PROTEZIONE CIVILE
Presidenza del Consiglio dei Ministri
Dipartimento della Protezione Civile

Manuale di Gestione

del protocollo informatico, dei flussi documentali

e degli archivi

Ge.Do.P.

* * *

Edizione 2025

Redatto da	*Dott.ssa Tiziana Tolli*	*Dott. Stefano Salomone*
Revisionato da	*Dott.ssa Tiziana Tolli*	*Dott. Stefano Salomone*

INDICE

INTRODUZIONE

Questa quarta edizione del *Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi* scaturisce dall'evoluzione tecno-normativa dell'ultimo quinquennio e dal processo di transizione al digitale, che ha coinvolto tutta l'organizzazione dipartimentale ed è culminato nella migrazione ad una nuova piattaforma documentale di tipo web oriented, integrata da servizi cloud.

Il nuovo sistema di gestione documentale è stato pianificato tenendo conto dei principi ispiratori dal regolamento eIDAS, UE 910/2014, che disciplina le interazioni elettroniche sicure tra imprese, cittadini e pubblica amministrazione all'interno dell'UE[1], della normativa nazionale e del Piano triennale per l'informatica nella PA 2024-2026, a sua volta allineato ai principi di digitalizzazione richiamati nel PNRR.

Le innovazioni tecno-normative dell'ultimo quinquennio hanno inteso incentivare un nuovo paradigma organizzativo della PA basato sull'ingegnerizzazione o re-ingegnerizzazione dei processi e la dematerializzazione dei procedimenti, da rendere trasparenti ed accessibili all'utenza interna ed esterna, con ogni tipo di device[2].

Nel Dipartimento si è ritenuto imprescindibile pianificare e implementare un nuovo sistema informativo con requisiti di:

- riusabilità, per superare i limiti di lock-in tipici dei software proprietari;
- accessibilità da remoto, grazie all'architettura web-oriented, che consente agli utenti interni di poter più agevolmente svolgere le proprie attività lavorative in ogni contesto, essendo fruibile su ogni tipo di device;
- scalabilità delle prestazioni; le funzionalità di sistema sono adeguate al volume dei dati trattati;
- flessibilità nella configurazione di soluzioni personalizzate;
- fruibilità di servizi cloud.

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

[2] art. 64, comma 2 septies, ibidem

Il sistema informativo risponde ad un modello gestionale orientato all'ingegnerizzazione ed interazione dei processi di core business, alla digitalizzazione dei contenuti informativi, all'interoperabilità, alla conservazione digitale.

Si è superato il modello lineare di gestione del nucleo minimo di protocollo in favore di una gestione integrata dei processi e dei procedimenti; attraverso il nuovo sistema gestionale è, infatti, possibile interfacciarsi con gli applicativi gestionali di contabilità pubblica e servizi cloud, come quello di conservazione, nonché configurare procedimenti intersettoriali.

Le interazioni con le istituzioni, il terzo settore, i cittadini, le aziende sono assicurate attraverso i canali telematici ordinari; il trasferimento e la ricezione dei big data è assicurata dal servizio di own cloud.

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;
- il workflow;
- i criteri e le regole di organizzazione dell'archivio analogico;
- l'accesso e la consultazione dei documenti;
- il piano di sicurezza;
- le procedure per la tutela dei dati personali;
- i principali processi di core business digitali;
- le modalità di aggiornamento e comunicazione del Manuale stesso.

CONTESTO ISTITUZIONALE E OPERATIVO

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

Le attività, sommariamente elencate, danno avvio a procedimenti ed atti amministrativi, che per le loro peculiarità particolarmente rilevabile in fase emergenziale, necessitano di una regolamentazione specifica.

In base a tali premesse, si è ritenuto opportuno adottare un Manuale di gestione documentale, in cui descrivere il modello organizzativo e la prassi adottata, anche durante gli stati di configurazione.

Tale autonomia operativa è stata concertata con l'Ufficio del Segretario generale, a cui è devoluto il compito di stabilire le linee guida della gestione documentale della Presidenza del Consiglio dei Ministri.

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

Il flusso informativo con la Presidenza avviene attualmente attraverso canali digitali diversificati e lo scambio posta interno.

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.

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;

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 *CAD*, il D. Lgs. 7 marzo 2005, n. 82, recante il *"Codice dell'Amministrazione digitale"* 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 è tratto;

q) per *copia informatica di documento informatico*, il documento informatico avente contenuto identico a quello del documento da cui è 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 del D.P.R. 14 novembre 2002, n. 313, recante il Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di casellario giudiziale europeo, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti;

s) per *dati particolari*, i dati personali idonei a rivelare l'origine razziale o etnica, l'orientamento politico, religioso, sessuale, l'appartenenza sindacale;

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

u) per *documento informatico*: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

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

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

x) *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;

y) per *domicilio digitale*: l'indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato;

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

z) 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 (art. 25 Regolamento eIDAS);

aa) per *firma elettronica avanzata (FEA)*, quella firma elettronica connessa ed identificativa del firmatario, creata mediante dati che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo e collegata ai dati sottoscritti, in modo da consentire l'identificazione di ogni loro successiva modifica (art. 26 Regolamento eIDAS);

ab) per *firma elettronica qualificata (FEQ)*: un particolare tipo di firma elettronica avanzata, creata con un dispositivo qualificato le cui caratteristiche ad effetto giuridico equivalente a quello di una firma autografa (all. II Regolamento eIDAS); la firma elettronica qualificata è associabile alla firma digitale 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 (art. 24 CAD);

ac) 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;

ad) 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;

ae) 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);

af) 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'modificabilità del documento stesso nel sistema di protocollo informatico;

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

ah) 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;

ai) 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;

al) 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;

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

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

ao) per *ricevuta di consegna* si intende il certificato inviato dal provider del servizio di posta elettronica certificata del destinatario al mittente;

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

aq) 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);

ar) 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 dei documenti in uscita: oggetto, mittente e destinatario;

as) per *servizio cloud di tipo SaaS* si intende un servizio gestito interamente da un soggetto esterno, il provider;

at) per *sigillo elettronico* si intende l'insieme di «dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi».

au) 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;

av) per *titolare del trattamento dei dati personali e giudiziari*, la figura istituzionale che per la normativa è responsabile del relativo trattamento, identificabile nel Capo del Dipartimento della Protezione civile;

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

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

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, articolata in nove Uffici, incluso quello del Vice Capo Dipartimento, e cinque Servizi di staff.

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, a cui è affidato, tra l'altro, il coordinamento dell'attività di gestione documentale.

Allo scopo è stato nominato il Responsabile della gestione documentale, del protocollo informatico e degli archivi e della conservazione digitale, supportato e sostituito dal Vice Responsabile.

Tale professionalità, in possesso di titoli e competenze tecno-archivistiche, definisce ed assicura[3]:

a) la predisposizione del Manuale di gestione, d'intesa con il Responsabile del Servizio sistemi informatici e infrastrutture di rete, acquisito il parere del Responsabile della protezione dei dati personali;

b) la predisposizione del piano di sicurezza informatica di competenza d'intesa con il Responsabile del Servizio sistemi informatici e infrastrutture di rete, acquisito il parere del Responsabile della protezione dei dati personali;

c) il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione degli archivi;

d) il ripristino delle funzionalità del sistema, in caso di guasti o anomalie entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;

e) la conservazione delle copie in luoghi sicuri;

[3] artt. 61,62,63, D.P.R. 28 dicembre 2000, n. 445 recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"; linee Guida Agid par. 3.4: par. 3.9.

f) le operazioni di annullamento;

g) l'osservanza delle disposizioni del DPR 445/2000 da parte del personale autorizzato e degli incaricati;

h) la pianificazione e il coordinamento del processo di adeguamento normativo e della manutenzione evolutiva del sistema gestionale;

i) la pianificazione del livello di qualità dei requisiti funzionali del sistema informativo;

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

k) l'accesso, in condizioni di sicurezza, alle informazioni del sistema, nel rispetto delle disposizioni in materia di tutela dei dati personali;

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

m) la pianificazione e supervisione dell'addestramento del personale all'uso della piattaforma gestionale,

n) 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;

o) 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;

p) la predisposizione del piano di classificazione.

Il Responsabile o il Vice Responsabile nell'assolvimento dei compiti, si avvale del supporto del Servizio sistemi informatici e infrastrutture di rete, nonché dei Referenti della gestione documentale di cui all'articolo successivo.

.

La società fornitrice della piattaforma di gestione documentale Ge.Do.P. supporta il Responsabile e il Vice Responsabile nei compiti di cui ai par. c) d); h); i); k); n).

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[4].

Tale Responsabile designa un referente della gestione documentale, che collabora con il

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

Responsabile e il *Vice Responsabile* della gestione documentale all'ottimizzazione delle procedure adottate.

I referenti hanno il compito di segnalare al *Responsabile e al Vice Responsabile* della gestione documentale le eventuali criticità rilevate, di fornire eventuali indicazioni di ottimizzazione dei requisiti funzionali della piattaforma, di trasmettere le richieste di abilitazione degli utenti, di sottoporre eventuali aggiornamenti della classificazione in uso, di cooperare per la regolare registrazione in partenza dei documenti.

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[5].

Art. 7
Formazione e accessibilità dei documenti amministrativi informatici

I documenti amministrativi informatici vengono prodotti all'interno del Dipartimento secondo le seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente[6].

Art. 8
Documenti informatici firmati elettronicamente

I documenti informatici, prodotti in una delle modalità di cui al precedente articolo, relativi ai negozi giuridici elencati all'art. 1350 del c.c., vengono sottoscritti per la loro validità con firma qualificata o digitale[7].

Gli atti pubblici, prodotti in una delle modalità di cui all'art. 7 e di competenza dell'ufficiale rogante, vengono sottoscritti da costui con firma qualificata o digitale, mentre le controparti, in sua presenza, possono apporre, in alternativa alla firma qualificata o digitale, una firma autografa acquisita digitalmente ed allegata agli atti [8].

[5] AGID Linee guida sulla conservazione dei documenti informatici, 10 dicembre 2015.
[6] AGID Linee guida sulla formazione, gestione e conservazione dei documenti informatici, 2021, par. 2.1.1;
[7] CAD art. 21 co 2 bis
[8]CAD art. 21 co 2 ter

Art. 9

Copie informatiche e duplicati e dei documenti amministrativi informatici

Le copie informatiche dei documenti amministrativi informatici vengono prodotte attraverso 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 Vice Responsabile provvederanno alla sottoscrizione di un'attestazione allegata alla copia.

I duplicati non vengono autenticati.

Art. 10

Copie analogiche di documenti amministrativi informatici

La conformità della copia analogica all'originale informatico è attestata con apposita 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 *Vice Responsabile* 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 particolari e giudiziari è disciplinato nell'art.15 quinquies e nell'allegato n. 2 del presente Manuale.

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'modificabilità e l'integrità nel tempo, dal momento che non possono esservi apportate variazioni al termine delle operazioni di registrazione.

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 assicuri modificabilità ed integrità nel tempo, e ne attesti la conformità all'originale, fino a disconoscimento espresso[9].

Fanno eccezione i documenti originali unici.

Qualora necessario, il *Responsabile* o il *Vice Responsabile* della gestione documentale rilascia attestazione di conformità associata alla copia per immagine; in tal caso non può esservi azione di disconoscimento[10].

Art. 12

Sottoscrizione ed elementi alternativi di validazione dei documenti informatici

I documenti informatici sottoscritti con firme qualificate, la cui certificazione risulti revocata, scaduta o sospesa, sono assimilabili a documenti non sottoscritti[11]; pertanto, non saranno registrati a protocollo, salvo che lo stato di sospensione sia stato annullato.

La trasmissione per posta elettronica certificata, costituendo elezione di domicilio speciale ai sensi dell'art. 47 del Codice civile, surroga la sottoscrizione , purché le credenziali dell'utente titolare di account siano state rilasciate dal provider, previa identificazione[12].

Qualora la firma abbia soltanto valore probatorio e non sia associabile a documenti originali unici, è possibile procedere alla sottoscrizione con firma omessa. per i funzionari pubblici[13].

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 di gestione, con la procedura di marcatura nella fase di conservazione.

[9] Art. 22, comma 3, D. Lgs 7 marzo 2005 n. 82 recante il "Codice dell'Amministrazione digitale" e s.m.i.
[10] Art. 22, comma 2, ibidem.
[11] Art. 24, comma 4bis, ibidem.
[12] Art. 65, ibidem".
[13] Art. 3, D. Lgs. 12 febbraio 1993, n. 39

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 unico , sono acquisiti e conservati su supporto cartaceo e contestualmente ne viene prodotta copia informatica[14].

[14] 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) decretazione (cfr. sezione V);
c) dematerializzazione
d) registrazione e segnatura di protocollo (cfr. sezione VI);
e) classificazione (cfr. sezione VII);
f) fascicolazione (cfr. sezione VIII);
g) 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 al Servizio di comunicazione e cultura della protezione civile, per i seguiti di competenza, in assenza di registrazione di protocollo**.**

Art. 16
Flusso di lavorazione dei documenti cartacei in uscita

Le fasi della gestione dei documenti sono:

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

e) spedizione (cfr. sezione IX);

f) archiviazione (cfr. sezione X).

Le comunicazioni cartacee in uscita saranno limitate ai documenti originali unici e/o agli utenti sprovvisti di identità digitale[15].

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) trasmissione via Ge.Do.P.;

e) archiviazione (cfr. sezione X**).**

Art. 18

Flusso di lavorazione di atti endo-procedimentali

Gli atti endo-procedimentali non verranno registrati a sistema, ma inoltrati tramite Ge.Do.P. alla UOR di riferimento.

Verranno trattati come atti endo-procedimentali, tra gli altri, le attestazioni /certificazioni rilasciate dalle autorità preposte ai fini degli accertamenti previsti dall'art. 52 del D.Lgs n. 36/2023 recante il "Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78 ".

[15] 'art. 3bis del D.Lgs 7 marzo 2005 recante il "Codice dell'Amministrazione digitale".

RICEZIONE DEI DOCUMENTI

Art. 19

Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo, possono pervenire alla AOO tramite 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 89.

Tale canale è ammesso per documenti originali unici, per i documenti classificati ai sensi della Legge 3 agosto 2007, n. 124, per comunicazioni provenienti da cittadini sprovvisti di domicilio digitale.

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[16].

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 debbono 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; tale procedura è giustificata dalla necessità di conservare le certificazioni attestanti l'avvenuto inoltro da parte del mittente.

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

I documenti informatici possono essere ricevuti anche su supporto removibile, attraverso il sistema postale oppure brevi manu, purché in formato ammesso per la conservazione e provvisti di attestazione di conformità all'originale conservato presso il mittente.

I documenti informatici di grandi dimensioni vengono presi in carico attraverso il canale cloud; il mittente dovrà inviare una email all'indirizzo protocollo@protezionecivile.it per chiedere l'attivazione del canale.

A seguito di tale attivazione, il mittente riceverà una email di istruzioni, in cui saranno riportati il link e la pw temporanea da utilizzare per accedere all'area cloud dove potrà depositare la documentazione.

Quando il mittente avrà completato le operazioni, il personale addetto riceverà la relativa notifica e potrà procedere alle operazioni di verifica e di eventuale registrazione.

Art. 21

Notifiche di eccezione

Le notifiche di eccezione vengono inviate automaticamente al mittente dalla piattaforma documentale Ge.Do.P. in caso di errore bloccante, ovverosia in presenza di :

a) file con estensione 0;

b) file con formato non ammesso dalla normativa vigente;

c) file contenente macroistruzioni.

Lo stesso accade in caso di errore non bloccante, ovverosia di mancata conformità della sintassi della segnatura di protocollo alle direttive tecno-giuridiche dell'AGID.

Le notifiche di eccezione vengono inviate dal personale addetto alla gestione documentale in tali fattispecie:

a) illeggibilità e/o mancata integrità del documento;

b) incongruità tra documentazione spedita e quella comunicata;

c) mancata sottoscrizione digitale del documento primario ed eventualmente degli allegati, qualora la firma abbia valore ad substantiam (v. contratti);

d) assenza di elementi di corroborazione alternativi alla firma, qualora questa abbia valore esclusivamente ad probationem, quali: la trasmissione via pec, o l'uso combinato di firma elettronica e copia allegata del documento di identità nella trasmissione via email, firma omessa per pubblici dipendenti.

e) incompetenza assoluta "ratione materiae".

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

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, 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 correntemente dal personale della Segreteria del Capo del Dipartimento; il Capo del Dipartimento e, in sua assenza, il Vice Capo Dipartimento disporranno eventuali integrazioni o correzioni.

L'assegnazione interna alle UOR è effettuata dal Responsabile del procedimento amministrativo e/o dal suo delegato, di cui all'art.5 del presente Manuale.

Per il trattamento dei dati particolari e giudiziari si rinvia all'allegato n. 2.

Art. 24
Modifica ed integrazione delle assegnazioni e delle riassegnazioni

La UOR assegnataria è tenuta a restituire immediatamente alla Segreteria del Capo del Dipartimento-Protocollo l'erronea assegnazione, avvalendosi del tasto "rifiuta" della piattaforma Ge.Do.P.; è consentita la restituzione entro una settimana lavorativa, solo in caso di comprovati impegni in attività emergenziali.

In caso di presa in carico dell'erronea assegnazione, la UOR ne chiederà la rimozione scrivendo alla email protocollo@protezionecivile.it.

Il log di sistema registrerà le modifiche intervenute, con riferimento all'id utente, alla data e all'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 apre al 1 gennaio e 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, ancorché afferenti al medesimo procedimento.

Art. 26
Documenti classificati

I documenti classificati[17] 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[18].

Art. 27
Personale adibito alla registrazione di protocollo

La registrazione di protocollo in entrata è eseguita dal personale 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.

Il Centro messaggi provvede ordinariamente alla registrazione in entrata ed in uscita delle seguenti tipologie documentarie: bollettini e report di eventi naturali, comunicazioni afferenti alla Direttiva P.C.M. 8 luglio 2014, al rinvenimento di ordigni bellici e all'attivazione delle strutture emergenziali territoriali (COC; COM; CCS).

In caso di necessità contingenti verificabili in orari notturni, in giorni prefestivi e festivi, il Centro messaggi provvede alla registrazione di tutte le tipologie documentarie.

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

[18] 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".

Non è previsto l'accesso del Centro messaggi ai documenti personali, particolari e classificati.

Le UOR sono tenute alla registrazione di protocollo dei documenti in uscita interna ed esterna; il Servizio delle politiche contrattuali provvede anche alla protocollazione delle fatture scaricate dalla piattaforma SDI.

I Responsabili unici del procedimento, i Direttori dei Lavori, i Direttori dell'esecuzione contrattuale, i segretari delle Commissioni di gara e dei gruppi di lavoro, sono tenuti a registrare le comunicazioni destinate alle UOR dipartimentali con protocollo interno e quelle destinate a soggetti esterni con protocollo in uscita.

Allo scopo vengono abilitati nel sistema informativo.

Art. 28
Prerequisiti per la registrazione di 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 essere integrate da elementi di chiara identificazione, in assenza dei quali, verranno inoltrate all'URP dipartimentale per i seguiti di competenza, senza registrazione di protocollo.

b) assenza di macroistruzioni;

c) formato immodificabile; il concetto di modificabilità 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;

d) linguaggio e contenuti idonei alla funzione amministrativa;

e) sottoscrizione ad substantiam o ad probationem o sistemi alternativi di validazione di cui all'art. 12 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.

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

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.

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[19], 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

Comunicazioni informali inter-istituzionali

Le comunicazioni informali inter-istituzionali vengono inoltrate alla UOR competente, attraverso il sistema Ge.Do.P., senza registrazione formale.

Art. 30

Modalità di registrazione a protocollo

Le operazioni di registrazione prevedono dati immodificabili e modificabili; gli elementi di segnatura di protocollo assegnati automaticamente dal sistema, quale numero e data di registrazione, sono immodificabili.

Sono modificabili parzialmente gli altri metadati, campo oggetto, in caso di errore di digitazione, e/o l'assegnatario interno, stante la memorizzazione dei dati originali.

Art. 31

Metadati obbligatori della registrazione dei documenti ricevuti elettronicamente

Ciascuna registrazione di protocollo contiene i seguenti metadati obbligatori:

a) segnatura di protocollo, immodificabile;

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

b) l’impronta del documento informatico, immodificabile;
c) attestazione di conformità all’originale analogico in caso di dematerializzazione;
d) tipologia flusso documentale;
e) tipologia documentale;
f) tipo di registro;
g) identificativo del documento primario;
h) data;
i) operatore di protocollo;
j) mittente;
k) assegnatario;
l) oggetto del documento
m) indicazione della tipologia dei dati ai sensi del GDPR;
n) versione del documento;
o) identificazione del formato;
p) classificazione.

.

Art. 32

Metadati opzionali della registrazione di protocollo dei documenti ricevuti

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

a) oggetto codificato;
b) indicazione eventuali allegati.

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;
b) l’impronta del documento informatico, immodificabile;
c) attestazione di conformità all’originale analogico in caso di dematerializzazione;

d) tipologia flusso documentale;
e) tipologia documentale;
f) tipo di registro;
g) identificativo del documento primario;
h) data;
i) operatore di protocollo;
j) mittente interno;
k) destinatario;
l) oggetto del documento;
m) indicazione della tipologia dei dati ai sensi del GDPR;
n) versione del documento;
o) identificazione del formato;
p) classificazione;
q) identificativo del fascicolo.

Art. 34
Elementi accessori della registrazione dei documenti spediti

I dati accessori di registrazione sono i seguenti:

a) oggetto codificato;
b) indicazione eventuali 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[20].

[20] 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"

Art. 36

Segnatura di protocollo dei documenti in uscita

Le informazioni minime apposte od associate al documento in partenza mediante 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.

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[21]:

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[22].

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

Gli annullamenti sono possibili, a seguito di inoltro al Servizio di Segreteria del Capo Dipartimento-Protocollo di motivazione scritta, a cura del dirigente della UOR interessata.

[21] art. 21, 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

[22] Art. 54 DPR 28 dicembre 2000 recante il "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"

In caso di documenti analogici, la copia originale da annullare deve essere inviata al Servizio di Segreteria del Capo Dipartimento-Protocollo

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

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 gli 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 di provenienza incerta o anonimi

I documenti di provenienza incerta, perché ricevuti da indirizzi email non direttamente

riconducibili ad un soggetto giuridico o fisico, e/o perché privi di elementi di identificazione, vengono registrati in apposito repertorio "Registro anonimi" dal Servizio di Segreteria del Capo del Dipartimento- Protocollo e inoltrati, all'URP.

Se contengono notizie di reato vengono inoltrati alle autorità competenti.

Art. 43

Atti di competenza di altre amministrazioni o di altri soggetti

I documenti di competenza di un altro Ente, se individuato, vengono direttamente inoltrati al corretto destinatario, al fine di non aggravare il procedimento amministrativo[23], 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, ovverosia trasmesse via email senza elementi di corroborazione previsti nell'art. 12 del presente Manuale, provenienti da persone fisiche e/o persone giuridiche private, vengono inoltrate direttamente al Servizio di comunicazione per i seguiti di competenza, senza registrazione di protocollo.

Le comunicazioni informali dei giornalisti, che presentano le caratteristiche del comma precedente, sono assegnate all'Ufficio stampa, senza registrazione di protocollo.

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 VI- Risorse umane e

[23] 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.

strumentali- Servizio gestione ed organizzazione del personale, 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 firma digitale o con firma omessa la dicitura "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 comunicazioni di permesso sindacale provenienti da componenti interni della RSU o da RLS vengono protocollate direttamente dai medesimi con protocollo interno e sottoscritti o con firma digitale o 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 registrate e trattate come dato sensibile, in conformità alla normativa vigente; a riguardo 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 al Servizio di Comunicazione e diffusione della cultura di protezione civile.

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[24] o a mezzo ufficiale giudiziario.

[24] 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 e s.m.i

Art. 49

Gestione dei dati particolari e giudiziari

I dati particolari 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[25].

Art. 50

Documenti inerenti a gare di appalto

Le offerte dei fornitori vengono inoltrate al Servizio di Segreteria del Capo del Dipartimento-Protocollo per la registrazione di protocollo dal funzionario delle politiche contrattuali, titolare del procedimento, che successivamente provvederà alla protocollazione dell'ordine diretto di acquisto.

Art. 51

Contratti

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

Ogni contratto viene registrato nell'apposito repertorio di cui all'art. 55.

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 seguenti metadati obbligatori:

a) identificativo univoco del documento;
b) data di registrazione;
c) mittente/destinatario;
d) oggetto del documento;

[25] D.Lgs 30.06.2003 n. 196 recante "Codice in materia di protezione dei dati personali" art. 11 e s.m.i.

e) impronta di hash di ogni documento;

f) codice identificativo del registro a cui è stato associato il documento;

g) eventuali annullamenti e modifiche.

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[26]:

h) soggetto produttore, denominazione del sistema informativo (Ge.Do.P.);

i) descrizione del 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. 53bis

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 dei pacchetti di versamento da parte del Responsabile della gestione documentale.

Le attività di conservazione sono dettagliate nel relativo Manuale.

Art. 54

Fatture e Registro delle fatture

Le fatture elettroniche, scaricate automaticamente dalla piattaforma SDI, dopo la validazione e la protocollazione da parte di funzionari dell'Ufficio Amministrazione e Bilancio, vengono registrate con numero progressivo automatico nell'apposito repertorio, inviato successivamente a conservazione digitale.

La contabilizzazione delle fatture avviene attraverso l'interoperabilità del sistema Ge.Do.P.

[26]http://www.agid.gov.it/notizie/2016/marzo/conservazione-pubblicate-istruzioni-il-registro-giornaliero-protocollo "Istruzioni per la produzione e conservazione del registro giornaliero di protocollo".

con gli applicativi verticali SICOGE e SIAB.

Le comunicazioni periodiche alla piattaforma dei crediti sono gestite dal sistema Ge.Do.P.

Tutte le operazioni sopra richiamate sono tracciate da log di sistema.

Art. 55

Repertorio amministrativo

Gli atti amministrativi concernenti nomine, convenzioni, emolumenti vengono registrati nel repertorio amministrativo.

Contestualmente alla registrazione delle nomine di RUP e DEC, il sistema invia una notifica agli amministratori di sistema finalizzata alla creazione delle relative posizioni organizzative nell'organigramma Ge.Do.P.

Il repertorio viene inviato annualmente in conservazione.

Art. 56

Registro del contenzioso

Gli adempimenti concernenti gli atti giudiziari ed extragiudiziari curati dal Servizio contenzioso vengono registrati in un apposito repertorio, che viene inviato in conservazione annualmente.

Art. 57

Registro dei contratti

I contratti stipulati dal Dipartimento vengono registrati in apposito repertorio, che viene inviato in conservazione annualmente.

.

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[27].

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

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

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 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[28].

[28] 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[29].

Per ogni fascicolo debbono essere registrate obbligatoriamente le seguenti informazioni:

a) tipologia fascicolo (procedimentale, personale, affare);
b) amministrazione titolare;
c) proprietario del fascicolo/soggetti assegnatari;
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) fase del procedimento in caso di fascicolo procedimentale;
i) identificazione dei documenti contenuti;
j) identificazione del livello superiore di fascicolazione (in caso di sotto fascicoli);
k) 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, sono abilitati alla creazione e/o implementazione di fascicoli elettronici, in base al ruolo assegnato nell'organigramma Ge.Do.P.

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.

[29] art.41, D.Lgs 7 marzo 2005, n. 82 recante il "Codice dell'Amministrazione digitale" e s.m.i..; art. 65 , DPR 28 dicembre 2000, n. 445 recante il "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa".

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;

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

c) estenderne la visibilità ai colleghi di settore e/o ai colleghi con cui condivide il procedimento, nel caso che non vengano trattati dati particolari e/o giudiziari.

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 e le ricevute di consegna dei documenti spediti attraverso la posta elettronica certificata.

Art. 62

Ricerca nei fascicoli

Il sistema Ge.Do.P. consente il rapido reperimento delle informazioni contenute nei fascicoli; in caso di fascicoli procedimentali consente la gestione delle seguenti fasi: preparatoria, istruttoria, consultiva, deliberatoria, conclusiva o dell'integrazione dell'efficacia.

SEZIONE IX
SPEDIZIONI

Art. 63
Verifica e monitoraggio delle spedizioni telematiche

Le UOR, che provvedono alla spedizione per canale telematico (pec, pei, cloud), sono tenute ad avvalersi esclusivamente dell'anagrafica Ge.Do.P. o IPA 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 menù gestioni ricevute spedizioni per accedere ad una lista riepilogativa degli esiti.

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 Ge.Do.P., 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 inoltrare 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. 64 bis
Spedizioni big data

Nel caso di spedizioni di volumi dati superiori a 70 MB, il sistema gestionale attiva automaticamente il canale cloud di trasmissione.

Il destinatario riceve una pec dipartimentale, in cui viene riportato il percorso di accesso alla risorsa documentaria e l'otp (password momentanea).

Art. 64 ter

Spedizioni UBRRAC

I documenti soggetti al controllo amministrativo contabile vengono inviati all'Ufficio di regolarità amministrativa contabile attraverso un canale telematico dedicato secondo una procedura concordata.

Art. 64 quater

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 imbustati dalla UOR mittente, che provvede anche alla compilazione dei bollettini postali.

Le operazioni di affrancatura sono a carico del Servizio di Segreteria del Capo del Dipartimento- Protocollo.

SEZIONE X
ARCHIVIAZIONE DEI DOCUMENTI

Art. 65
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 Ge.Do.P. ed inoltrati via Ftps al Servizio di conservazione esterno

Le unità documentarie vengono conservate per tipologia, tenendo conto dei legami logici e sintattici tra le serie archivistiche omogenee.

Art. 66
Versamento dei documenti analogici nell'archivio di deposito

Nel corso di ogni anno, i referenti della gestione documentale degli Uffici, individuano in accordo con i Responsabili delle UOR i fascicoli chiusi 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 (ad esempio nel 2025 si possono versare fascicoli antecedenti al 2020).

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 Referente della gestione documentale 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 Referente della gestione documentale è tenuto a rilasciare apposita dichiarazione di lacunosità della serie e/o del fascicolo.

Art. 67

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).

I Referenti della gestione documentale sono tenuti a monitorare tale attività insieme al personale di archivio.

Art. 68

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. [30]

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

La proposta di scarto viene vagliata dalla Commissione, che, all'unanimità, richiede il nulla osta alla Direzione generale degli archivi del Ministero della Cultura.

La presenza di dati particolari e/o giudiziari, è evidenziata nella documentazione allegata alla proposta.

In caso di parere favorevole da parte del Ministero della Cultura, 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 della Cultura.

[30] 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";"

SEZIONE XI
ACCESSO AI DOCUMENTI

PREMESSA

L'accesso ai documenti e alle serie archivistiche è conforme alla disciplina di settore[31] , tenuto conto della tutela della riservatezza e del principio di ponderazione[32].

Le richieste di accesso concernenti dati particolari e/o giudiziari, dovranno essere preventivamente vagliate ed autorizzate dal Titolare del trattamento dei dati, previa istruttoria del Servizio del Contenzioso, per quanto concerne l'accesso procedimentale, sentiti i controinteressati.

Art. 69
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.

In caso di dati particolari e giudiziari, 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.

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

L'utenza esterna non accede al sistema informativo, ma può ricevere duplicati informatici a riscontro di istanze di accesso procedimentale o di accesso civico o civico generalizzato via email, con le restrizioni previste dalla normativa vigente, con particolare riguardo ai dati particolari e giudiziari

Le istanze di accesso e i relativi esiti sono registrati, a seconda della tipologia, nel Registro del contenzioso o nel Registro FOIA, descritti nell'allegato 8.

Le spese di accesso e di visura sono riportate nell'allegato 9.

[31] Art. 24, Legge 7 agosto 1990, n. 241 recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e s.m.i.; DPCM 12 febbraio 2010 recante "La disciplina del funzionamento dell'Archivio e l'accesso alla documentazione per scopi di ricerca"

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

Art. 70

Modalità di accesso e di consultazione delle serie archivistiche cartacee

La consultazione degli atti analogici, depositati presso l'archivio di deposito, deve essere preceduta da richiesta formale da parte dell'utenza interna, implementabile dall'intranet dipartimentale.

L'accesso procedimentale da parte dell'utenza esterna, previa istruttoria del Servizio del Contenzioso, può avvenire mediante consultazione in loco o invio di copia scansionata via email, come chiarito nell'art. 69 del presente Manuale.

In entrambe le fattispecie, la consultazione viene ammessa previa verifica della legittimazione del richiedente e delle condizioni materiali della documentazione richiesta.

Qualora ricorrano entrambe le condizioni, il personale preposto alla gestione archivistica dovrà inserire, al posto dell'originale, un cartoncino sul quale verranno trascritti i dati del consultatore (dati anagrafici, motivazione e durata prevista della consultazione).

Art. 71

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 al consultatore e ne farà una registrazione apposita.

Il Responsabile della gestione documentale, valutata la situazione e verificato lo stato del materiale, procederà, ad avviare le iniziative del caso.

SEZIONE XII
NORME FINALI

Art. 72
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.

Il Manuale viene aggiornato in linea con l’evoluzione tecno-normativa.

ALLEGATO N. 1

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

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 del Servizio sistemi informatici e infrastrutture di rete e dal Responsabile della gestione documentale.

È compito del Responsabile del Servizio sistemi informatici e infrastrutture di rete procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza, in accordo o su indicazioni del Capo del Dipartimento.

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 particolari 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 relativo ai dati particolari e giudiziari;

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 dei sistemi informativi e di comunicazione;

Responsabile della protezione dei dati personali.

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;
  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 Ufficio VI - Risorse umane e strumentali - Servizio di gestione attività 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.

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.

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.

La sicurezza della piattaforma di gestione documentale Ge.Do.P.

Sono stati eseguiti penetration test per verificare le vulnerabilità di sistema e si è provveduto ad implementare le relative misure di mitigazione di rischio da parte della società DEDA BIT.

Le misure operative adottate sono state:

a) la verifica e controllo degli accessi avviene attraverso l’active directory di Microsoft che gestisce le richieste di autenticazione della sicurezza;

b) la tracciatura delle operazioni effettuate dagli utenti accreditati sulla piattaforma di gestione documentale Ge.Do.P. attraverso i log di sistema

c) la gestione giornaliera delle copie di back-up dei dati e dei documenti;

d) l’eventuale ripristino applicativo della piattaforma di gestione documentale Ge.Do.P.

e) la gestione delle situazioni di emergenza con supporto del Fornitore dei servizi di gestione documentale;

f) la 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 presenti nella piattaforma Ge.Do.P.

Attività / Informazioni Registrate

- Registrazione dei metadati 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)
- Creazione numero di protocollo Data e ora, nome utente operazione, numero di protocollo
- 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 Data, nome utente operazione, numero protocollo, nome utente assegnatario;

- Richiesta spedizione tramite PEC \ email Data e ora, nome utente operazione, numero protocollo;

- Spedizione tramite PEC \ email Data e ora, nome utente operazione, elenco dei documenti spediti

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 particolari e giudiziari

- Attivazione gestione dati particolari e giudiziari 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:

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

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.

Sono altresì tassativamente esclusi i formati audio, video e vettoriali.

Sottoscrizione

I documenti in cui la firma ha valore ad substantiam viene apposta la firma CADES o PADES; per gli altri documenti, nei quali la firma ha valore probatorio, si utilizza la firma elettronica o la firma omessa.

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 Ge.Do.P.

In aggiunta alle informazioni indicate nei paragrafi precedenti, anche in riferimento ai dati particolari e giudiziari, si evidenzia che la gestione dei documenti presuppone:

- il recupero dei contenuti nella loro integrità;
- la relazione logica dei documenti e delle loro aggregazioni attraverso la struttura gerarchico-enumerativa del titolario.

Ruoli degli utenti Ge.Do.P.

Ogni utente ha uno o più ruoli all'interno della struttura organizzativa Ge.Do.P.

Ad ogni ruolo corrispondono abilitazioni diverse.

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

a) implementazione/modifica struttura organizzativa di ogni AOO;

b) accesso ai log di sistema;

c) gestione delle tabelle (oggetto codificato, titolario, tipologia dati, spedizione);

d) annullamento/modifica parziale dei dati in caso di errore materiale.

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

L'utente che riveste tale ruolo accetta e riassegna le comunicazioni di competenza della UOR o delega tale compito al facente funzione o al ruolo di Segreteria.

Il Facente funzione è il sostituto o Vice Responsabile 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 Funzionario 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 di pertinenza;

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.

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; tale livello è riservato al personale delle segreterie degli Uffici, con esclusione dei documenti dell'Ufficio Risorse umane e strumentali e servizi generali di funzionamento e del Servizio del contenzioso;

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

c) livello dati personali: 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 dati particolari: la scheda di protocollo e il documento non sono visibili agli incaricati finché non sia stata loro estesa nominativamente la visibilità da parte del Responsabile dell'Ufficio o del Servizio o dal facente funzione.

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.

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

Accessibilità e leggibilità dei documenti

Le basi di dati afferenti alla AOO Dipartimento della Protezione civile sono accessibili agli utenti profilati.

Il livello di autorizzazione all'utilizzo del sistema di gestione informatica dei documenti è attribuito dal Responsabile della gestione documentale su indicazione delle UOR.

Interscambio dei documenti informatici

La trasmissione dei documenti informatici avviene quasi esclusivamente attraverso il servizio di posta elettronica certificata.

.

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.

Conservazione del Registro giornaliero di protocollo

Il Dipartimento ha sottoscritto un contratto di servizio con il conservatore accreditato Trust Technology. 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 FTPS 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 Ge.Do.P. 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 Ge.Do.P. 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.

Continuità operativa e disaster ricovery

La funzionalità dell’applicativo Ge.Do.P. è garantita dal sistema di gestione di continuità operativa e disaster recovery. Sono pianificate, infatti, procedure di gestione, esecuzione, manutenzione e monitoraggio dei meccanismi di backup e ripristino necessari alla continuità operativa, alla ricostruzione del sistema, all’analisi degli incidenti.

Registro di emergenza

L’erogatore del Sistema di gestione informatica dei documenti assicura che, ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura informatica real-time, le operazioni di protocollo siano svolte sul registro di emergenza informatico.

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

In particolare sul registro di emergenza sono riportate:

a) la causa, la data e l’ora d’inizio dell’interruzione nonché la data e l’ora del ripristino della funzionalità del sistema;

b) il numero totale di operazioni registrate;

c) la sequenza numerica utilizzata come segnatura di protocollo, anche a seguito di successive interruzioni;

Con il ripristino delle funzionalità ordinarie di gestione documentale, alla segnatura di protocollo attribuita in fase di emergenza viene associata una ulteriore, creata automaticamente dal sistema al momento dei riversamenti delle registrazioni nel Registro ordinario di protocollo.

Gestione incidenti di sicurezza e violazione dei dati personali

L'incidente di sicurezza informatica è qualsiasi evento o insieme di eventi derivanti da esternalità negative volontarie o accidentali, o da inadeguate misure di sicurezza, o dalla concorrenza di entrambe le cause.

Di regola, a seguito del verificarsi di un incidente, si procede con le macro-attività di seguito riportate:

- Rilevazione, identificazione e classificazione degli incidenti;
- Gestione degli incidenti;
- Chiusura degli incidenti.

In caso di violazione di dati personali (data breach), consultato il Responsabile della protezione dei dati (RPD), proporzionalmente alla gravità della violazione, si provvede alla notifica al Garante privacy e/o comunicazione agli interessati, secondo il combinato disposto del Regolamento UE 2016/679 e del D. Lgs 196/2003 e s.m.i, recante il Codice della privacy.

L'argomento è trattato più diffusamente nell'allegato 2.

Gestione segnalazioni anomalie e richieste di supporto

L'assistenza ed il supporto agli utenti della piattaforma applicativa Ge.Do.P., è gestito in prima istanza dal Responsabile e dal Vice Responsabile della gestione documentale.

L'assistenza specialistica è curata in presenza e da remoto dal personale tecnico del Fornitore dei servizi.

Tutte le misure adottate garantiscono complessivamente la conformità ai requisiti di sicurezza richiamati nello standard ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security management systems — Requirements"

ALLEGATO N. 2

GESTIONE DEI DATI PARTICOLARI/GIUDIZIARI

La gestione dei dati particolari e giudiziari è conforme alle prescrizioni della normativa di settore, che prevede la gestione informatica o analogica[33].

Tipi di dati trattati:

a) convinzioni: religiose, filosofiche politiche, sindacali;

b) stato di salute: patologie attuali, patologie pregresse, terapie in corso, anamnesi familiare, riconoscimento cause di servizio o assenza per malattia, rimborso per spese mediche;

c) vita sessuale;

d) dati giudiziari: 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[34]:

a) costituzione e gestione del rapporto di lavoro subordinato e non subordinato, anche non retribuito; dati raccolti nell'ambito di procedimenti afferenti al riconoscimento di cause di servizio o assenza per malattia, rimborso per spese mediche, concessione di permessi per festività la cui fruizione è connessa all'appartenenza a determinate confessioni religiose. I dati che concernono convinzioni filosofiche e di altro genere venuti in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come i volontari del servizio civile. I dati sindacali e politici, acquisiti nel caso di versamento di quota a favore di organizzazioni sindacali, ovvero nell'ipotesi di nomina a carica elettiva.

[33] D.Lgs 30 giugno 2003 n. 196 recante il "Codice in materia di protezione dei dati personali" e s.m.i.; DPCM 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".

34 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".

I dati particolari o giudiziari in quanto necessari alla definizione delle controversie, ovvero, alla risoluzione del rapporto di lavoro in presenza di condanne penali e di conseguente sospensione dal servizio, o all'accoglimento delle richieste patrimoniali del giudice contabile (es. procedure per fermi amministrativi).

Le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso;

b) gestione delle nomine di vertice; dati desunti dai curricula indispensabili per la nomina e per la verifica da parte dei competenti organi di controllo circa i requisiti richiesti, ivi inclusi quelli di moralità, ai fini dell'assunzione dell'incarico;

c) concessione, revoca benefici, patronati, patrocini, benemerenze; contributi a valere sul fondo per la ripartizione della quota dell'otto per mille dell'imposta sul reddito delle persone fisiche, devoluta alla diretta gestione statale;

d) atti di organizzazione e gestione dei volontari del servizio civile di protezione civile coinvolte nell'attività di previsione, prevenzione e soccorso in vista o in occasione di eventi calamitosi;

e) gestione delle liste di mobilità;

f) gestione del contenzioso giudiziale e stragiudiziale, e presso le Corti sopranazionali; attività rivolta alla tutela degli interessi dell'amministrazione in sede amministrativa, di giurisdizione ordinaria o amministrativa e di giurisdizione amministrativa speciale, 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;

g) gestione dei distacchi e dei permessi sindacali provenienti dalle OO.SS.;

h) procedimenti correlati ad atti di sindacato ispettivo degli organi parlamentari;

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

j) 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, e del D. Lgs. 33/2013;

k) atti relative a irregolarità e frodi comunitarie in riferimento ai fondi strutturali.

Modalità di raccolta La raccolta per tutti gli ambiti di trattamento è presso gli interessati o presso terzi.

Gestione dei dati particolari e dati giudiziari

Premessa

La gestione dei dati particolari 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.

I documenti potranno essere richiamati dal Responsabile dell'Ufficio o del Servizio a seguito di richiesta motivata all'Amministratore di sistema.

Documenti contenenti dati particolari 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 particolari, 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) alla protocollazione;
d) all'inoltro al Responsabile della UOR individuata.

In caso di documenti pervenuti al Dipartimento in busta chiusa con dicitura dati particolari o dati giudiziari ed indicazione della UOR competente, il Servizio di Segreteria del Capo Dipartimento-Protocollo osserverà le procedure elencate nei paragrafi a), c), d).

In caso di documenti pervenuti in busta chiusa con dicitura dati particolari ed indirizzati nominativamente ad un destinatario interno, costui dovrà 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 particolari e giudiziari su supporto analogico

Modalità di trattamento in fase di uscita interna o esterna

Le UOR sono tenute al trattamento dei dati particolari o giudiziari attraverso il modulo "Dati particolari" di Ge.Do.P. anche nel caso di documenti originali unici; qualora non dovessero procedere alla scansione dei documenti, 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 particolari e giudiziari su supporto digitale

Modalità di trattamento in fase di ingresso.

Il trattamento dei dati particolari e giudiziari avviene attraverso una procedura dedicata dell'applicativo Ge.Do.P. denominata "Gestione dei dati particolari", a cui accedono solo gli incaricati dal Titolare del trattamento dei dati, su indicazione dei Responsabili delle UOR.

L'operatore, al momento della registrazione di protocollo, deve selezionare la tipologia documentale "dati particolari", che corrisponde all'omologo livello di accessibilità descritto nell'allegato 1 sulla sicurezza.

Il documento viene trasmesso con ragione "dati particolari" al Responsabile e Facente funzione dell'Ufficio o del Servizio, le uniche posizioni organizzative in grado di estenderne la visibilità al singolo incaricato.

A riguardo, si precisa che il Responsabile o il Facente funzione sono impossibilitati a trasmettere il documento al personale non incaricato tramite Ge.Do.P.

I documenti contenenti dati particolari saranno accessibili nei fascicoli solo agli incaricati ai quali sia stata estesa la visibilità.

È possibile per l'operatore, prima del consolidamento della registrazione di protocollo, modificare la selezione iniziale e trasformare il dato da particolare a ordinario e viceversa.

In conformità al principio di pertinenza, l'incaricato, al termine del procedimento amministrativo, sarà tenuto all'archiviazione definitiva dei documenti, che verranno conservati in un luogo fisico-logico del sistema reso inaccessibile agli utenti, perfino al Titolare del trattamento e al Responsabile della UO.

Tali documenti possono essere richiesti di nuovo in visibilità dal Responsabile della UOR all'Amministratore di sistema per sopraggiunte necessità, che debbono essere esplicitate.

Finito il trattamento, verranno di nuovo archiviati.

Tutte le operazioni descritte sono tracciate da log di sistema.

Documenti contenenti dati particolari 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 descritto nel paragrafo precedente; i documenti inoltrati ad altre UOR e/o spediti all'esterno debbono essere trasmessi per conoscenza al Responsabile dell'Ufficio o del Servizio mittente, a meno che non siano implicati nel relativo procedimento.

Dati personali

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

Le misure organizzative del trattamento

Il trattamento dei dati particolari e giudiziari richiede, in conformità alla normativa vigente, l'individuazione e la nomina di figure professionali specifiche, nonché la formazione e l'addestramento del personale in servizio.

Si è provveduto a riguardo alla nomina del Responsabile della protezione dei dati personali e degli autorizzati al trattamento, individuati in tutti i dirigenti e nei funzionari che, in ragione dei compiti istituzionali, gestiscono i dati in argomento.[35]

In caso di violazione dei dati particolari e giudiziari, il Responsabile della protezione dei dati personali informa il Titolare del trattamento, tenuto ad informare a sua volta il Garante della protezione dei dati personali entro 72 ore, purché non risulti probabile un effettivo rischio per la tutela dei diritti e delle libertà delle persone fisiche.

Tali violazioni debbono essere comunicate dal Titolare del trattamento anche al Segretario generale della Presidenza del Consiglio dei Ministri.

[35] DPCM 25 maggio 2018 recante "Criteri e modalità per l'individuazione del responsabile della protezione dei dati personali, mediante il quale la Presidenza del Consiglio dei ministri esercita le funzioni di titolare del trattamento dei dati personali, ai sensi del regolamento (UE) n. 2016/679"

ALLEGATO N. 3

UNITA' ORGANIZZATIVE RESPONSABILI

- Capo Dipartimento
- Vice Capo Dipartimento
- Consigliere giuridico
- Segreteria del Capo del Dipartimento
- Ufficio Stampa
- Servizio comunicazione
- Servizio rapporti ed iniziative istituzionali
- Servizio attività giuridica e normativa
- Servizio del contenzioso e della trasparenza
- Volontariato, formazione e assistenza
- Previsione e prevenzione del rischio
- Attività per il superamento dell'emergenza
- Innovazione tecnologica e telecomunicazioni
- Attività e relazioni internazionali
- Risorse umane e strumentali
- Amministrazione e Bilancio
- Gestione delle emergenze

ALLEGATO N.4

PRINCIPALI PROCEDURE DEMATERIALIZZATE

Fatturazione elettronica e modulo di contabilizzazione

La piattaforma Ge.Do.P. gestisce il ciclo di vita delle fatture interfacciandosi con gli applicativi verticali (SIAB e SICOGE) di gestione contabile.

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.

La fattura registrata viene associata nella maggior parte dei casi ad un contratto e schedulata, grazie ad uno specifico algoritmo; nella fase successiva è possibile collegarla ad un mandato di pagamento, scaricato da SIAB.

Le fatture contabilizzate, insieme alla documentazione di supporto, vengono spedite via pec all'UBRRAC per il controllo di regolarità contabile.

Per ogni fattura è possibile visionare on time lo stato dell'arte: accettazione, rifiuto, avvenuta contabilizzazione, non avvenuta contabilizzazione, in pagamento, da spedire.

È possibile estrarre dati dalle linee di contabilizzazione per le comunicazioni alla Piattaforma dei crediti; è altresì possibile utilizzare tali dati per la simulazione del Piano dei conti.

Tutte le operazioni sono tracciate da log di sistema.

Procedimento amministrativo digitale

Il procedimento amministrativo digitale è stato pianificato come un processo ricorsivo le cui istanze principali sono: evento, attesa, sottoscrizione, avanzamento iter.

Per ogni struttura organizzativa dipartimentale sono stati predefiniti modelli di processo, che prevedono il coinvolgimento dei funzionari, dei dirigenti, del Capo Dipartimento.

Il funzionario responsabile del singolo procedimento attiva il processo, personalizzando il template scaricato nella piattaforma, tale documento viene vagliato nelle istanze successive dalla linea gerarchica di appartenenza, che può richiederne la revisione o procedere alla sottoscrizione tout court.

Per ogni istanza riscontrata negativamente, viene riattivato il processo dall'inizio, ovverosia il documento ritorna al funzionario istruttore; per ogni istanza riscontrata positivamente, il processo avanza in linea gerarchica.

L'iter si conclude con la firma del Capo Dipartimento; sono previste eccezioni in caso di deroghe esplicite di firma.

Le versioni del documento (prodotto di output del processo), sono conservate fino alla fase di consolidamento finale.

Iter istruttorio elettronico

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 della UOR proponente con le altre UOR.

Il fascicolo non viene condiviso contestualmente tra tutti gli attori del processo, ma viene gestito in modo sequenziale, secondo un iter di volta in volta predeterminato, che consente l'inserimento di documenti e note da parte di ogni UOR partecipante.

La seconda fase contempla l'inoltro da parte della UOR proponente, una volta acquisiti i pareri delle altre UOR, del fascicolo alla Segreteria del Capo del Dipartimento per l'approvazione finale dei documenti da parte del vertice amministrativo.

Il fascicolo viene restituito alla UOR proponente sia in caso di mancata approvazione per eventuali correzioni da apportare che in caso di approvazione per gli adempimenti relativi alla registrazione di protocollo.

Rimborsi del volontariato

Il procedimento è finalizzato al rimborso ai datori di lavoro degli oneri sostenuti nei giorni di impiego del proprio personale in attività di volontariato.

Il processo implementato in Ge.Do.P. prevede due fasi: la prima, a carattere istruttorio, gestita dall'Ufficio Volontariato e risorse del Servizio Nazionale, la seconda, a carattere deliberativo, gestita dall'Ufficio Amministrazione e Bilancio.

Nelle prime istanze di processo vengono validate, registrate, indicizzate e trasmesse all'Ufficio Volontariato e risorse del Servizio Nazionale le richieste singole o multiple di rimborso.

I funzionari del Servizio del volontariato, presa in carico la documentazione, assegnata dal dirigente, istruiscono le pratiche verificando i presupposti di procedibilità; in caso di esito negativo la richiesta viene respinta al mittente.

In caso di esito positivo, viene preparata una nota per l'Ufficio Amministrazione e Bilancio, utilizzando i template caricati nell'applicativo, che vengono personalizzati con i dati dei richiedenti.

Il decretino viene inviato dal funzionario responsabile del procedimento al Dirigente del Servizio del Volontariato per la sottoscrizione digitale; una volta sottoscritto viene inoltrato dal funzionario all'Ufficio Amministrazione e Bilancio.

In assenza di tale documento, non è possibile procedere nell'istanza successiva di inoltro della documentazione all'Ufficio Amministrazione e Bilancio.

Il personale assegnatario dell'Ufficio Amministrazione e Bilancio verifica i presupposti della procedibilità della richiesta formulata dall'Ufficio Volontariato e risorse del Servizio Nazionale; in caso di inesattezze può restituirla a tale Ufficio per le modifiche o revisioni necessarie.

In caso di riscontro positivo, il funzionario dell'Ufficio Amministrazione e Bilancio responsabile del procedimento, provvede alla decretazione dell'impegno di spesa, firmato digitalmente dal responsabile dell'Ufficio, alla preparazione del mandato ed all'inoltro via pec all'UBRRAC di tutta la documentazione contabile relativa alla specifica richiesta di rimborso.

Le istanze di processo sono monitorabili dagli addetti ai lavori in tempo reale.

Accesso Foia

Il processo pianificato prevede la gestione di tre procedimenti differenziati: l'accesso civico semplice, l'accesso civico generalizzato e il riesame dell'accesso.

Il primo procedimento, definibile di base, consente di gestire le istanze finalizzate all'accesso a documenti, che avrebbero dovuto essere giù pubblicati sul sito internet dipartimentale nella sezione trasparenza.

In tali fattispecie è contemplata un'annotazione, con cui viene giustificato e/o chiarito il motivo della mancata pubblicazione.

Il secondo procedimento è oggettivamente più articolato, sia in ordine al vaglio istruttorio che al numero delle potenziali UOR partecipanti; le istanze troppo generiche, ad esempio, con ricadute negative sulla sostenibilità organizzativa, potrebbero essere oggetto di richieste di chiarimento, di accoglimento parziale o di mancato accoglimento.

Per ognuna di tali evenienze, è prevista una specifica annotazione nel registro FOIA, da dove vengono importati i dati che popolano il file trimestrale da inoltrare all'Ufficio del controllo interno della Presidenza del Consiglio dei Ministri.

Analogamente, si procede nel caso di parziali/mancati accoglimenti *ratione materiae*, motivati dall'incompetenza relativa/assoluta del Dipartimento o dai limiti di accesso imposti dalla normativa vigente.

Gli utenti, in conformità al proprio ruolo, possono verificare in tempo reale lo stato di avanzamento del procedimento di interesse.

ALLEGATO N. 5

PROCEDURE DI GESTIONE DOCUMENTALE IN SITUAZIONI DI EMERGENZA NAZIONALE ED INTERNAZIONALE

Negli stati di configurazione S2 e 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 gestione documentale h 24.

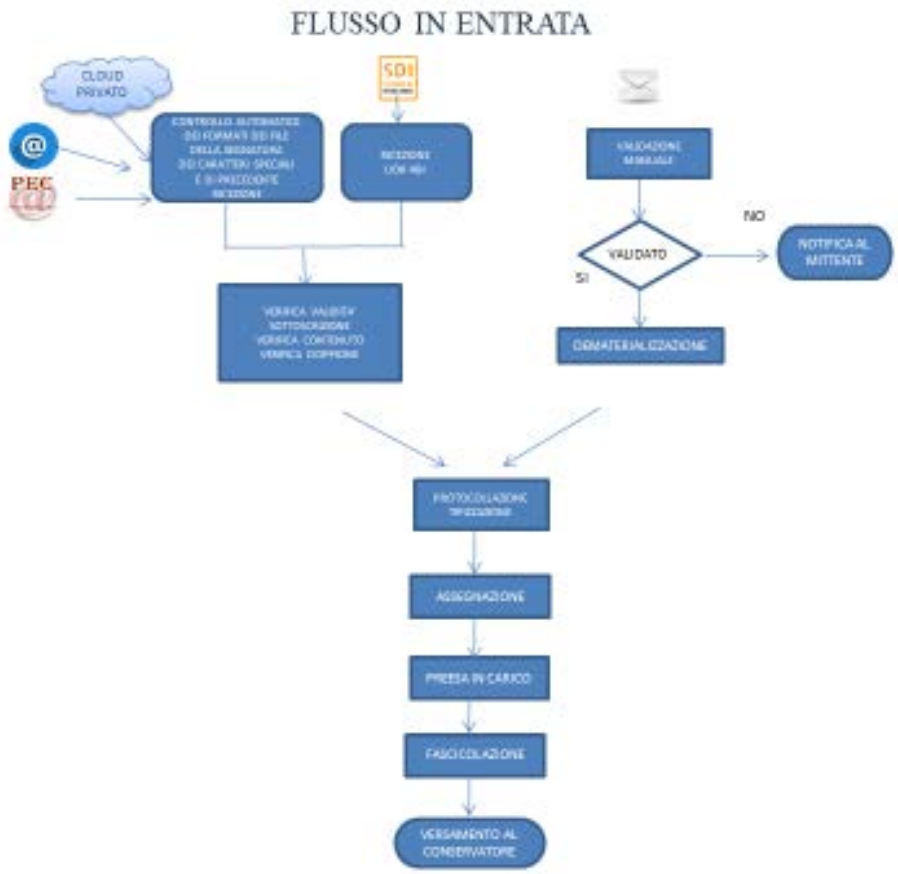
Al fine di fronteggiare situazioni emergenziali, che comportino la momentanea o prolungata interruzione degli ordinari servizi di gestione documentale, erogati tramite la rete internet, il Responsabile della gestione documentale predispone l'implementazione di postazioni *stand alone.*

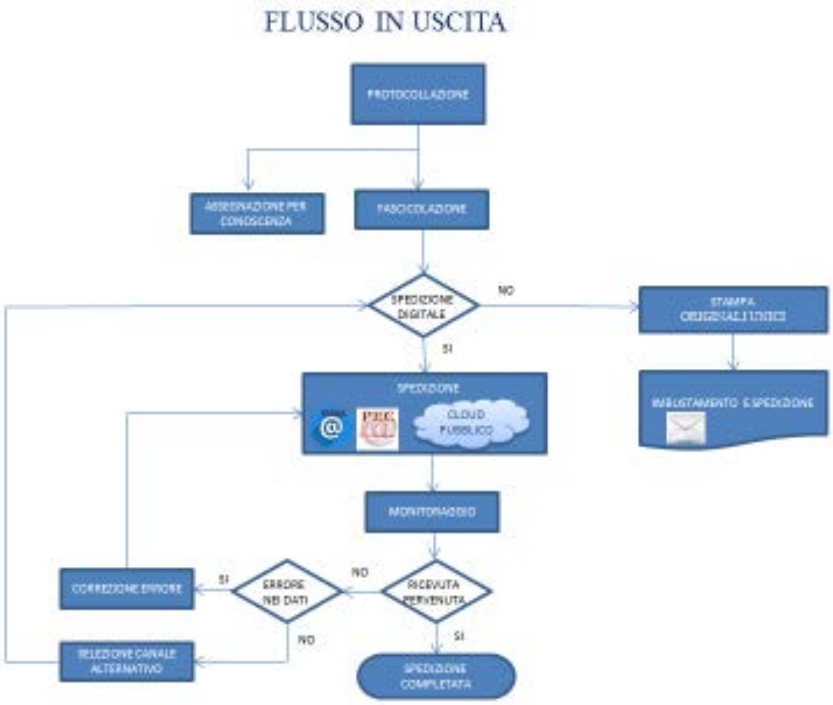
Con tali postazioni viene assicurata la gestione del nucleo minimo del protocollo anche per i dati particolari e giudiziari.

Le registrazioni effettuate vengono conservate su unità removibili, per essere riversate, in date prestabilite, in un'area dedicata del server centrale del Dipartimento.

ALLEGATO N. 6

WORKFLOW




FLUSSO IN USCITA
PROTOCOLLAZIONE
ASSEGNAZIONE PER CONOSCENZA
FASCICOLAZIONE
SPEDIZIONE DIGITALE
NO
SI
STAMPA
SPEDIZIONE
CLOUD PUBBLICO
MONITORAGGIO
CORREZIONE ERRORE
SI
ERRORE NEI DATI
NO
RICEVUTA PERVENUTA
NO
SI
SELEZIONE CANALE ALTERNATIVO
SPEDIZIONE COMPLETATA

ALLEGATO N. 7

REGISTRO DEL CONTENZIOSO

Il registro raccoglie i metadati afferenti i contenziosi civili, penali ed amministrativi in cui è attore o convenuto il Dipartimento, nonché le attività extragiudiziali, senza soluzione di continuità a far data dall'anno 2007.

Ogni registrazione individuata con numerazione progressiva annuale, attribuita automaticamente dal sistema, riporta i nomi dei ricorrenti, la tipologia della pratica, l'oggetto, la data di scadenza, il tipo di giudizio, l'organo giudicante, l'esito, il funzionario incaricato del procedimento, il numero di protocollo del documento correlato.

È possibile eseguire ricerche mirate utilizzando come filtri il tipo e il grado di giudizio, il nome dei ricorrenti, l'organo giudicante.

Le registrazioni sono correlate ai fascicoli.

Il registro viene inviato annualmente in conservazione.

REGISTRO FOIA

Il registro è stato realizzato in conformità alle indicazioni operative contenute nella circolare n.2/2019 del Dipartimento della Funzione pubblica.

Lo scopo del registro è duplice: a) consolidare una buona prassi amministrativa che orienti all'efficace trattamento delle richieste; b) monitorare e analizzare le richieste e i relativi esiti.

Per la realizzazione del Registro si è adottato lo schema XSD-FOIA-RA-EXT-BULK, previsto dalla richiamata circolare.

I dati implementati nel registro vengono periodicamente estratti, previa anonimizzazione, ed inviati all'Ufficio del controllo interno della Presidenza del Consiglio per gli adempimenti di competenza.

Nel registro vengono riportati i seguenti metadati: n. istanza, attribuita automaticamente dal sistema Ge.Do.P., dati anagrafici del mittente, oggetto e data di ricevimento della richiesta; esiti dell'istruttoria (accoglimento, richieste di integrazione, parziale accoglimento, differimento, rigetto); dati identificativi della notifica ad eventuali controinteressati; l'eventuale riesame della richiesta di accesso da parte del Responsabile della prevenzione della corruzione e della trasparenza; gli eventuali ricorsi giurisdizionali di I e II grado.

Il Registro viene inviato in conservazione annualmente.

REGISTRO DELLE FATTURE

Il Registro raccoglie i metadati afferenti le fatture passive provenienti dal sistema di interscambio dell'Agenzia delle Entrate consistenti in:

a) numero identificativo automatico della registrazione;

b) numero di protocollo attribuito alla fattura;

c) dati anagrafici e fiscali del fornitore;

d) numero di fattura,

e) data di emissione della fattura,

f) oggetto della fattura;

g) riferimenti contrattuali (CIG, CUP, numero e data del contratto, RUP, UOR proponente), importo.

Il Registro viene inviato in conservazione annualmente.

REPERTORIO AMMINISTRATIVO

Il Repertorio raccoglie i metadati concernenti le determine a contrarre, i decreti di pagamento di vario titolo, decreti di nomina del personale interno o esterno (collaboratori/esperti).

Per ogni registrazione sono contemplati i seguenti metadati:

a) numero identificativo del documento;

b) numero identificativo automatico della registrazione;

c) beneficiario;

d) oggetto;

e) importo;

f) proponente;

g) RUP/DEC

h) stato della registrazione.

Il Registro viene inviato in conservazione annualmente.

REGISTRO DEGLI ANONIMI

Nel registro sono raccolti i metadati e i documenti provenienti da fonti anonime o non identificabili (nick name), in assenza assoluta di dati anagrafici e di contatto.

Per ogni registrazione sono contemplati i seguenti metadati:

a) numero identificativo del documento;

b) numero identificativo automatico della registrazione;

c) pseudonimo;

d) UOR interna assegnataria;

e) corrispondente esterno (in caso di inoltro ad altre amministrazioni);

f) esito istruttoria

Il Registro viene inviato in conservazione annualmente.

REGISTRO DEI CONTRATTI

Il Registro raccoglie tutti i metadati afferenti i contratti quali: il CIG, il nome del responsabile unico del procedimento, l'oggetto del contratto, i dati del contraente, la data di riferimento.

Ogni registrazione del repertorio è correlata alla scheda di protocollazione e all'oggetto-dati.

Possono essere eseguite operazioni massive quali: la sottoscrizione, la trasmissione e rimozione dall'area di lavoro dei documenti collegati.

Il Registro viene inviato in conservazione annualmente.

REGISTRO DEI RIMBORSI

Nel registro confluiscono i metadati concernenti la procedura dei rimborsi, quali: il numero identificativo, l'oggetto, la data, il numero di protocollo della richiesta.

Vengono, inoltre, tracciati gli atti prodotti dall'Ufficio del Volontariato e risorse del Servizio Nazionale in fase istruttoria (decretino, lettera di trasmissione per l'Ufficio

Amministrazione e bilancio) che costituiscono il presupposto del decreto e del mandato di pagamento, gestiti dall'Ufficio Amministrazione e Bilancio ai fini della liquidazione delle competenze accertate e consolidate.

Il Registro viene inviato in conservazione annualmente.

ALLEGATO N. 8

PIANO DI CONSERVAZIONE

MASSIMARIO DI CONSERVAZIONE E SCARTO

DOCUMENTAZIONE INELIMINABILE

1. Decreti istitutivi e di organizzazione.
2. Direttive della PCM.
3. Regolamenti.
4. Attestati di formazione.
5. Fascicoli del personale in servizio e in quiescenza, di ruolo e non di ruolo.
6. Ruoli riassuntivi del personale e libri matricola.
7. Libri infortuni o documentazione equivalente.
8. Assenze malattie e visite fiscali
9. Ordinanze e decreti di emergenza in originale; normativa di settore
10. Registri dei verbali e protocolli delle commissioni e dei comitati.12. Bilanci e consuntivi originali (o nell'unica copia esistente).
11. Contratti originali
12. Bandi, capitolati, gare e verbali di aggiudicazione
13. Verbali del fuori uso
14. Rilevazioni di carattere statistico
15. Originali dei verbali delle commissioni di concorso
16. Atti relativi ai lavori pubblici, eseguiti e non eseguiti, limitatamente a: originali dei progetti e dei loro allegati, perizie di spesa, libri delle misure, relazioni di collaudo.
17. Atti e documenti del contenzioso
18. Accessi procedimentali
19. Accessi procedimentali
20. Graduatorie, inquadramenti e riqualificazioni: decreto istitutivo, istruttorie e verbali della commissione esaminatrice
21. Verbali ed accordi sindacali
22. Visite mediche del personale e attestazioni di idoneità
23. Valutazione della dirigenza
24. Applicativi di protocollo informatico
25. Controllo di regolarità amministrativo-contabile atti non comportanti spesa
26. Repertorio CCNL e CCNQ (Contratto, delibera CdM, lettera ARAN) e relativa istruttoria
27. ANTICORRUZIONE E TRASPARENZA
28. Atti Organi consultivi e di *coordinamento* - Soggetti delegati
29. Atti Commissione per la previsione e prevenzione dei grandi rischi
30. Consulta nazionale del volontariato di protezione civile
31. Classificazione sismica
32. Microzonazione sismica
33. Vulnerabilità urbana
34. Atti concernenti le reti accelerometrica idropluviometrica
35. Atti osservatorio sismico delle strutture
36. Rete radar
37. Reti GPS

38. Reti centri funzionali
39. Rapporti post evento
40. Emergenze nazionali e internazionali
41. Esercitazioni nazionali e internazionali
42. Esercitazioni volontariato
43. Logistica di emergenza
44. Piani dei rischi (emergenza)
45. Eventi straordinari: pianificazione e gestione
46. Intese internazionali
47. Qualunque atto o documento per il quale una legge speciale imponga la conservazione illimitata

.

DOCUMENTAZIONE PER LA QUALE PUO' ESSERE PROPOSTO LO SCARTO

A - DOCUMENTAZIONE ELIMINABILE DOPO CINQUE ANNI

1. Pareri alla PA;
2. Lettere di rifiuto di partecipazione alle gare;
3. Copie di attestati di servizio;
4. Corrispondenza per commemorazioni e solennità civili;
5. Avvisi di convocazione delle commissioni;
6. Copie e minute dei progetti, sia realizzati che non;
7. Corrispondenza relativa alla manutenzione ordinaria e pulizia locale (conservando proposte di spesa, verbali di gara e contratti);
8. Corrispondenza relativa a sottoscrizione di abbonamenti a giornali e riviste e ad acquisto di pubblicazioni amministrative;
9. Corrispondenza relativa all'acquisto di arredi, dotazioni d'ufficio, e di materiale per la loro manutenzione (conservando verbali di gara, contratti);
10. Corrispondenza relativa all'acquisto di materiale di facile consumo (conservando verbali di gara e contratti);
11. Corrispondenza relativa all'acquisto di materiale di facile consumo (conservando verbali di gara e contratti);
12. Copie dei preventivi e dei consuntivi (conservando il progetto del bilancio e, caso per caso, la corrispondenza ad essi relativi);
13. Corrispondenza relativa al personale di comitati, commissioni e alla liquidazione dei loro compensi;
14. Corrispondenza per carico e scarico;
15. Visite fiscali dei dipendenti;
16. Modelli 740 (copia per il Dipartimento). I cinque anni decorrono dall'anno cui si applica la dichiarazione;
17. Avvisi meteo;
18. Direttive annuali per l'azione amministrativa e la gestione;
19. Adempimenti controllo di gestione;
20. Adempimenti contabilità analitica;
21. Budget dipartimentali;
22. Impegni;
23. Presentazione delle ditte;
24. Circolari;

25. UE e Parlamento europeo;
26. Patti, accordi e trattati;
27. Corsi di formazione: domande e partecipazione;
28. Organizzazioni e istituti italiani e internazionali;
29. Sviluppo software in house;

.

B – DOCUMENTAZIONE ELIMINABILE DOPO DIECI ANNI

1. Inviti alle sedute delle Commissioni e dei Comitati (conservando gli ordini del giorno con elenco dei destinatari, eventuali progetti e relazioni);
2. Atti dei concorsi, copie dei verbali della commissione giudicatrice, domande di partecipazione; copie di manifesti inviati ad altri enti e restituite, elaborati scritti e pratici, copie di avvisi diversi, copie di delibere;
3. Liquidazione delle missioni ai dipendenti, con relative tabelle di missione e documentazione allegata, salvo, se esistenti, prospetti generali;
4. Domande di concessione di contributi straordinari per calamità;
5. Atti relativi all'alienazione dei beni mobili fuori uso;
6. Mandati di pagamento e relativi allegati;
7. Fatture liquidate;
8. Scritture contabili obbligatorie in base alle leggi fiscali;
9. Documentazione generale per la richiesta di mutui, anche estinti;
10. Atti relativi all'acquisto di autoveicoli, aeromobili e alla loro manutenzione (conservando proposte di spesa, verbali di gara, contratti);
11. Matrici di bollettari per acquisto materiali di consumo;
12. Atti di controllo di gestione;
13. ordini di servizio, comandi;
14. Comunicazioni, campagne informative, comunicati stampa;
15. Seminari, convegni incontri;
16. Corrispondenza con cittadini;
17. Controllo strategico e di gestione con l'UCI;
18. Gestione documentale;
19. Atti di sindacato ispettivo;
20. gare e capitolati;
21. Rapporti Parlamento;
22. Rapporti UE;
23. Controllo di regolarità amministrativo-contabile atti comportanti spesa;
24. Acquisizione e assegnazione hardware;
25. Aran;
26. Formez – convenzioni;
27. Sspa – convenzioni;
28. Previdenza obbligatoria;
29. Pareri normativa di settore;
30. Gestione amministrativa flotta aerea;

C – DOCUMENTAZIONE ELIMINABILE DOPO VENT'ANNI

1. Diplomi originali di studio conservati nella documentazione relativa ai concorsi;
2. Certificazioni ditte;
3. Accesso civico e accesso civico generalizzato;
4. Prevenzione della corruzione;

5. Fogli di lavoro straordinario (originali, conservando eventuali prospetti riassuntivi), indennità, trattamenti accessori;
6. Gestione crisi cibernetiche;
7. PON GAT-Programma operativo nazionale Governance e assistenza tecnica;
8. ANTICORRUZIONE E TRASPARENZA;
9. Rischi naturali Atti di prevenzione;
10. Scenari di rischio;
11. Scenari di danno;
12. Piani dei rischi (prevenzione);
13. Segnalazioni;
14. Sopralluoghi;
15. Emergenze eventi territoriali;
16. Esercitazioni locali/regionali;
17. Rapporti con i gestori dei servizi essenziali e della viabilità;
18. Gestione tecnica della telefonia;
19. Gestione degli apparati e delle reti radio;
20. Sala regia;
21. Presidi informatici e supporto specialistico;
22. Sistema informativo territoriale;
23. Patrocini;
24. Benemerenze;
25. Relazioni Enti locali;
26. Visite istituzionali;
27. Iscrizioni Rimborsi e contributi alle organizzazioni di volontariato;
28. Formazione;
29. Gestione operativa flotta aerea;
30. Contabilità speciali.

Per il Titolario di Classificazione si rinvia a:
http://www.pcm.it/Informazione/Notizie/Notizia.asp?t_id=17378

.

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 D.Lgs 81/2008
Statistiche interne
Stime di danno
Studi di caratterizzazione dei siti
Valutazioni tecno-economiche
Verbali

ALLEGATO 9

SPESE PER L'ACCESSO

TIPOLOGIA	COSTO
Riproduzione - digitale in formato analogico - di documento analogico in formato digitale	- € 0,10 a facciata formato UNI A4 € 0,20 a facciata formato UNI A3 - € 0,10 a facciata formato UNI A4 € 0,20 a facciata formato UNI A3
Rimborso delle spese di ricerca e visura: - per l'accesso documentale -	a) oltre 1 e fino a 5 anni prima della richiesta di accesso: € 2,00; b) oltre 5 anni prima della richiesta di accesso: € 5,00
per l'accesso generalizzato	spese effettivamente sostenute e documentate

-

Per gli importi inferiori a € 3 non è dovuto alcun rimborso. Al di sopra di tale importo, viene riscossa l'intera cifra. Ai fini del rimborso, non è consentito frazionare la richiesta.
Nel caso di richiesta di rilascio di copia conforme, si applica l'imposta di bollo nella misura prevista dalla Tariffa allegato A al D.P.R. n. 642 del 1973. Al pagamento dell'imposta dovuta sull'istanza e sulla copia rilasciata provvede direttamente il richiedente.
L'eventuale supporto per la riproduzione in formato elettronico dei documenti, se non fornito dal richiedente, andrà rimborsato in base ai relativi costi sostenuti dall'amministrazione.
Per l'eventuale spedizione a mezzo posta, andrà rimborsato il relativo costo, secondo le tariffe applicate dall'operatore affidatario del servizio.

ALLEGATO N. 10

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 conformità 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) In assenza di indirizzo digitale 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). Si prega, pertanto, di individuare l'anagrafica appropriata, tenendo conto che il Ge.Do.P. seleziona automaticamente la prima scheda associata a tale indirizzo pec;

b) per ogni UOR dotata di indirizzo digitale autonomo, dovrà essere redatta 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;

Agenzia delle Entrate - Direzione Provinciale – Caserta - Ufficio territoriale - Aversa

- 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*,.