PROTEZIONE CIVILE
Presidenza del Consiglio dei Ministri
Dipartimento della Protezione Civile

Manuale di Gestione

del protocollo informatico, dei flussi documentali

e degli archivi

* * *

Edizione 2017

INDICE

INTRODUZIONE

Questa terza edizione del *Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi* trae origine dagli aggiornamenti normativi, intervenuti a far data dal 2013, concernenti: fatturazione elettronica[1], criteri di registrazione al protocollo[2], formazione[3] e tecniche di corroborazione del documento informatico originale e in copia[4], conservazione[5] .

Il legislatore in un triennio ha accelerato il processo di ammodernamento e di razionalizzazione della gestione della documentazione amministrativa, introducendo, obblighi di tracciabilità informatica dei flussi finanziari nei rapporti commerciali tra PA e privati (fatturazione elettronica), di utilizzo esclusivo delle tecnologie dell'informazione nei rapporti inter-istituzionali e con cittadini digitalmente evoluti.

I più recenti adeguamenti del Codice dell'Amministrazione digitale al regolamento eIDAS, che disciplina le interazioni elettroniche sicure tra imprese, cittadini e pubblica amministrazione all'interno dell'UE[6], hanno introdotto nell'ordinamento italiano nuovi strumenti di autenticazione dei documenti, quali il sigillo elettronico[7], il concetto di neutralità

[1] Ministero dell'economia e delle finanze, Decreto 3 aprile 2013, n. 55 recante "Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.

[2] DPCM 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale".

[3] DPCM 13 novembre 2014 recante "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis , 23 -ter , 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

[4] DPCM 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71".

[5] DPCM 3 dicembre 2013 recante Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

[6] Il Regolamento eIDAS (electronic IDentification Authentication and Signature) –Regolamento UE n°910/2014 sull'identità digitale.

[7] art. 35, comma 1bis e 5, D.Lgs 7 marzo 2005, n. 82, recante il "Codice dell'Amministrazione digitale" e s.m.i.

tecnologica[8], evidenziato la centralità dei sistemi di identificazione ed autenticazione negli interscambi[9], ampliato la portata del concetto di democrazia partecipata[10] .

L'adeguamento tecno-normativo ha implicato la revisione delle procedure interne, la reingegnerizzazione dei flussi documentari, l'implementazione dell'applicativo gestionale in uso, previa verifica della sostenibilità organizzativa interna, in termini di efficienza ed efficacia.

Si è proceduto così alla progressiva eliminazione delle ridondanze di flusso, all'introduzione di canali di interoperabilità performanti, quali la spedizione massive pec/pei/fax server da adottare particolarmente in contesti emergenziali, e di nuovi moduli applicativi, come la fatturazione elettronica, il trattamento elettronico dei dati sensibili e giudiziari, la stipula contrattuale conforme al D.L.gs 179/2012, la produzione dei pacchetti di versamento dei registri e dei relativi metadati da trasmettere al conservatore esterno.

Le interazioni con le istituzioni e le aziende sono assicurate ordinariamente attraverso canali telematici, con esclusione dei documenti originali unici e i bandi di gara, gestiti al di fuori del MEPA; quelle con i cittadini avvengono con più frequenza in modalità analogica.

Le attività e le procedure sommariamente descritte sono raccolte nel *Manuale* che disciplina:

- l'organizzazione delle attività di gestione documentale;
- i flussi documentali;
- i prerequisiti e le modalità di registrazione dei documenti;
- i criteri e le regole di organizzazione dell'archivio;
- il piano di sicurezza;
- le procedure per la tutela dei dati personali;
- l'accesso e la consultazione dei documenti;
- le modalità di aggiornamento e comunicazione del *Manual*e stesso.

[8] art. 20, comma 1bis, ibidem.
[9] art. 64, ibidem.
[10] art. 64, comma 2 septies, ibidem

CONTESTO ISTITUZIONALE E OPERATIVO

Il Dipartimento della Protezione civile è una struttura organizzativa della Presidenza del Consiglio dei Ministri e, in quanto tale, svolge attività di indirizzo e coordinamento del Servizio nazionale di Protezione civile in riferimento alla previsione degli eventi, alla pianificazione della riduzione del rischi, al soccorso alle popolazioni in caso di emergenze nazionali, al ripristino delle condizioni di normalità.

In considerazione dei compiti istituzionali richiamati, di particolare impatto sulla gestione documentale soprattutto in fase emergenziale, si è ritenuto opportuno adottare un Manuale, in cui descrivere il modello organizzativo e la prassi adottata, anche in tali circostanze.

Tale autonomia operativa è comunque concertata con l'Ufficio del Segretario generale che stabilisce le linee guida della gestione archivistica della Presidenza del Consiglio dei Ministri.

Il Dipartimento adotta , infatti, il titolario unico e il piano di conservazione della Presidenza del Consiglio dei Ministri.

L'interoperabilità con l'Ufficio del Segretario generale e gli altri Dipartimenti è assicurata, al momento, dal servizio di posta elettronica certificata; è prevista nel prossimo futuro l'adozione di un sistema di gestione documentale interoperabile con quello della Presidenza del Consiglio dei Ministri.

SEZIONE I
DEFINIZIONI ED AMBITO DI APPLICAZIONE

Art. 1
Ambito di applicazione

Il presente Manuale, adottato ai sensi della normativa vigente, regolamenta le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti amministrativi del Dipartimento della Protezione Civile[11] .

Art. 2
Definizioni

Ai fini del presente *Manuale* si intende :

a) per *allineamento dei dati*: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;

b) per *Amministrazione*, il Dipartimento della Protezione Civile;

c) per *archiviazione elettronica*, il processo di memorizzazione di documenti informatici, univocamente identificati da un codice di riferimento;

d) per *area organizzativa omogenea - AOO*, un insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato;

e) per *archivio corrente*, la parte di documentazione relativa ai procedimenti in corso di trattazione, o comunque verso i quali sussiste un interesse corrente;

f) per *archivio di deposito*, il complesso delle serie archivistiche non più afferenti all'amministrazione corrente, ma non ancora destinate alla conservazione permanente;

g) per *archivio storico*, il complesso delle serie archivistiche relative a procedimenti conclusi e destinati, previe operazioni di scarto, alla conservazione permanente per la consultazione al pubblico, in conformità alle disposizioni del D.Lgs 22 gennaio 2004; n. 42;

h) per *assegnazione*, l'operazione di individuazione dell'ufficio competente, per responsabilità o per conoscenza, della trattazione del procedimento amministrativo a cui i documenti si riferiscono;

[11] DPCM 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale".

i) per *autenticazione del documento informatico*: la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione;

j) per *autorizzazione informatica*, la verifica della corrispondenza tra le abilitazioni in capo al soggetto richiedente ed il tipo di operazione che il soggetto intende eseguire;

k) per *chiave privata*, l'elemento della coppia di chiavi asimmetriche, utilizzato soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

l) per *chiave pubblica*, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

m) per *classificazione d'archivio*, l'attività consistente nell'attribuzione ai documenti di una corretta posizione logica e fisica nel sistema di conservazione, attraverso una codifica alfa-numerica (classe);

n) per *Codice il Codice dell'Amministrazione digitale*, D.Lgs 7 marzo 2005, n. 82, che raccoglie ed integra la normativa preesistente inerente alla gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitali;

o) per *copia informatica di documento analogico*, il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

p) per *copia per immagine su supporto informatico di documento analogico*: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui e' tratto;

q) per *copia informatica di documento informatico*: il documento informatico avente contenuto identico a quello del documento da cui e' tratto su supporto informatico con diversa sequenza di valori binari;

r) per *dati giudiziari*, i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del codice di procedura penale;

s) per *dati territoriali*, i dati che attengono, direttamente o indirettamente, a una località;

t) per *documento informatico*: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

u) per *documento amministrativo*, ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa;

v) per *documento analogico*, un documento di grandezza fisica variabile, quale il documento cartaceo, il microfilm, il nastro magnetico;

w) per *documento informatico*, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti o, comunque, utilizzati ai fini dell'attività amministrativa;

x) per *documento digitale*, la scansione del documento analogico;

y) per *domicilio digitale*: l'indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato di cui al Regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito «Regolamento eIDAS»

x) per *fax server*, sistema di comunicazione che consente di ricevere comunicazioni - inviate via fax o attraverso un analogo sistema - in formato digitale su una casella di posta elettronica, utilizzando linee telefoniche dedicate;

ya) per *fascicolazione*, l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi;

yb) per *firma elettronica*, l'insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (regolamento EIDAS);

yc) per firma elettronica avanzata, l'insieme di dati in forma elettronica creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, connessi a un documento informatico, per consentire l'identificazione del firmatario in modo univoco e l'integrità del documento stesso (regolamento EIDAS);

yd) per *firma elettronica qualificata*, la firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma qualificata (regolamento (EIDAS);

ye) per *firma digitale*: un particolare tipo di firma elettronica, basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, 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;

yf) per *firma omessa* si intende la sostituzione della firma autografa con indicazione delle generalità del funzionario pubblico, seguita da riferimento normativo; la firma è da apporre nel gruppo firma del documento[12];

z) per *gestione dei documenti*, l'insieme delle attività finalizzate alla registrazione di protocollo, classificazione, assegnazione, fascicolazione, conservazione e consultazione dei documenti formati o acquisiti dall'Amministrazione, nell'ambito del sistema di classificazione adottato;

aa) per *identificazione digitale,* la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale nel Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni (SPID);

ab) per *funzione di hash*, una funzione matematica univoca ed unidirezionale, che trasforma un testo elettronico di qualunque lunghezza (input) in testo di lunghezza fissa (output) , ovverosia in una stringa alfanumerica, assimilabile ad un'impronta digitale non riproducibile, al fine di garantire l'integrità e l'immodificabilità del documento stesso nel sistema di protocollo informatico;

ac) per *notifica di eccezione*, il messaggio pec con cui il destinatario informa il mittente di errori/ o carenze della comunicazione pervenuta via pec;

ad) per *originali non unici*, i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi; ad esempio dati anagrafici in possesso di altro Ente possono essere ricavati da dichiarazioni o atti di altra natura;

ae) per *piano di conservazione degli archivi*, il piano integrato con il sistema di classificazione, contenente i criteri di organizzazione dell'archivio, di selezione periodica e conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;

af) per *posta elettronica certificata*, il sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;

ag) per *pubblico ufficiale*, il responsabile della gestione documentale e vicario, che attestano la conformità della copia informatica o analogica delle unità documentarie;

[12] Firma omessa ai sensi dell'art. . 3,D.L.gs 12 febbraio 1993 n. 39 recante "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421"

ah) per *ricevuta di accettazione* si intende il certificato inviato dal provider del mittente con cui si comunica la presa in carico della spedizione;

ai) per *ricevuta di consegna* si intende il certificato inviato dal provider del destinatario al mittente;

al) per *riversamento diretto*, il trasferimento di un documento da un supporto ottico ad un altro senza modifiche;

am) per *riversamento sostitutivo*, il trasferimento di un documento da un supporto ottico all'altro con modifiche della loro rappresentazione informatica; ovverosia la migrazione da un supporto ad un altro con modifica dello standard di conservazione utilizzato (da jpg a tif per esempio);

an) per *segnatura di protocollo*, l'apposizione sull'originale del documento, in forma permanente e non modificabile, dei seguenti metadati: codice identificativo dell'amministrazione, e dell'area organizzativa omogenea, data e progressivo di protocollo, ai quali si aggiungono, nel file XML di accompagno, oggetto, mittente e destinatario. Sono da considerarsi opzionali e nel solo file XML: oggetto, mittente e destinatario;

ao) per *sistema di gestione informatica dei documenti*, l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dall'Amministrazione per la gestione dei documenti;

ap) per *SPID* il Sistema Pubblico per la gestione dell'Identità Digitale, ovverosia l'insieme dei soggetti pubblici e privati che garantisce l'accesso ai servizi in rete ai cittadini ed alle imprese;

aq) per *titolario di classificazione*, un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle competenze dell'Amministrazione, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la sedimentazione secondo un ordine logico, che rispecchi storicamente lo sviluppo dell'attività svolta;

ar) per *titolare del trattamento dei dati sensibili e giudiziari*, il Capo Del Dipartimento della Protezione civile;

as) per *unità organizzativa responsabile*, UOR, la struttura responsabile dei procedimenti amministrativi, che corrisponde all'Ufficio;

at) per *validazione temporale*, il risultato della procedura informatica con cui si attribuiscono data ed orario ad uno o più documenti informatici;

au) per *stato di configurazione*, l'assetto che il Dipartimento della Protezione Civile assume per fronteggiare un evento. Le procedure del Dipartimento in caso di emergenza si articolano in 4 Stati di configurazione – S0 (Ordinaria), S1 (Vigilanza), S2 (Presidio

operativo), S3 (Unità di crisi) – corrispondenti al crescente grado di attivazione del Dipartimento, con il coinvolgimento progressivo di Uffici e Servizi

SEZIONE II
MODELLO ORGANIZZATIVO

Art. 3
Aree organizzative omogenee

Ai fini della gestione documentale generale, è stata individuata una AOO denominata Dipartimento della Protezione Civile.

La AOO indicata è collegata ad un indirizzo di posta elettronica certificata, protezionecivile@pec.governo.it

Art. 4
Le figure professionali responsabili della gestione documentale

Nella AOO opera una struttura denominata Segreteria del Capo del Dipartimento-Protocollo, che gestisce l'intero ciclo di vita della documentazione prodotta e ricevuta dal Dipartimento.

A capo di tale struttura è preposto il Responsabile della gestione documentale, del protocollo informatico e degli archivi, supportato e sostituito da Vicario in caso di assenza e/o impedimento.

Tale professionalità, in possesso di titoli e competenze tecno-archivistiche, definisce ed assicura[13]:

a) la predisposizione del Manuale di gestione, approvato dal Capo del Dipartimento;

b) la predisposizione del piano di sicurezza informatica di concerto con il Responsabile dei sistemi informativi, il Responsabile della conservazione, il Responsabile del Servizio di conservazione (SIAV), il Responsabile della sicurezza;

c) l'attribuzione e l'aggiornamento dei livelli di accesso al sistema informativo, sulla base delle indicazioni fornite dai Responsabili delle UOR;

d) la pianificazione e il coordinamento del processo di adeguamento normativo e della manutenzione evolutiva del sistema gestionale, con particolare riferimento alla registrazione di protocollo, alla gestione dei flussi documentali;

e) la supervisione dell'accessibilità nel tempo dei documenti trasmessi e ricevuti dalla AOO;

f) l'accesso, in condizioni di sicurezza, alle informazioni del sistema, nel rispetto delle

[13] artt. 61, 62 D.P. R. 28 dicembre 2000, n. 445 recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"; art. 4, comma 1, DPCM 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del "Codice dell'amministrazione digitale" di cui al decreto legislativo n. 82 del 2005.

disposizioni in materia di tutela dei dati personali;

g) la corretta esecuzione delle operazioni di salvataggio dei dati e la loro conservazione;

h) la supervisione della formazione dei pacchetti di versamento dei dati da inviare al sistema di conservazione esterno;

i) la corretta formazione ed invio a conservazione dei registri;

j) le operazioni di annullamento e/o di modifica delle registrazioni di protocollo consentite, previa motivazione;

k) la supervisione dello svolgimento, anche manuale, delle operazioni di registrazione di protocollo su registro di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica;

l) la pianificazione e il coordinamento del ripristino delle attività di gestione documentale in caso di guasto o anomalie;

m) la definizione e l'implementazione delle procedure di gestione documentale in fase di emergenza, sulla base delle scelte e degli indirizzi assunti dalla UOR istituzionalmente preposta al coordinamento delle emergenze;

Il Responsabile o Vicario nell'assolvimento dei compiti, previsti alle lettere g), k); l) si avvale del supporto di due referenti informatici; per le attività previste alle lettere g), l) i referenti verranno individuati di concerto con il Servizio informatico.

I referenti dovranno, per quanto concerne i compiti di cui ai par. g), predisporre le copie di backup), per quelli di cui al par. k) verificare la funzionalità della postazione di emergenza; per quelli di cui al par. l) monitorare il ripristino delle attività di gestione documentale; per quelli di cui al par m) provvedere alla predisposizione delle infrastrutture dedicate ad un sistema di gestione documentale delocalizzato.

La società fornitrice supporta il Responsabile e il Vicario nei compiti di cui ai par. d); e); f); g), h); i); k); l); m).

Art. 5

Modello operativo adottato per la gestione dei documenti

Ogni UOR ha il proprio *Responsabile del procedimento amministrativo*, l'elenco dei quali è riportato nell'allegato 3[14].

Tale Responsabile designa un referente della gestione documentale, che collabora con il *Responsabile* della gestione documentale all'ottimizzazione delle procedure adottate.

I referenti hanno il compito di segnalare al *Responsabile* della gestione documentale le criticità gestionali della UOR, di trasmettere le richieste di abilitazione degli utenti, di sottoporre eventuali aggiornamenti della classificazione in uso, di cooperare per la regolare registrazione in uscita dei documenti.

[14] art. 5, Legge 8 agosto 1990, n. 241 recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi".

SEZIONE III

TIPOLOGIA E VALORE GIURIDICO DEI DOCUMENTI

Art. 6

Le tipologie documentarie

Le tipologie documentarie detenute dal Dipartimento sono riportate nell'all. 8 bis[15].

Art. 7

Formazione dei documenti amministrativi informatici

I documenti amministrativi informatici vengono prodotti all'interno del Dipartimento secondo le modalità individuate dalle Regole tecniche[16].

Art. 8

Valore giuridico dei documenti amministrativi informatici firmati digitalmente

I documenti informatici, prodotti nelle modalità di cui al precedente articolo, e sottoscritti digitalmente soddisfano il requisito di cui all'art. 2702 del codice civile[17].

Art. 9

Duplicati e copie informatiche dei documenti amministrativi informatici

Le copie informatiche dei documenti amministrativi informatici vengono prodotte attraverso apposti modulo dell'applicativo gestionale in uso.

Qualora fosse richiesta una conformità opponibile a terzi, senza possibilità di azione di disconoscimento, il Responsabile della gestione documentale o il Vicario provvederanno alla sottoscrizione di un'attestazione allegata alla copia[18].

Art. 10

Copie analogiche di documenti amministrativi informatici

La conformità della copia analogica all'originale informatico è attestata con apposita

[15] AGID Linee guida sulla conservazione dei documenti informatici, 10 dicembre 2015.

[16] art. 3 ,9, DPCM 13 novembre 2014 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 7 marzo 2005".

[17] Art. 21, comma 2; art. 23 ter, D.Lgs 7 marzo 2005, n. 82 recante il "Codice dell'Amministrazione digitale" e s.m.i..

[18] art. 6, comma 3, DPCM 13 novembre 2014 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 7 marzo 2005".

dicitura, riportata nel margine del documento; l'attestazione è circoscritta alle attività correnti.

Qualora fosse richiesta una conformità opponibile a terzi, senza possibilità di azione di disconoscimento, il Responsabile della gestione documentale o il Vicario provvederanno alla sottoscrizione di un'attestazione allegata alla copia e conservata nel repository documentale.

Art. 11

Dematerializzazione dei documenti analogici

I documenti ricevuti o prodotti su supporto cartaceo, sono scansionati integralmente con i loro allegati.

Il trattamento dei dati personali, sensibili e giudiziari è disciplinato nell'art.15 quinquies e nell'allegato n. 2.

Il processo di scansione si articola nelle seguenti fasi:

a) acquisizione del documento principale in unico file;

b) acquisizione successiva in file diversi degli allegati;

c) verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza agli originali cartacei;

d) collegamento delle immagini alle rispettive registrazioni di protocollo, in modo non modificabile;

I documenti digitali, ottenuti al termine del processo, sono gestiti all'interno del sistema informativo che ne assicura l'immodificabilità e l'integrità nel tempo, dal momento che non possono esservi apportate variazioni al termine delle operazioni di registrazione[19].

Art. 11 bis

Valore giuridico delle copie per immagine dei documenti analogici

I documenti scansionati nelle modalità descritte nell'art.11, hanno la stessa efficacia probatoria dell'originale cartaceo, in quanto protocollati ed archiviati in un sistema che ne assicura immodificabilità ed integrità nel tempo, fino a disconoscimento espresso[20].

Fanno eccezione i documenti originali unici.

Qualora necessario, il Responsabile o il Vicario della gestione documentale rilascia attestazione di conformità associata alla copia per immagine; in tal caso non può esservi azione di disconoscimento[21].

---

[19] art. 9, comma 5, DPCM 13 novembre 2014 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 7 marzo 2005".

[20] Art. 22, comma 3, D.Lgs 7 marzo 2005 n. 82 recante il "Codice dell'Amministrazione digitale" e s.m.i.

Art. 12

Sottoscrizione ed elementi di validazione dei documenti informatici

I documenti informatici sottoscritti con firme qualificate ed avanzate, la cui certificazione risulti revocata, scaduta o sospesa, sono assimilabili a documenti non sottoscritti[22]; pertanto, non saranno registrati a protocollo, qualora la sottoscrizione abbia valore ad substantiam o non siano riscontrabili elementi di corroborazione alternativi.

La trasmissione per posta elettronica certificata surroga la firma avanzata, purchè le credenziali dell'utente titolare di account siano state rilasciate dal provider, previa identificazione, e la certificazione pec includa il documento originale o il documento sia sottoscritto in altra forma e accompagnato da carta di identità[23].

I documenti oggetto dei flussi interni e gli avvisi meteo saranno sottoscritti con firma omessa, che ha lo stesso valore giuridico della firma autografa[24].

Art. 13

Validazione temporale dei documenti informatici

I documenti informatici saranno validati temporalmente attraverso la registrazione di protocollo e i metadati di interoperabilità nella fase corrente, e con la procedura di marcatura nella fase di conservazione[25].

Art. 14

Documenti analogici originali unici

I Decreti del Presidente del Consiglio dei Ministri, i Decreti ministeriali e interministeriali, gli atti di decretazione dirigenziale e direttoriali, i protocolli di intesa, gli atti amministrativi approvati nella forma di Decreto del Presidente della Repubblica in originale, sono acquisiti e conservati su supporto cartaceo.

---

[21] Art. 22, comma 2, ibidem.

[22] Art. 24, comma 4bis, ibidem.

[23] art. 61 D.P.C.M. 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71" .

[24] Art. 3, D.Lgs 12 febbraio 1993, n. 39

[25] art. 41 DPCM 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71".

In caso di conservazione digitale, la dichiarazione di conformità all'originale sarà del Responsabile della gestione documentale, o del Vicario, con dichiarazione da questi firmata digitalmente ed allegata alla copia informatica[26].

[26] DPCM 21 marzo 2013 recante **"**Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e s.m.i".

SEZIONE IV
FLUSSO IN ENTRATA ED IN USCITA

Art. 15
Flusso di lavorazione dei documenti cartacei in entrata

Le fasi della gestione dei documenti sono:

a) ricezione (cfr. sezione IV);
b) assegnazione (cfr. sezione V);
c) registrazione e segnatura di protocollo (cfr. sezione VI);
d) classificazione(cfr. sezione VII);
e) fascicolazione (cfr. sezione VIII);
f) archiviazione (cfr. sezione X).

Art. 15 bis
Flusso di lavorazione dei documenti informatici in entrata

Le fasi della gestione dei documenti sono:

a) ricezione (cfr. sezione IV);
b) registrazione e segnatura di protocollo (cfr. sezione VI);
c) assegnazione (cfr. sezione V);
d) classificazione(cfr. sezione VII);
e) fascicolazione (cfr. sezione VIII);
f) archiviazione (cfr. sezione X).

Fanno eccezione al flusso descritto le comunicazioni dei cittadini pervenute via email in assenza di documento di identità e sottoscrizione, che verranno inoltrate direttamente all'indirizzo urp@protezionecivile.it per i seguiti di competenza**.**

Art. 16
Flusso di lavorazione dei documenti cartacei in uscita

Le fasi della gestione dei documenti sono:

a) registrazione e segnatura di protocollo (cfr. sezione VI);
b) classificazione (cfr. sezione VII);
c) fascicolazione (cfr. sezione VIII);
d) spedizione (cfr. sezione IX);
e) archiviazione (cfr. sezione X).

Le comunicazioni cartacee in uscita dovranno essere limitate ad utenti privi di domicilio

digitale ai sensi dell'art. 3bis del Codice dell'Amministrazione digitale; a documenti originali unici nel caso di pubbliche amministrazioni.

Art. 16 bis

Flusso di lavorazione dei documenti informatici in uscita

Le fasi della gestione dei documenti sono:

a) registrazione e segnatura di protocollo (cfr. sezione VI);
b) classificazione (cfr. sezione VII);
c) fascicolazione (cfr. sezione VIII);
d) spedizione (cfr. sezione IX);
e) archiviazione (cfr. sezione X**).**

Art. 17

Flusso di lavorazione dei documenti informatici in uscita (interna)

Le fasi della gestione dei documenti sono:

a) registrazione e segnatura di protocollo (cfr. sezione VI);
b) classificazione (cfr. sezione VII);
c) fascicolazione (cfr. sezione VIII);
d) assegnazione solo via S.I.Ge.D.®;
e) archiviazione (cfr. sezione X**).**

Art. 18

Flusso di lavorazione di atti endo procedimentali

Gli atti endo-procedimentali non verranno registrati a protocollo, ma inoltrati all'indirizzo email della UOR di riferimento, se pervenuti alla casella di posta elettronica certificata del Dipartimento.

RICEZIONE DEI DOCUMENTI

Art. 19

Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono pervenire alla A.O.O. tramite:

a) il servizio postale, ma solo dopo opportune procedure di bonifica da effettuarsi presso la sede della Presidenza del Consiglio dei Ministri di via dell'Impresa 9.

Tale canale è ammesso per documenti originali unici, per i documenti classificati ai sensi della Legge 3 agosto 2007, n. 124, di atti di gara (al di fuori del MEPA), per comunicazioni

provenienti da cittadini sprovvisti di domicilio digitale;

b) telefax in caso di cittadini sprovvisti di domicilio digitale; il numero di telefax deve coincidere con un recapito telefonico direttamente riconducibile al mittente; oppure nella comunicazione debbono esservi riferimenti di recapito ulteriori.

Tale canale è altresì ammesso in tutte le fattispecie di eccezionalità riconducibili a particolari scenari di evento o cause di forza maggiore che impediscano l'utilizzo di canali telematici.

c) circolazione interna, con esclusione tassativa di stampa di documenti pervenuti da canali informatici.

I documenti, ricevuti nelle modalità suindicate, vengono timbrati a cura del personale della Segreteria del Capo del Dipartimento-Protocollo, una volta accertati i prerequisiti per la registrazione ai sensi del successivo art. 28.

Art. 20
Ricezione dei documenti informatici

La ricezione dei documenti informatici avviene attraverso la casella di posta elettronica certificata istituzionale protezionecivile@pec.governo.it, nonché attraverso ogni altra forma di trasmissione informatica e telematica, che ne attesti con certezza la provenienza[27].

La data e l'ora della ricezione della posta elettronica certificata, riportata nell'avviso di consegna rilasciata dal provider al mittente della comunicazione, è opponibile a terzi.

Gli addetti della Segreteria del Capo del Dipartimento-Protocollo verificano giornalmente la corretta migrazione dei dati dalla casella di posta elettronica certificata al sistema di gestione documentale, ivi inclusa la data e l'ora .

L'indirizzo della casella di posta elettronica certificata è pubblicato sul sito istituzionale del Dipartimento e nell'indice IPA.

Le comunicazioni digitali dovranno essere indirizzate alla posta elettronica certificata del Dipartimento e non agli indirizzi email delle UOR.

Qualora dovessero pervenire agli indirizzi email delle UOR, queste si attiveranno presso il mittente per il corretto inoltro all'indirizzo protezionecivile@pec.governo.it.

I documenti informatici possono essere ricevuti anche su supporto removibile, attraverso il sistema postale oppure brevi manu, purché di volume non superiore a 4,5 GB, in formato ammesso per la conservazione e provvisti di attestazione di conformità all'originale

[27] Artt. 45, 47, D.L.gs 7 marzo 2005, n 82 recante il "Codice dell'Amministrazione digitale" e s.m.i..

conservato presso il mittente, tramite impronta informatica (HASH) associata univocamente al contenuto del supporto removibile,

Art. 21

Notifiche di eccezione

Le notifiche di eccezione vengono inviate dalla pec dipartimentale, a cura del Servizio di Segreteria del Capo Dipartimento- Protocollo, al mittente in tali casi:

a) illeggibilità e/o mancata integrità del documento;

b) dati incongruenti nella segnatura informatica;

c) assenza di elementi obbligatori nella segnatura xml;

d) mancata congruità tra documento o allegati dichiarati all'interno del file segnatura.xml con quanto inviato;

e) adozione di formato non accettato;

f) testo contenente macroistruzioni;

g) mancata sottoscrizione digitale del documento primario ed eventualmente degli allegati, qualora la firma abbia valore ad substantiam (v. contratti); o qualora abbia valore ad probationem in assenza di elementi sostitutivi, quali trasmissione via pec con certificazione lunga, firma elettronica e copia allegata del documento di identità, firma omessa per pubblici dipendenti.

h) incompetenza assoluta ratione materiae.

Il Servizio di Segreteria del Capo Dipartimento- Protocollo darà comunicazione via email delle notifiche di eccezione di cui ai par. c, alle UOR potenzialmente destinatarie ratione materiae.

Tale comunicazione in nessun caso implica l'avvio del procedimento amministrativo.

Art. 22

Rilascio di ricevute attestanti ricezione, e protocollazione dei documenti

Su richiesta dell'utenza, si rilascia, come ricevuta di avvenuta ricezione di documenti cartacei, la copia fotostatica del primo foglio, con indicazione di data, ora di arrivo e sigla dell'operatore.

I documenti pervenuti all'indirizzo protezionecivile@pec.governo.it, da altro indirizzo di posta elettronica certificata, sono accompagnati da notifica al mittente dell'avvenuta consegna, che assume lo stesso valore legale della ricevuta a/r.

SEZIONE V
ASSEGNAZIONE DEI DOCUMENTI

Art. 23
Responsabili dell'assegnazione dei documenti.

L'assegnazione alle UOR dei documenti in ingresso, pervenuti in modalità analogica o digitale, è effettuata dal personale della Segreteria del Capo del Dipartimento e dal Capo del Dipartimento, in sua assenza dal Vice Capo Dipartimento.

Gli originali dei documenti verranno assegnati alla UOR competente individuata.

L'assegnazione interna alle UOR è effettuata dal *Responsabile del procedimento amministrativo,* o da persona delegata.

Tale riassegnazione deve essere riportata all'interno del sistema gestionale informatico.

Per il trattamento dei dati sensibili si rinvia all'allegato n. 2

Art. 24
Modifica ed integrazione delle assegnazioni e delle riassegnazioni

In caso di assegnazione errata, la UOR che riceve il documento è tenuta a restituirlo alla Segreteria del Capo del Dipartimento- Protocollo entro una settimana lavorativa , tranne nel caso di comprovati impegni in attività emergenziali.

Le modifiche di assegnazioni comporteranno la registrazione della motivazione nel campo note della scheda di protocollo.

Nel caso di modifiche di assegnazioni relative a documenti informatici, le UOR si avvarranno esclusivamente del tab restituzioni presente nel sistema di gestione documentale; in caso di mancato funzionamento del tab, la UOR ne darà tempestiva comunicazione all'indirizzo email protocollo@protezionecivile.it.

In caso di assegnazioni interne agli Uffici, solo la UOR assegnante, su eventuale indicazione della UOR assegnataria, è deputata alla rettifica**.**

Il log di sistema storicizza le modifiche, registrando l'id utente, la data e l'ora di esecuzione.

SEZIONE VI
REGISTRAZIONE DEI DOCUMENTI

Art. 25
Unicità del protocollo informatico

Nell'ambito della AOO Dipartimento della Protezione Civile la numerazione delle registrazioni di protocollo è unica e rigidamente progressiva; si chiude al 31 dicembre di ogni anno.

Il numero di protocollo è costituito da almeno sette cifre numeriche.

Non sono previsti registri di protocollo di settore, né protocolli a fronte, ovverosia assegnazione di un unico numero di protocollo per documenti in entrata ed in uscita afferenti al medesimo procedimento.

Art. 26
Documenti classificati

I documenti classificati[28] non sono trattati nell'ambito del sistema di gestione documentale della AOO generale, ma su postazione dedicata stand alone e conservati, in conformità alla normativa vigente, dal punto NATO-UE/S[29].

Art. 27
Personale adibito alla registrazione di protocollo

La registrazione di protocollo in entrata è eseguita dagli operatori del Servizio di Segreteria del Capo del Dipartimento-Protocollo nell'orario diurno e nei giorni feriali, salvo quanto previsto nelle procedure di emergenza, di cui all'allegato n. 5, e dal Centro messaggi, nell'orario notturno e nei giorni prefestivi e festivi, limitatamente agli atti urgenti.

Fanno eccezione le fatture, la cui protocollazione è curata dal personale del Servizio delle politiche contrattuali, e i documenti classificati, registrati dal punto NATO-UE**.**

Le UOR sono tenute alla registrazione di protocollo dei documenti in uscita interna ed esterna.

I Responsabili unici del procedimento, i Direttori dei Lavori, i Direttori dell'esecuzione contrattuale, i componenti delle Commissioni di gara e dei gruppi di lavoro, sono tenuti a

[28] L. 3 agosto 2007, n. 124 recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto"

[29] DPCM 06/11/2015, n. 5/2015 recante "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva".

registrare le comunicazioni destinate alle UOR dipartimentali con protocollo interno e quelle destinate a soggetti esterni con protocollo in uscita.

Allo scopo saranno abilitati nel sistema informativo, previa comunicazione all'indirizzo email protocollo@protezionecivile.it

Art. 28

Prerequisiti per la registrazione di protocollo

Non si accettano documenti plurimi, afferenti a procedimenti diversi, inviati con un'unica spedizione e/o protocollo.

I documenti informatici in ingresso debbono presentare i seguenti prerequisiti per poter essere registrati al protocollo:

a) provenienza da una fonte certa (pec, e-mail istituzionale/ aziendale/ associativa).

Le comunicazioni ufficiali debbono pervenire da un indirizzo pec/email di AOO.

In caso di comunicazioni di cittadini, quelle pervenute via email, debbono riportare elementi di chiara identificazione, in assenza, verranno inoltrate all'URP dipartimentale per i seguiti di competenza.

b) assenza di macroistruzioni[30];

c) formato immodificabile; il concetto di immodificabilità è però dinamico. Il documento può essere reso immodificabile da elementi di corroborazione quali: la sottoscrizione digitale, la trasmissione via pec , la validazione temporale, la segnatura di protocollo informatico[31];

d) linguaggio e contenuti idonei alla funzione amministrativa;

e) firma vedi art. 10 del presente Manuale; nel caso di comunicazione proveniente da email istituzionale , il documento deve riportare, in assenza di firma digitale o qualificata, la firma elettronica o la firma omessa e la segnatura di protocollo .

f) riferimento temporale ;

g) dimensioni non superiori a 4,5 GB.

I documenti analogici in ingresso debbono presentare i seguenti prerequisiti per poter essere registrati al protocollo:

[30] art. 4, comma 3,.DPCM 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71."

[31] art. 4, DPCM 13 novembre 2013 recante " Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005"

a) provenienza da una fonte certa;

b) segnatura di protocollo informatico, se pervengono da pubbliche amministrazioni o aziende;

c) oggetto;

d) linguaggio e contenuti idonei alla funzione amministrativa;

e) firma.

I documenti informatici in uscita trasmessi via pec non potranno superare la dimensione massima di 100 MB.

Art. 29

Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo: le gazzette ufficiali, i bollettini ufficiali, la normativa, i notiziari della pubblica amministrazione, le note di ricezione di circolari, i materiali statistici, gli atti preparatori interni a carattere non ufficiale (ivi inclusi i preliminari di accordi), i giornali, le riviste, i libri, i materiali pubblicitari[32], gli inviti a manifestazioni informali, le conferme di protocollazione, le notifiche di eccezione, gli scambi di comunicazioni informali con soggetti esterni o interni al Dipartimento, pubblici e privati, gli appunti al Capo del Dipartimento, le richieste di spedizioni postali, i documenti in formati non ammessi.

Art. 29 bis

Atti endo-procedimentali, comunicazioni informali inter-istituzionali

Gli atti endo-procedimentali, le comunicazioni informali inter-istituzionali, vengono inoltrate alla UOR competente attraverso il sistema di messaggistica interno.

Art. 30

Modalità di registrazione a protocollo

Le operazioni di registrazione al protocollo avvengono in un'unica sessione, non si può, infatti, procedere all'integrazione dei dati per fasi successive; è esclusa ogni modifica degli elementi di segnatura di protocollo assegnati automaticamente dal sistema, quale numero e data di registrazione.

Sono modificabili parzialmente gli altri metadati, in caso di errore, con la

[32] Art. 53 , DPR 28 dicembre 2000, n. 45 recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"

memorizzazione del dato originale[33].

Art. 31

Metadati minimi della registrazione dei documenti ricevuti

Ciascuna registrazione di protocollo contiene i seguenti metadati obbligatori:

a) segnatura di protocollo, immodificabile;

b) mittente;

c) oggetto del documento oggetto del documento, registrato in forma estesa, modificabile solo per errori materiali;

d) tipologia documentale;

e) modalità di trasmissione;

f) classificazione;

g) l'impronta del documento informatico, immodificabile [34]

Art. 32

Metadati opzionali della registrazione di protocollo dei documenti ricevuti

I metadati opzionali di registrazione di protocollo, sono i seguenti:

a) data e numero di protocollo del documento in arrivo;

b) indicazione e sintetica descrizione degli allegati;

c) estremi del provvedimento di differimento dei termini di registrazione;

Art. 33

Metadati obbligatori della registrazione dei documenti spediti

Per ogni documento prodotto all'interno delle UOR e spedito all'interno e/o all'esterno della AOO è effettuata una corrispondente registrazione di protocollo, a carico del personale abilitato.

I metadati di riferimento al minimo sono:

a) segnatura di protocollo, immodificabile;

[33] art. 8, comma 2 del DPCM 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale

[34] art. 3, comma 9 del DPCM 13 novembre 2014 recante "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis , 23 -ter , 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

b) indicazione del mittente interno;

c) indicazione del destinatario, immodificabile;

d) oggetto del documento, registrato in forma estesa, modificabile solo per errori materiali;

e) classificazione;

f) tipologia documentale;

g) modalità di trasmissione;

h) impronta del documento informatico, immodificabile, calcolata automaticamente in base alle caratteristiche ed agli elementi di corroborazione del documento principale e degli allegati[35].

Art. 34

Elementi accessori della registrazione dei documenti spediti

I dati accessori di registrazione sono i seguenti:

a) indicazione e sintetica descrizione degli allegati.

Art. 35

Segnatura di protocollo dei documenti in entrata

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

Le informazioni minime apposte od associate al documento in ingresso mediante l'operazione di segnatura sono :

a) codice identificativo dell'amministrazione;

b) codice identificativo della AOO;

c) codice identificativo del registro di protocollo;

d) data di protocollo, inserita automaticamente dal sistema[36].

Art. 36

Segnatura di protocollo dei documenti in uscita

Le informazioni minime apposte od associate al documento in partenza mediante

[35] art. 9, DPCM 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale".

[36] art. 20, DPCM 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale"

l'operazione di segnatura sono :

a) progressivo di protocollo, inserito automaticamente dal sistema;
b) data di protocollo, inserita automaticamente dal sistema;
c) codice identificativo della AOO, inserito automaticamente dal sistema;
d) codice identificativo della UOR proponente e/o assegnataria, inserito dall'operatore;
e) voce di classificazione, inserita dall'operatore **.**

Art. 37

Segnatura xml dei documenti trasmessi in interoperabilità

I dati relativi alla segnatura di protocollo di un documento trasmesso in interoperabilità sono associati al documento stesso e contenuti, in un file XML, in cui oltre i metadati indicati nell'art. 36, afferiscono anche i seguenti[37]:

a) oggetto;
b) mittente;
c) destinatario.

Art. 38

Annullamento e modifiche delle registrazioni di protocollo

L'annullamento di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in formato immodificabile, quali la segnatura di protocollo, determina l'automatico annullamento dell'intera registrazione di protocollo[38].

Le registrazioni di protocollo debbono essere annullate esclusivamente dal Servizio di Segreteria del Capo Dipartimento, con una specifica funzione del sistema di gestione informatica dei documenti, entro massimo 36 ore lavorative.

Gli annullamenti sono possibili solo previa restituzione del documento analogico originale o inoltro di quello informatico al Servizio di Segreteria del Capo Dipartimento-Protocollo, riportante motivazione scritta a cura del dirigente della UOR interessata.

Le registrazioni annullate rimangono memorizzate nella base dati e sono evidenziate dal sistema con un simbolo.

Le modifiche da apportare agli altri metadati di registrazione immodificabili, non generati automaticamente dal sistema gestionale, giustificate da errori materiali, verranno

[37] art. 21, ibidem

[38] Art. 8, comma1, DPCM 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale"

eseguite esclusivamente dal personale del Servizio di Segreteria del Capo Dipartimento-Protocollo, entro le 24 ore lavorative dalla registrazione; tutte le operazioni saranno rese trasparenti attraverso il log di funzione del sistema gestionale.

Art. 39

Differimento dei termini di registrazione

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e, comunque, non oltre le ventiquattro ore lavorative dal ricevimento degli atti.

In deroga a quanto previsto dal precedente comma, il Responsabile della gestione documentale può autorizzare la posticipazione delle registrazioni.

Art. 40

Documenti ricevuti su supporti e/o modalità diversi

I documenti pervenuti su supporti e con mezzi di trasmissione diversi, sono registrati una sola volta con un unico numero di protocollo; nella scheda di registrazione originale viene successivamente riportata un'annotazione immodificabile che esplica la correlazione tra i due esemplari.

Art. 41

Documenti indirizzati nominativamente al personale della AOO

Non è ammesso il recapito della corrispondenza privata presso la struttura dipartimentale.

La posta cartacea indirizzata nominalmente al personale, priva di qualsiasi riferimento al Dipartimento e/o alla UO di appartenenza, o proveniente da autorità giudiziaria o legali, anche se pervenuta per raccomandata a/r, non viene registrata, ma inoltrata al destinatario interno, che è tenuto a farla pervenire di nuovo al Servizio di Segreteria del Capo del Dipartimento-Protocollo, qualora abbia carattere di ufficialità.

Le comunicazioni ufficiali destinate al Dipartimento, ma pervenute alla casella istituzionale del dipendente, dovranno essere inoltrate esclusivamente dal mittente originale alla pec dipartimentale.

Art. 42

Documenti anonimi e/o non sottoscritti

Le lettere anonime non sono registrate dal Servizio di segreteria del Capo del Dipartimento- Protocollo e vengono inoltrate alle UOR di competenza, per una valutazione sull'opportunità di dare seguito alla comunicazione.

I documenti di provenienza incerta e/o privi di sottoscrizione, non sono registrati; se

provengono da cittadini, vengono inoltrati all'URP per i seguiti di competenza.

Art. 43

Atti di competenza di altre amministrazioni o di altri soggetti

I documenti di competenza di un altro Ente, vengono direttamente inoltrati al corretto destinatario, al fine di non aggravare il procedimento amministrativo[39], con notifica di eccezione al mittente.

Nel caso in cui venga registrato un documento di altrui competenza, si procederà ad un'annotazione di annullamento della registrazione, con relativa motivazione.

Art. 44

Atti di competenza del Dipartimento privi di riferimenti formali

Gli atti inoltrati al Dipartimento, in assenza di un riferimento esplicito, vengono registrati qualora sia riscontrabile una competenza istituzionale, al fine di agevolare il procedimento amministrativo.

Art. 45

Istanze e richieste informali

Le istanze e richieste informali provenienti da persone fisiche e/o persone giuridiche private, vengono inoltrate direttamente all'indirizzo email dell'URP per i seguiti di competenza.

Le comunicazioni dei giornalisti sono assegnate all'Ufficio stampa.

Art. 46

Istanze, richieste del personale in servizio; permessi sindacali

Le istanze del personale in servizio indirizzate alla Presidenza del Consiglio dei Ministri e/o ad Istituzioni terze, da trasmettersi per il tramite dell'Ufficio Risorse umane e strumentali e servizi generali di funzionamento, debbono essere inoltrate a codesto Ufficio con lettera di trasmissione della UOR presso cui il dipendente è assegnato.

Le istanze del personale indirizzate a UOR dipartimentali vengono inviate all'indirizzo pec dipartimentale, tramite email istituzionale del dipendente; il documento deve essere sottoscritto dall'istante con la dicitura "firma omessa ai sensi dell'art. 3 del D.Lgs 12 febbraio

[39] art. 2 della Legge 2 agosto 1990, n. 241 recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

1993, n. 39 recante "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421" .

Le comunicazioni di permesso sindacale provenienti da componenti interni della RSU o da RLS vengono protocollate direttamente dai medesimi con protocollo interno e con firma omessa , ai sensi dell'art. 3 del D.Lgs 12 febbraio 1993 n. 39 recante "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421".

Le richieste di permesso sindacale provenienti dalle organizzazioni sindacali vengono trattate come dato sensibile , in conformità alla normativa vigente; si rinvia all'allegato 2.

Art. 47

Esposti , diffide, messe in mora nei confronti dell'Amministrazione

Gli esposti, le diffide, le messe in mora dell'Amministrazione provenienti dagli organi preposti e da studi legali vengono assegnati per competenza al Servizio del Contenzioso giuridico, con esclusione di quelli provenienti dai cittadini o da associazioni, che vengono assegnati all'URP dipartimentale.

Art. 48

Comunicazioni e notifiche dell'autorità giudiziaria

Le comunicazioni e le notifiche provenienti dall'autorità giudiziaria, in sede civile ed amministrativa, vengono accettate se recapitate via pec[40] o a mezzo ufficiale giudiziario.

Art. 49

Gestione dei dati personali, sensibili e giudiziari

I dati sensibili e giudiziari vengono gestiti dagli incaricati al trattamento in modalità cartacea e/o elettronica in conformità ai requisiti minimi di sicurezza richiesti dalla normativa vigente, come dettagliato nell'allegato 2[41].

[40] art. 16, comma 4, Decreto-Legge 18 ottobre 2012 n. 179 recante "Ulteriori misure urgenti per la crescita del Paese", come convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221.

[41] D.Lgs 30.06.2003 n. 196 recante "Codice in materia di protezione dei dati personali" art. 11 e ss.

Art. 50

Documenti inerenti a gare di appalto

Gli atti di gara su supporto analogico vengono gestiti secondo le seguenti modalità: all'atto della ricezione vengono scansionate le sole buste e registrati i relativi metadati su apposito registro informatico, richiamati successivamente nella scheda di protocollazione.

La Commissione interna, espletate le procedure di gara, provvede alla protocollazione dei verbali di gara; la registrazione delle sole copie informatiche delle offerte è a carico della Segreteria del Capo Dipartimento-Protocollo.

La documentazione inerente le gare telematiche, invece, viene inoltrata alla pec dipartimentale per la registrazione di protocollo dal funzionario delle politiche contrattuali, che ha istruito la procedura, in quanto la piattaforma MEPA non è interoperabile con il sistema di gestione documentale.

Art. 51

Contratti

I contratti in forma pubblica amministrativa sono redatti su supporto informatico, e sottoscritti elettronicamente con firme qualificate o avanzate, pena nullità dell'atto.

Qualora le parti contraenti non disponessero degli strumenti di firma elettronica, l'Ufficiale rogante sottoscriverà digitalmente l'attestazione della procedura adottata consistente nell'apposizione della firma autografa in sua presenza e della relativa scansione, previo accertamento dell'identità personale del contraente[42].

Art. 52

Avvisi meteo

Gli avvisi meteo, formati in modalità elettronica, con firma omessa del direttore dell'Ufficio, trasmessi per canali telematici, hanno valore di originale.

Art. 53

Registro giornaliero di protocollo

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

Per ogni documento incluso nel registro giornaliero di protocollo sono contemplati i

[42] art. 25, comma 2, del D.lgs. 7 marzo 2005, n. 82 recante il "Codice dell'Amministrazione digitale" e s.m.i.; art. 52 bis L. 3 agosto 1913, n. 89 recante "Ordinamento del notariato e degli archivi notarili" ; parere Funzione Pubblica_77/13/UL/P del 28/02/2013.

metadati obbligatori di seguito contemplati:

a) identificativo univoco del documento;
b) data di registrazione;
c) mittente/destinatario;
d) oggetto del documento ;
e)
f) impronta di hash di ogni documento;
g) codice identificativo del registro.

Oltre i metadati comuni a tutte le tipologie documentali, l'identificazione del produttore e del Responsabile della gestione documentale, sono da contemplare anche i metadati indicati dall'AGID come di stretta pertinenza del registro[43]:

h) soggetto produttore, denominazione del sistema informativo (S.I.Ge.D.®);
i) oggetto, descrizione della tipologia di registro;
j) codice identificativo del registro;
k) numero progressivo del registro;
l) anno;
m) numero della prima registrazione effettuata sul registro;
n) numero dell'ultima registrazione effettuata sul registro;
o) data della prima registrazione effettuata sul registro;
p) data dell'ultima registrazione effettuata sul registro.

Art. 54

Conservazione del Registro giornaliero di protocollo

Al fine di assicurare l'integrità e l'originalità dei dati contenuti nel registro di protocollo il sistema provvede, entro la giornata lavorativa successiva, ad effettuare le seguenti operazioni:

a) estrazione quotidiana delle registrazioni e conservazione in file PDF/ A;
b) apposizione di un riferimento temporale al file estratto;
c) invio del file e dei metadati al Conservatore esterno, previa supervisione del Responsabile della gestione documentale dei pacchetti di versamento[44].

Le attività di conservazione sono dettagliate nel relativo Manuale.

[43] http://www.agid.gov.it/notizie/2015/10/06/conservazione-pubblicate-istruzioni-il-registro-giornaliero-protocollo "Istruzioni per la produzione e conservazione del registro giornaliero di protocollo".
[44] Art. 7, comma 5, DPCM 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale"

Art. 55

Registro delle fatture

Le fatture elettroniche, dopo la validazione e la protocollazione da parte della UOR competente, vengono registrate con numero progressivo automatico nell'apposito repertorio.

Tutte le operazioni sono tracciate da log di sistema.

Art. 56

Registro delle raccomandate

Le raccomandate pervenute al Dipartimento vengono registrate in apposito repertorio con numerazione progressiva; tale registrazione è riportata nella scheda di protocollo in modo immodificabile.

Art. 57

Registro del contenzioso

In tale repertorio informatico vengono registrati gli adempimenti, le scadenze afferenti la documentazione acquisita/prodotta dal Servizio contenzioso.

Art. 58

Registro di emergenza e continuità operativa

Il Responsabile della gestione documentale autorizza lo svolgimento, anche manuale, di registrazione di protocollo su registri di emergenza, ogni qualvolta che, per cause tecniche, non sia possibile utilizzare il sistema informatico[45].

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora del ripristino della funzionalità del sistema.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana.

Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione.

Per ogni giornata è riportato sul registro di emergenza il numero totale di segnature di protocollo.

La sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive

[45] art. 63, D.P.R. 28 dicembre 2000, n. 445 recante il "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa".

interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.

Le informazioni concernenti i documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati.

Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

Il Dipartimento provvede alla predisposizione di un piano di emergenza, in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività, previo parere obbligatorio di AGID[46].

[46] art. 50 bis, D.Lgs 7 marzo 2005 n 82, recante il "Codice dell'Amministrazione Digitale" e s.m.i.

SEZIONE VII
CLASSIFICAZIONE DEI DOCUMENTI

Art. 59
Classificazione dei documenti

Tutti i documenti ricevuti e prodotti dagli Uffici della AOO, indipendentemente dal supporto sul quale vengono formati, debbono essere classificati in base al titolario unico della Presidenza del Consiglio dei Ministri di cui all'allegato 8.

L'indice di classificazione rappresenta concettualmente l'articolazione delle attività interne; il raccordo tra attività e documentazione facilita l'indicizzazione dei contenuti, con particolare riferimento ai documenti elettronici.

Il titolario viene aggiornato sulla base delle esigenze espresse dagli Uffici interni ed in accordo con la Presidenza del Consiglio dei Ministri.

SEZIONE VIII
FASCICOLAZIONE DEI DOCUMENTI

Art. 60
Identificazione dei fascicoli ed uffici abilitati alla loro formazione

Tutti i documenti classificati, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli elettronici.

La fascicolazione elettronica è obbligatoria, in quanto funzionale agli obiettivi di economicità e trasparenza richiesti dalla normativa vigente[47].

Per ogni fascicolo debbono essere registrate obbligatoriamente le seguenti informazioni:

a) amministrazione titolare;
b) amministrazioni partecipanti, in caso di conferenza di servizi;
c) Responsabile del procedimento;
d) voce del titolario di classificazione nell'ambito del quale il fascicolo si colloca;
e) numero del fascicolo, generato automaticamente dal sistema informatico;
f) oggetto del fascicolo;
g) anno di apertura e chiusura;
h) servizio a cui è assegnata la relativa pratica;
i) livello di riservatezza, se diverso da quello standard applicato da sistema.

Nel fascicolo è possibile inserire anche materiale non protocollato e creare collegamenti con altri fascicoli.

Gli utenti a prescindere dal ruolo sono abilitati alla creazione e/o implementazione di fascicoli elettronici.

I fascicoli debbono essere creati, tenendo conto delle linee di attività individuate nel titolario, dalla UOR assegnataria per competenza, che si periterà di estenderne la visibilità ad altre UOR coinvolte nel procedimento.

Art. 61
Processo di formazione dei fascicoli elettronici

Il funzionario delegato al procedimento amministrativo stabilisce se il documento è da collocare nell'ambito di un procedimento in corso o se dare avvio ad una nuova pratica.

Qualora il documento si riferisca ad un procedimento in corso, per il quale si è già provveduto a fascicolazione, il funzionario deve:

a) selezionare il relativo fascicolo;

[47] art.41, D.Lgs 7 marzo 2005, n. 82 recante il "Codice dell'Amministrazione digitale" e s.m.i..

b) collegare la registrazione di protocollo del documento al fascicolo selezionato.

Qualora si tratti di un nuovo procedimento amministrativo, il funzionario deve:

a) eseguire l'operazione di apertura del fascicolo;

b) collegare la registrazione di protocollo del documento al fascicolo aperto.

Nel fascicolo debbono essere inseriti tutti documenti relativi al procedimento di cui il Dipartimento è titolare, inclusi gli atti endo-procedimentali, le ricevute di consegna dei documenti spediti attraverso la posta elettronica certificata.

Art. 62

Condivisione dei fascicoli

Il funzionario delegato al procedimento amministrativo stabilisce, con la supervisione del *Responsabile del procedimento amministrativo,* quali fascicoli condividere o dare in visibilità ad altre UOR.

SEZIONE IX
SPEDIZIONI

Art. 63
Verifica e monitoraggio delle spedizioni telematiche

Le UOR che provvedono alla spedizione per canale telematico (pec, pei, fax server), sono tenute ad avvalersi esclusivamente dell'anagrafica S.I.Ge.D.® nella compilazione del campo destinatario.

Nel caso in cui il destinatario non fosse presente nell'anagrafica, il personale della UOR mittente provvederà a creare la relativa scheda, che verrà tempestivamente approvata dalla Segreteria del Capo Dipartimento-Protocollo.

Il monitoraggio delle spedizioni e la conservazione della certificazione nel fascicolo elettronico sono di competenza del funzionario della UOR mittente, che dovrà avvalersi del tab spedizioni per accedere ad una lista riepilogativa degli esiti.

In caso di mancata consegna, il funzionario dovrà ricorrere a misure correttive o a segnalazioni di disservizio al Responsabile della gestione documentale, che si attiverà.

Le spedizioni dirette a cittadini che hanno comunicato il proprio domicilio digitale dovranno avvenire in modalità elettronica.

Art. 64
Spedizioni massive

Il modulo spedizione massive implementato nel sistema informativo consente l'inoltro contestuale ad un numero illimitato di destinatari, raggruppati con criteri diversificati, in conformità alle esigenze della UOR interessata.

Il modulo consente di spedire le note attraverso canali di spedizione eterogenei e di verificare in tempo reale la presenza di errori nella scheda anagrafica e/o nella trasmissione dei dati.

Art. 65
Spedizione ad altri Enti e /o soggetti di documenti cartacei

La spedizione analogica è da intendersi residuale e riguarderà gli originali unici cartacei e/o i destinatari privi di domicilio digitale; i documenti da spedire su supporto cartaceo sono trasmessi all'esterno tramite il Servizio di Segreteria del Capo del Dipartimento- Protocollo, solo previa richiesta scritta e motivata della UOR.

I documenti prima della spedizione debbono essere affrancati dalla UOR mittente.

SEZIONE X
ARCHIVIAZIONE DEI DOCUMENTI

Art. 66
Archiviazione dei documenti elettronici

Le procedure afferenti al versamento, all'archiviazione e distribuzione dei pacchetti informativi digitali, viene trattato nel Manuale di conservazione in conformità alla normativa vigente.

Il Responsabile della gestione documentale deve supervisionare l'invio in conservazione dei pacchetti di versamento alle scadenze concordate con il Conservatore esterno.

I pacchetti vengono prodotti tramite l'applicativo SIGED ed inoltrati via ftp al Servizio di conservazione.

Art. 67
Versamento dei documenti analogici nell'archivio di deposito

All'inizio di ogni anno, il *Responsabile del procedimento amministrativo,* con il supporto del referente della gestione documentale dell'Ufficio, individua i fascicoli da versare nell'archivio di deposito, in base al Piano di conservazione.

In ogni caso è escluso il trasferimento per i fascicoli che, a far data dal 1 gennaio 2011, non abbiano un corrispettivo informatico e che siano stati formati nel periodo successivo al quinquennio di riferimento.

Il trasferimento deve essere effettuato rispettando l'organizzazione dei fascicoli e delle serie dell'archivio corrente, previo accurato scarto di duplicati e documentazione personale (attestati di servizio, curricula), avvalendosi di apposita procedura elettronica presente nell'Intranet dipartimentale.

Ogni *Responsabile del procedimento amministrativo* cura la formazione e la conservazione di un elenco delle serie trasferite nell'archivio di deposito, la cui congruità è verificata dal Responsabile della gestione documentale.

In caso di mancata congruità, il *Responsabile del procedimento amministrativo* è tenuto a rilasciare apposita dichiarazione di lacunosità della serie e/o del fascicolo.

Art. 68

Scarto in itinere

Gli Uffici sono tenuti, prima del versamento degli atti di archivio, a procedere allo scarto di copie di lavoro, duplicati di atti amministrativi detenuti da altri uffici (tabulati di presenze, straordinari, missioni) e di documenti non archiviabili (gazzette ufficiali, brochure, raccolte di leggi, documenti personali, pratiche inevase, minute, opuscoli, libri).

Art. 69

Selezione e scarto delle serie archivistiche

Le procedure di scarto e versamento sono effettuate secondo le modalità indicate nella normativa vigente, sulla base del piano di conservazione riportato nell'allegato 8. [48]

Il Responsabile della gestione documentale ogni anno solare individua le serie archivistiche da proporre per lo scarto alla Commissione di sorveglianza.

Nel caso di documentazione tecnica, il Responsabile si avvale del supporto degli Uffici interessati.

La proposta di scarto viene vagliata dalla Commissione, che, all'unanimità, richiede il nulla osta alla Direzione generale degli archivi del Ministero dei Beni e delle attività culturali e del Turismo[49].

La presenza di dati personali, sensibili, giudiziari è evidenziata nella documentazione allegata alla proposta.

In caso di parere favorevole dell'autorità di vigilanza, il Dipartimento procede all'individuazione della ditta specializzata per la distruzione della documentazione; a smaltimento avvenuto, l'azienda rilascia un'attestazione dell'operazione, che viene notificata alla Direzione generale degli archivi del Ministero dei Beni e delle Attività culturali e del Turismo.

[48] DPR 8 gennaio 2001, n. 37 recante il "Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato"; DPCM 12 febbraio 2010 recante "La disciplina del funzionamento dell'Archivio e l'accesso alla documentazione per scopi di ricerca"

[49] D.L.gs 22 gennaio 2004, n. 42 recante "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137"

SEZIONE XI

ACCESSO AI DOCUMENTI

PREMESSA

L'accesso ai documenti e alle serie archivistiche è conforme alla disciplina di settore[50] , tenuto conto della tutela della riservatezza e del principio di ponderazione[51].

Le richieste concernenti dati personali, sensibili e giudiziari dovranno essere preventivamente vagliate ed autorizzate dal Titolare del trattamento dei dati. L'autorizzazione o diniego del diritto di accesso è di competenza del Capo del Dipartimento, previa istruttoria del Servizio del Contenzioso.

Art. 70

Accesso alle serie archivistiche informatiche

L'accesso ai documenti informatici è garantito dal sistema, attraverso dispositivi di autenticazione sicura; tale tipo di accesso diretto è garantito all'utenza interna.

Gli utenti interni accedono all'archivio elettronico corrente, in base alle abilitazioni predeterminate dalla UOR di appartenenza.

Le richieste afferenti documentazione contenente dati personali, sensibili e giudiziari dovranno essere preventivamente vagliate ed autorizzate dal Titolare del trattamento dei dati, ovverosia dal capo del Dipartimento.

In tali fattispecie, l'accesso degli utenti interni ai documenti e/o ai fascicoli è più selettivo, dal momento che viene adottato all'atto della registrazione di protocollo un livello di riservatezza diverso da quello standard.

Il livello di riservatezza applicato ad un fascicolo è ereditato automaticamente da tutti i documenti che vi confluiscono.

I livelli di riservatezza e le abilitazioni degli utenti interni, gestiti da sistema, sono riportati nell'allegato 1.

L'utenza esterna può ricevere estrazione e/o duplicato via email dalla UOR che detiene o ha prodotto il documento ed avere informazioni sul nominativo del Responsabile del procedimento.

---

[50] Art. 24 Legge72 agosto 1990, recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e s.m.i.

[51] Art. 60, D.Lgs 30 giugno 2003, n. 196 recante il " Codice in materia di protezione dei dati personali"

Art. 71

Modalità di accesso e di consultazione delle serie archivistiche cartacee

L'accesso agli atti da parte dell'utenza esterna autorizzata può avvenire mediante consultazione in loco o invio di copia scansionata via email.

La consultazione degli atti analogici da parte dell'utenza interna avviene previa richiesta all'indirizzo email archivio@protezionecivile.it.

In entrambe le fattispecie la consultazione sarà ammessa previa verifica delle condizioni materiali della documentazione richiesta.

Qualora ricorrano le condizioni materiali per la consultazione, il personale preposto deve inserire, al posto dell'originale, un cartoncino sul quale verranno trascritti i dati del consultatore (ufficio, funzionario, durata prevista della consultazione).

Art. 72

Consegna e verifica del materiale consultato

I documenti consultati, all'atto della consegna, vengono prima esaminati dal personale preposto per verificarne gli eventuali danneggiamenti, poi scaricati dal registro delle consultazioni e ricollocati in archivio.

Qualora, al momento della riconsegna, il personale dell'archivio rilevi anomalie o danneggiamenti della documentazione consultata, notificherà verbalmente tali evenienze.

Il Responsabile della gestione documentale, valutata la situazione e verificato lo stato del materiale, procederà, di concerto con il responsabile della UOR interessata, ad avviare le iniziative del caso.

SEZIONE XII
NORME FINALI

Art. 73
Approvazione ed aggiornamento del Manuale di gestione

Il presente Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi è approvato con decreto del Capo del Dipartimento.

ALLEGATO N. 1

PIANO DI SICUREZZA INFORMATICA RELATIVO ALLA FORMAZIONE, GESTIONE, TRASMISSIONE, INTERSCAMBIO, ACCESSO E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Obiettivi

Le misure di sicurezza garantiscono che:

a) le informazioni e i dati siano disponibili, integri e protetti;

b) gli oggetti digitali e le aggregazioni informatiche (fascicoli) siano archiviati in modo da ridurre al minimo i rischi di distruzione o perdita anche accidentale, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta e della gestione, con particolare riguardo ai dati sensibili e giudiziari.

Il piano di sicurezza definisce:

a) le politiche generali e particolari di sicurezza da adottare dalla AOO;
b) le modalità di accesso al Sistema di gestione informatica dei documenti;
c) gli aspetti operativi della sicurezza, con particolare riferimento alle misure minime di sicurezza, di cui al Disciplinare tecnico richiamato nell'allegato B) del D.lgs. 196/2003 Codice in materia di protezione dei dati personali;
d) i piani specifici di formazione degli addetti;
e) le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Componente organizzativa della sicurezza

Le figure professionali individuate per la sicurezza sono:

Responsabile della gestione documentale;

Responsabile dei sistemi informativi;

Responsabile del sistema di conservazione;

Responsabile del Servizio di conservazione (SIAV);

Responsabile della sicurezza.

Componente fisica della sicurezza

Il controllo degli accessi fisici alle risorse della sede del CED è regolato secondo i seguenti principi:

● l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;

● i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti devono esplicare la procedura di registrazione stabilita per l'accesso alle sedi disponibile sulla intranet dipartimentale all'indirizzo:

http://intranet.protezionecivile.it/sicurezza/documenti/Procedura_ingresso_lavoratori_ditte_esterne.pdf

Non possono entrare e trattenersi nelle aree protette se non accompagnati da personale dell'erogatore del servizio autorizzato a quel livello di protezione;

● ogni persona che accede alle risorse della sede in locali protetti è identificata in modo certo con sistemi di autenticazione forte;

● gli accessi alla sede sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;

● il personale della sede ha l'obbligo di utilizzare il *badge* sia in ingresso che in uscita dalla sede stessa.

Le misure di sicurezza fisica hanno un'architettura multilivello così articolata:

● a livello di edificio, attengono alla sicurezza perimetrale e sono atte a controllare l'accesso alla sede in cui sono ospitate risorse umane e strumentali;

● a livello di locali CED, sono finalizzate a controllare l'accesso ai locali interni alla sede.

Il controllo degli accessi fisici alle risorse della sede dell'amministrazione/AOO è regolato secondo i principi stabiliti dall'Ufficio - Risorse umane e strumentali - servizio gestione affari generali di funzionamento

Componente logica

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, è stata realizzata attraverso:

● l'attivazione dei seguenti servizi di sicurezza in grado di mitigare i rischi derivanti dalle minacce sulle vulnerabilità del sistema informatico:

• identificazione, autenticazione ed autorizzazione degli addetti della AOO e degli operatori dell'erogatore del Sistema informatico di gestione dei documenti;

• riservatezza dei dati;

- integrità dei dati;
- integrità del flusso dei messaggi;
- non ripudio dell'origine (da parte del mittente);
- non ripudio della ricezione (da parte del destinatario);
- audit di sicurezza;
- la ridondanza dei sistemi di esercizio: Cluster SiGeD (sede di via Vitorchiano) e replica SiGeD – CED secondario (sede di via Ulpiano)

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata un'infrastruttura tecnologica di sicurezza con un'architettura "a strati multipli di sicurezza" conforme alle *best practices* correnti.

L'architettura realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione degli addetti della AOO e degli operatori dell'erogatore del Sistema informatico di gestione dei documenti, con le seguenti caratteristiche:

- *login server* per la gestione dei diritti di accesso ai servizi applicativi: Operatori della Soc. Joint o del gestore dei sistemi informatici (HPE/Open System/Eustema/Infordata) (Active Directory), Amministratori e Addetti SiGeD dell'AOO.
- unico sistema di repository delle credenziali di accesso degli utenti;
- unico database delle anagrafiche contenente tutti i profili di utenza.

Componente infrastrutturale

Presso le sedi del Dipartimento sono disponibili i seguenti impianti:

- antincendio;
- rilevazione dell'allagamento;
- luci di emergenza;
- continuità elettrica;
- controllo degli accessi e dei varchi fisici.

Il CED, lontano da insediamenti industriali e posto all'interno di un edificio adibito ad uffici, non risulta un ambiente esposto a particolare rischio biologico, chimico, elettromagnetico e , pertanto, richiede le misure di prevenzione ordinarie.

Misure generali di sicurezza per la gestione documentale

Le misure generali tecniche e organizzative inerenti alla gestione documentale, adottate in riferimento allo standard ISO/IEC 27001/2013, sono:

a) protezione dei sistemi di accesso, gestione e conservazione dei file di log di sistema contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata. e conservazione delle informazioni (log di sistema).

La tracciatura degli eventi nel sistema di gestione documentale S.I.Ge.D.® si basa sul sistema di logging della piattaforma IBM® Domino e su strumenti personalizzati integrati nelle procedure applicative;

b) assegnazione ad ogni utente del sistema di una credenziale riservata di autenticazione (password) e di un profilo di accesso;

c) cambio delle password con frequenza periodica semestrale durante la fase di esercizio;

d) gestione delle copie di back-up dei dati e dei documenti con le seguenti schedulazioni:

- backup dei dati effettuato giornalmente, con inizio alle ore 02.00 am;
- conservazione per 60 gg. delle copie di backup;
- export dei dati su DVD, effettuato annualmente dalla Joint società fornitrice dell'applicativo SIGED;

e) ripristino applicativo del sistema informatico; viene effettuato restore su database in ambiente di test ogni 12 mesi a cura di Joint, società fornitrice dell'applicativo SIGED;

f) gestione delle situazioni di emergenza da parte di un gruppo di risorse interne qualificate (Responsabile della gestione documentale, referenti informatici);

g) cifratura degli oggetti documentali allo scopo di renderli inintelligibili anche a chi è autorizzato ad accedervi per le attività di manutenzione.

Log operativi e registrazioni di sicurezza

Di seguito vengono elencati i principali log operativi e le principali registrazioni di sicurezza eseguite dal modulo S.I.Ge.D.® "Protocollo Informatico".

ATTIVITA' INFORMAZIONI REGISTRATE

- Gestione registrazione scheda di protocollo
- Creazione numero di protocollo (log obbligatorio) Data e ora, nome utente operazione, numero di protocollo
- Registrazione dei metadati (log opzionale) Data e ora, nome utente operazione, nome corrispondente, oggetto, tipologia documento, tipologia trasmissione, classificazione
- Acquisizione nuovo documento Data e ora, nome utente operazione

- Cancellazione documento Data e ora, nome utente operazione, documento rimosso(operazione consentita solo agli utenti abilitati e solo fintantoché il documento non viene reso persistente)
- Modifica metadati- Annullo parziale Data e ora, nome utente, valore precedente (operazione consentita solo agli utenti abilitati)
- Annullo di un protocollo Data e ora, nome utente operazione, motivazione (operazione consentita solo agli utenti abilitati) su disposizione del Responsabile della gestione documentale
- Modifiche da amministratore Data e ora, nome utente operazione, valori precedenti
- Gestione flusso documentale
- Trasmissione ad una UOR Data e ora, nome utente che ha effettuato la trasmissione, UOR assegnataria, numero di protocollo
- Presa visione da parte di una UOR per conoscenza Data e ora, nome utente operazione, UOR assegnataria, numero di protocollo
- Accettazione da parte di una UOR per competenza Data e ora, nome utente operazione, UOR assegnataria, numero di protocollo;
- Assegnazione interna Data, nome utente operazione, numero protocollo, nome utente assegnatario;
- Annullamento assegnazione;
- (log opzionale) Data e ora, nome utente operazione, UOR assegnataria, numero di protocollo;
- Richiesta spedizione tramite PEC \ Fax-server \ email\ Data e ora, nome utente operazione, numero protocollo;
- Spedizione tramite PEC \ Fax-server \ email\ Data e ora, nome utente operazione, elenco dei documenti spediti
- Consultazione
- Ricerca strutturata, per numero, per impronta file informatico
- (log opzionale) Data e ora, nome utente operazione, criteri di ricerca impostati
- Apertura scheda di protocollo
- (log opzionale) Data e ora, nome utente operazione, numero di protocollo
- Visualizzazione documento principale
- (log opzionale in caso di documenti non sottoposti a restrizioni di visibilità) Data e ora, nome utente operazione, numero di protocollo

- Gestione dati sensibili
- Attivazione gestione dati sensibili Data e ora, nome utente dell'operazione
- Estensione visibilità Data e ora, nome utente operazione, utenti a cui si è estesa la visibilità
- Rimozione di visibilità Data e ora, nome utente operazione, utenti a cui è state revocata la visibilità
- Invio email Data e ora, nome utente operazione, indirizzi email a cui è stato inoltrato l'alert.
- Stampa documenti Data e ora, nome utente dell'operazione
- Apertura documenti Data e ora, nome utente dell'operazione
- Richiesta di invio ad archivio Data e ora, nome utente operazione, motivazione di archiviazione
- Richiesta di recupero da archivio Data e ora, nome utente operazione, motivazione di de-archiviazione
- Invio ad archivio Data e ora operazione, nome utente operazione, elenco documenti archiviati
- Recupero da archivio Data e ora operazione, e nome utente operazione, elenco documenti de-archiviati

Formazione dei documenti

Formati

Il Dipartimento adotta formati che possiedono requisiti di leggibilità, interscambiabilità, non alterabilità durante le fasi di accesso e conservazione, immutabilità nel tempo del contenuto e della struttura.

I documenti informatici redatti all'interno dell'AOO dipartimentale con prodotti di text editor sono convertiti, prima della loro sottoscrizione e registrazione, nel formato standard (PDF/A) al fine di garantirne la non alterabilità durante le fasi successive di accesso, di conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

I documenti ricevuti per interoperabilità possono avere i seguenti formati (come da allegato 2 al DPCM 3.11.2014 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici"):

Documenti /testo : PDF, PDF/A, CSV, DOC , DOCX, TXT, XLSX, PPTX, XML, ODP, ODS, ODT.

Immagini : JPG, TIF.

I formati testuali sono ammessi solo in presenza di elementi di corroborazione alternativi tra di loro (fonte di provenienza sicura, sottoscrizione, validazione temporale, segnatura di protocollo); sono comunque esclusi quelli contenenti macroistruzioni.

Sottoscrizione

I documenti vengono sottoscritti con firma digitale, per la cui generazione e verifica è utilizzata la funzione SHA-256; in alternativa con la firma omessa oppure con la firma elettronica qualificata.

Datazione

Gli elementi di validazione temporale sono: la datazione della segnatura di protocollo, la data di invio/ricezione della PEC, la marca temporale.

Gestione dei documenti in SIGED

La piattaforma di gestione documentale in dotazione alla AOO è conforme alle specifiche di sicurezza previste dalla normativa vigente.

In particolare consente:

● l'accesso esclusivo al server dedicato alla gestione documentale agli utenti autorizzati.

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

Le regole per la composizione delle password e il blocco delle utenze valgono sia per l'amministratore che per gli utenti della AOO.

Le relative politiche di composizione, aggiornamento e, in generale, di sicurezza, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo (vedi circolare RUS/6628 del 8.02.16 relativa al cambio di password e policy);

● il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;

● il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore;

- il collegamento tra i documenti ricevuti e quelli adottati a riscontro;
- il recupero delle informazioni nella loro integrità;
- la relazione logica dei documenti e delle loro aggregazioni attraverso la struttura gerarchico-enumerativa del titolario.

Ruoli degli utenti SIGED

Ogni utente ha uno o più ruoli all'interno della struttura organizzativa SIGED.

Ad ogni ruolo corrispondono abilitazioni diverse.

L'Amministratore di sistema è una figura di supervisore che ha le seguenti abilitazioni:

a) creazione id utente su piattaforma IBM Domino;
b) implementazione/modifica struttura organizzativa di ogni AOO;
c) accesso ai log di sistema;
d) gestione delle tabelle (oggetto codificato, titolario, tipologia dati, spedizione);
e) annullamento/modifica parziale dei dati in caso di errore materiale**.**

Il **Responsabile UOR** corrisponde funzionalmente al Dirigente di Ufficio o Servizio .

L'utente che riveste tale ruolo accetta e riassegna le comunicazioni di competenza della UOR;

Il **Facente funzione** è il sostituto o vicario del Responsabile;

La **Segreteria** è il ruolo di supporto al Responsabile. L'utente con tale ruolo accetta e riassegna le comunicazioni di competenza della UOR;

Il **Componente** è l'assegnatario ultimo della comunicazione.

Le abilitazioni per ogni ruolo sono:

a) *consultazione*, ovverosia la visualizzazione dei documenti;

b) *inserimento*, ovverosia l'abilitazione ad inserire le registrazioni di protocollo, le registrazioni nei repertori e registri;

c) *modifica*, ovverosia l'abilitazione a modificare i dati gestionali in caso di errore, in conformità alla normativa vigente. L'abilitazione è ristretta al solo personale del Servizio di Segreteria del Capo del Dipartimento.

d) *annullamento*, ovverosia l'abilitazione ad annullare la registrazione di protocollo, mantenendone la visibilità, ma non la validità ai fini giuridici; funzione riservata al solo personale del Servizio di Segreteria del Capo del Dipartimento, sotto il controllo del Responsabile della gestione documentale.

I livelli di visibilità nel sistema sono:

a) *livello pubblico*: la scheda di protocollo ed il documento sono visibili a tutti gli utenti interni abilitati alla consultazione;

b) *livello ristretto* : la scheda di protocollo ed il documento sono visibili ai componenti delle UOR assegnatarie, in base ai profili assegnati;

c) *livello riservato:* la scheda di protocollo è visibile al personale autorizzato, mentre il documento solo a coloro tra gli autorizzati ai quali il Responsabile abbia esteso la visibilità;

d) *livello riservato/dati sensibili* : la scheda di protocollo ed il documento sono visibili agli incaricati del trattamento dei dati personali, sensibili e giudiziari ai quali sia stata estesa la visibilità da parte del Responsabile ed al protocollatore estensore.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una Access Control List (ACL), che consente di stabilire quali utenti, o gruppi di utenti, vi abbiano accesso (sistema di autorizzazione o profilazione utenza).

I documenti non vengono visualizzati dagli utenti privi di diritti di accesso.

Impronte dei documenti

Per la generazione delle impronte dei documenti informatici, il sistema utilizza la funzione di HASH.

Modifica o annullamento delle registrazioni di protocollo

Solo il Responsabile della gestione documentale può autorizzare l'annullamento del numero di protocollo; l'annullamento è segnalato dal sistema ed è integrato dalla motivazione.

Accessibilità e leggibilità dei documenti

Le basi di dati afferenti alla AOO Dipartimento della Protezione civile sono accessibili agli utenti profilati, dall'aprile 2002 fino all'anno corrente, come quelle afferenti ad AOO emergenziali chiuse.

Il livello di autorizzazione all'utilizzo del sistema di gestione informatica dei documenti è attribuito dal Responsabile della gestione documentale su indicazione delle UOR; il controllo degli accessi ai dati di protocollo e alla base documentale da parte del personale dell'amministrazione è assicurato utilizzando user id e password assegnata ad ogni utente.

Interscambio dei documenti informatici

La trasmissione dei documenti informatici avviene quasi esclusivamente attraverso il servizio di posta elettronica certificata, in conformità agli standard della rete nazionale delle pubbliche amministrazioni.

Il servizio di posta certificata di cui si avvale la Presidenza del Consiglio dei Ministri è fornito dal provider TELECOMPOST in virtù di una convenzione Consip.

Il provider assicura:

a) l'autenticità della provenienza, con verifiche nell'indice dei gestori di PEC;

b) l'integrità del messaggio attraverso la certificazione contente il messaggio originale;

c) la riservatezza del messaggio attraverso il tracciamento delle attività nel file di log della posta e la gestione automatica delle ricevute di consegna.

L'interscambio con la Presidenza del Consiglio dei Ministri- Ufficio del bilancio e per il riscontro di regolarità amministrativo-contabile è assicurato attraverso Web service.

Conservazione del Registro giornaliero di protocollo

Il Dipartimento ha sottoscritto un contratto di servizio con il conservatore accreditato, SIAV. Le procedure di conservazione sono analiticamente descritte nel Manuale di conservazione.

L'applicativo gestionale produce automaticamente il registro di protocollo in PDF che viene trasferito al conservatore via ftp entro le 24 ore lavorative dalla registrazione attraverso dei pacchetti di versamento conformi allo standard OAIS.

Conservazione delle registrazioni di sicurezza

Le registrazioni di sicurezza sono informazioni da conservarsi per motivi strettamente legali e/o operativi, quali:

●log dei dispositivi di protezione periferica del sistema informatico (intrusion detection system-IDS, sensori di rete e firewall),

●log di sistema SiGeD relativi agli accessi, alle operazioni di modifica e di annullamento.

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:

●l'accesso è limitato, esclusivamente, ai sistemisti;

●le registrazioni del SiGeD sono elaborate tramite procedure automatiche dal sistema di autenticazione e di autorizzazione;

●i log di sistema sono accessibili ai sistemisti in sola lettura al fine di impedirne la modifica;

●le registrazioni sono soggette a copia giornaliera su disco.

Registro di emergenza

L'erogatore del Sistema di gestione informatica dei documenti assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica *realtime*, le operazioni di protocollo siano svolte sul registro di emergenza informatico su postazioni di lavoro operanti fuori linea.

Una postazione, stand-alone, è situata presso il Centro messaggi del Dipartimento; l'altra è in dotazione al Responsabile della gestione documentale..

L'aggiornamento e il monitoraggio delle funzionalità dell'applicativo SIGED sono a cura della JOINT, con cadenza semestrale; il monitoraggio del funzionamento del sistema operativo è a cura del Servizio informatico.

In condizioni di emergenza si applicano le modalità di registrazione e di recupero dei dati, di seguito riportate:

a) sul registro di emergenza sono riportate la causa, la data e l'ora d'inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;

b) per ogni giornata è riportato sul registro di emergenza il numero totale di operazioni registrate;

c) la sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive interruzioni, garantisce l'identificazione univoca dei documenti registrati;

d) al ripristino delle funzionalità ordinarie di gestione documentale, la segnatura di protocollo assegnata al documento in fase di emergenza viene associata ad una nuova .

Politiche di sicurezza adottate dalla AOO

Le politiche di sicurezza stabiliscono le misure di prevenzione e di mitigazione dei rischi di distruzione, manipolazione, alterazione dei dati, nonché il monitoraggio e l'analisi degli incidenti informatici.

L'aggiornamento delle politiche di sicurezza è pianificato in conformità all'evoluzione tecno-normativa, all'analisi dei risultati dell'attività di audit, alle necessità specifiche manifestate dal Responsabile della sicurezza, Responsabile dei sistemi informativi , dal Responsabile della gestione documentale.

È compito del responsabile della sicurezza procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza, in accordo o su indicazioni del Capo del Dipartimento.

In ogni caso, tale attività è svolta almeno con cadenza annuale.

ALLEGATO N. 2

GESTIONE DEI DATI SENSIBILI /GIUDIZIARI e RISERVATI

La gestione dei dati sensibili e giudiziari è conforme alle prescrizioni della normativa di settore, che prevede la gestione informatica o analogica[52].

tipi di dati trattati:

a) convinzioni: religiose, filosofiche, d'altro genere

b) convinzioni: politiche, sindacali

c) stato di salute: patologie attuali, patologie pregresse, terapie in corso, anamnesi familiare

d) vita sessuale (solo in caso di rettifica di attribuzione di sesso)

e) dati di carattere giudiziario : provvedimenti giudiziari penali iscrivibili nel casellario giudiziale, sanzioni amministrative dipendenti da reato, illeciti amministrativi, la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Gli **ambiti di trattamento** riportati nelle fonti normative della Presidenza del Consiglio dei Ministri, per quanto di specifico interesse del Dipartimento, concernono[53]:

a) costituzione e gestione del rapporto di lavoro subordinato e non subordinato, ivi compresi gli aspetti relativi alla tutela della salute e della sicurezza nei luoghi di lavoro;

b) gestione delle nomine di vertice;

c) concessione revoca benefici, patronati, patrocini, benemerenze;

d) funzioni di controllo e ispettive; denunce e segnalazioni provenienti da amministrazioni, pubblici dipendenti e privati cittadini; acquisizione di dati giudiziari, al fine di verificare i requisiti richiesti per le associazioni di volontariato di protezione civile

[52] D.Lgs 30 giugno 2003 n. 196 recante il "Codice in materia di protezione dei dati personali"; DPCM 30 novembre 2006, n. 312 recante "Regolamento concernente il trattamento dei dati sensibili e giudiziari presso la Presidenza del Consiglio dei Ministri"; DPCM 31 marzo 2009, n. 49 recante "Regolamento di integrazione al decreto del Presidente del Consiglio dei Ministri 30 novembre 2006, n. 312, concernente il trattamento dei dati sensibili e giudiziari presso la Presidenza del Consiglio dei Ministri".

[53] Le casistiche richiamate sono riportate negli allegati al DPCM 30 novembre 2006, n. 312 recante "Regolamento concernente il trattamento dei dati sensibili e giudiziari presso la Presidenza del Consiglio dei Ministri"; DPCM 31 marzo 2009, n. 49 recante "Regolamento di integrazione al decreto del Presidente del Consiglio dei Ministri 30 novembre 2006, n. 312, concernente il trattamento dei dati sensibili e giudiziari presso la Presidenza del Consiglio dei Ministri".

coinvolte nell'attività di previsione, prevenzione e soccorso in vista o in occasione di eventi calamitosi;

e) gestione delle liste di mobilità ;

f) atti di organizzazione e gestione dei volontari del servizio civile;

g) dati giudiziari; gestione del contenzioso giudiziale e stragiudiziale, anche presso le Corti sopranazionali; attività rivolta alla tutela degli interessi dell'amministrazione in sede amministrativa, nonché in sede stragiudiziale; costituzione di parte civile in procedimenti penali; risarcimento danni; procedure esecutive; accertamento della responsabilità' personale e disciplinare; erogazione degli indennizzi per violazione del termine ragionevole del processo;

h) distacchi e permessi sindacali provenienti dalle OO.SS.;

i) atti di sindacato ispettivo degli organi parlamentari;

j) verbali di commissioni, comitati e altri organi istituiti;

k) accesso agli atti e dati inerenti l'attuazione del principio della piena conoscibilità e trasparenza della pubblica amministrazione ai sensi della Legge 2 agosto 1990, n. 241 in materia di procedimento amministrativo;

l) atti relative a irregolarità e frodi comunitarie.

Gestione dei dati sensibili e giudiziari.

Premessa

La gestione dei dati sensibili e giudiziari prevede prioritariamente la nomina formale degli incaricati al trattamento da parte del Titolare del trattamento, sia appartenenti alle qualifiche che ai ruoli dirigenziali.

Gli incaricati dovranno attenersi scrupolosamente ai principi di pertinenza e di necessità nel trattamento della documentazione.

Nella fase di ricezione gli incaricati presso il Servizio di Segreteria del Capo Dipartimento- Protocollo dovranno verificare la legittimità al trattamento dei dati da parte del mittente.

In assenza di tale prerequisito si provvederà alla restituzione al mittente.

Il trattamento dei dati sensibili e giudiziari avviene attraverso un modulo dedicato dell'applicativo SIGED, a cui accedono solo ali incaricati dal Titolare del trattamento dei dati, su indicazione dei Responsabili delle UOR.

Tutte le operazioni eseguite sono tracciate da log di sistema.

Documenti contenenti dati sensibili e giudiziari su supporto analogico

Modalità di trattamento in fase di ingresso-

In caso di documenti pervenuti al Dipartimento in busta chiusa con dicitura dati sensibili, non indirizzati ad una UOR specifica , il Servizio di Segreteria del Capo Dipartimento-Protocollo provvederà:

a) all'apertura della busta;

b) all' individuazione della UOR destinataria;

c) all'inoltro al Responsabile della UOR

Il Responsabile della UOR, in qualità di incaricato, ne stabilirà il trattamento, fornendo le seguenti indicazioni al Servizio di Segreteria del Capo Dipartimento-Protocollo :

a) procedere alla gestione integrale del documento nel sistema informativo, attraverso il modulo "dati sensibili e giudiziari" di S.I.Ge.D.®;

b) procedere all'acquisizione parziale del documento, nel sistema informativo, attraverso il modulo "dati sensibili e giudiziari" di S.I.Ge.D.®, sulla base di un'attestazione sottoscritta dal medesimo, acquisibile in fase di protocollazione.

In caso di documenti pervenuti al Dipartimento in busta chiusa con dicitura dati sensibili e indicazione della UOR competente, il Servizio di Segreteria del Capo Dipartimento-Protocollo provvederà all'inoltro al relativo Responsabile; costui provvederà al trattamento nelle modalità sopra riportate.

In caso di documenti pervenuti in busta chiusa con dicitura dati sensibili ed indirizzati nominativamente al personale, il Servizio di Segreteria del Capo Dipartimento-Protocollo provvederà al relativo inoltro.

Sarà cura del destinatario interno restituire al Servizio di Segreteria del Capo Dipartimento-Protocollo il documento in busta chiusa, qualora non riguardi atti o fatti strettamente personali, per gli adempimenti illustrati.

Documenti contenenti dati sensibili e giudiziari su supporto analogico

*Modalità di trattamento in fase di uscita interna o esterna***.**

Le UOR sono tenute al trattamento dei dati sensibili o giudiziari attraverso il modulo dati sensibili e giudiziari di S.I.Ge.D.®, anche nel caso di documenti originali unici; qualora non dovessero procedere alla scansione dei documenti o non dovessero accludere l'attestazione che ne comprovi le motivazioni, in fase di inoltro dei pacchetti di versamento al Servizio di conservazione, il Responsabile della gestione documentale si riserva l'annullamento di tali registrazioni.

Documenti contenenti dati sensibili e giudiziari su supporto digitale

Modalità di trattamento in fase di ingresso.

Tali documenti vengono gestiti direttamente dal Servizio di Segreteria del Capo Dipartimento-Protocollo, che provvede alla registrazione nel sistema informativo e all'assegnazione solo per competenza alla UOR selezionata, il cui Responsabile provvede, se del caso, all'estensione della visibilità a incaricati individuati nominativamente.

I documenti al termine del trattamento vengono archiviati in uno spazio logico-fisico non accessibile ad alcun utente, neppure al Titolare del trattamento o al Responsabile della UOR.

I documenti possono essere richiesti di nuovo in visibilità dal Responsabile della UOR al server per sopraggiunte necessità, che debbono essere esplicitate; finito il trattamento, verranno di nuovo archiviati.

Documenti contenenti dati sensibili e giudiziari su supporto digitale

*Modalità di trattamento in fase di uscita interna o esterna***.**

Le UOR sono tenute a conformarsi al trattamento dei dati nelle modalità descritte nei paragrafi precedenti; per la descrizione di dettaglio si rinvia a Documenti contenenti dati sensibili e giudiziari su supporto analogico- *Modalità di trattamento in fase di uscita interna o esterna***.**

Dati personali

Sono trattati come tali, con apposito modulo dell'applicativo SIGED, ad esempio: le note caratteristiche del personale militare in posizione di comando, i procedimenti disciplinari non collegati a procedimenti penali.

ALLEGATO N. 3

UNITA' ORGANIZZATIVE RESPONSABILI

U.O.R.

Capo Dipartimento

Vice Capo Dipartimento
Segreteria del Capo del Dipartimento

Attività giuridica e legislativa

Servizio contenzioso

Ufficio Stampa

Ufficio del Direttore operativo per

ilcoordinamento delle emergenze

Volontariato e risorse del Servizio Nazionale

Promozione e integrazione del Servizio

Nazionale

Attività tecnico-scientifiche per la previsione e

prevenzione dei rischi

Risorse umane e strumentali

Amministrazione e Bilancio

ALLEGATO N.4

PRINCIPALI PROCEDURE DEMATERIALIZZATE

Fatturazione elettronica

Il workflow delle fatture elettroniche consiste nella migrazione all'interno del sistema informativo dipartimentale dei relativi file XML, provenienti dalla piattaforma SDI , attraverso una pec dedicata, in conformità alle disposizioni normative correnti.

Le operazioni di validazione o di rifiuto di tali dati sono a carico dell'Ufficio Amministrazione e Bilancio; in caso di riscontro negativo, il documento viene rinviato al soggetto emittente con relativa causale, entro 15 gg dalla ricezione.

In caso di esito positivo si provvederà alla registrazione di protocollo ed all'annotazione nel registro delle fatture.

Tutte le operazioni sono tracciate da log di sistema.

Fogli di coordinamento elettronici

La procedura finalizzata alla gestione di atti complessi, prevede due fasi. La prima contempla l'apertura e la condivisione di un nuovo fascicolo elettronico o la condivisione di un fascicolo preesistente, da parte dell'ufficio proponente il coordinamento, all'interno del quale gli altri uffici inseriscono pareri. La seconda fase prevede l'inoltro telematico del fascicolo dall'Ufficio proponente alla Segreteria del Capo del Dipartimento per l'approvazione finale, e la restituzione da parte di quest'ultima del fascicolo all'ufficio proponente per la registrazione di protocollo.

ALLEGATO N. 5

PROCEDURE DI GESTIONE DOCUMENTALE IN SITUAZIONI DI EMERGENZA NAZIONALE ED INTERNAZIONALE

Negli stati di configurazione S2 ed S3, qualora il Direttore dell'Ufficio Emergenze lo ritenga opportuno, viene attivato un coordinamento tra il Servizio di Segreteria del Capo Dipartimento-Protocollo e il Centro messaggi al fine di garantire un servizio di registrazione di protocollo h24.

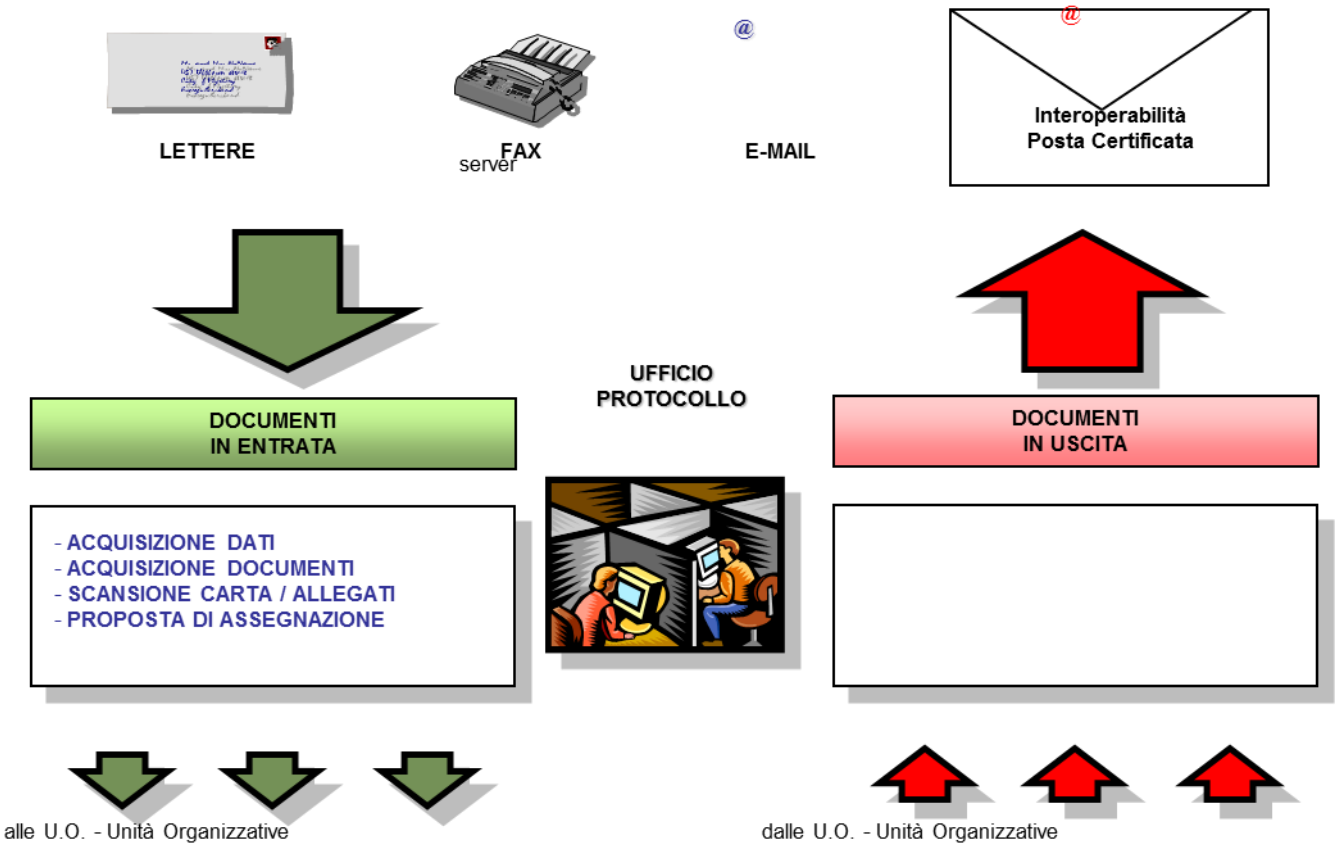
Al fine di fronteggiare situazioni emergenziali che comportino una gestione documentale de-localizzata sono predisposte, a cura del Servizio informatico, due postazioni *stand alone* da attivare a richiesta, in modo alternativo. Su tali postazioni verrà assicurata la gestione del nucleo minimo del protocollo anche per i dati sensibili. Le registrazioni effettuate verranno conservate su unità removibili, per essere riversati, in date prestabilite, in un'area dedicata del server centrale del Dipartimento.

Il Responsabile della gestione documentale provvederà ad attivare le procedure descritte nel presente comma, avvalendosi del supporto dei referenti informatici.

Qualora lo scenario di evento impedisca di attivare gli ordinari canali di comunicazione telematici, si utilizzeranno canali analogici.

ALLEGATO N. 6

WORKFLOW

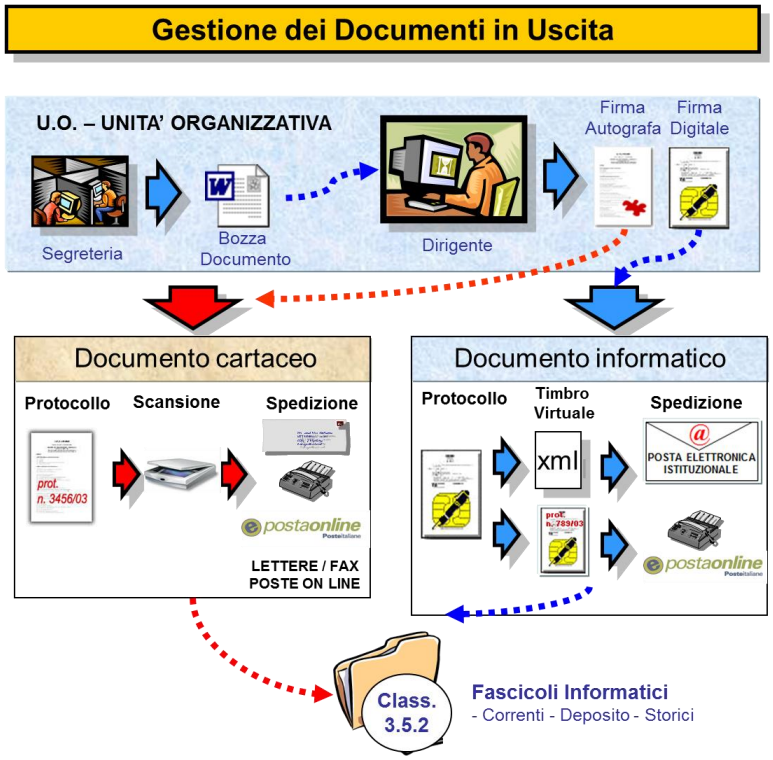


Archiviazione dei Documenti Correnti

FLUSSO DOCUMENTALE IN USCITA

S.I.Ge.D.®
Sistema Integrato di Gestione Documentale
Joint

Le norme di riferimento:



ALLEGATO N. 7

PROCEDURE IN CASO DI MALFUNZIONAMENTI DI SISTEMA O DI ERRONEE PROCEDURE

Nel caso di malfunzionamenti di sistema e/o di anomalie, di seguito riportati, gli utenti dovranno inoltrare una email all'indirizzo *siged@protezionecivile.it*, gli operatori di protocollo all'indirizzo assistenza*siged@protezionecivile.it*,*:*

- Data base non trovato
- Prenotazione numero di protocollo non riuscita
- Conflitto di replica
- Documento aperto in modifica da altro utente
- Id utente non trovato
- Mancato aggiornamento della password
- Mancata trasmissione dei documenti o mancata variazione di stato
- Mancato accesso alla documentazione
- Password dimenticata (creazione di nuovo ID)
- Modifica dei permessi degli accessi per l'utente (con autorizzazione del Dirigente)

Qualora i malfunzionamenti riguardassero la scansione, la stampa delle etichette, la mancata visualizzazione del documento (errore 31) gli utenti e gli operatori di protocollo si dovranno rivolgere all'help desk, raggiungibile attraverso l'applicativo di interfaccia web "Assistenza informatica", attivo nell'Intranet dipartimentale.

ALLEGATO N. 8

Per il Titolario di Classificazione e il Piano di conservazione si rinvia rispettivamente:

febbraio.docxhttp://www.pcm.it/NormeDocumenti/Archivi/doc/TITOLARIO_aggiornamento2015.pdf

http://www.pcm.it/NormeDocumenti/Archivi/doc/piano_conservazione_2015.pdf

IL REPERTORIO DEI FASCICOLI

Il repertorio dei fascicoli è un registro dove vengono riportate informazioni sui fascicoli riepilogate nel modello qui di seguito riportato, a cura del Responsabile della gestione documentale.

- Titolo: denominazione attribuita al fascicolo
- Classe: stringa alfa numerica con cui viene rappresentato un dominio del titolario
- Anno di apertura del fascicolo
- Sottoclasse: stringa alfa numerica con cui viene rappresentato un sotto dominio del titolario
- Numero di protocollo
- Descrizione: indicazione sommario del contenuto del fascicolo
- Anno di chiusura del fascicolo
- Status chiuso o aperto

ALLEGATO 8BIS

TIPOLOGIE DOCUMENTARIE TRATTATE

Accordi/convenzioni internazionali
Albo fornitori
Attestati formativi
Attestazioni di idoneità
Attestazioni di servizio
Atti di accertamento
Atti di impiego flotta
Atti di revoca degli interventi
Avvisi e bollettini
Bandi
Benemerenze
Cartografia
Censimenti del danno (schede)
Certificazioni
Circolari
Collaudi
Comandi
Comunicazioni con fornitori /gestori dei servizi
Comunicazioni inter-istituzionali
Comunicazioni con cittadini
Contratti
Decreti a contrarre
Decreti Attuativi
Decreti istitutivi di organizzazione
Diffide
Dinieghi dichiarazione stato di emergenza
Disposizioni e ordini di servizio
Gare
Inventari
Inviti
Istanze cittadini
Istanze rimborsi associazioni volontariato
Missioni
Modelli operativi per eventi straordinari
Ordinativi di pagamento
Pareri normativi

Pareri tecnici
Passi
Permessi personali
Permessi sindacali
Piani CLE
Piani dell'assetto idrogeologico
Piani di emergenza in funzione dei rischi
Piani esercitazione
Piani di formazione
Piani di impiego mezzi e beni
Piani di lotta contro incendi boschivi
Piani di volo
Piani sanitari
Piano di addestramento
Piano di sicurezza informatica
Presentazioni convegni seminari
Progetti di logistica
Progetti europei
Progetti internazionali
Rapporti post-evento
Registri di protocollo
Verifiche attuazione interventi post-emergenziali
Segnalazioni danno **Relazioni di sopralluogo**
Relazioni tecniche
Repertori di opere strategiche
Richieste di concorso aereo
Richieste di risarcimento
Ricorsi
Rilevazioni presenze
Risposte ad atti sindacato ispettivo
Scheda d'analisi degli indicatori di esposizione e vulnerabilità sismica
Schemi di Ordinanze/dichiarazione stati di emergenza
Segnalazioni eventi
Sopralluoghi ex Dlgs 81/2008
Statistiche interne
Stime di danno
Studi di caratterizzazione dei siti
Valutazioni tecno-economiche
Verbali

ALLEGATO N 9

NORMALIZZAZIONE DELLE INTESTAZIONI

Al fine di garantire la necessaria omogeneità dell'anagrafica, tutti coloro che sono abilitati alla protocollazione dovranno rispettare le seguenti indicazioni:

a) eliminare qualsiasi riferimento personale e riportare l'ufficiale denominazione dell'organo istituzionale o della società (ad esempio non Sergio Mattarella ,ma Presidenza della Repubblica;

b) riportare nella sua interezza l'articolazione della struttura, utilizzando trattini e spazi tra i diversi livelli gerarchici (Ministero dell'Economia e delle Finanze- Dipartimento del Tesoro- Direzione 6- Operazioni finanziarie- Analisi di conformita' con la normativa UE-);

c) riportare l'acronimo , laddove più noto, seguito dalla denominazione estesa INPS- Istituto Nazionale previdenza Sociale;

d) eliminare preposizioni iniziali (al, allo etc.);

e) compilare in modo completo la scheda; inserendo obbligatoriamente oltre l'intestazione: indirizzo e CAP; indirizzo pec;

Istruzioni per la compilazione di schede afferenti la P.A.

a) Qualora il livello gerarchico descritto non sia detentore di pec, si inserisce indirizzo email. Non possono essere inseriti due indirizzi pec nella stessa scheda; possono essere inseriti un indirizzo email ed uno pec, purché si riferiscano allo stesso intestatario;

Si fa presente che alcune Amministrazioni con struttura complessa utilizzano lo stesso indirizzo pec per vari uffici (es. PCM = diprus@pec.governo.it). Si prega, pertanto, di individuare l'anagrafica appropriata, tenendo conto che il S.I.Ge.D.® seleziona automaticamente la prima scheda associata a tale indirizzo pec;

b) Qualora in anagrafica fosse già presente una scheda dedicata (es. Comune- Paliano) ma il documento di riferimento è indirizzato ad un ufficio e/o settore specifico (es. Comune- Paliano- Settore tecnico), si dovrà procedere alla creazione di altra ed apposita scheda anagrafica;

c) Per gli enti territoriali o le strutture periferiche di enti nazionali, il toponimo è un elemento di indicizzazione di rilievo; per tal motivo si è scelto di compilare l'intestazione nelle modalità in esempio.

Regione autonoma - Sicilia;

- tutti i nomi di comuni che hanno nella loro denominazione san , santa, sant' dovranno essere inseriti con S. *(esempio:* Santa Maria a Vico = S. Maria a Vico*)*

- le preposizioni non vanno inserite per gli enti territoriali *(es.* Comune di Paliano = COMUNE - PALIANO*)*

- ma vanno inserite per i Ministeri

- le aziende sanitarie locali dovranno essere precedute dall'acronimo AUSL ed inserite come istituzione;
- le Ambasciate dovranno essere inserite in italiano*: es.* Ambasciata della Repubblica del Messico in Italia,

Istruzioni per la compilazione di schede concernenti professionisti ed imprese

Per i professionisti e le imprese - obbligati *ex lege* ad avere indirizzo pec - , qualora non sia stato fornito, al fine di completare l'inserimento dei dati nella scheda anagrafica, si consiglia di consultare *www.inipec.gov.it*,.