittente/Destinatario) - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'annullamento parziale della registrazione di protocollo. Conformemente alla normativa, il sistema adottato consente quindi l'inserimento di nuovi valori tenendo traccia del valore originario e della data dell'annullamento.

L'operatore, qualora si accorga di eventuali errori effettuati in fase di immissione dei dati, potrà modificare uno dei dati obbligatori riportando nel campo "info" le motivazioni della modifica.

4.7 Annullamento di un protocollo (del registro ufficiale di corrispondenza)

L'annullamento totale di un protocollo è il provvedimento che coinvolge tutto il documento.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo. Nella stampa del Registro giornaliero, come in tutta la reportistica di sistema, la procedura evidenzia il record corrispondente al protocollo annullato con la dicitura "annullato" in posizione visibile e tale da consentire la lettura di tutte le informazioni originarie. Il sistema richiede di specificare il motivo. Pertanto, qualora l'operatore che ha eseguito la protocollazione ritenesse di dover annullare un protocollo, deve specificare in modo dettagliato la motivazione dell'annullamento.

4.8 Protocollazione di documenti riservati e livelli di riservatezza

4.8.1 documenti riservati

La riservatezza su sistema VIGILa ha la funzionalità di marcare un documento come "riservato", permettendo di trattare correttamente i documenti che sono definiti come tali dalla Legislazione vigente. Il numero di protocollo attribuito dal programma è progressivo all'interno del registro di protocollo. La visione dei documenti marcati come riservati è consentita solo al personale con ruolo di "utente riservato", "operatore riservato" e "responsabile di registro".

Documenti contenenti i dati di cui al D.Lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) es. dati personali sulla salute psico-fisica, orientamento sessuale, convinzioni politiche e religiose. Alcune tipologie di documenti, per il loro particolare contenuto, debbono considerarsi riservati. Si tratta di tipologie documentali che contengono dati personali e/o sensibili e/o segreti (ad esempio perché coperti da segreto di Stato o afferenti la Difesa e/o la Sicurezza nazionale etc, di norma sottratti al diritto di accesso ai sensi della legge 241 del 1990 e del D.Lgs 33 dl 2013).

Si definiscono dati personali le informazioni che identificano o rendono identificabile, direttamente e/o indirettamente una persona fisica e/o che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita etc. Tra essi possiamo fondamentalmente distinguere in dati che permettono un'identificazione diretta, come i dati anagrafici (nome, cognome, immagini etc) e che permettono un'identificazione indiretta (codice fiscale, numero di carta d'identità, numero di targa di automobile, indirizzo IP , etc).

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Tra essi i dati sensibili sono quelli tali da rivelare l'origine etnica o razziale, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute e/o alla vita e/o orientamento sessuale, i dati biometrici, i dati genetici, i dati giudiziari, cioè relativi a procedimenti penali in corso e/o conclusi (ad es. sentenze di assoluzione /o condanna, certificati del casellario giudiziale).

I predetti documenti debbono essere protocollati su sistema VIGILIA in modalità riservata, assegnando il livello di riservatezza adeguato.

Come già sopra esposto, come previsto dalla normativa in materia di tutela dei dati personali, gli addetti al protocollo adottano tutti gli accorgimenti necessari per la tutela dei dati sensibili e giudiziari non inserendoli nel campo "oggetto" del registro di protocollo.

Oltre ai documenti sopradescritti, di seguito sono riportate alcune tipologie di documenti considerati riservati e come tali sottratti all'accesso agli atti:

- a) documenti relativi a vicende di persone o a fatti privati o particolari;
- b) documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
- c) documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- d) le tipologie di documenti individuati dall'art. 24 della Legge 7 agosto 1990 n. 241:
 - documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
 - relativi ai procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
 - documenti che riguardano l'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
 - nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi; (sono sia sensibili che sottratti all'accesso) documenti di cui all'art. 8 del D.P.R.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

27 giugno 1992 n. 352 ovvero i documenti sottratti all'accesso individuati nel Regolamento del Ministero dell'Interno D.M. del 16 Marzo 2022 allegato al presente manuale:

- i documenti di cui all'art. 12 della legge 24 ottobre 1977, n. 801 (Sono coperti dal segreto di Stato gli atti, i documenti, le notizie, le attività e ogni altra cosa la cui diffusione sia idonea a recare danno alla integrità dello Stato democratico, anche in relazione ad accordi internazionali, alla difesa delle istituzioni poste dalla Costituzione a suo fondamento, al libero esercizio delle funzioni degli organi costituzionali, alla indipendenza dello Stato rispetto agli altri Stati e alle relazioni con essi, alla preparazione e alla difesa militare dello Stato. In nessun caso possono essere oggetto di segreto di Stato fatti eversivi dell'ordine costituzionale.
- i documenti da possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, nonché all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste nei trattati e nelle relative leggi di attuazione;
- i documenti la cui divulgazione possa recare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
- i documenti che riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, nonché all'attività di polizia giudiziaria e di conduzione delle indagini;
- i documenti riguardino la vita privata o la riservatezza di persone fisiche, di persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono.

4.8.2 Livelli di riservatezza

Il programma VIGILIA ha una funzionalità, la cui applicazione è facoltativa, che permette di associare ad ogni documento un livello di riservatezza variabile (non classificato, classificato, ristretto, segreto, top secret) indipendentemente se lo stesso è stato marcato come "riservato" o meno.

L'attribuzione di un livello, determinando la visibilità del documento solo agli operatori e/o utenti aventi livello di accesso uguale o superiore, permette la gestione flessibile dell'archivio e la creazione di una scala gerarchica di accesso.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Per una gestione completa e corretta dell'accesso agli atti riservati dei documenti viene stabilito di utilizzare il livello di riservatezza in abbinata alla marcatura del documento come "riservato". Pertanto ogni documento marcato con il flag "riservato" deve avere associato almeno un livello di riservatezza non inferiore a "classificato", mentre possono esistere documenti non marcati come riservati ma ai quali è stato associato un livello di riservatezza specifico.

Per il documento in uscita il livello è stabilito dal Comandante oppure dal Dirigente della competente Area su richiesta del RPA che lo ha redatto.

In modo analogo, il Responsabile del Procedimento Amministrativo che effettua l'operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza. Il livello di riservatezza applicato ad un fascicolo ne determina la possibilità di accesso esclusivamente agli utenti con livello uguale o superiore indipendentemente dalla lista di accesso ad esso associata. I documenti contenuti nei fascicoli non ereditano il livello di riservatezza stabiliti per lo stesso.

VIGILIA dispone di diversi livelli di riservatezza ma per esigenze organizzative e di classificazione con il presente manuale vengono adottati in via generale nelle ordinarie attività esclusivamente due livelli di riservatezza.

In funzione di quanto sopra è in via generale stato previsto l'utilizzo dei seguenti livelli di riservatezza disponibili da VIGILIA:

- classificato: documenti relativi a vicende di persone o a fatti privati o particolari (es. pratiche di contenzioso civile e/o amministrativo e risarcimento danni purché non contengano dati sensibili (e relativi alla vita sessuale, appartenenza politica o sindacale, orientamento religioso o filosofico etc.) (con esclusione dei pignoramenti che sono classificati con livello ristretto);
- ristretto:
 - documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
 - documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
 - documenti riservati relativi a relazione valutativa relativi a tutto il personale;
 - documenti relativi a provvedimenti disciplinari;
 - tutti i documenti relativi a dati personali sensibili (relativi alla vita sessuale, appartenenza politica o sindacale, orientamento religioso o filosofico etc), o relativo alla salute psico-fisica (ad es. certificati medici, documenti

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

relativi a cause di servizio) o contenenti riferimenti che possono rivelare lo stato di salute psico-fisica (es. la giustificazione relativa al permesso per visita medica, esiti di test psicoattitudinali etc)

- i documenti riguardanti la vita privata o la riservatezza di persone fisiche e giuridiche (richieste di trasferimento ai sensi della legge 104/92, atti di pignoramento *et similia*, richieste di prestito etc.)
- Documenti contenenti dati giudiziari di carattere penale (es. relativi a persone sottoposte a procedimento penale e/o condannate, come certificati dei carichi pendenti, del casellario giudiziale etc);

In via eccezionale, Segreto/ top secret: livelli attribuito su indicazione del Comandante o dei Dirigenti dell'Area a cui si riferisce il documento;

In caso di dubbio l'operatore di protocollo deve rivolgersi al Comandante oppure al Dirigente e/o Responsabile della competente Area e chiede di determinare il livello da attribuire.

Ogni Responsabile di Ufficio e/o Settore deve autorizzare il personale all'accesso di ogni livello di riservatezza e comunicarlo all'amministratore e all'Ufficio Segreteria. Saranno abilitati al protocollo riservato esclusivamente il Comandante, i responsabili di ufficio e/o settore, coloro che ne necessitano per l'istruttoria delle pratiche e/o servizi.

4.9 Casi particolari di registrazioni di protocollo

Qui di seguito vengono fornite alcune indicazioni pratiche riguardo ai comportamenti operativi che sono stati stabiliti per le situazioni più comuni:

Documenti cartacei o informatici in partenza con più destinatari

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è comunque unica.

Circolari e disposizioni generali

Le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale.

Lettere prive di firma

Le lettere prive di firma vanno protocollate in quanto la funzione notarile del protocollo (cioè della registratura) è quella di attestare data e provenienza certa di un documento senza interferire su di esso. In fase di registrazione può essere apposta la dicitura "documento non sottoscritto". Sarà poi compito della UO e, in particolare, del RPA (ai sensi

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

della L. 241/90) valutare, caso per caso ai fini della sua efficacia riguardo ad un affare o un determinato procedimento amministrativo, cioè se la lettera priva di firma debba ritenersi valida o meno.

Registrazione "a fronte"

Ogni documento è individuato da un unico numero di protocollo.

Non è pertanto consentita 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, neppure se la pratica si esaurisce con la risposta e neppure se la registrazione avviene nel medesimo giorno lavorativo.

E' in ogni caso possibile ed utile creare dei collegamenti tra i documenti anche tramite le operazioni di fascicolazione.

Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma regolarmente registrati, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

Posta elettronica certificata

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario in maniera certa se trasmesso da una casella di posta elettronica certificata all'indirizzo di posta elettronica certificata da questi dichiarato.

Pertanto viene privilegiato tale canale di comunicazione, sia in ingresso che in uscita. Potranno essere protocollati sia il corpo del messaggio che uno o più dei file ad esso allegati.

Il messaggio, compreso l'eventuale documento allegato, sarà sottoposto a registrazione di protocollo ritenendo soddisfatta la forma scritta ai sensi dell'art 43 del DPR 445/2000.

Ricezione di documenti informatici su supporti rimovibili

Qualora il documento sia in formato digitale conforme agli standard previsti, viene protocollato e trattato come previsto per i documenti ricevuti via e-mail.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Qualora il documento informatico su supporto rimovibile sia accompagnato da una lettera di trasmissione cartacea, è quest'ultima ad essere protocollata come documento principale con le modalità previste, mentre gli altri documenti informatici vanno acquisiti come allegati nel programma VIGILIA.

Protocollo dei messaggi di posta elettronica convenzionale

Considerato che l'attuale sistema di posta elettronica non certificata non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata nei seguenti modi:

- in caso di invio, come allegato, di un documento scansionato e munito di firma autografa il RPA deve verificare la provenienza certa del documento;
- in caso di mittente non verificabile, il RPA valuta caso per caso l'opportunità di trattare il documento;
- in caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale, il documento e/o il messaggio sono considerati come un documento inviato con qualunque mezzo di posta;
- in caso di invio di una e-mail contenente un testo non sottoscritto o non contenente informazioni dalle quali sia possibile risalire in modo certo al mittente, sarà considerata come missiva anonima;
- In caso di contenuto non chiaramente riconducibile ai casi per i quali non è prevista la protocollazione, la necessità di procedere alla protocollazione sarà decisa dal RGD.

Corrispondenza personale o riservata e documenti in arrivo da non aprire

La corrispondenza non viene aperta nei seguenti casi:

- a) corrispondenza riportante l'indicazione "offerta", "gara d'appalto", "concorso" o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara;
- b) corrispondenza indirizzata nominativamente (senza indicazione dell'ente) oppure riportante l'indicazione "riservata", "personale", "confidenziale" o simili, o comunque dalla cui confezione si evinca il carattere di corrispondenza privata.

La corrispondenza descritta al punto a) e b) va inoltrata, nel caso di una gara, direttamente al responsabile del procedimento amministrativo subito dopo la protocollazione effettuata con le modalità di seguito riportate, oppure, nel caso di corrispondenza privata, direttamente al destinatario.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

La corrispondenza riportante l'indicazione "offerta", "gara d'appalto", "concorso" o simili o comunque dalla cui confezione si evinca la partecipazione ad una gara, non viene aperta, ma viene protocollata chiusa in arrivo con l'apposizione del numero di protocollo e della data di registrazione direttamente sulla busta (plico o simili).

Dopo l'apertura delle buste, è cura della UO responsabile del procedimento di gara riportare gli estremi di protocollo, già registrati sul plico, su tutti i documenti in esso contenuti.

La corrispondenza con la dicitura "riservata" o "personale" non è aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli all'ufficio protocollo per la registrazione prevista.

Differimento delle registrazioni e protocollazioni urgenti

Le registrazioni di protocollo dei documenti pervenuti sono effettuate nella giornata di arrivo.

La richiesta di protocollare urgentemente un documento è collegata ad una dimostrata necessità indifferibile e di tipo straordinario. Solo in questo caso il RGD si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento.

Nei casi in cui le operazioni di protocollazione non possono oggettivamente essere svolte nello stesso giorno di arrivo, si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza e/o urgenza, che sarà valutata dall'operatore, eventualmente sentito il Responsabile della Gestione Documentale.

Viene stabilito a priori il seguente ordine di priorità:

Documenti in ingresso:

- documenti inerenti il soccorso;
- documenti in cui viene richiesto al Comando di rispondere a vista;
- documenti inerenti una gara o appalto;
- ordinanze con entrata in vigore in tempi ristretti;
- provvedimenti disciplinari;
- istanze o documenti che richiedono l'attivazione di determinate procedure amministrative in tempi ridotti;

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

- convocazioni a commissioni imminenti;
- in caso di presenza del mittente al quale deve essere rilasciata la ricevuta cartacea;
- documenti segnalati dai Responsabili dei vari Uffici del Comando, che hanno carattere di urgenza

Documenti in uscita:

- documenti inerenti il soccorso;
- riposte “a vista” o richieste in tempi ridotti;
- provvedimenti disciplinari;
- missioni con inizio in tempi ridotti;
- convocazioni e notifiche imminenti;
- documenti segnalati dai Responsabili dei vari Uffici del Comando, che hanno carattere di urgenza.

Documenti di competenza di altre amministrazioni pervenuti erroneamente

Ai sensi dell’art. 18 DPR 445 del 2000 e ss.mm.ii., qualora pervenga erroneamente alla casella pec un documento indirizzato ad altro ente pubblico, l’addetto rispedisce il messaggio al mittente, se individuabile, con la dicitura "Messaggio pervenuto per errore, non di competenza di questa amministrazione"; in caso non sia individuabile il mittente, il documento viene inoltrato all’ente di competenza con nota formale protocollata.

Nel caso in cui un documento della fattispecie sopra indicata venga erroneamente registrato al protocollo, esso verrà spedito a chi di competenza oppure rispedito al mittente, sempre e comunque accompagnato da una lettera di trasmissione opportunamente protocollata in uscita indicando nell'oggetto "protocollato per errore".

In caso di ricezione di documenti cartacei indirizzati ad altri soggetti, possono verificarsi le seguenti possibilità:

- busta indirizzata ad altro soggetto: si restituisce al servizio postale o corriere;
- se la busta viene aperta per errore e il documento non viene protocollato, il plico sarà restituito al destinatario, apponendo sulla busta la nota "PERVENUTA ED APERTA PER ERRORE";

Integrazioni documentarie

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.

Tale verifica spetta al responsabile del procedimento amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UO sul protocollo generale come nuovo documento e, a cura del RPA, sono inseriti nel fascicolo relativo.

E-mail di mancata consegna verso indirizzo e-mail ordinario

In caso di mancata consegna di una e-mail ad un indirizzo ordinario il server invia alla casella spedente una e-mail di mancata spedizione (es. mail delivery failed: returning message to sender) l'operatore di posta deve aprire il messaggio, trovare gli estremi di protocollazione del documento, cercarlo nell'archivio, controllare se l'indirizzo e-mail del destinatario è sbagliato o se ci sono altri problemi che possono aver inficiato l'invio.

Individuate le anomalie, comunica le anomalie all'operatore che ha protocollato che provvederà a correggerle. Vigili© provvede al nuovo invio automaticamente.

E-mail di mancata consegna verso indirizzo e-mail certificato

In caso di mancata consegna o accettazione di una e-mail ad un indirizzo di posta elettronica certificata, viene ricevuta una notifica specifica, che Vigilia provvede ad allegare al documento relativo.

Le notifiche sono pertanto allegate al documento e devono essere controllate dagli utenti assegnatari prima dell'archiviazione del documento stesso nel fascicolo, accertandosi della effettiva avvenuta consegna al server del destinatario (notifica di "AVVENUTA CONSEGNA").

Fatture

Le fatture elettroniche e non elettroniche debbono essere obbligatoriamente protocollate.

Secondo prassi contabile, se una ditta, dopo aver emesso una fattura (che è già stata protocollata dal Comando), si accorge di aver sbagliato l'importo o qualche altro dato, deve fare una nota di accredito e poi rimettere una nuova fattura con nuovo numero. In questo caso si protocolla la nota di accredito e la nuova fattura con registrazioni diverse.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Quando invece la ditta, non seguendo la procedura di cui sopra, invia comunque una fattura che sostituisce una precedentemente arrivata e già protocollata, che ha lo stesso numero e cambia solo l'importo o qualche altro particolare bisogna:

- 1) protocollare la nuova fattura scrivendo sulle info che "*sostituisce la fattura stesso numero - vedi prot. n. per cambio importo (o dati) -*" e collegandola al precedente protocollo;
- 2) scrivere sulle info della vecchia fattura "*annullata da emissione di nuova fattura stesso numero - vedi prot. n.*"

4.10 Documenti oggetto di protocollazione obbligatoria ed esclusi dalla registrazione di protocollo.

Sono oggetto di protocollazione obbligatoria ai sensi dell'art. 53 del D.P.R. 445 del 2000, paragrafo 1, i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ai sensi dell'art. 40 bis del CAD "formano comunque oggetto di registrazione di protocollo ai sensi dell'art. 53 del D.P.R. 445 del 2000 e ss.mm.ii e le comunicazioni che provengono o sono inviate ai domicili digitali eletti ai sensi di quanto previsto dall'art. 3 bis CAD nonché le istanze e le dichiarazioni di cui all'art. 65 CAD in conformità alle Linee Guida".

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del decreto del Presidente della Repubblica 20 dicembre 2000. n. 445, in particolare le seguenti tipologie:

- Gazzette Ufficiali;
- Bollettini Ufficiali P.A.;
- Notiziari P.A.;
- Giornali, Riviste, Libri, Materiali pubblicitari;
- Materiali statistici;
- Atti preparatori interni;
- Inviti a manifestazioni che non attivino procedimenti amministrativi;
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti, ecc.);
- Mail SPAM;

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

- Pubblicità di convenzioni e sconti per i V.F. che verranno messi a disposizione in apposita cartella sulla intranet ai fini della consultazione. Gli addetti dell'Ufficio segreteria provvederanno all'archiviazione dei predetti documenti nell'apposita cartella.

Il Comando di Cagliari protocolla in ingresso le circolari dell'Amministrazione Centrale, del Dipartimento di Vigili del Fuoco, della Ragioneria di Stato, dell'Inps concernenti le proprie attività e comunque ogni altra circolare di interesse ai fini dello svolgimento delle attività istituzionali, con le relative note di accompagnamento, inserendole a fini di raccolta in apposite cartelle sulla intranet del Comando.

4.11 Registri di protocollo

In considerazione delle competenze assegnate all'Amministrazione e delle procedure e delle tipologie ad esse correlate, sono istituiti all'interno di Vigilia i seguenti registri di protocollo:

- Registro Ufficiale AOO COM - CA ;
- Registro Disposizioni di Servizio;
- Registro Atti Esterni (Verbali e Decreti interni);
- Registro Ordini del Giorno

4.12 Registro Ufficiale AOO COM-CA

E il registro che raccoglie la corrispondenza in entrata ed in uscita con l'esterno (altre Direzioni regionali, Comandi, Enti e soggetti esterni ecc.). All'interno di tale tipologia di registro rientrano anche gli atti riservati e gli atti contenenti dati sensibili, caratterizzati dall'applicazione di un apposito flag su VIGILIA al momento della protocollazione, in modo tale da garantirne il rispetto della normativa riguardante il relativo trattamento.

Sono autorizzate ad operare su tale registro tutti gli Uffici.

4.13 Registro Ordini del Giorno

E' il registro dedicato alla numerazione ed alla raccolta degli ordini del giorno, al quale ha accesso solo la Segreteria del Comando che protocolla gli Ordini del giorno predisposti da tutti gli Uffici.

La pubblicazione degli Ordini del giorno avviene nel sito intranet del Comando.

L'Ufficio Segreteria, ogni giorno, invia a tutto il personale una mail con gli OdG registrati e pubblicati nel sito.

4.14 Registro delle Disposizioni di Servizio

E' il registro dedicato alla numerazione ed alla raccolta delle disposizioni di servizio, al quale ha accesso l'Ufficio Segreteria che protocolla tali atti predisposti da tutti gli Uffici della Comando.

La pubblicazione delle Disposizioni di Servizio avviene nel sito intranet del Comando.

L'Ufficio Segreteria invia a tutto il personale interessato una mail con le DDS registrate e pubblicate nel sito.

4.15 Registro Atti Interni (Verbali e Decreti interni)

E' il registro dedicato alla numerazione ed alla raccolta Verbali e Decreti interni, al quale ha accesso l'Ufficio Segreteria che protocolla tali atti predisposti da tutti gli Uffici del Comando.

4.16 Registro interno atti contabili

E' il registro dedicato alla numerazione ed alla raccolta degli atti contabili al quale ha accesso l'Ufficio Acquisti del Comando.

4.17 Disposizioni finali in merito alle abilitazioni sui singoli Registri

E' facoltà del R.G.D. o degli operatori del servizio di protocollo dell'Ufficio segreteria aggiornare le abilitazioni sopra menzionate sui singoli Registri o crearne di nuovi secondo le necessità che si dovessero rappresentare di volta in volta chiedendone autorizzazione al Comandante oppure ai Dirigenti del Comando di Cagliari.

5. ORGANIZZAZIONE E GESTIONE DELL'ARCHIVIO CORRENTE SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE.

5.1 Generalità

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (titolario), cioè di quello che si suole definire "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti".

Il piano di conservazione, collegato con il titolario ed elaborato tenendo conto dei flussi documentali dipendenti dai procedimenti e dalle prassi seguiti dall'AOO nell'espletamento delle funzioni istituzionali, definisce i tempi di conservazione dei documenti e dei fascicoli nella sezione di deposito dell'archivio.

Il piano di conservazione del Dipartimento VV.F non è stato al momento definito da parte dei competenti uffici centrali.

5.2 Misure di protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti degli enti pubblici non territoriali sono beni culturali inalienabili (art 822 e 824 c.c.). I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'AOO, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

L'archivio non può essere smembrato, a qualsiasi titolo, e deve essere conservato nella sua organicità.

Il trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della direzione generale per gli archivi. L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della generale per gli archivi.

Lo scarto dei documenti degli archivi delle amministrazioni/AOO statali è subordinato all'autorizzazione della direzione generale per gli archivi, su proposta delle commissioni di sorveglianza istituite presso ciascun ufficio con competenza corrispondente alla provincia o delle commissioni di scarto istituite presso ogni ufficio con competenza subprovinciale.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Per l'archiviazione e la custodia nella sezione di deposito o storica dei documenti contenenti dati personali, si applicano in ogni caso le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che convenzionali.

5.3 Titolario

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.

Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello, etc.

Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolare di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito.

Il titolare è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali e/o regionali. Dopo ogni modifica del titolare, il RGD provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

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

Viene garantita la storicizzazione delle variazioni di titolare e la possibilità di ricostruire le diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolare vigente al momento della produzione degli stessi.

Per ogni modifica di una voce viene riportata la data di introduzione e la data di variazione. L'indice di classificazione (TITOLARIO) adottato dall'AOO è allegato al presente Manuale (Allegato A), nel quale è riportato il "TITOLARIO UNICO" adottato dal Dipartimento a valere anche per gli uffici territoriali quali le Direzioni Regionali e i Comandi.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

A tale TITOLARIO UNICO dovrà farsi riferimento per una corretta gestione della procedura, in particolare per quanto riguarda la “Classificazione” e/o la “Fascicolazione”. Esso è strutturato su 3 livelli di classificazione immutabili in codifica e descrizione.

5.3.1 Classificazione dei documenti

Tutti i documenti ricevuti e prodotti dagli Uffici del Comando, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario. Mediante la classificazione si assegna al documento il codice completo dell'indice di classificazione (titolo, classe, sottoclasse, etc.).

L'attività di classificazione può essere effettuata dal Responsabile del Procedimento (utente che prende in carico il documento).

5.4 Fascicolazione dei documenti

Tutti i documenti registrati nel sistema informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli. Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento.

5.4.1 Apertura e chiusura del fascicolo

Il Responsabile del Procedimento Amministrativo o dell'Ufficio provvede all'apertura dei fascicoli, organizzandoli sulla base dei procedimenti amministrativi gestiti e dell'organizzazione del Comando, tenendo conto dell'organizzazione stabilita con il titolario.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni:

- indice di classificazione, (cioè titolo, classe, sottoclasse, etc.);
- oggetto del fascicolo;
- data di apertura del fascicolo;
- AOO e UO;
- responsabile;
- collocazione fisica di eventuali documenti cartacei;

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

- ACL (Access Control List, liste di controllo accessi);

- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Si stabilisce che i fascicoli sono associabili all'ultimo livello di dettaglio della struttura gerarchica del titolare. Il fascicolo può essere chiuso al termine del procedimento amministrativo o dei procedimenti amministrativi ad esso afferente. In ogni caso il fascicolo può essere riaperto dall'utente successivamente.

5.4.2 Processo di assegnazione dei documenti ad un fascicolo

Quando un nuovo documento viene recapitato all'amministrazione, il Responsabile del Procedimento Amministrativo, abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso debba essere ricollegato ad un affare o procedimento in corso, e pertanto debba essere inserito in un fascicolo già esistente, oppure se il documento si riferisce ad un nuovo procedimento per cui è necessario aprire un nuovo fascicolo.

6. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Per descrivere i flussi di lavorazione dei documenti all'interno del Comando si fa riferimento ai documenti:

- ricevuti dalla AOO, dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno alla AOO;

- inviati dalla AOO, all'esterno o anche all'interno della AOO in modo formale.

Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione.

Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e non interessano il sistema di protocollo.

Per la trattazione del flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione si fa riferimento a quanto già descritto nel precedente cap. 4.

La gestione della protocollazione in ingresso è gestita dall'Ufficio Segreteria.

Eccezioni a quanto sopra sono:

- Ufficio Prevenzione incendi per le comunicazioni ed istanze relative ai procedimenti di prevenzione incendi;
- Sala Operativa per le comunicazioni di soccorso;
- tutti gli Uffici per le comunicazioni di competenza, sia in formato analogico che informatico, pervenute direttamente a loro.

La gestione della protocollazione all'interno del Comando di Cagliari in uscita è gestita da tutti gli Uffici.

6.1 Flusso dei documenti ricevuti dalla AOO

6.1.1 Documenti in arrivo

I documenti che sono trasmessi al Comando, con qualsiasi mezzo (e-mail, posta ordinaria, ecc.), sia dall'esterno che dall'interno in maniera formale, sono di norma recapitati direttamente all'ufficio Segreteria, tranne per le eccezioni riportate nel paragrafo precedente.

Per i suddetti documenti si provvederà alla registrazione su registro di protocollazione secondo le regole descritte nel presente manuale e le procedure previste dal manuale dell'applicativo Vigilia.

In caso di incertezza sulla qualificazione del documento tra quelli non soggetti a protocollazione obbligatoria di cui al paragrafo 4.10, l'ufficio preposto, chiede indicazioni all'Ufficio Segreteria.

Per i documenti cartacei l'ufficio che ne esegue la protocollazione deve preventivamente procedere alla scansione del documento. Non saranno distribuite copie cartacee. L'originale sarà conservato dall'ufficio di competenza.

6.1.1.1 Rilascio di ricevute attestanti l'avvenuta registrazione di protocollo

La ricezione di documenti comporta la generazione di due tipologie diverse di ricevute: una legata al servizio di posta certificata, una al servizio di protocollazione informatica.

Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'AOO con gli standard specifici.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, prevede l'emissione della ricevuta di avvenuta registrazione di protocollo. Per le comunicazioni giunte via e-mail, quindi, (sia ordinaria che certificata), viene generata automaticamente dal sistema ed inviata all'indirizzo spedente, una ricevuta di avvenuta registrazione, in conformità ed ottemperanza a quanto previsto dal DPR 445/2000.

La ricevuta di protocollazione viene inviata ad ogni modifica parziale od annullamento completo del protocollo.

Vigilia, inoltre, permette di stampare la ricevuta di protocollazione.

6.1.2 Documenti in uscita

Prioritariamente i documenti sono firmati digitalmente ed inviati tramite pec istituzionale.

L'invio cartaceo è riservato alle tipologie di documenti obbligatoriamente previsti dalla normativa in tale forma.

I documenti contenenti dati sensibili devono riportare in oggetto anche la dicitura "CONTIENE DATI SENSIBILI".

L'ufficio mittente prepara il documento in formato PDF/A e li predispone per la firma secondo le procedure informatiche predisposte, con gli eventuali allegati informatici.

In caso di documento che obbligatoriamente deve essere inviato in forma cartacea, dopo la firma, il documento viene spedito dall'ufficio a cui appartiene il Responsabile del Procedimento.

6.1.3 Assegnazione dei documenti

Un documento protocollato deve essere assegnato agli utenti/uffici per la sua trattazione e successiva archiviazione.

Sono previste tre tipologie di assegnazione:

- per competenza;
- per conoscenza;
- per smistamento.

I documenti vanno assegnati agli Uffici, sono quindi escluse le comunicazioni di carattere strettamente personale, che possono essere assegnate al solo destinatario.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Ogni ufficio assegnatario, al suo interno avrà un addetto che assegnerà il documento a coloro che sono incaricati dell'istruttoria della pratica.

Le assegnazioni **per competenza** devono limitarsi ai soli Uffici direttamente interessati e coinvolti nel procedimento ai quali viene richiesta l'adozione di specifici provvedimenti o azioni per dare seguito al documento.

Sono pertanto da evitare assegnazioni:

- ad un Ufficio e contestualmente alle persone che vi appartengono;
- ad una sola persona all'interno di un Ufficio (salvo non sia interessata in modo diretto);
- a più Uffici o persone non direttamente competenti.

Nel caso il documento sia di interesse di un Ufficio o utente per il corretto svolgimento dei compiti assegnati ma, non richiede l'adozione di specifici provvedimenti o azioni il documento andrà assegnato per conoscenza.

I termini per la definizione del procedimento amministrativo che prende avvio dal documento, decorrono comunque dalla data di protocollazione. Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

6.1.3.1 Modifica delle assegnazioni

Nel caso di assegnazione errata, l'ufficio che riceve il documento, provvede alla restituzione motivata all'ufficio assegnante. Quest'ultimo procederà ad una nuova assegnazione.

La modifica delle assegnazioni può essere effettuata anche dall'operatore di protocollo se si accorge di una anomalia o di un errore. Quest'ultimo potrà riassegnare direttamente all'ufficio di competenza evitando la restituzione all'ufficio assegnante.

6.1.4 Presa in carico dei documenti

L'ufficio o l'utente assegnatario di un documento:

- verifica se il documento è di competenza dell'ufficio;

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

- in caso di errore ritrasmette il documento all'Ufficio assegnante;
- se il documento in uscita è stato inviato tramite pec ad un indirizzo pec, verifica che siano presenti le notifiche di sistema e l'assenza di messaggi di errore che assicurano la ricezione da parte del destinatario ("ricevuta di accettazione" da parte del server della AOO e "ricevuta di consegna" al server o di destinazione) e in caso di verifica positiva lo prende in carico.

L'ufficio segreteria provvede a smistare la corrispondenza assegnando di volta in volta al singolo ufficio/settore e non al singolo UU.

All'interno dell'ufficio il responsabile dell'ufficio o altra unità delegata provvede ad assegnare il documento al singolo UU-RPA incaricato della trattazione della pratica e/o servizio. Il Responsabile del Procedimento Amministrativo (RPA) è individuato, all'interno dell'Ufficio, in base all'organizzazione delle competenze della suddetta Unità Organizzativa.

L'assegnazione diretta del documento alle singole UU è facoltà esclusiva del Comandante o di unità da lui delegate che di norma sono costituite dal personale dell'ufficio Segreteria.

6.1.5 Classificazione ed archiviazione

Dopo la presa in carico e la sua trattazione con il completamento dell'iter amministrativo richiesto (compreso l'invio di documenti di risposta), il documento deve essere archiviato nel fascicolo. Per l'archiviazione corretta e secondo le disposizioni legislative vigenti, il documento deve essere classificato con lo stesso codice di titolare del fascicolo nel quale andrà inserito. In caso di inserimento in diversi fascicoli con diverse classificazioni, al documento dovranno essere associate le classificazioni di tutti i fascicoli.

Al fine di garantire il rispetto delle norme in materia di riservatezza, ad ogni fascicolo andrà associato il livello di riservatezza adeguato ai documenti in esso contenuti e i singoli fascicoli saranno accessibili esclusivamente alle UU inserite nelle relative liste di competenza, secondo l'organigramma del Comando. La creazione delle liste di competenza vengono realizzate dagli Amministratori informatici di VIGILI@ su richiesta dei responsabili degli uffici, previa comunicazione dei nominativi/uffici.

7. ACCESSO AL SISTEMA DI PROTOCOLLO INFORMATICO

7.1 Abilitazioni di accesso al sistema

Il presente paragrafo riporta i criteri e le modalità per il rilascio delle abilitazioni di accesso alle informazioni documentali gestite da "Vigilia" adottato dal Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile.

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/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.

Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da:
- una userID che permette l'identificazione dell'utente da parte del sistema;
- una password privata o riservata di autenticazione con scadenza ogni 90 giorni;
- una autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

I diversi livelli di autorizzazione sono assegnati dall'utente con credenziali di "amministratore", su indicazione del Dirigente Responsabile oppure del Responsabile dell'Ufficio.

Il ruolo di "Amministratore" è assegnato solamente ad una o più unità autorizzate dal RgD.

Gli utenti del servizio di protocollo una volta identificati sono suddivisi in profili d'accesso, sulla base delle rispettive competenze.

Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Tutte le utenze dell'AOO sono configurate con un time-out che provvede a disconnettere automaticamente l'applicazione dopo 40 minuti di inattività.

Le sessioni multiple con la stessa user ID sono proibite e impedita da VIGILIA.

7.2 Profili di accesso

- Amministratore di Ente
- Amministratore di Area Organizzativa Omogenea
- Operatore (di protocollo)
- Operatore uscita (per la corrispondenza in sola modalità uscita)
- Operatore riservato (per la corrispondenza riservata)
- Operatore posta (con abilitazione anche alla lettura della posta)
- Utente
- Responsabile di registro
- Utente responsabile
- Utente riservato
- Utente assegnatario (utente che riassegna sull'organigramma completo)
- Operatore documentale
- Utente visibilità ridotta pratica

Il dettaglio dei ruoli applicativi è illustrato nei manuali d'uso dell'applicativo.

8. Piano di sicurezza

Il presente capitolo riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

Quasi la totalità delle misure di sicurezza sono adottate direttamente a livello di struttura centrale, che si occupa di garantire efficienza e una standardizzazione fornendo il servizio di protocollo informatico a tutte le sedi periferiche del territorio nazionale. Per questo motivo, il piano di sicurezza nel seguito si limita a riportare le politiche di sicurezza già in essere nella struttura centrale che gestisce i server.

8.1 Obiettivo del Piano di Sicurezza

L'obiettivo del piano di sicurezza (PdS) è strettamente correlato agli obiettivi della sicurezza informatica che si possono riassumere nella triade CIA: Confidentiality (Confidenzialità), Integrity (Integrità) e Availability (Disponibilità). Nello specifico, il PdS garantisce infatti che i dati siano riservati, quindi consultabili solo da personale preventivamente autorizzato, integri ovvero non manomessi, e disponibili nonché resistenti alla distruzione o perdita anche accidentale.

8.2 Generalità

Il PdS, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza previste dalle disposizioni normative in materia di tutela dei dati personali e/o sensibili;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi particolari.

Vengono adottate le misure tecniche e organizzative di seguito specificate, al fine di garantire la sicurezza dell'impianto tecnologico dell'AOO relativo all'amministrazione centrale, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Rete Intranet dell'Amministrazione/AOO;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password ogni n. 90 giorni, con l'impossibilità di riutilizzare le ultime tre password precedentemente usate;
- tramite il coordinamento delle Strutture Centrali, piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informatico entro sette giorni in caso di disastro;
- tramite il coordinamento delle Strutture Centrali, impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service PACK) correttivi dei sistemi operativi;
- attraverso le funzionalità del PdP, cifratura dei dati sensibili e giudiziari contenuti nella documentazione acquisita al protocollo, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- conservazione delle copie di riserva dei dati e dei documenti, in cassaforte ignifuga dislocata presso il locali del CED delle Strutture Centrali;
- archiviazione giornaliera, attraverso l'apporto delle Strutture Centrali, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RGD e dal titolare dei dati e, ove normativamente stabilito, dalle forze dell'ordine.

8.3 Formazione dei documenti – aspetti di sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti dell'AEO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adotta preferibilmente il formato PDF, o più nello specifico il formato PDF/A utilizzato per preservare il documento intatto e accessibile nel tempo indipendentemente dall'applicativo usato per la sua creazione o lettura.

I documenti informatici prodotti dall'AEO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale o firma autografa da parte del Comandante o dei sostituti e/o responsabili/incaricati del procedimento, seguendo il Codice di Amministrazione Digitale (CAD).

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Per attribuire una data certa a un documento informatico prodotto all'interno dell'AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al Decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

8.4 Gestione dei documenti informatici

Il sistema operativo del PdP utilizzato dall'amministrazione/AOO, è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzione (scritture di sicurezza e controllo accessi).

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

8.5 Componente fisica della sicurezza

Il CED delle Strutture Centrali dove sono ubicati i server su cui risiedono le banche dati dei trattamenti di dati eseguiti con l'ausilio di strumenti elettronici risulta essere un'area ad accesso controllato. Al fine di impedire accessi di personale non autorizzato, sono state adottate le seguenti misure di sicurezza:

- il locale deve essere sempre chiuso, anche se presidiato;
- l'accesso è consentito solo al personale autorizzato, munito di badge;
- composizione di una lista delle persone autorizzate ad accedere;

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

- composizione di una lista delle persone a cui è stato rilasciato il badge, con eventuale data di riconsegna dello stesso;
- la lista deve essere periodicamente controllata;
- i visitatori occasionali devono essere accompagnati.

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi, i locali del CED sono protetti da:

- rivelatori di incendio;
- dispositivi antincendio manuali;
- gruppo di continuità dell'alimentazione elettrica;
- impianto di condizionamento.

8.6 Custodia e archiviazione dei dati

Per quanto riguarda gli archivi cartacei, la documentazione non utilizzata dovrà essere rigorosamente collocata all'interno di appositi armadi chiusi a chiave, per ridurre il rischio di visione impropria, distruzione, appropriazione da parte di esterni. Al fine di impedire l'accesso ai non autorizzati, quando gli uffici non sono direttamente presidiati da parte del personale addetto, gli stessi dovranno essere chiusi a chiave e le chiavi saranno custodite dagli Incaricati (addetti all'UU).

Per quanto riguarda gli archivi informatici, al personale addetto del CED delle Strutture Centrali, al fine di preservare dal rischio di perdita dei dati trattati con strumenti informatici o dalla divulgazione non autorizzata, sono state impartite istruzioni per la gestione e la custodia dei supporti di memorizzazione. In particolare sono state fornite direttive per:

- l'utilizzo di specifici software per salvataggi automatizzati;
- la conservazione e la custodia delle copie di backup;
- la definizione delle persone autorizzate ad accedere ai locali e le modalità di accesso.

8.7 Misure logiche di sicurezza

Per il trattamento effettuato con strumenti elettronici si sono individuate le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici;
- la password delle credenziali di autenticazione deve possedere determinate caratteristiche stabilite dalle Strutture Centrali in modo tale da garantirne la relativa riservatezza;
- al primo utilizzo, l'utente provvederà a modificarla e successivamente la modificherà periodicamente ogni n. 90 giorni;
- il sistema di protocollo informatico VIGILIA è sottoposto alle stesse regole d'accesso e autenticazione del dominio, con modifica periodica della password da effettuarsi non oltre 90 (novanta) giorni e coincidenza di tale password con quella da utilizzarsi per l'accesso alla propria casella di posta elettronica lavorativa;
- autorizzazione e definizione delle tipologie di dati ai quali gli incaricati possono accedere e utilizzare al fine del proprio profilo lavorativo;
- protezione di strumenti e dati da malfunzionamenti e attacchi informatici;
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali.

8.8 Norme di comportamento per la sicurezza informatica

E' essenziale che ciascun incaricato abbia consapevolezza delle responsabilità insite nel fatto di avere accesso a trattamenti di dati personali e a servizi forniti da sistemi condivisi; è l'utente infatti ad essere responsabile delle proprie azioni, sia nell'utilizzo della propria postazione di lavoro sia nell'accesso ai servizi di rete.

Accanto all'adozione di misure tecnologiche e soluzioni informatiche, vengono definite le seguenti norme comportamentali che tutti gli utenti, ed in particolari gli incaricati al trattamento dei dati, dovranno osservare:

- obbligo di custodire i dispositivi di accesso agli strumenti informatici (username e password);
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- obbligo di bloccare l'accesso alla propria postazione quando questa rimane non presidiata;
- obbligo di assoluta riservatezza;
- divieto di divulgazione della password di accesso al sistema.

8.9 Infrastruttura di rete

A livello di infrastruttura, sono state adottate le seguenti soluzioni informatiche per diminuire la vulnerabilità dei sistemi:

- Antivirus centralizzato e periferico;
- Firewall centralizzato;
- Apparati IDS (Rilevamento di intrusione);
- Apparati di controllo del traffico;
- Sistema di aggiornamento di windows centralizzato;
- Sistema di filtro delle e-mail;
- Backup dei Sistemi centralizzato;
- Policy restrittive di accesso ai sistemi.

8.10 Criteri e procedure per il salvataggio e il ripristino dei dati (di competenza delle Strutture Centrali)

Il backup delle banche dati sui server della sede Centrale è gestito e monitorato dal personale in servizio presso il CED delle Strutture Centrali.

Le procedure di ripristino dei dati, in caso di loro danneggiamento o di inaffidabilità del database, sono a carico di un presidio DBA, costituito da personale tecnico che svolge attività di gestione delle banche dati di tutti i server del Dipartimento.

8.11 Trasmissione e interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (*provider*) di cui si avvale l'amministrazione, (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/AOO) oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dalla normativa vigente.

8.11.1 All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss.mm.ii.).

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

Il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal Codice dell'Amministrazione Digitale.

8.11.2 All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

8.12 Accesso al PdP da parte degli utenti interni alla AOO

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso pubblica (*UserId*) e privata (*Password*) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale. Queste vengono descritte nei manuali applicativi del PdP presenti sulla intranet al seguente percorso: Direzione Centrale per l'innovazione Tecnologica, la digitalizzazione e per i beni e le Risorse Logistiche e Strumentali Ufficio per i Servizi Informatici – Protocollo Informatico – Accedi alla sezione guide e manuali.

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password, in parte riportate di seguito, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.

Il PdP adottato dall'amministrazione/AOO:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente del PdP può accedere solamente ai documenti che sono stati a lui assegnati.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

8.12.1 Utenti esterni alla AOO – Altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 42.

Le AOO che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzano funzioni di accesso per ottenere le seguenti informazioni:

- numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
- identificazione dell'UU di appartenenza del RPA.

8.12.2 Utenti esterni alla AOO – Privati

Per l'esercizio del diritto di accesso ai documenti, sono possibili due alternative: l'accesso diretto per via telematica e l'accesso presentando istanza all'Ufficio Segreteria del Comando.

L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettano di identificare in modo certo il soggetto richiedente, quali: firme elettroniche, firme digitali, Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE), Sistema Pubblico di Identità Digitale (SPID) sistemi di autenticazione riconosciuti dall'AOO. L'accesso attraverso l'Ufficio Segreteria prevede che questo ufficio sia direttamente collegato con il sistema di protocollo informatico e di gestione documentale sulla base di apposite abilitazioni concesse al personale addetto.

Se la consultazione avviene allo sportello, di fronte all'interessato, a tutela della riservatezza delle registrazioni di protocollo, l'addetto posiziona il video in modo da evitare la diffusione di informazioni di carattere personale.

Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

Si evidenzia che le suddette procedure sono subordinate all'attivazione del SPC nella Regione Sardegna.

9. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Il presente capitolo illustra le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente, prevista dal Prodotto di Protocollo Informatico.

9.1 Il registro di emergenza

Qualora non fosse disponibile fruire di Vigili© per una interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza.

Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.

Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite su registro di protocollo generale. Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale. La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.

In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

9.2 Modalità di apertura del registro di emergenza

Il Responsabile della Gestione Documentale assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica, le operazioni di protocollo sono svolte manualmente sul registro di emergenza informatico, su postazioni di lavoro operanti fuori linea.

Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari

L'autorizzazione perviene di norma dal Responsabile del Servizio di Protocollo della Direzione Centrale per l'innovazione Tecnologica, la digitalizzazione e per i beni e le Risorse Logistiche e Strumentali o dal servizio di assistenza di VIGILIA in base alle problematiche riscontrate ed ai tempi di ripristino previsti.

Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il Responsabile imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare.

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale. Nell'ambito del Comando dei Vigili del Fuoco di Cagliari viene abilitata una postazione presso l'ufficio Segreteria ed una presso la Sala Operativa.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo, su indicazione del servizio di assistenza centrale, o, se indisponibile, su sua iniziativa, autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana. Per semplificare e normalizzare la procedura di apertura del registro di emergenza è stato predisposto il modulo (cartaceo o digitale) riportato di seguito:



Ministero dell'Interno

DIPARTIMENTO DEI VIGILI DEL FUOCO

DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVILE

Comando dei Vigili del Fuoco di Cagliari

Servizio di gestione informatica del protocollo

SCHEDA DI APERTURA/CHIUSURA DEL REGISTRO DI EMERGENZA

Causa dell'interruzione:

Data: gg/mm/aaaa di inizio/ fine interruzione _____

(depennare la voce incongruente con l'evento annotato)

Ora dell'evento hh /mm _____

Annotazioni:

Numero protocollo xxxxxxxx iniziale/finale _____

(depennare la voce incongruente con l'evento annotato)

Pagina n.

***Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari***

Firma del responsabile del servizio di protocollo

9.3 Modalità di utilizzo del registro di emergenza

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro il numero totale di operazioni registrate manualmente.

La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario del Comando.

Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono uguali a quelli previsti dal protocollo generale.

Durante il periodo di interruzione del servizio di protocollo informatico generale, il responsabile del sistema informatico del CED del Dipartimento o il servizio di assistenza di Vigili© provvede a tener informato il Responsabile per la tenuta del Protocollo sui tempi di ripristino del servizio.

9.4 Modalità di chiusura e recupero del registro di emergenza

E' compito del Responsabile per la tenuta del Protocollo verificare la chiusura del registro di emergenza, far importare dal registro di emergenza al sistema di protocollo generale le protocollazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.

Al fine di ridurre la probabilità di commettere errori in fase di trascrizione dei dati riportati dal registro di emergenza (postazione di lavoro stand alone) a quello del protocollo generale e di evitare la duplicazione di attività di inserimento, le informazioni relative ai documenti protocollati in emergenza su una o più postazione di lavoro dedicate della AOO, sono inserite nel sistema informatico di protocollo generale, utilizzando un'apposita funzione di recupero dei dati.

Una volta ripristinata la piena funzionalità del Prodotto di Protocollo Informatico, il Responsabile provvede alla chiusura del registro di emergenza.

Per semplificare la procedura di chiusura del registro di emergenza il RGD può utilizzare un modulo analogo a quello utilizzato nella fase di apertura del registro di emergenza.

Gli uffici del Comando segnaleranno tempestivamente al RGD ogni eventuale problematica o evento suscettibile di incidere sull'operatività ed efficacia del Manuale, al fine di un'eventuale aggiornamento, modifica e/o integrazione.

***Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile
Area Organizzativa Omogenea
Comando dei Vigili del Fuoco di Cagliari***

IL RESPONSABILE DEL SERVIZIO

DI GESTIONE DOCUMENTALE

DVLG Elisabetta CARTA