



CORTE DEI CONTI

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO

Versione 1.0

*Emanato il 10 ottobre 2016
Entrato in vigore il 30 dicembre 2016*

Autori del documento

Rosamaria Berté, Antonella Saddi, Gennaro Tortorelli, Maurizio Piacitelli, Erika Miglietta

*Responsabile della redazione:
Alessandra Madaro*

*Approvato da:
Michele Melchionda*

SOMMARIO	
GLOSSARIO5
CAPITOLO 1. IL MANUALE DI GESTIONE8
1.1. Che cos’è, a cosa serve e a chi serve	8
1.2. Modalità di redazione	8
1.3. Forme di pubblicità e di divulgazione	9
CAPITOLO 2. QUADRO ORGANIZZATIVO ISTITUZIONALE10
2.1. Area organizzativa omogenea e unità organizzativa responsabile	10
2.2. Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti	10
2.3. Coordinatore della gestione documentale/Responsabile della gestione documentale	10
2.4. Posta elettronica istituzionale (PEO).....	11
2.5. Posta Elettronica Certificata (PEC) istituzionale.....	11
2.6. Registri di protocollo	11
2.7. Responsabile della conservazione	12
CAPITOLO 3. IL DOCUMENTO	13
3.1. Documento informatico e analogico: definizione e disciplina giuridica.....	13
3.2. Redazione/formazione del documento informatico	15
3.2.1. Validazione temporale	16
3.2.2. Formati.....	17
3.3. Redazione/formazione del documento amministrativo informatico	18
3.4. Metadati.....	19
3.4.1. Obiettivi dei metadati archivistici	19
3.4.2. Metadati associati al documento informatico.....	19
3.5. Documenti redatti in originale su supporto analogico	20
3.6. Il documento amministrativo informatico costituito dal corpo della PEC istituzionale.....	21
3.7. Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale	21
3.8. Distinzione dei documenti in base allo stato di trasmissione	21
3.9. Duplicato del documento informatico	22
3.10. Copia del documento informatico e analogico: nozione.....	23
3.11. Copia informatica del documento amministrativo analogico	23
3.12. Estratto informatico di documento amministrativo informatico	24
3.13. Copia analogica di documento amministrativo informatico.....	25
CAPITOLO 4. IL FASCICOLO	25
4.1. Il fascicolo: definizione e funzione	25
4.2. Il fascicolo informatico: formazione, implementazione e gestione	26
4.3. I fascicoli annuali ripetitivi.....	26
4.4. Metadati del fascicolo informatico	27
4.5. Il repertorio dei fascicoli informatici	27
CAPITOLO 5. LA GESTIONE DEGLI ARCHIVI	29
5.1. Definizione	29
5.2. Concetti di base	29
5.3. Archivio personale	31
5.4. Archivio applicativo	32
5.5. Archivio istituzionale	33
5.6. Archivio di conservazione	34
5.7. La gestione documentale.....	35
5.8. Gli strumenti di gestione degli archivi	36
5.8.1. Strumenti per l’archivio personale.....	36



5.8.2.	Strumenti per l'archivio applicativo	36
5.8.3.	Strumenti per l'archivio istituzionale	36
5.8.4.	La tutela dei dati personali	37
5.8.5.	Registro di protocollo	37
5.8.6.	Titolario (piano di classificazione)	38
5.8.7.	Repertorio dei fascicoli	38
5.8.8.	Repertori	38
5.8.9.	Massimario di selezione	39
CAPITOLO 6. IL PROTOCOLLO INFORMATICO		40
6.1.	Protocollazione	40
6.1.1.	Elementi obbligatori immodificabili (Registratura)	41
6.1.2.	Elementi obbligatori modificabili	41
6.1.3.	Elementi non obbligatori modificabili	41
6.2.	Data e ora regolate sul UTC	42
6.3.	Segnatura	42
6.3.1.	Per il documento informatico	42
6.3.2.	Per il documento analogico	43
6.4.	Modalità di produzione e di conservazione delle registrazioni	44
6.5.	Annulloamento di una registrazione	44
6.6.	Protocollo differito	44
6.7.	La ricevuta di avvenuta protocollazione	45
6.8.	Documenti esclusi dalla protocollazione	45
6.9.	Il registro giornaliero di protocollo	46
6.10.	Il registro di emergenza	47
CAPITOLO 7. FLUSSO DI LAVORAZIONE DEI DOCUMENTI		48
7.1.	La norma in materia	49
7.2.	Documenti in ingresso	49
7.2.1.	Gestione dei flussi analogici residuali	50
7.2.2.	Flusso del documento informatico in entrata	51
7.2.3.	Ricezione di documenti informatici nella casella di posta elettronica (PEO) istituzionale	52
7.2.4.	Ricezione di documenti informatici su supporti rimovibili	53
7.2.5.	Ricezione dei documenti informatici tramite la casella di posta elettronica certificata (PEC) istituzionale	53
7.2.6.	Ricezione di PEC interoperante (contenente il file segnatura)	54
7.2.7.	Ricezione di documenti informatici da flussi informatici applicativi	54
7.3.	Documenti in uscita indirizzati ad un soggetto pubblico (interno o esterno) o privato e anche ai propri dipendenti come persone fisiche e non nell'esercizio delle loro funzioni	55
7.3.1.	Invio di comunicazioni a mezzo PEC	55
7.4.	Flusso di lavorazione dei documenti interni alla Cdc	57
7.4.1.	Flusso del documento informatico tra UO della stessa AOO	57
7.4.2.	Flusso del documento informatico tra AOO della Cdc	57
7.5.	Flusso di pubblicazione dei documenti sui siti web della Cdc	58
7.5.1.	Flusso di pubblicazione in home page e nelle pagine di interesse nazionale	58
7.5.2.	Flusso di pubblicazione nella sezione "Amministrazione trasparente"	59
7.5.3.	Flusso di pubblicazione nelle sezioni regionali	60
7.5.4.	Flusso di pubblicazione sul sito web Biblioteca	60
7.5.5.	Flusso di pubblicazione sul sito Rivista web	60
7.5.6.	Flusso di pubblicazione sul sito intranet	61
7.5.7.	Gestione delle eccezioni	61
CAPITOLO 8. PROCEDURE PARTICOLARI		63
8.1.	Gestione delle gare d'appalto	63

8.1.1.	Gare e procedure negoziate gestite in modalità telematica	63
8.2.	Gestione di concorsi e selezioni	63
8.3.	Fatture elettroniche (Fattura PA)	63
8.4.	DURC on-line.....	65
8.5.	Certificati di malattia.....	65
8.6.	Documenti del portale degli acquisti della Pubblica Amministrazione	65
8.6.1.	Affidamenti diretti sulla piattaforma MePA (OdA)	66
8.6.2.	Adesioni – Convenzioni (OdA).....	67
8.6.3.	Procedure negoziate (RdO) - MePA.....	67
8.7.	Gestione del secondo esemplare	68
8.8.	Documenti anonimi	68
CAPITOLO 9. IL SISTEMA INFORMATICO		69
9.1.	Il modello organizzativo	69
9.2.	La conduzione operativa	71
9.3.	Sicurezza del sistema informatico	71
9.3.1.	Il sistema di gestione documentale.....	72
9.3.2.	Sicurezza fisica dei data center.....	73
9.3.3.	La manutenzione e la continuità operativa degli impianti elettrici	74
9.3.4.	Rete dati	74
9.3.5.	Le postazioni di lavoro	74
9.4.	Sicurezza dei documenti informatici.....	75
9.4.1.	Accesso e profili di abilitazione ai dati e ai documenti informatici	77
CAPITOLO 10. ALLEGATI.....		81
10.1.	Allegato 1: Riferimenti normativi	81
10.2.	Allegato 2: AOO – UO	83
10.3.	Allegato 3: Riferimenti normativi interni	88
10.4.	Allegato 4: Titolario	89
10.4.1.	Titolario Amministrazione attiva.....	89
10.4.2.	Titolario Sezioni controllo regionali	93
10.4.3.	Titolario Segreterie dei Presidenti delle Sezioni di Controllo regionali	96
10.4.4.	Titolario Segreterie dei Presidenti delle Sezioni di Giurisdizionali regionali	97
10.4.5.	Titolario Procuratori regionali.....	97
10.4.6.	Titolario Segretariato Generale	98
10.5.	Allegato 5: Registri e Repertori Informatici.....	106
10.5.1.	Repertorio - Nozione	106
10.5.2.	Repertori attivi	106
10.5.3.	Repertorio dei fascicoli.....	106



GLOSSARIO

Definizioni

Definizione	Descrizione
Copia di documento informatico	La copia di un documento informatico è un documento informatico che, mediante processi e strumenti adeguati, assicura la corrispondenza della copia alle informazioni del documento informatico di origine attraverso l'utilizzo di uno dei formati idonei ai sensi della normativa vigente.
Documento amministrativo	Qualsiasi rappresentazione, comunque formata, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una Pubblica Amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica.
Documento analogico	Il documento analogico è la rappresentazione non informatica, di atti, fatti o dati giuridicamente rilevanti. Qualsiasi documento non informatico (ad es., un documento cartaceo) è, dunque, un documento analogico.
Documento elettronico	“Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva” (definizione eIDAS).
Documento informatico	Il documento informatico è il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Fascicolazione	La fascicolazione è l'attività di riconduzione logica (e, nel caso di documenti cartacei, anche fisica) di un documento all'interno dell'unità archivistica che ne raccoglie i precedenti, al fine di mantenere vivo il vincolo archivistico che lega ogni singolo documento alla pratica relativa. Tale attività permette di costruire un sistema basato sull'organizzazione funzionale dei documenti in unità complesse stabili nel tempo (i fascicoli), che riflettono la concreta attività del soggetto produttore. La classificazione e la fascicolazione favoriscono la sedimentazione stabile dei documenti prodotti e acquisiti dall'Amministrazione nel corso della propria attività: solo così si assicura la possibilità per l'Amministrazione stessa e per il cittadino di accedere ad una informazione contestualizzata, che dia conto del patrimonio informativo utilizzato a supporto di una determinata attività amministrativa (definizione AgID).
Firma elettronica	La Firma Elettronica è definita dal CAD come l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
Firma elettronica avanzata	La Firma Elettronica Avanzata (FEA) è l'insieme di dati in forma elettronica, allegati oppure connessi a un documento informatico, che consentono l'identificazione del firmatario del documento. La FEA garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo,



Definizione	Descrizione
	collegata ai dati ai quali detta firma si riferisce in modo da consentire il rilevamento in caso di successive modifiche dei dati (definizione AgID).
Firma elettronica qualificata	La Firma Elettronica Qualificata (FEQ) garantisce tutte le caratteristiche della Firma Elettronica Avanzata e inoltre è basata su un certificato qualificato (rilasciato da un Certificatore accreditato dall'AgID). Nell'utilizzo della FEQ, il firmatario deve utilizzare un dispositivo sicuro con le caratteristiche identificate dalla norma (definizione AgID).
Manuale di gestione	Il manuale di gestione è uno strumento operativo che descrive il sistema di produzione e di gestione documenti (tradizionali e digitali), come previsto dall'art. 3 e dall'art. 5 del DPCM 3 dicembre 2013. Nel presente manuale è solo incidentalmente indicato il trattamento dei documenti non digitali, considerandoli residuali rispetto alla maggioranza costituita dai documenti digitali.
Protocollazione	Apposizione o associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.
Registratura	L'insieme degli elementi obbligatori immodificabili che servono ad attribuire al documento data e provenienza certa. Sono informazioni rilevanti sul piano giuridico-probatorio.
Validazione temporale elettronica	Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento.
Validazione temporale elettronica qualificata	Validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS.
Workflow	Flusso di lavoro; serie di obiettivi e compiti interni a un'organizzazione, svolti al fine di produrre un risultato finale.

Acronimi

Nome	Descrizione
ACL	Access Control List
AD	Microsoft Active Directory
ADFS	Microsoft Active Directory Federation Services
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
BCP	Business Continuity Plan
BYOD	Bring Your Own Device
CAD	Codice dell'Amministrazione Digitale
CAdES	CMS Advanced Electronic Signatures
Cdc	Corte dei conti
CeDeCU	Centro di Dematerializzazione e Conservazione Unico della Difesa



Nome	Descrizione
CO	Continuità Operativa
DGSIA	Direzione Generale Sistemi Informativi Automatizzati
DocsPA	Sistema per la gestione del protocollo informatico
DPCM	Decreto del Presidente del Consiglio dei Ministri
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DURC	Documento Unico di Regolarità Contributiva
eIDAS	electronic IDentification Authentication and Signature
INRiM	Istituto Nazionale di Ricerca Metrologica
IPA	Indice delle Pubbliche Amministrazioni
MePA	Mercato Elettronico Pubblica Amministrazione
OdA	Ordine di Acquisto
PAdES	PDF Advanced Electronic Signatures
PEC	Posta elettronica certificata
PEO	Posta elettronica ordinaria
RdO	Richiesta di Offerta
RGS	Ragioneria Generale dello Stato
RPA	Responsabile Procedimento Amministrativo
RPO	Restore Point Objective
RTI	Raggruppamento Temporaneo di Imprese
RTO	Recovery Time Objective
s.m.i.	Successive modificazione e integrazioni
SDAPA	Sistema Dinamico di Acquisizione della P.A.
SdI	Sistema di interscambio
SGCUS	Servizio per la Gestione del Centro Unico dei Servizi
SIAP	Sistema Informativo Amministrazione del Personale
SICOGE	Sistema Informativo per la gestione integrata della contabilità economica e finanziaria
SIGI	Sistema Informativo Gestione Iniziative
SPC	Sistema Pubblico di Connattività
UO	Unità Organizzativa
UPS	Uninterruptible Power Supply - Gruppo statico di continuità
UTC	Tempo universale coordinato
XML	eXtensible Markup Language



CAPITOLO 1. IL MANUALE DI GESTIONE

1.1. Che cos'è, a cosa serve e a chi serve

Il manuale di gestione è uno strumento operativo che descrive il sistema di produzione e di gestione dei documenti digitali, come previsto dall'art. 3 e dall'art. 5 del DPCM (Decreto del Presidente del Consiglio dei Ministri) 3 dicembre 2013¹.

Serve a indicare le procedure e a fornire le istruzioni per la corretta formazione, gestione, tenuta e conservazione della documentazione digitale. Esso descrive, altresì, le modalità di gestione dei flussi documentali e degli archivi, in modo tale da organizzare e governare la documentazione ricevuta, inviata o comunque prodotta dall'Amministrazione secondo parametri di corretta registrazione di protocollo, smistamento, assegnazione, classificazione, fascicolatura, reperimento e conservazione dei documenti. Solo incidentalmente è indicato il trattamento dei documenti non digitali, considerandoli residuali rispetto alla maggioranza costituita dai documenti digitali.

Il manuale di gestione costituisce una guida per chiunque all'interno dell'Amministrazione gestisca documenti digitali, al fine di porre in essere le corrette operazioni di gestione documentale. Tale manuale costituisce, altresì, una guida per cittadini, imprese e Amministrazioni che intrattengono rapporti con la Corte dei conti (Cdc) per comprendere e collaborare nel flusso di gestione documentale (ad es., utilizzando formati idonei per la formazione delle istanze, ecc.).

1.2. Modalità di redazione

La redazione del manuale di gestione deve contemplare l'assolvimento dell'obbligo normativo e le esigenze concrete dell'Amministrazione (si vedano l'Allegato 1: Riferimenti normativi e l'Allegato 3: Riferimenti normativi interni).

Ispirandosi ai manuali proposti dall'Università degli Studi dell'Insubria e dal Gruppo di lavoro nell'ambito del progetto *Procedamus* per gli atenei aderenti (www.procedamus.it) il presente documento è stato redatto previa verifica e analisi del modello organizzativo e delle procedure amministrative della Cdc.

¹ Il legislatore ha approvato due DPCM 3 dicembre 2013, contenenti entrambi le regole tecniche previste dall'art. 71 del CAD (D.Lgs. 7 marzo 2005, n. 82) ed entrambi pubblicati nella Gazzetta ufficiale 12 marzo 2014, n. 59 – SO n. 20. Il primo contiene le *Regole tecniche in materia di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*, mentre il secondo contiene le *Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*. Se non diversamente indicato, in questo manuale si fa riferimento al secondo, citato semplicemente come DPCM 3 dicembre 2013.

1.3. Forme di pubblicità e di divulgazione

Il manuale di gestione è reso pubblico mediante la diffusione sul sito istituzionale, come previsto dal DPCM 3 dicembre 2013, art. 5, comma 3. Deve, inoltre, essere capillarmente divulgato alle unità organizzative responsabili (UO) delle Aree Organizzative Omogenee (AOO) dell'Amministrazione, al fine di consentire la corretta diffusione delle nozioni e delle procedure documentali e di favorire la necessaria collaborazione di cui al paragrafo 1.1.

È prevista, infine, un'attività di formazione continua e permanente in materia di gestione documentale per tutte le UO dell'Amministrazione.



CAPITOLO 2. QUADRO ORGANIZZATIVO ISTITUZIONALE

2.1. Area organizzativa omogenea e unità organizzativa responsabile

L'AOO è l'insieme di strutture individuate dall'Amministrazione cui sono assegnate funzioni omogenee. Essa, pertanto, presenta esigenze di gestione documentale in modo unitario e coordinato, ai sensi della normativa vigente.

La Cdc è organizzata nelle AOO istituite a livello centrale e regionale con decreto del Presidente del 22 maggio 2014 e riportate nell'Allegato 3: Riferimenti normativi interni, come previsto dalla legge 7 agosto 1990, n. 241 (artt. 4-6), dal DPR 28 dicembre 2000, n. 445 e dal DPCM 3 dicembre 2013, art. 3, comma 1, lett. a).

All'interno di ciascuna AOO è stato individuato il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa – DPR n. 445 del 20 dicembre 2000. In particolare, il Servizio suddetto è anche titolare della casella di posta certificata istituzionale associata all'AOO.

Le AOO e le UO ad essa afferenti sono descritte, unitamente alle altre informazioni richieste, nell'Indice delle Pubbliche Amministrazioni - IPA. È compito del Referente IPA dell'Ente provvedere all'accreditamento, alla trasmissione delle informazioni richieste dalla legge e all'aggiornamento senza ritardo dei dati nel sito IPA.

2.2. Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti

Il servizio per la tenuta del protocollo informatico, come da Decreto Presidenziale n. 24 del 22 maggio 2014, viene individuato all'interno di ciascuna AOO.

Il servizio di gestione del protocollo centrale presso il Segretariato Generale si occupa esclusivamente della protocollazione di decreti e circolari del Segretario Generale, decreti e ordinanze del Presidente, atti del Direttore Generale della Direzione Generale Gestione Risorse Umane e Formazione e del protocollo riservato del Segretario Generale.

Nel caso in cui un documento pervenga alla sede centrale indirizzato genericamente alla Cdc, il servizio di gestione del protocollo centrale presso il Segretariato Generale verifica il contenuto e lo smista alla competente AOO/UO per la protocollazione.

2.3. Coordinatore della gestione documentale/Responsabile della gestione documentale

Come previsto dalla normativa vigente in materia (vedi Allegato 1: Riferimenti normativi), le Amministrazioni devono nominare, in ciascuna delle AOO, il Responsabile della gestione documentale, e un suo vicario, per casi di vacanza, assenza o impedimento del primo. Le Amministrazioni con più AOO devono inoltre nominare il Coordinatore della gestione documentale e un suo vicario per i casi di vacanza, assenza o impedimento del primo.



E' compito del Coordinatore della gestione documentale e dei Responsabili della gestione documentale per le rispettive AOO di competenza:

- definire e assicurare criteri uniformi di trattamento dei documenti e di classificazione e archiviazione, nonché di comunicazione interna tra le AOO;
- predisporre e mantenere aggiornato il manuale di gestione;
- predisporre, di concerto con il Responsabile della conservazione, il Responsabile dei sistemi informativi e il Responsabile del trattamento dei dati personali, il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici secondo quanto dettagliato al paragrafo 9.3;
- produrre il pacchetto di versamento e assicurare il trasferimento del suo contenuto al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione.

Il Coordinatore della gestione documentale è coadiuvato dal Referente dei sistemi informatici documentali e della sicurezza informatica e dal Referente della protezione dei dati personali relativamente al sistema documentale come previsto dal D.Lgs. 7 marzo 2005, n. 82 e s.m.i. (successive modifiche e integrazioni).

2.4. Posta elettronica istituzionale (PEO)

Ogni AOO è dotata della casella istituzionale di posta elettronica.

Tutti i dipendenti sono dotati di una casella di posta elettronica istituzionale.

L'utilizzo delle casella istituzionale di posta elettronica è regolamentato dalla circolare DGSIA (Direzione Generale Sistemi Informativi Automatizzati) del 04 luglio 2013.

2.5. Posta Elettronica Certificata (PEC) istituzionale

La Cdc ha attivato una o più caselle PEC per ogni AOO; sono state inoltre istituite ulteriori PEC per ufficio per specifiche esigenze e altre sono associate a ruoli apicali. L'elenco delle caselle PEC attive deve essere tenuto aggiornato sull'IPA.

Sono state emanate le regole tecniche e operative per l'utilizzo della PEC nei giudizi innanzi alla Cdc (Circolare 52 dell'ottobre del 2015 emanata dal Segretariato Generale).

Il dettaglio dell'assegnazione è riportato nella circolare 8 del 31 gennaio 2012 e nella circolare 31 del 17 giugno 2016 entrambe emanate dal Segretariato Generale.

2.6. Registri di protocollo

In Cdc sono stati eliminati tutti i registri cartacei di settore in quanto ad ogni AOO è associato un registro di protocollo informatico.

La registrazione dei documenti avviene mediante il sistema di protocollo informatico, ad esclusione dei protocolli riservati per la corrispondenza con i vertici istituzionali.



2.7. Responsabile della conservazione

La Cdc secondo quanto previsto dall'art. 5 del DPCM 3 dicembre 2013 "Regole tecniche in materia di sistema di conservazione..", ha affidato ad un soggetto esterno (Aruba Pec) il servizio di conservazione.

L'Istituto ha, altresì, attivato un accordo di servizio per la conservazione con il Centro di Dematerializzazione e Conservazione Unico della Difesa (CeDeCU).

Con il decreto 84 del 4 novembre 2015 del Segretario Generale, è stato nominato il Responsabile della conservazione a cui sono stati affidati contestualmente i compiti di coordinamento per le attività propedeutiche all'utilizzo del Servizio di conservazione, nelle more della completa attuazione delle norme relative alla conservazione dei documenti informativi, secondo i principi e le regole tecniche attualmente in vigore.



CAPITOLO 3. IL DOCUMENTO

3.1. Documento informatico e analogico: definizione e disciplina giuridica

Il presente manuale fornisce anche indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno e all'esterno delle AOO. Prima di entrare nel merito, occorre caratterizzare l'oggetto di tale scambio: il documento amministrativo.

Ai sensi dell'articolo 22 comma 1, lett. d della Legge n.241/1990, per documento amministrativo si intende ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una Pubblica Amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale. Questa sezione evidenzia le caratteristiche dei documenti amministrativi, il criterio di formazione, le modalità di sottoscrizione e la loro protocollabilità.

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

- ricevuto;
- inviato;
- interno formale;
- interno informale.

Il documento amministrativo oggetto di scambio, in termini tecnologici, è così classificabile:

- informatico;
- analogico.

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Il documento informatico è, quindi, un *file*, cioè una sequenza determinata di valori binari indipendente dal supporto fisico su cui è memorizzata.

Il documento analogico è la rappresentazione non informatica, di atti, fatti o dati giuridicamente rilevanti. Qualsiasi documento non informatico (ad es., un documento cartaceo) è, dunque, un documento analogico.

A differenza del documento analogico, che si caratterizza per la pluralità di forme (scrittura privata, atto pubblico, scrittura privata autenticata) che ne sostanziano il diverso valore giuridico-probatorio, il documento informatico si caratterizza per la pluralità di firme elettroniche (con il valore di sottoscrizione, firma, sigla o visto), che caratterizzano e diversificano l'efficacia giuridico-probatoria del documento.

La firma elettronica non è, infatti, la rappresentazione informatica grafica della firma, ma un meccanismo di associazione di dati per l'imputazione di effetti giuridici in capo a un determinato soggetto che ne risulta l'autore.

L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono valutabili in giudizio tenuto conto delle caratteristiche oggettive

di qualità, sicurezza, integrità e immodificabilità. Il documento informatico assume la caratteristica di immodificabilità se prodotto in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

Il documento informatico può essere sottoscritto con firma **elettronica, avanzata, qualificata**²: il tipo di firma utilizzata differenzia il valore giuridico del documento, secondo le norme previste dalla legge, in conformità con quanto stabilito dal Regolamento eIDAS (electronic IDentification Authentication and Signature) - **Regolamento UE n° 910/2014 sull'identità digitale** – che ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri. Il Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno che abroga la direttiva 1999/93/CE, è in vigore in tutta la UE dal 1 luglio 2016. Il regolamento permette di adottare a livello europeo un quadro tecnico-giuridico omogeneo e interoperabile nei campi più importanti e distintivi della digitalizzazione a norma: firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici-informatici, i servizi di raccomandata elettronica e i servizi di certificazione per autenticazione web.

Alla definizione di documento informatico quale rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, si accosta la definizione, ripresa dal Regolamento eIDAS, di documento informatico come: “*qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva*”. Esso stabilisce, di conseguenza, la non discriminazione dei documenti elettronici rispetto ai documenti cartacei, principio pienamente condiviso dall'Amministrazione.

Il documento informatico privo di sottoscrizione è una copia informatica, come tale forma piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime (2712 cc, 23 quater CAD, 2713 cc).

Il documento informatico sottoscritto con firma elettronica semplice è liberamente valutabile dal giudice sia per quanto riguarda l'efficacia giuridica che per quanto riguarda l'efficacia probatoria tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Il documento informatico sottoscritto con firma avanzata, se formato nel rispetto delle regole tecniche che garantiscono l'identificabilità dell'autore, l'integrità e l'immodificabilità, al pari di una scrittura privata, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta, se colui contro il quale è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta.

Il documento informatico sottoscritto con firma qualificata, se formato nel rispetto delle regole tecniche che garantiscono l'identificabilità dell'autore, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta. L'utilizzo del dispositivo si presume riconducibile al titolare, salvo che questi ne dia prova contraria³.

² In Cdc è disponibile la firma qualificata.

³ Rif. CAD art. 20-21-22-23.

L'associazione a un documento informatico di una firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione; tuttavia le firme elettroniche qualificate, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.⁴

Tutte le scritture private se stipulate sotto forma di documento informatico, devono essere sottoscritte a pena di nullità, salvo i casi di firma autenticata, con firma elettronica qualificata.

Gli altri atti per cui la legge prevede obbligatoriamente la forma scritta soddisfano tale requisito se sottoscritti con firma elettronica avanzata qualificata. Si precisa che tutti i contratti stipulati dalla Pubblica Amministrazione, anche quando quest'ultima agisce *iure privatorum*, richiedono la forma scritta *ad substantiam*⁵.

3.2. Redazione/formazione del documento informatico

Il documento informatico è formato mediante una delle seguenti principali modalità:

- a) redazione tramite l'utilizzo di **appositi strumenti software**: in tal caso il documento informatico assume le caratteristiche di immodificabilità e di integrità con la sottoscrizione con firma elettronica, avanzata o qualificata o con l'apposizione di una validazione temporale o con il trasferimento a soggetti terzi con PEC con ricevuta completa o con la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza o con il versamento ad un sistema di conservazione;
- 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: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;
- c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso appositi moduli resi disponibili all'utente: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dalla corretta esecuzione dell'operazione di registrazione e dall'esito della medesima unitamente all'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log inerenti le transazioni

⁴ Rif. CAD art. 21.

⁵ Art. 32, comma 14 del d.lgs 50/2016 che recita: "Il contratto è stipulato, a pena di nullità, con atto pubblico notarile informatico, ovvero, in modalità elettronica secondo le norme e per ciascuna stazione appaltante, in forma pubblica amministrativa a cura dell'Ufficiale rogante della stazione appaltante o mediante scrittura privata; in caso di procedura negoziata ovvero per gli affidamenti di importo non superiore a 40.000 euro mediante corrispondenza secondo l'uso del commercio consistente in un apposito scambio di lettere, anche tramite posta elettronica certificata o strumenti analoghi negli altri Stati membri".



- o i processi informatici utilizzati, ovvero con la produzione di una estrazione **statica** dei dati e il trasferimento della stessa nel sistema di conservazione;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dalla corretta esecuzione dell'operazione di registrazione e dall'esito della medesima unitamente all'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei *log* inerenti la particolare operazione informatica afferente la generazione o il raggruppamento di un insieme di dati o registrazioni, ovvero con la produzione di una estrazione **statica** dei dati e il trasferimento della stessa nel sistema di conservazione.

3.2.1. Validazione temporale

Il Regolamento UE eIDAS introduce due definizioni afferenti la validazione temporale:

- **validazione temporale elettronica**, dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;
- **validazione temporale elettronica qualificata**, una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS.

La validazione temporale elettronica dà luogo a una presunzione legale relativa alla certezza della data e dell'ora. Essa è normata dagli articoli 41 e 42 del Regolamento eIDAS:

- Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata.
- Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.
- Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri.

Una validazione temporale elettronica qualificata soddisfa i requisiti seguenti:

- collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati;
- si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato;
- è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.

Costituiscono validazione temporale:

- i riferimenti temporali realizzati dai certificatori accreditati mediante marche temporali;
- i riferimenti temporali apposti sul “giornale di controllo” da un certificatore accreditato secondo la scala di tempo nazionale italiana UTC (IT), in base alle indicazioni dell’Istituto nazionale di ricerca metrologica – INRIM, con una differenza non superiore ad un minuto primo;
- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una Pubblica Amministrazione;
- il riferimento temporale ottenuto attraverso l’utilizzo di PEC;
- il riferimento temporale ottenuto attraverso l’utilizzo della marcatura postale elettronica.

3.2.2. Formati

L’Amministrazione usa per la formazione e per la gestione dei documenti informatici le tipologie di formato di seguito riportate coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico e tali da garantire i principi di interoperabilità tra i sistemi di conservazione in base alla normativa vigente.

La scelta del formato è stata effettuata considerando che essa, come da previsione normativa, deve garantire la leggibilità e la reperibilità del documento informatico nell’intero ciclo di vita dello stesso; pertanto nella scelta si è valutata l’apertura, la sicurezza, la portabilità, la funzionalità, il supporto allo sviluppo e la diffusione dello stesso.

Per tale motivo, sono considerati utilizzabili i seguenti formati standard:

- Testo = Docx; Ods; Pdf/a;
- Calcolo = Xlsx; Odt;
- Immagini = Jpg; Tiff;
- Suoni = Mp3;
- Video = Avi;
- Dati = XML (eXtensible Markup Language);
- Archiviazione e compressione = Zip;
- Formati e-mail = RFC 2822/MIME.

I file .zip devono contenere file in formato ammesso.



3.3. Redazione/formazione del documento amministrativo informatico

Il documento amministrativo è qualsiasi rappresentazione, comunque formata, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una Pubblica Amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica.

Il documento amministrativo può assumere la forma di documento informatico o analogico.

Le Pubbliche Amministrazioni formano gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici disponibili, descritti in questo manuale ovvero acquisendo le istanze, le dichiarazioni e le comunicazioni previste dalla legge.

Gli atti formati dalle Pubbliche Amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria e originale da cui è possibile effettuare duplicazioni e copie.

Il documento amministrativo informatico e le istanze, le dichiarazioni e le comunicazioni previste dalla legge sono soggette, ove necessario, a registrazione di protocollo, segnatuta, fascicolatura e repertorizzazione.

Il documento amministrativo informatico, contenuto nel sistema di gestione documentale, assume le caratteristiche di immodificabilità e di integrità oltre che nei modi descritti in precedenza, anche con la registrazione nel registro di protocollo unico per ciascuna AOO.

Il documento amministrativo informatico deve, di norma, contenere la denominazione dell'Amministrazione e l'indicazione di:

- AOO/UO;
- Sottoscrizione e data di sottoscrizione;
- Classificazione (vedi anche CAPITOLO 7);
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati se presenti (indicare 0 *zero* se non presenti);
- Oggetto;
- Destinatario;
- Testo;
- Redattore;
- Elementi identificativi del responsabile del procedimento.

Il documento è sottoscritto prima di essere protocollato.

Le informazioni relative alla classificazione atte a identificare il fascicolo di competenza, la data di sottoscrizione, il numero di allegati sono inserite prima della sottoscrizione del documento.

Di norma, la data di sottoscrizione e la data di protocollazione coincidono.



3.4. Metadati

La codifica dell'informazione digitale, a differenza di altre, non è mai né auto-sufficiente né auto-esplicativa, ma deve sempre e necessariamente documentare se stessa al livello minimo del singolo *atomo* di informazione, aggiungendo al dato/contenuto vero e proprio molte informazioni necessarie per la decodifica, l'identificazione, il recupero, l'accesso e l'uso⁶. Nel contesto degli oggetti digitali il termine metadati può essere associato a tre categorie funzionali:

- *Descrittiva*: ha lo scopo di facilitare il recupero e l'identificazione dell'oggetto digitale;
- *Gestionale*: ha lo scopo di supportare la gestione dell'oggetto digitale all'interno di una collezione;
- *Strutturale*: ha lo scopo di collegare fra loro i componenti di oggetti informativi complessi.

3.4.1. Obiettivi dei metadati archivistici

Gli obiettivi dei metadati archivistici sono:

- garantire l'identificazione permanente dei singoli oggetti informativi, ad es.: identificativo univoco (numero di protocollo, data, autore, ecc.);
- garantire l'identificazione permanente delle relazioni tra gli oggetti informativi, ad es.: indici di classificazione e fascicolatura;
- conservare le informazioni che supportano l'intellegibilità degli oggetti informativi, ad es.: procedimento amministrativo cui il documento è connesso.

3.4.2. Metadati associati al documento informatico

Gli elementi essenziali minimi (definiti metadati) associati al documento informatico sono i seguenti (rif. Art. 3 DPCM 13 novembre 2014⁷):

- a) l'identificativo univoco e persistente;
- b) il riferimento temporale;
- c) l'oggetto;

⁶ L'oggetto digitale (*data object*) in ambito Open Archive Information System è un «oggetto costituito da un insieme di sequenze di bit» e costituisce un oggetto informativo sempre e soltanto se in congiunzione con «le informazioni sulla sua rappresentazione».

⁷ Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle Pubbliche Amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

- d) il soggetto/i che ha/hanno l'autorità e la competenza a produrre il documento informatico (Nome, Cognome, Codice Fiscale);
- e) gli eventuali destinatari (Nome e Cognome/Denominazione, Codice Fiscale/P. IVA);
- f) l'impronta del documento informatico.

A questi si aggiungono i seguenti metadati ritenuti obbligatori per la gestione dei documenti all'interno dell'Amministrazione:

- g) il numero degli allegati e, facoltativamente, il codice identificativo di ogni allegato e la relativa descrizione;
- h) la classificazione del documento (classe di appartenenza);
- i) la data di validità;
- j) il periodo di validità del documento (anni);
- k) la destinazione dopo la scadenza del periodo di validità (stringa);
- l) il codice identificativo dell'eventuale fascicolo di appartenenza del documento;
- m) l'indicazione della AOO e dell'eventuale UO di appartenenza del soggetto di cui alla lettera "d";
- n) indicazioni sul diritto di accesso (di utenti o gruppi di utenti) ad ogni singolo documento (ACL).

Al documento informatico immodificabile vengono associati i metadati indicati che sono stati generati durante il relativo procedimento di formazione.

3.5. Documenti redatti in originale su supporto analogico

Ai sensi del DPCM 21 marzo 2013, per particolari tipologie di documenti analogici originali unici, 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.

Per documenti originali unici si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta (ad es., i verbali di una riunione o di un'assemblea).

Pertanto, tutti i documenti su cui vengono apposti manualmente dati di registrazione a protocollo, sigle e firma autografa (che non sono sottoscritti con firma elettronica, semplice o avanzata), sono documenti amministrativi analogici.



3.6. Il documento amministrativo informatico costituito dal corpo della PEC istituzionale

La posta elettronica certificata costituisce un mezzo di comunicazione che consente lo scambio di informazioni e documenti le cui trasmissioni e ricezioni sono giuridicamente rilevanti.

Tale modalità di trasmissione dei documenti viene utilizzata nei casi in cui è necessario avere prova opponibile dell'invio e della consegna del messaggio di posta.

Il documento trasmesso/ricevuto con PEC ha lo stesso valore legale della raccomandata con avviso di ricevimento. In tal caso, l'avvenuta consegna del messaggio elettronico consente tra l'altro di ricorrere contro terzi.

La PEC, a differenza della posta elettronica semplice, ha le seguenti peculiarità:

- identificazione del mittente, se coincide con l'autore del documento;
- garanzia dell'integrità e della riservatezza dei messaggi;
- data certa di spedizione e consegna dei messaggi;
- ricevuta di avvenuta consegna o avviso di mancato recapito;
- tracciatura dei messaggi a cura del gestore.

Di norma, si dovrebbe usare la PEC per trasmettere e/o ricevere un documento informatico, ma può accadere che la comunicazione/istanza ricevuta sia costituita dal mero corpo della e-mail. In questo caso si procede alla registrazione del messaggio in entrata nel sistema di gestione documentale.

3.7. Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale

L'e-mail costituisce un documento informatico sottoscritto con firma elettronica semplice, in quanto il mittente viene identificato inserendo il proprio *username* e la propria *password*.

Le *e-mail* inviate da una casella istituzionale dell'Amministrazione sono considerate sottoscritte con firma elettronica semplice e sono soggette a protocollazione solo se il contenuto è rilevante a fini giuridico-probatori.

3.8. Distinzione dei documenti in base allo stato di trasmissione

I documenti, siano essi analogici o informatici, in base allo stato di trasmissione si distinguono in:

- documenti in entrata;
- documenti in uscita;
- documenti interni (scambiati tra UO della stessa AOO).

N.B. I documenti scambiati tra AOO dell'Amministrazione sono documenti in entrata (per l'AOO ricevente) e in uscita (per l'AOO mittente).

Per documenti in arrivo si intendono tutti i documenti di rilevanza giuridico-probatoria acquisiti dall'Amministrazione nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato.

Per documenti in uscita si intendono i documenti di rilevanza giuridico-probatoria prodotti dall'Amministrazione nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato e anche ai propri dipendenti come persone fisiche e non nell'esercizio delle loro funzioni.

Per documenti interni o tra uffici si intendono i documenti scambiati tra le diverse UO afferenti alla stessa AOO. I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti dal personale nell'esercizio delle proprie funzioni al fine di documentare fatti inerenti l'attività svolta e la regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi.

Per comunicazioni informali tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e di norma non sono protocollate.

Per documenti scambiati tra AOO dello stesso Ente/Amministrazione si intendono documenti di preminente carattere giuridico-probatorio sottoposti alla protocollazione in uscita per la AOO mittente, e alla protocollazione in entrata per la AOO ricevente. Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale – PEC – accessibile al servizio per la tenuta del protocollo responsabile della protocollazione in entrata per la AOO di appartenenza. Il documento informatico trasmesso tramite casella di posta elettronica certificata – PEC si intende spedito dal mittente se inviato al proprio gestore e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

3.9. Duplicato del documento informatico

Il duplicato del documento informatico è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto. I duplicati informatici hanno il medesimo valore giuridico del documento informatico da cui sono tratti se prodotti in conformità delle regole tecniche.

Il “duplicato informatico” è dunque un documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari



e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

3.10. Copia del documento informatico e analogico: nozione

La copia di un documento informatico è un documento informatico che, mediante processi e strumenti adeguati, assicura la corrispondenza della copia alle informazioni del documento informatico di origine attraverso l'utilizzo di uno dei formati idonei ai sensi della normativa vigente. La copia di documento informatico è, dunque, un documento informatico che muta il formato del documento originario o che muta il supporto del documento originario informatico (ad es., il salvataggio di un file in un formato differente: da *.doc* a *.pdf*, oppure da *.doc* a *.ods*).

Le copie del documento informatico hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta, fermo l'obbligo di conservazione dell'originale informatico.

La copia di un documento analogico è la trascrizione o riproduzione dell'originale. Si distingue in copia semplice, imitativa e conforme.

La copia semplice è la pura trascrizione dell'originale senza riguardo agli elementi formali. La copia imitativa riproduce sia il contenuto che la forma (es. fotocopia).

La copia conforme è la copia certificata come conforme all'originale da un pubblico ufficiale autorizzato ad eseguire tale attestazione nell'esercizio delle sue funzioni (copia "autentica").

3.11. Copia informatica del documento amministrativo analogico

È possibile produrre la copia su supporto informatico di documenti amministrativi in origine su supporto analogico. La copia informatica ha il medesimo valore dell'originale analogico da cui è tratta se attestata conforme dal funzionario a ciò delegato nei modi stabiliti dalla legge. L'attestazione di conformità può essere inserita nel documento informatico contenente la copia informatica o può essere prodotta come documento separato contenente un riferimento temporale e l'impronta di ogni copia.

In entrambi i casi l'attestazione dev'essere sottoscritta con firma elettronica qualificata dal funzionario a ciò autorizzato; se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l'impronta di ogni copia o estratto informatico oggetto dell'attestazione.

Per copia informatica di un documento analogico si intende:

- copia informatica del documento analogico, data dal documento informatico avente contenuto identico a quello del documento analogico da cui è tratto ma diverso come forma;
- copia per immagine su supporto informatico del documento analogico, avente contenuto e forma uguali all'originale.

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

Le copie informatiche di documenti analogici, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali hanno la medesima efficacia probatoria degli originali se a esse è apposta o associata, da parte di colui che le spedisce o le rilascia, una firma elettronica qualificata e una dichiarazione di conformità:

- per “rilascio” si intende la consegna di un supporto fisico idoneo a ricevere la memorizzazione della rappresentazione corrispondente al documento analogico e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale;
- per “spedizione” si intende l’inoltro telematico del/dei file corrispondenti per il tramite di un sistema di posta elettronica o di altro sistema di comunicazione informatica e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale.

Le copie per immagine su supporto informatico di documenti originali formati su supporto analogico hanno la medesima efficacia probatoria degli originali, se:

- la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche;
- sono formate nel rispetto delle regole tecniche e se la loro conformità all’originale non è espressamente disconosciuta.

3.12. Estratto informatico di documento amministrativo informatico

La copia che riproduce solo una parte del contenuto del documento, viene definita “estratto”. Gli estratti informatici devono essere prodotti in uno dei formati idonei già definiti e riportati nel paragrafo 3.2.2.

L’estratto così formato, di uno o più documenti informatici, se sottoscritto con firma elettronica qualificata da chi effettua l’estratto ha la stessa efficacia probatoria dell’originale, salvo che la conformità allo stesso non sia espressamente disconosciuta.

Laddove richiesta dalla natura dell’attività, l’attestazione di conformità può essere inserita nello stesso documento informatico contenente l’estratto, oppure prodotta come documento informatico separato; in entrambi i casi l’attestazione dev’essere sottoscritta con firma qualificata del notaio o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l’impronta di ogni copia o estratto informatico oggetto dell’attestazione.



3.13. Copia analogica di documento amministrativo informatico

La copia analogica di documento amministrativo informatico è, di norma, la stampa cartacea.

La copia su supporto analogico di un documento informatico, sottoscritto con firma elettronica avanzata qualificata, per avere la stessa efficacia probatoria dell'originale da cui è tratta, deve essere certificata come conforme all'originale in tutte le sue componenti da un pubblico ufficiale autorizzato a eseguire tale attestazione nell'esercizio delle sue funzioni (copia “autentica”) salvo che la conformità allo stesso non sia espressamente disconosciuta. Resta fermo, ove previsto, l’obbligo di conservazione dell’originale informatico.

CAPITOLO 4. IL FASCICOLO

4.1. Il fascicolo: definizione e funzione

Il fascicolo è il componente fondamentale dell’unità archivistica. Ogni fascicolo contiene documenti che ineriscono a uno stesso affare, attività o procedimento e sono classificati in maniera omogenea, in base al contenuto e secondo il grado divisionale attribuito dal titolare (o piano di classificazione). Pertanto il fascicolo può anche essere definito come un’aggregazione documentale informatica.

All’interno di ciascun fascicolo i documenti sono inseriti secondo l’ordine cronologico di protocollazione e la loro sedimentazione avviene in modo tale che si individui subito il documento più recente. L’ordine cronologico di sedimentazione è rispettato anche all’interno dei sottofascicoli, se istruiti.

La corretta tenuta del fascicolo garantisce sia la sedimentazione che l’esercizio del diritto di accesso.

Si possono distinguere cinque tipologie di fascicolo:

- *Affare (o materia)*: conserva i documenti relativi a una competenza non proceduralizzata né proceduralizzata. Per gli affari non esiste un termine per la conclusione previsto da norme;
- *Attività*: conserva i documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque prevista l’adozione di un provvedimento finale;
- *Procedimento amministrativo*: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un atto finale;
- *Persona fisica (o fascicolo nominativo)*: conserva i documenti relativi a diversi procedimenti amministrativi, distinti per affari o per attività, ma legati da un vincolo archivistico interno, relativo a una persona fisica determinata. La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l’Ente;
- *Persona giuridica (o fascicolo societario)*: conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica.



E' importante considerare che il fascicolo può essere a carattere temporale (es. annuale) oppure a carattere permanente. Nel primo caso l'intervallo di validità è il periodo di riferimento (es. l'anno), nel secondo, invece, il periodo di validità deve essere determinato.

Il fascicolo può essere ulteriormente suddiviso in sottofascicoli (o sub-fascicoli). Queste suddivisioni sono identificate grazie a un'ulteriore sequenza numerica progressiva.

Il sottofascicolo può essere chiuso prima del fascicolo, ma non viceversa, in quanto di norma trattasi di un subprocedimento o di un endoprocedimento.

4.2. Il fascicolo informatico: formazione, implementazione e gestione

Per specifici procedimenti, affari e attività, l'Amministrazione ha l'obbligo di conservare in un fascicolo informatico gli atti, i documenti e i dati da chiunque formati su supporto informatico; cioè un documento nativo su supporto informatico deve essere conservato in originale su tale supporto all'interno dell'apposito fascicolo.

Ovviamente un fascicolo informatico può contenere anche copie di qualunque tipo di documenti nativi cartacei.

Il fascicolo informatico è creato dal responsabile del procedimento o da una persona incaricata all'interno del sistema di gestione documentale ed è visualizzabile con possibilità di intervento da parte degli utenti abilitati.

Istruendo i fascicoli, è necessario evitare la frammentazione delle pratiche, l'accorpamento eccessivo di documenti all'interno della stessa unità, la tendenza a costituire fascicoli intestati ai destinatari invece che basati sull'analisi di processi e funzioni.

Se necessario, i fascicoli possono essere rinominati attraverso una specifica procedura o servizio.

Se il contenuto è costituito da documenti esclusivamente informatici questa attività è sufficiente; se è costituito da documenti informatici e documenti cartacei bisogna rinominare anche il fascicolo cartaceo e i relativi sottofascicoli.

Il fascicolo informatico in un sistema totalmente digitale garantisce la possibilità di essere direttamente consultato e alimentato dalle Amministrazioni coinvolte nel procedimento. Le regole per l'istruzione, l'identificazione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale e alla disciplina della formazione, gestione, trasmissione e conservazione del documento informatico.

I fascicoli informatici saranno trasferiti in conservazione, mediante pacchetto di versamento, a cura del Coordinatore/Responsabile della gestione documentale o dal suo vicario dopo la loro chiusura, nelle modalità previste dal Manuale di conservazione.

4.3. I fascicoli annuali ripetitivi

È possibile prevedere la possibilità di aprire automaticamente fascicoli annuali ripetitivi. L'indicazione della UO e del Responsabile Procedimento Amministrativo (RPA) concorrono all'identificazione del fascicolo e all'individuazione del responsabile. La UO e il RPA devono essere gli stessi di ciascun documento, del fascicolo e degli eventuali sottofascicoli.



Ogni qualvolta cambia il RPA il fascicolo informatico deve essere immediatamente trasferito per competenza al nuovo responsabile del procedimento, attraverso apposite procedure o servizi.

4.4. Metadati del fascicolo informatico

I metadati sono un insieme di dati associati a un fascicolo informatico per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.

I metadati minimi del fascicolo informatico e dell'aggregazione documentale informatica rispettano la codifica di caratteri ISO-8859-1.

I metadati minimi del fascicolo informatico sono:

- identificativo univoco e persistente rappresentato da una sequenza di caratteri alfano-merici associata in modo univoco e permanente al fascicolo in modo da consentirne l'identificazione;
- indicazione o codice della AOO;
- indicazione o codice della UO responsabile del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- indicazione del procedimento amministrativo cui il fascicolo si riferisce, se disponibile;
- responsabile del procedimento: cognome e nome;
- eventuali Amministrazioni partecipanti al procedimento;
- oggetto: metadato funzionale a riassumere brevemente il contenuto del fascicolo o comunque a chiarirne la natura;
- elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità;
- data di apertura del fascicolo;
- data di chiusura del fascicolo;
- classificazione del fascicolo;
- durata e decorrenza della conservazione.

4.5. Il repertorio dei fascicoli informatici

Il repertorio dei fascicoli informatici è costituito da un elenco ordinato e aggiornato dei fascicoli istruiti all'interno di ciascuna classe e di ciascun titolo del titolario di classificazione adottato, riportante:

- anno e numero progressivo del fascicolo;
- classificazione nell'ambito del titolario adottato;



- oggetto dell'affare/procedimento/attività;
- UO responsabile dell'affare/procedimento/attività;
- nominativo del responsabile dell'affare/procedimento/attività;
- date di apertura e chiusura del fascicolo;
- numero dei documenti contenuti nel fascicolo;
- stato: chiuso/aperto.

Il repertorio dei fascicoli informatici è unico per ogni AOO, e generato e gestito in forma automatica dal sistema di gestione informatica dei documenti.



CAPITOLO 5. LA GESTIONE DEGLI ARCHIVI

5.1. Definizione

In Cdc sono istituiti i seguenti archivi, differenziati per colori al fine di facilitarne l'individuazione e la contestualizzazione:

- Archivio personale (ROSSO);
- Archivio applicativo (GIALLO);
- Archivio istituzionale (VERDE);
- Archivio di conservazione (BLU).

Di seguito vengono descritte le quattro tipologie di archivio su indicate.

Per **archivio personale** si intende l'insieme dei documenti relativi ad affari e attività di carattere personale oppure relativi a compiti assegnati “ad personam” nell'ambito di procedimenti amministrativi, di varia natura, in corso di istruttoria e di trattazione o, comunque, verso i quali sussista un interesse non ancora esaurito. L'archivio contiene, quindi, documenti a preminente carattere personale e non a valenza istituzionale ufficiale.

Per **archivio applicativo** si intende l'insieme dei documenti relativi ad affari, attività o compiti concernenti procedimenti amministrativi in corso di istruttoria e di trattazione e verso i quali sussista un interesse non ancora esaurito, che sono in corso di definizione attraverso l'utilizzo di applicazioni o sistemi applicativi che favoriscono e supportino la collaborazione fra più utenti, UO, AOO. L'archivio applicativo comprende i documenti elaborati in modo prevalentemente collaborativo o sottoposti a specifici flussi di lavoro (workflow), mediante appositi strumenti informatici (fra i quali sono da annoverare anche le applicazioni informatiche o i sistemi informatici), e che non siano ancora completi (es. mancano dei metadati, sono versioni “bozza” da consolidare, ecc.).

Per **archivio istituzionale** si intende l'insieme dei documenti relativi ad affari, attività o compiti concernenti procedimenti amministrativi in corso di istruttoria e di trattazione e verso i quali sussista un interesse non ancora esaurito o sporadico, che siano, però, completamente definiti, per quanto attiene il profilo formale, e ufficiali, ai quali siano associati gli opportuni metadati previsti. I documenti facenti parte di tale archivio dovranno risiedere obbligatoriamente, nel sistema di gestione documentale.

Per **archivio di conservazione** si intende l'insieme dei documenti inviati a un sistema di conservazione, che garantisce autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici, come previsto dal CAD (art.44).

5.2. Concetti di base

L'archivio, nelle sue varie tipologie, non è un “magazzino” in cui collocare documenti, ma è un servizio e come tale va organizzato e gestito fin dal suo nascere.

L'archivio non è una somma di documenti, ma è un complesso di documenti.



Indipendentemente dal profilo giuridico del soggetto produttore e dalle prescrizioni normative in essere, l'archivio deve essere considerato come risorsa dell'Amministrazione e anche come misuratore di efficienza dei soggetti che lo alimentano e lo utilizzano.

L'organizzazione dell'archivio deve rispondere a criteri di efficienza ed efficacia al fine di garantire la certezza dell'attività giuridico amministrativa dell'Istituto, la conservazione stabile nel tempo nonché la facile reperibilità delle informazioni eventualmente ricercate.

Le finalità operative di un archivio sono:

- Conoscere in modo autentico le situazioni e i precedenti amministrativi;
- Programmare per obiettivi, tenendo conto delle risorse;
- Verificare i risultati raggiunti;
- Provare diritti nel contesto della certezza del diritto;
- Lasciare traccia di sé e della società in cui si vive e si agisce.

Ciascuna tipologia di archivio descritta in precedenza è attuata mediante specifici strumenti tecnologici che saranno illustrati nel presente capitolo.

Gli archivi, come entità logiche, sono gli elementi gestionali fondamentali per il corretto funzionamento del sistema documentale⁸.

Il responsabile del procedimento amministrativo è tenuto alla corretta gestione, conservazione e custodia dei documenti e dei fascicoli, relativi ai procedimenti di propria competenza; a esso è quindi affidata l'attuazione delle disposizioni contenute in questo manuale in merito al corretto funzionamento degli archivi di propria pertinenza, usufruibili attraverso appositi strumenti e applicazioni.

Il responsabile del procedimento amministrativo e, in sua vece, la UO di appartenenza, crea il fascicolo e mantiene la responsabilità amministrativa dei documenti manipolati durante tutte le fasi del ciclo di vita del documento, ad eccezione della fase di conservazione; viene garantito il libero accesso, da parte delle sole UO che hanno la titolarità dei documenti, attraverso il sistema di gestione documentale.

E' bene precisare che durante le fasi di transito di un documento/fascicolo fra i vari archivi indicati ad essi passa la gestione degli oggetti, ma non la responsabilità amministrativa. Ciò significa che ogni archivio è responsabile dell'applicazione delle politiche di gestione e messa in sicurezza stabilite, ma non del contenuto né dell'eventuale validità probatoria.

Resta inteso, comunque, che il responsabile del procedimento amministrativo è incaricato della corretta gestione dei documenti di sua pertinenza da inserire e collocare nel gi-

⁸ P. Carucci e M. Guercio *Manuale di archivistica*, Urbino, Carocci, 2009, p. 204: «Per gestione dell'archivio corrente si intende quindi la funzione di organizzazione e controllo generale e sistematico esercitata da un Ente sulla propria documentazione corrente al fine di disporre del necessario supporto informativo-documentario per lo svolgimento efficiente della propria attività sia a fini interni che a fini giuridici e di trasparenza amministrativa». Questi principi di carattere generale sono funzionali all'adempimento delle disposizioni contenute nel DPR n. 445/2000 art. 65.

sto archivio; ciò comporta in primo luogo la corretta creazione dei fascicoli e inserimento dei relativi documenti⁹; in secondo luogo la corretta gestione dei fascicoli stessi.

I documenti creati nel corso dell'attività d'ufficio sono soggetti a **fascicolazione obbligatoria** ai sensi del DPR 445/2000, art. 64, c. 4. Inserire i documenti nell'apposito fascicolo permette la costituzione di un archivio organizzato essendo essi le unità logiche del sistema di gestione documentale e, di conseguenza, consente il facile e veloce reperimento dei documenti di un determinato procedimento permettendo il rispetto del principio di trasparenza e dell'istituto del diritto di accesso. La fascicolazione deve essere effettuata in maniera continuativa e sistematizzata da parte di tutte le UO constituenti l'Amministrazione.

Un'attività secondaria, ma molto utile da un punto di vista di gestione corrente delle unità di archivio, è lo **sfoltimento dei fascicoli**. Lo sfoltimento è l'operazione propedeutica a una corretta conservazione documentale: al momento della chiusura del fascicolo, ad esempio, oppure prima del trasferimento dello stesso all'archivio di conservazione, l'eventuale carteggio di carattere transitorio e strumentale deve essere selezionato ed estratto dal fascicolo da parte dell'operatore incaricato del trattamento della pratica. Si tratta, cioè, di estrarre dal fascicolo le copie e i documenti che hanno appunto carattere strumentale e transitorio, utilizzati dall'operatore incaricato o dal responsabile del procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad es., appunti, promemoria, copie di normativa e documenti di carattere generale).

E' importante anche sottolineare la distinzione esistente fra **dematerializzazione** e **digitalizzazione**, che l'Amministrazione intende fortemente perseguire.

I processi di Digitalizzazione sono diversi dai processi di Dematerializzazione. Si definisce Dematerializzazione il processo di passaggio da documenti analogici a documenti digitali, utilizzando varie tipologie di strumenti; i documenti ottenuti da tale processo sono assimilabili ai documenti cartacei, non ravvisandosi sostanziali diversità fra di essi.

Il processo di Digitalizzazione è il processo di formazione dei documenti in modalità nativamente digitale; tale processo è importante perché consente all'Amministrazione un rilevante recupero di tempo, di economicità, di razionalizzazione procedimentale e di organizzazione del lavoro. Formare i documenti in modalità nativamente digitale è pienamente concorde alla normativa vigente; tale formazione deve avvenire attraverso l'utilizzo di specifici strumenti informatici (applicazioni, sistemi applicativi, suite di produttività individuale, tools di utility, ecc.).

5.3. Archivio personale

L'archivio personale è a disposizione degli utenti e di chiunque ne abbia i diritti di accesso e utilizzo; le sue finalità sono essenzialmente di carattere strumentale ai fini della lavorazione di una serie di informazioni, raccolte in una struttura documentale o fascolare. Pertanto gli utenti avranno a disposizione specifici dispositivi, descritti nel seguito, atti a semplificare e a supportare la loro azione lavorativa e non.

⁹ A proposito si vedano i capitoli 4 e 6.

Un documento, per poter essere posizionato in un archivio personale, non deve essere necessariamente corredata delle informazioni previste nel CAPITOLO 3 del presente manuale; pertanto non è necessario che siano valorizzati i metadati ad esso associati. Solo gli utenti possono accedere all'archivio personale: alle applicazioni, pertanto, tale archivio è precluso.

L'archivio tendenzialmente non ha un carattere di transitorietà, nel senso che i documenti in esso presenti, a preminente carattere personale, possono permanere a discrezione dell'utente proprietario del documento, fino a saturazione delle risorse a disposizione di tale archivio.

Non è previsto, a meno di eccezioni approvate dal Coordinatore della gestione documentale, che i documenti transitino dall'archivio personale direttamente all'archivio di Conservazione, non ravvisando tale esigenza nelle attuali politiche di Gestione documentale della Cdc.

I documenti presenti nell'archivio personale, invece, possono transitare nell'archivio istituzionale qualora un documento vari la sua tipologia di appartenenza nel corso del suo ciclo di vita a condizione che siano rispettate le caratteristiche previste per l'archivio di destinazione.

Non è previsto che i documenti transitino dall'archivio personale a quello applicativo.

E' importante sottolineare che agli oggetti residenti o collocati nell'archivio personale sono applicate le politiche generali in vigore nel sistema di gestione documentale e che la responsabilità è a carico degli utenti a cui tali oggetti afferiscono.

5.4. Archivio applicativo

L'archivio applicativo è a disposizione degli utenti delle applicazioni e/o dei sistemi informatici che ne abbiano i diritti di accesso e utilizzo; le sue finalità sono essenzialmente di carattere strumentale ai fini della lavorazione di una serie di informazioni, raccolte in una struttura documentale o fascicolare.

La finalità dell'archivio applicativo è essenzialmente quella di contenere i documenti o i fascicoli generati dai vari sistemi applicativi durante l'esecuzione degli specifici workflow di lavorazione. Esso potrà contenere documenti e/o fascicoli appena creati o comunque che risultino privi delle informazioni necessarie alla sua finalizzazione (ad. esempio può contenere le versioni bozza o in lavorazione dei documenti). La memorizzazione nell'archivio applicativo si colloca, anche temporalmente, prima della memorizzazione nell'archivio istituzionale per quanto attiene i documenti di rilevanza istituzionale.

Non è previsto, a meno di eccezioni approvate dal Coordinatore della gestione documentale, che i documenti transitino dall'archivio applicativo direttamente all'archivio di conservazione, non ravvisando tale esigenza nelle attuali politiche di gestione documentale della Cdc.



I documenti presenti nell'archivio applicativo possono transitare nell'archivio istituzionale qualora un documento vari la sua tipologia di appartenenza¹⁰ nel corso del suo ciclo di vita a condizione che siano rispettate tutte le caratteristiche previste per l'archivio di destinazione, con particolare riferimento ai metadati a contorno di un documento e/o fascicolo. Quando un documento transita nell'archivio istituzionale dovrà essere eliminato dall'archivio applicativo, non avendo quest'ultimo caratteristiche di mantenimento o salvaguardia documentale, ma solo di supporto avanzato al corretto ciclo lavorativo.

I documenti possono transitare dall'archivio applicativo all'archivio personale a condizione che vi sia una particolare funzionalità nelle applicazioni e/o sistemi informativi utilizzati dagli utenti che sia stata appositamente progettata per tale scopo.

E' importante sottolineare che agli oggetti residenti o collocati nell'archivio applicativo sono applicate le politiche generali in vigore nel sistema di gestione documentale e che la responsabilità è a carico delle applicazioni/sistemi informatici a cui tali oggetti afferiscono.

5.5. Archivio istituzionale

L'archivio istituzionale incorpora, in se, sia la fase attiva che la fase intermedia (semiativa) del processo di tenuta dei documenti prodotti dall'Amministrazione nel corso della propria attività istituzionale e non; si colloca, anche temporalmente, tra l'archivio applicativo o personale e l'archivio di conservazione per quanto attiene i documenti di rilevanza istituzionale.

In tale archivio vanno anche posizionati i documenti di interesse delle UO e i documenti che sono inerenti le attività, anche interne, delle varie UO componenti le AOO dell'Amministrazione.

E' assolutamente fondamentale tenere ben presente che un documento, per poter essere posizionato nell'archivio istituzionale, deve avere tutte le caratteristiche di cui al CAPITOLO 3, a cominciare dalla valorizzazione di tutti i metadati ritenuti obbligatori. Sia gli utenti che le applicazioni possono posizionare i documenti di specifico interesse nell'archivio istituzionale, purché rispettino quanto appena riportato, utilizzando, per farlo, gli strumenti tecnologici a disposizione e/o servizi specifici.

L'archivio istituzionale pur avendo un carattere di transitorietà, ha una dimensione logica e un'importanza funzionale rilevanti. Rappresenta il momento di decantazione dei documenti e delle informazioni relative, organizzati in fascicoli inerenti ad affari, ad attività e a procedimenti definiti, per i quali non risulta più necessaria la trattazione corrente o verso i quali sussista un interesse sporadico.

Le attività che connotano questa fase d'archivio, almeno per la componente semiativa, sono definite dal DPR 445/2000, artt. 67, 68 e 69, e riguardano l'obbligo della periodicità dei trasferimenti di documenti dall'archivio corrente, la conservazione ordinata delle unità archivistiche e la disponibilità dei mezzi di corredo per assicurare le funzioni di controllo e

¹⁰ Per esempio: cambio di versioni, cambio dei destinatari, finalizzazione del documento, ecc..



di ricerca del materiale (registri di protocollo, piani di classificazione repertori dei fascicoli, ecc.)¹¹.

Il fine dell'archivio istituzionale non è quello di conservare un documento ma di consentirne la lavorazione attraverso specifici workflow.

La produzione e gestione informatica di dati e di documenti comporta una diversificazione delle procedure di gestione durante le varie fasi di utilizzo degli archivi determinata dalla peculiarità del procedimento amministrativo cui il documento si riferisce. Ciononostante non cambia il ruolo e la funzione concettuale svolta dall'archivio istituzionale nella tenuta del sistema documentale.

Si tratta, in ogni caso, di una fase di sedimentazione della documentazione, ossia di un periodo in cui i documenti esauriscono nel tempo le proprie funzioni rivelando la propria natura temporanea o permanente, a seconda del valore delle informazioni in essi contenute.

I documenti nativi digitali sono caratterizzati dalla predeterminazione dei termini di conservazione. Ciò significa che la durata della vita di un documento è determinata nel momento stesso in cui il documento viene creato.

Quando un documento viene collocato nell'archivio istituzionale, va indicato il periodo di validità del documento e la sua destinazione trascorso tale periodo (eliminazione o conservazione)

I documenti dell'archivio istituzionale che vanno in conservazione seguono procedure e politiche specifiche; allo scadere del periodo di permanenza nell'archivio istituzionale, i documenti vanno posizionati nell'archivio di conservazione attraverso la costituzione di appositi pacchetti di versamento secondo quanto previsto dal manuale della conservazione documentale. Si sottolinea che l'unico esemplare del documento con valore legale è quello contenuto nell'archivio di conservazione.

5.6. Archivio di conservazione

Il Coordinatore della gestione documentale provvede, almeno una volta all'anno, a generare e a trasmettere dei pacchetti di versamento al sistema di conservazione, secondo le regole previste nel manuale di conservazione, avvalendosi anche di processi di automazione disponibili nel sistema di gestione documentale. Per l'Amministrazione il conservatore è stato individuato in un soggetto esterno.

Qualora, per determinate tipologie di fascicoli o di documenti, si rendesse necessario predisporre l'attivazione della procedura di conservazione con tempistiche particolari, il RPA interessato deve darne tempestiva comunicazione al Coordinatore della gestione documentale, al fine di valutare congiuntamente con il Responsabile della conservazione e con il Responsabile dei sistemi informativi le modalità più idonee per dare attuazione a tale esigenza.

A titolo di esempio, per tutti i documenti informatici a rilevanza fiscale occorre rispettare le tempistiche previste dal D.M 17 giugno 2014 quindi, nel caso in esame, delle fatture

¹¹ P. Carucci, Maria Guercio, *Manuale di archivistica*, p. 217.

elettroniche attive e passive, inserite nel fascicolo della procedura di acquisto, si dovrà procedere al versamento anticipato in conservazione secondo le regole previste nel manuale di conservazione e gli specifici accordi di versamento stipulati con il soggetto esterno cui è affidato il processo di conservazione¹².

Altro esempio riguarda la collocazione nell'archivio di conservazione dei registri di protocollo che avviene con frequenza giornaliera.

I documenti che hanno esaurito la loro funzione, anche archivistica, al decorrere del periodo di validità inserito come informazione nei metadati di ogni singolo documento, saranno eliminati attraverso apposita procedura di scarto senza richiedere nessuna autorizzazione e senza comunicazione e notifica di sorta per quanto attiene gli attori interni all'Amministrazione.

5.7. La gestione documentale

Il termine “gestione documentale” presuppone un atteggiamento attivo e riguarda l'archivio come complesso unitario, cioè l'insieme delle attività finalizzate alla registrazione di protocollo, alla classificazione, alla fascicolazione, all'assegnazione, al reperimento, alla conservazione e all'accesso dei documenti amministrativi formati o acquisiti dal produttore di archivio.

Il sistema di gestione informatica dei documenti:

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

Il sistema di gestione documentale gestisce anche i documenti denominati “allegato”. L'allegato è un documento unito ad altro documento per prova, per chiarimento o integrazione di notizie, per memoria; il legame tra documento principale (ad es. lettera di trasmis-

¹² Si precisa che con FATTURAPA, la fatturazione elettronica verso la Pubblica Amministrazione è gestita da Agenzia delle entrate e da Sogei che ne assicura la conservazione.



sione) e allegato non va mai spezzato e l'allegato deve rimanere sempre unito al documento cui si riferisce e riportare la medesima segnatura di protocollo.

5.8. Gli strumenti di gestione degli archivi

Il trattamento dell'intero sistema documentale dell'Amministrazione comporta la predisposizione di strumenti di gestione dei vari archivi (applicativo e istituzionale soprattutto) i quali permettano un'efficiente organizzazione e consultazione della documentazione.

5.8.1. Strumenti per l'archivio personale

L'archivio personale è costituito dal repository collocato in cloud Microsoft OneDrive che ogni utente può usufruire, da supporti removibili, dai dischi locali eventualmente messi a disposizione nelle postazioni client degli utenti, e dai device personali o aziendali interagenti con il sistema informatico di Cdc (es. smartphone, tablet, ecc.). Per quanto attiene l'archivio personale nessuna particolare forma di backup o di security è applicata; fa eccezione a ciò l'insieme dei documenti posizionati in MS OneDrive sottoposti a procedure periodiche di salvataggio e verifica di sicurezza.

5.8.2. Strumenti per l'archivio applicativo

L'archivio applicativo è principalmente costituito dai servizi in cloud e/o on premise di tipologia “Blob storage” e dai servizi di database che abbiano attivate estensioni particolari per la gestione dei documenti. A tale categoria sono anche afferenti i database (denominati nosql).

Anche il sistema di gestione documentale può fornire specifici servizi per la collocazione e il dislocamento dei documenti facenti parte dell'archivio applicativo.

5.8.3. Strumenti per l'archivio istituzionale

L'archivio istituzionale è interamente contenuto nel sistema di gestione documentale. In Cdc esso è implementato come un servizio SaaS (Software as a Service) di un fornitore esterno: SharePoint on line, facente parte della suite Office365 (Microsoft).

Attraverso particolari costrutti in esso presenti la piattaforma documentale certifica, conserva e “muove” il documento dall'autore al destinatario.

Il sistema di gestione documentale registra ogni modifica per conoscere, in ogni situazione e in ogni momento, quando è stata fatta, da chi e in che cosa consiste tale modifica. Ogni utente, applicazione o sistema informatico interno (back office) è registrato e riconosciuto; ogni utente, applicazione o sistema informatico esterno (front office) può essere registrato e riconosciuto.

Il sistema di gestione documentale assicura una serie di servizi accessori indispensabili, quali il backup e la messa in sicurezza dei documenti secondo particolari politiche.

Il sistema di gestione documentale scelto da Cdc adotta un meccanismo di Rights management (diritti di accesso) basato sull'utilizzo delle ACL che garantisce:

- l'accesso esclusivamente ai soggetti dotati degli opportuni permessi in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori delle specifiche politiche di accesso stabilite nel sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di impedire modifiche non autorizzate.

5.8.4. La tutela dei dati personali

Il sistema di gestione documentale scelto da Cdc adotta un meccanismo di compliance e rispetto delle normative in tema di gestione dei dati personali e in particolare delle prescrizioni adottate per aderire al D. Lgs. 30 giugno 2003 n. 196 in materia di protezione dei dati personali.

Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo, vengono incaricati dal titolare della AOO o su delega, dal RSP. Di ciò da evidenza il manuale di AOO.

Il sistema di gestione documentale consente di registrare le informazioni derivanti da certificati e documenti scambiati con altre Pubbliche Amministrazioni con diversi livelli di riservatezza: a tal fine è presente un registro di protocollo riservato, il cui accesso è consentito solo a personale specificamente abilitato. L'Amministrazione titolare dei dati, in caso di accesso diretto ai propri archivi, rilascia all'Amministrazione precedente apposita autorizzazione in cui vengono indicati eventuali limiti e condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente anche mediante la stipula di apposite convenzioni di servizio.

In relazione alla protezione dei dati personali trattati al proprio interno, si evidenzia che la Cdc ha ottemperato a quanto previsto dal D. Lgs. 30 giugno 2003, n. 196, con particolare riferimento:

- al principio di necessità nel trattamento dei dati;
- al diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati e al relativo consenso quando dovuto;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.

5.8.5. Registro di protocollo

Il registro di protocollo è lo strumento finalizzato all'identificazione univoca e certa dei documenti ricevuti e spediti mediante la registrazione di determinati elementi che caratterizzano ogni singolo documento. Il registro di protocollo svolge, quindi, una fondamentale funzione giuridico probatoria attestando l'esistenza di un determinato documento

all'interno del sistema di gestione documentale e garantendone l'autenticità. Il registro di protocollo è un atto pubblico di fede privilegiata¹³. Per maggiori dettagli si faccia riferimento al CAPITOLO 6: IL PROTOCOLLO INFORMATICO.

5.8.6. Titolario (piano di classificazione)

Il titolario è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (titolo/classe/eventuale sottoclasse) stabilite sulla base delle funzioni dell'Ente. Ciascun documento, registrato in modalità arrivo, partenza, interno, anche non protocollato, è classificato in ordine alla corrispondenza tra il suo contenuto e la relativa voce attribuibile, desunta dal titolario e successivamente fascicolato.

La classificazione, necessaria e fondamentale, è prodromica all'inserzione di un documento all'interno di un determinato fascicolo. La relazione tra i documenti (vincolo archivistico) di un'unità archivistica è garantita dalla segnatura archivistica completa (anno di istruzione, classificazione, numero del fascicolo).

Il sistema di gestione documentale garantisce che le voci del titolario siano storicizzate, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della loro registrazione.

Ogni AOO adotta il proprio titolario; l'insieme complessivo si trova nell'Allegato 4: Titolario.

5.8.7. Repertorio dei fascicoli

I fascicoli istruiti durante lo svolgimento dell'attività amministrativa, sono annotati nel repertorio dei fascicoli. Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio rispecchia quella del titolario di classificazione e, di conseguenza, varia in concomitanza con l'aggiornamento di quest'ultimo. Mentre il titolario rappresenta, in astratto, le funzioni e le competenze che l'Ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta, in concreto, le attività svolte e i documenti prodotti in relazione a tali attività. Il repertorio dei fascicoli è costantemente aggiornato.

5.8.8. Repertori

I repertori formano serie omogenee di documenti uguali per forma e diversi per contenuto. Essi sono soggetti a registrazione particolare, cioè con l'assegnazione di una numerazione continua e progressiva per anno. Sono un esempio la registrazione di decreti, sentenze, ordinanze, contratti e convenzioni, deliberazioni, ecc.

¹³ La fede privilegiata dell'atto pubblico riguarda, in effetti, non solo fatti compiuti dal pubblico ufficiale o avvenuti in sua presenza, ma anche dichiarazioni ricevute, quando di queste ultime si dia attestazione, nell'esercizio del potere di documentazione e nella contestualità della formazione dell'atto, a prescindere dall'intrinsicità veridicità delle dichiarazioni stesse.



5.8.9. Massimario di selezione

Il massimario di selezione è lo strumento, previsto dall'art. 68 del DPR 445/2000, con cui l'Ente individua le disposizioni di massima e definisce i criteri e le procedure attraverso i quali i documenti, non rivestendo interesse storico ai fini della conservazione permanente e avendo esaurito un interesse pratico e corrente, possono essere eliminati legalmente.

Il massimario individua le tipologie documentali in rapporto ai procedimenti che le costituiscono a partire dalle quali si applicano i criteri e le disposizioni atte ad individuare i termini di conservazione; inoltre, è uno strumento indirizzato sia alla conservazione che all'eliminazione. In altri termini il massimario consente la selezione che ha come conseguenze o la conservazione o la distruzione.

Del massimario è parte integrante l'insieme delle regole di scarto¹⁴ che definiscono i tempi di conservazione in relazione alle tipologie documentarie. Le operazioni di selezione, necessarie a garantire la corretta gestione e la conservazione del complesso documentale dell'Ente, avvengono nella fase di transito dall'archivio istituzionale a quello di conservazione, in modo tale da sedimentare solo la documentazione ritenuta rilevante ai fini della conservazione a lungo termine.

¹⁴ Determinazioni presidenziali 375/81 e 14/87.

CAPITOLO 6. IL PROTOCOLLO INFORMATICO

Il registro di protocollo è un atto pubblico di fede privilegiata. Come tale, fa fede fino a querela di falso circa la data e l'effettivo ricevimento o spedizione di un documento determinato, di qualsiasi forma e contenuto. Esso, dunque, è idoneo a produrre effetti giuridici tra le parti.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Quindi, non è consentita la protocollazione di un documento già protocollato afferente alla stessa AOO.

Il numero di protocollo è costituito da sette cifre numeriche con degli “zero” iniziali laddove la numerazione fosse inferiore alle sette cifre previste dalla normativa vigente.

All'interno di ciascuna AOO il sistema di protocollazione è totalmente distribuito per la corrispondenza in ingresso e in uscita, ossia ogni ufficio è autonomo ai fini della protocollazione.

Ogni AOO della Cdc ha un registro di protocollo la cui numerazione si chiude al 31 dicembre dell'anno in corso e ricomincia il 1° gennaio dell'anno successivo.

6.1. Protocollazione

I documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi devono essere registrati a protocollo o a repertorio.

Sono oggetto di protocollazione obbligatoria i documenti ricevuti e spediti dalla Corte, ossia i cui destinatari sono esterni all'Ente o scambiati tra AOO dello stesso Ente, e tutti i documenti informatici, ad eccezione di quelli espressamente esclusi dalla normativa vigente (DPR 445/2000, art. 53, comma 5) e altri documenti informatici già soggetti a registrazione particolare.

Per protocollazione si intende l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. La protocollazione dei documenti in entrata si effettua di norma entro la giornata di arrivo o comunque entro 24 ore lavorative dal ricevimento o, se intercorrono dei giorni festivi o di chiusura programmata dell'Istituto, nel primo giorno lavorativo utile. Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immodificabile.

La protocollazione per ogni documento è effettuata mediante la memorizzazione di elementi obbligatori immodificabili, elementi obbligatori modificabili e elementi non obbligatori e modificabili.

La registrazione degli elementi obbligatori immodificabili del protocollo informatico non può essere modificata, integrata, cancellata ma soltanto annullata mediante un'apposita procedura in capo al Responsabile della gestione documentale e a persone espressamente delegate. L'inalterabilità e l'immodificabilità della registrazione di protocollo sono garantite dal sistema di gestione documentale.



6.1.1. Elementi obbligatori immodificabili (Registratura)

Gli elementi obbligatori immodificabili servono ad attribuire al documento data e provenienza certa attraverso la registrazione di determinate informazioni rilevanti sul piano giuridico-probatorio.

Essi sono:

- numero di protocollo progressivo e costituito da sette cifre numeriche;
- data di registrazione;
- corrispondente, ovvero mittente per il documento in entrata, destinatario per il documento in uscita;
- oggetto;
- impronta del documento informatico;
- numero degli allegati;
- descrizione degli allegati.

L'insieme di tali elementi è denominato registratura.

L'annullamento anche di una sola di queste informazioni determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo.

6.1.2. Elementi obbligatori modificabili

Gli elementi obbligatori modificabili sono:

- UO;
- RPA;
- classificazione archivistica;
- fascicolo.

L'annullamento anche di una sola di queste due informazioni viene tracciata dal sistema in modo permanente con l'indicazione dell'autore, della data e del valore precedentemente attribuito alla modifica.

6.1.3. Elementi non obbligatori modificabili

Gli elementi non obbligatori modificabili sono:

- collegamento ad altri documenti o a fascicoli diversi da quello d'inserimento;
- tipologia di documento;
- durata e decorrenza della conservazione;

- altri tipi di annotazioni (ad es., si può annotare l'arrivo in data successiva di un secondo esemplare dello stesso documento precedentemente ricevuto e protocollato, previa verifica della sua conformità al primo).

6.2. Data e ora regolate sul UTC

Il servizio del protocollo informatico è regolato sul tempo universale coordinato (UTC) e, in particolare, sulla scala di tempo nazionale italiana UTC (IT), secondo le indicazioni dell'INRiM.

6.3. Segnatura

La segnatura di protocollo consiste nell'apposizione o nell'associazione al documento in originale, in forma non modificabile e permanente, delle informazioni memorizzate nel registro di protocollo.

Essa consente di individuare ciascun documento in modo univoco.

6.3.1. Per il documento informatico

Le informazioni minime da associare al documento informatico sono:

- codice identificativo dell'Amministrazione;
- codice identificativo della AOO;
- codice identificativo del registro;
- numero di protocollo,
- data di protocollo;
- anno solare di riferimento del registro di protocollo.

Oltre alle informazioni minime la segnatura deve prevedere:

- classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento;
- codice identificativo dell'ufficio a cui il documento è assegnato;
- ogni altra informazione utile o necessaria, già disponibile al momento della registrazione.

Quando il documento è indirizzato ad altre Amministrazioni ed è sottoscritto con firma elettronica e trasmesso con strumenti informatici, la segnatura di protocollo può includere le informazioni di registrazione del documento purché siano adottate idonee modalità di formazione dello stesso in formato pdf/a e sia utilizzato per la sottoscrizione il formato di firma elettronica PAdES.

La firma elettronica, infatti, produce un file, definito “busta crittografica”, che racchiude al suo interno il documento originale, l'evidenza informatica della firma e la chiave per la



verifica della stessa, che, a sua volta, è contenuta nel certificato emesso a nome del sottoscrittore.

Nel caso in cui si debbano riportare sul documento annotazioni successive alla sottoscrizione (quali i dati della segnatura di protocollo), lo stesso dovrà essere validato attraverso l'apposizione di una firma automatica.

Resta inteso che la soluzione indicata nel capoverso precedente può essere superata nel caso in cui si faccia ricorso a sistemi applicativi in grado di usufruire di appositi servizi di protocollazione, firma digitale e archiviazione documentale.

6.3.2. Per il documento analogico

Le informazioni da associare al documento analogico, tramite stampante di etichette o altro sistema di identificazione del documento come la stampa della segnatura, desunte dal sistema di protocollo e gestione documentale, sono:

- descrizione dell'Amministrazione;
- codice a barre legato all'identificativo interno del documento nel sistema di protocollo;
- numero di protocollo a sette cifre;
- data di protocollazione del documento;
- codice della AOO;
- codice identificativo della UO che ha prodotto il documento;
- una lettera (E/U) per indicare il flusso del documento, rispettivamente E per entrata oppure U per uscita.

Gli elementi della segnatura devono essere presenti nei documenti prodotti da registrare in uscita. Sui documenti scambiati tra le UO della medesima AOO (privi di protocollo) deve essere apposto l'identificativo univoco del documento e la data di creazione.

La segnatura di protocollo avviene attraverso l'apposizione di un'etichetta prodotta da un'apposita apparecchiatura hw (stampante di etichette) sulla quale vengono riportate le informazioni suddette.

L'operazione di segnatura dei documenti in uscita viene effettuata dalla UO competente che redige il documento.

L'operazione di acquisizione delle immagini dei documenti cartacei è eseguibile solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.

L'etichetta della segnatura di protocollo deve essere apposta sulla prima pagina dell'originale.



6.4. Modalità di produzione e di conservazione delle registrazioni

Ogni registrazione di protocollo informatico produce un record nel sistema di gestione documentale che viene accodato in una base dati accessibile esclusivamente all'amministratore del sistema. Ogni operazione di inserimento e modifica viene registrata inoltre sul sistema di protocollo dal quale è possibile ottenere l'elenco delle modifiche effettuate su una data registrazione, permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione (smistamento, invio per conoscenza, restituzione, fascicolatura, ecc.), ottenendo in dettaglio:

- nome dell'utente;
- data e ora;
- postazione di lavoro;
- tipo di operazione (inserimento/modifica/visualizzazione/cancellazione);
- valore dei campi soggetti a modifica.

Al fine di garantire l'immodificabilità delle registrazioni, il registro informatico di protocollo giornaliero deve essere trasmesso in conservazione entro la giornata lavorativa successiva.

6.5. Annullamento di una registrazione

La necessità di modificare dati oppure di correggere errori verificatisi in sede di immisione manuale di dati o per interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo specificandone la motivazione.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo. In DocsPA (Sistema per la gestione del protocollo informatico), in fase di ricerca, viene riportata la dicitura “annullato” evidenziando in rosso la segnatura del documento, che comunque rimane sempre visibile nel sistema.

Gli utenti abilitati ad annullare un protocollo o a effettuare modifiche dopo la protocolloazione sono indicati dal responsabile della AOO.

6.6. Protocollo differito

Il registro di protocollo è aggiornato alla data corrente in maniera automatica e pertanto non è possibile riservare numeri di protocollo o posticipare la protocollazione conservandone una data pregressa.

Nel caso di carico di lavoro superiore alla norma o di ritardata protocollazione di un documento in ingresso, previa autorizzazione del Responsabile, occorre valorizzare l'effettiva data di arrivo.

La registrazione differita non si applica per i documenti informatici pervenuti via PEC, in quanto le date di invio/ricezione sono certificate dal sistema di gestione della PEC, la quale ha lo stesso valore giuridico della raccomandata AR.



6.7. La ricevuta di avvenuta protocollazione

La ricevuta di avvenuta protocollazione può essere prodotta dal sistema di protocollo e riporta i seguenti dati:

- il numero e la data di protocollo;
- la segnatura completa di protocollo;
- l'oggetto.

6.8. Documenti esclusi dalla protocollazione

Sono esclusi per legge dalla registrazione di protocollo¹⁵:

- le gazzette ufficiali;
- i bollettini ufficiali P.A.;
- i notiziari P.A.;
- le note di ricezione delle circolari;
- le note di ricezione di altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali;
- le riviste;
- i libri;
- i materiali pubblicitari;
- gli inviti a manifestazioni.

Sono parimenti esclusi dalla protocollazione altre tipologie documentali che possono essere individuate nell'ambito della specifica AOO, previa autorizzazione del direttore del servizio.

Sono altresì esclusi dalla protocollazione i documenti formati all'interno della AOO e scambiati tra le UO ad essa appartenenti, nonché le sintesi e circolari del Consiglio di Presidenza, le Circolari del Segretario Generale, del Vice Segretario Generale e dei Dirigenti generali in materia di organizzazione e gestione del personale, le Circolari del consegnatario, le comunicazioni aventi ad oggetto la sicurezza sul luogo di lavoro, pubblicate sulla Intranet.

¹⁵ DPR 28 dicembre 2000, n. 445, art. 53 comma 5.

6.9. Il registro giornaliero di protocollo

La stampa del registro giornaliero di protocollo è prodotta automaticamente dal sistema contestualmente alla chiusura/apertura automatica giornaliera.

Il Responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi provvede al controllo del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

La stampa del registro giornaliero di protocollo contiene anche le modifiche (annullamenti e modifiche oggetti) relative ai protocolli già inclusi in una stampa registro; tali modifiche sono riportate all'ultima pagina della stampa giornaliera del registro. Il Responsabile del registro verificherà se gli annullamenti e le modifiche sono state autorizzate.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo deve essere riversato quotidianamente nel sistema di conservazione.¹⁶

Gli elementi memorizzati del registro giornaliero sono i seguenti:

- Identificativo univoco e persistente;
- Data di chiusura (data di creazione del registro);
- Soggetto produttore (denominazione del sistema di protocollo);
- Destinatario (Nome, Cognome, Codice fiscale se disponibile);
- Impronta del documento informatico;
- Codice identificativo dell'Amministrazione (codice IPA);
- Denominazione dell'Amministrazione;
- Codice identificativo della AOO;
- Responsabile (Responsabile del servizio per la tenuta del protocollo informatico - Nome, Cognome, Codice fiscale);
- Oggetto (“Registro giornaliero delle modifiche di protocollo”, ecc.);
- Codice identificativo del registro;
- Numero progressivo del registro;
- Anno;
- Numero della prima registrazione effettuata sul registro;
- Numero dell'ultima registrazione effettuata sul registro;
- Data della prima registrazione effettuata sul registro;

¹⁶ Art. 7, comma 5 del DPCM 3 dicembre 2013 “Regole tecniche in materia di protocollo informatico”.

- Data dell'ultima registrazione effettuata sul registro.

6.10. Il registro di emergenza

Il Responsabile di ciascuna AOO attiva il registro di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica, dandone immediata comunicazione.

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 le 24 ore, per cause di eccezionale gravità, il Responsabile di ciascuna AOO autorizza l'uso del registro di emergenza per periodi successivi fino al ripristino funzionale del sistema di protocollo informatico. Sul registro di emergenza devono essere riportati gli estremi del provvedimento di autorizzazione.

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 della AOO.

Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema.

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

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo ordinario.

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo. In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

Il registro di emergenza si rinnova ogni anno solare: inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Il registro di emergenza è conservato con le stesse modalità del registro ufficiale come descritto in precedenza.

CAPITOLO 7. FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Nei paragrafi che seguono sono descritti i flussi dei lavorazione dei documenti, distinti tra documenti in ingresso, documenti in uscita e documenti interni.

Le attività di classificazione e fascicolazione, che riguardano tutte le tipologie di documenti, sono di seguito descritte.

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

Essa è eseguita a partire dal titolario di classificazione e tutti i documenti ricevuti e prodotti dagli uffici utente della AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al titolario riportato nell'Allegato 2: AOO – UO.

Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse, ecc.), anche l'eventuale riconoscimento alfnumerico del fascicolo.

Gli utenti abilitati all'operazione di classificazione dei documenti sono individuati dai responsabili delle UO e/o della AOO.

I documenti classificati possono essere riuniti in fascicoli (vedi anche il CAPITOLO 4). Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo/i di riferimento. Per una migliore organizzazione dei documenti si possono usare i sottofascicoli.

Ogni ufficio si fa carico di gestire le pratiche di propria competenza.

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'Ente, il soggetto preposto può provvedere all'apertura di un nuovo fascicolo. Un documento può essere assegnato anche a più fascicoli.

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

- nodo del titolario di classificazione nell'ambito del quale il fascicolo si colloca;
- numero del fascicolo, attribuito automaticamente dal sistema;
- descrizione del fascicolo;
- data di apertura (in fase di creazione viene attribuita automaticamente dal sistema e coincide con la data di creazione).

Il fascicolo viene aperto sulla base delle certificazioni del titolario. Occorre individuare, salvo particolari eccezioni, nella struttura gerarchica più bassa del titolario, il nodo di interesse e procedere, di conseguenza, all'operazione di fascicolazione. Quest'ultima è particolarmente delicata per l'eventuale successiva ricerca dei singoli atti.

Il fascicolo deve essere chiuso dal responsabile del procedimento al termine del relativo procedimento amministrativo o all'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto e deve essere impostata dall'operatore. In ogni modo, è sempre possibile riaprire il fascicolo.



Quindi, mentre il titolario rappresenta le funzioni e le competenze che l’Ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività.

7.1. La norma in materia

Ai sensi del DPCM 13 novembre 2014, articolo 17 co.2, le Pubbliche Amministrazioni e i soggetti tenuti all’attuazione del Codice dell’Amministrazione Digitale (CAD) devono completare il processo di dematerializzazione documentale e adottare un sistema di gestione dei documenti in formato esclusivamente elettronico.

La Cdc ha adeguato i propri sistemi di gestione informatica dei documenti ed è quindi in grado di consentire la formazione e la trasmissione dei propri documenti come prescritto dal citato Decreto.

Pertanto in questo documento vengono descritti i flussi di lavorazione dei documenti digitali. Solo per quanto riguarda i documenti in ingresso vengono riportate le indicazioni per la gestione di eventuali residuali flussi analogici, per i quali comunque dovrà essere prevista la conversione in digitale conformemente a quanto previsto dal citato Decreto (vedi il paragrafo 3.11)¹⁷.

7.2. Documenti in ingresso

Per documenti in ingresso si intendono tutti i documenti di rilevanza giuridico-probatoria acquisiti dall’Amministrazione nell’esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato.

Le principali fasi della gestione dei documenti in ingresso sono le seguenti:

¹⁷ Art. 4 del DPCM 13 novembre 2014: La copia per immagine su supporto informatico di un documento analogico di cui all’art. 22, commi 2 e 3, del Codice è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell’originale e della copia.

Fermo restando quanto previsto dall’art. 22, comma 3, del Codice, la copia per immagine di uno o più documenti analogici può essere sottoscritta con firma digitale o firma elettronica qualificata da chi effettua la copia.

Laddove richiesta dalla natura dell’attività, l’attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico di cui all’art. 22, comma 2, del Codice, può essere inserita nel documento informatico contenente la copia per immagine. Il documento informatico così formato è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato. L’attestazione di conformità delle copie per immagine su supporto informatico di uno o più documenti analogici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l’impronta di ogni copia per immagine. Il documento informatico così prodotto è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.



- a) ricezione dell'ufficio competente all'interno della AOO;
- b) eventuale verifica delle firme;
- c) protocollazione (tranne che per i casi previsti nel paragrafo 6.8);
- d) classificazione e fascicolazione;
- e) assegnazione al responsabile del procedimento;
- f) eventuale trasmissione ad altre UO o AOO destinatarie;
- g) archiviazione.

Le attività di protocollazione sono descritte nel CAPITOLO 6.

Le attività di classificazione e fascicolazione sono descritte all'inizio di questo capitolo.

Le attività di archiviazione sono descritte al CAPITOLO 5.

L'assegnazione nell'ambito della UO, che viene garantita dal dirigente dell'Ufficio, deve essere informaticamente effettuata tramite le funzionalità offerte dal sistema di gestione documentale, al fine di ridurre la produzione e la circolazione di copie cartacee.

Si rammenta che la protocollazione certifica la presa in carico da parte dell'ufficio competente per l'inizio del procedimento, tranne casi specifici in cui fa fede la data di arrivo (es. le domande di concorso, la presentazione di offerte economiche), come descritto al paragrafo 6.7.

La trasmissione ad altre UO o AOO destinatarie è necessaria nel caso di corresponsabilità nella gestione del processo amministrativo a cui il documento ricevuto fa riferimento. La corresponsabilità di un documento e/o di un fascicolo è la partecipazione al procedimento amministrativo di:

- più UO della stessa AOO (corresponsabilità di servizi interna);
- più AOO dello stesso Ente (corresponsabilità esterna di 1° livello);
- più AOO di enti diversi (corresponsabilità di servizi esterna di 2° livello).

7.2.1. Gestione dei flussi analogici residuali

La corrispondenza analogica in entrata perviene allo specifico ufficio della AOO secondo le seguenti modalità:

- servizio postale tradizionale e di altri gestori autorizzati, con o senza ricevuta di ritorno;
- consegna manuale all'Ufficio di corrispondenza;
- consegna manuale diretta presso l'ufficio competente.

La gestione di tali documenti prevede, oltre alle fasi descritte nel paragrafo precedente valide per i documenti digitali in ingresso, l'esecuzione delle fasi di gestione del cartaceo di seguito riportate:

- a) ricezione dell'ufficio competente all'interno della AOO;

- b) consegna al dirigente/direttore o al funzionario incaricato per l'apertura;
- c) smistamento della posta verso i protocollisti competenti;
- d) protocollazione;
- e) apposizione della segnatura di protocollo sul documento e scansione (laddove possibile);
- f) classificazione e fascicolazione;
- g) assegnazione al responsabile del procedimento;
- h) eventuale trasmissione ad altre UO o AOO destinatarie.

Anche per gli atti analogici valgono le medesime regole di protocollazione e fascicolazione.

Fa eccezione al flusso sopra descritto la posta indirizzata nominativamente al personale della AOO, che non viene aperta ma recapitata direttamente in busta chiusa al destinatario, il quale dopo averla aperta e preso visione del contenuto, valuta se il documento ricevuto è soggetto a protocollazione.

La UO che dovrà effettuare la protocollazione provvederà alla scansione del cartaceo e alla relativa classificazione e fascicolazione. Nel caso in cui altre UO della medesima AOO siano destinatarie dirette o per conoscenza della corrispondenza ricevuta, occorrerà estendere ad esse la visibilità di tale corrispondenza.

I documenti ricevuti su supporto cartaceo sono acquisiti in formato immagine con l'ausilio di scanner. Il responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi individua i documenti da sottrarre al processo di scansione che nel ciclo di lavorazione dei documenti ricevuti segue le operazioni di registrazione e segnatura di protocollo. Inoltre, il Responsabile individua anche, nel caso di acquisizione parziale del documento, il numero di pagine da acquisire (ad es. la sola lettera di frontespizio), anche in base alle tipologie dei documenti ricevuti.

In ogni caso non devono essere acquisiti i seguenti documenti:

- certificati medici contenenti la diagnosi;
- certificati di invalidità;
- certificati contenenti dati sensibili (Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali);
- documenti riportati su moduli continui;
- documenti riportati su formato superiore da quello standard (A4);
- documenti riportati su supporto cartaceo che non consente la scansione.

7.2.2. Flusso del documento informatico in entrata

I documenti amministrativi informatici in entrata possono pervenire con diverse modalità:

- a) tramite posta elettronica convenzionale (PEO);
- b) tramite posta elettronica certificata (PEC);
- c) tramite flussi informativi da altre banche dati.

7.2.3. Ricezione di documenti informatici nella casella di posta elettronica (PEO) istituzionale

L'e-mail è un mezzo di trasmissione che può anche costituire documento informatico se il messaggio è contenuto nel corpo della mail stessa (vedi anche paragrafo 3.7).

Si possono avere i seguenti casi:

- mail provenienti da terzi esterni;
- mail provenienti da AOO di Cdc.

Nel caso di e-mail provenienti da terzi esterni, se richiesto dal responsabile del procedimento, o da suo delegato, si registrano a protocollo anche le e-mail semplici, limitatamente ai casi in cui il loro contenuto sia rilevante nell'ambito di un procedimento, valutando caso per caso¹⁸.

Invece lamentele, doglianze, comunicazioni di disservizi devono essere valutate caso per caso. Nei casi di particolare gravità e rilevanza, si procede alla registrazione a protocollo.

L'e-mail relativa a scambi di documenti tra AOO di Cdc, contenente dati o informazioni prodromiche alla formazione di un provvedimento amministrativo non sono soggette a registrazione di protocollo; sono, altresì, esclusi dalla protocollazione gli atti preparatori (bozze, proposte non ufficiali, ecc.). Per i documenti registrati a protocollo e trasmessi a mezzo e-mail si valuta caso per caso.

Il flusso di lavorazione dei documenti ricevuti via PEO prevede i seguenti passi:

- a) ricezione dell'ufficio competente all'interno della AOO;
- b) eventuale verifica della firma;
- c) protocollazione del corpo della e-mail o del documento di trasmissione (se presente tra gli allegati); nel caso residuale di e-mail con corpo in bianco e allegati senza nota di trasmissione si valuta caso per caso la modalità di protocollazione (tranne che per i casi previsti nel paragrafo 6.8);
- d) classificazione e fascicolazione;
- e) assegnazione al responsabile del procedimento;
- f) eventuale trasmissione dei documenti protocollati ad altre UO o AOO.

¹⁸ L'art. 65 comma 1 lettera c) del CAD recita: "Le istanze e le dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica..." "...sono valide..." "... quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'art. 64, comma 2". L'insieme di queste disposizioni fornisce la possibilità di sostituire la firma autografa su un modulo analogico con l'invio del modulo compilato da un indirizzo di posta elettronica istituzionale fornito dall'Ente.

7.2.4. Ricezione di documenti informatici su supporti rimovibili

Nel caso di particolare documentazione che pervenga su supporto rimovibile (Cd ROM, DVD, ecc.) con consegna diretta o trasmesso a mezzo servizio postale o corriere, il flusso di lavorazione prevede i seguenti passi:

- a) ricezione dell'ufficio competente all'interno della AOO;
- b) eventuale verifica della firma;
- c) protocollazione del documento di trasmissione (se presente); nel caso di documenti senza nota di trasmissione si valuta caso per caso la modalità di protocollazione (tranne che per i casi previsti nel paragrafo 6.8);
- d) classificazione e fascicolazione;
- e) assegnazione al responsabile del procedimento;
- f) eventuale trasmissione dei documenti protocollati ad altre UO o AOO.

7.2.5. Ricezione dei documenti informatici tramite la casella di posta elettronica certificata (PEC) istituzionale

La posta elettronica certificata costituisce un mezzo di comunicazione che consente lo scambio di informazioni e documenti le cui trasmissioni e ricezioni sono giuridicamente rilevanti.

Tale modalità di trasmissione dei documenti viene utilizzata nei casi in cui è necessario avere prova opponibile dell'invio e della consegna del messaggio di posta (vedi anche paragrafo 3.6).

Il documento trasmesso/ricevuto con PEC ha lo stesso valore legale della raccomandata con avviso di ricevimento. In tal caso, l'avvenuta consegna del messaggio elettronico consente tra l'altro di ricorrere contro terzi. La PEC consente di spedire e ricevere documenti informatici che possono essere allegati o incorporati nel corpo stesso della e-mail.

Le caselle di PEC istituzionali sono “chiuse” quindi possono ricevere messaggi e documenti solo da altri vettori qualificati (altre caselle di PEC).

Il flusso di lavorazione dei documenti ricevuti via PEC prevede i medesimi passi previsti per la PEO.

La conferma di ricezione per il mittente è effettuata direttamente dal sistema PEC che non certifica, tuttavia, la protocollazione della corrispondenza, i cui estremi potranno essere successivamente notificati su richiesta del mittente.

Di norma sono soggetti a protocollazione in maniera esclusiva:

- il messaggio (se presente);
- il documento principale;
- la nota di trasmissione.



In assenza di tutte e tre le tipologie predette e in presenza di file allegati, il Responsabile della gestione documentale valuta se protocollarli tutti singolarmente (ad esempio nel caso di firmatari diversi) o se registrarli sotto medesimo protocollo.

La protocollazione di un documento informatico sottoscritto con firma elettronica è, di norma, eseguita dopo aver accertato l'autenticità, la provenienza, l'integrità e verificato la validità della firma.

Il documento informatico che perviene nella casella di PEC va gestito, di norma, entro le 24 ore lavorative successive alla ricezione.

Qualora il messaggio di posta elettronica pervenga a una casella di PEC di una AOO dello stesso Ente, ma diversa da quella competente, si annulla il documento in entrata e nel- la causale si indica l'AOO corretta e il relativo indirizzo PEC. Il mittente riceve il messaggio e ha quindi la possibilità di inoltrare il messaggio PEC alla casella corretta. Può capitare che il messaggio di notifica non possa raggiungere il mittente per problemi tecnici, quindi è be-ne, prima di procedere all'annullamento, inoltrarla a mezzo e-mail alla UO/AOO compe-tente, precisando quanto avvenuto.

Il messaggio contenuto nel corpo della PEC deve considerarsi come documento sotto-scritto e valido a tutti gli effetti di legge e, pertanto, va protocollato.

7.2.6. Ricezione di PEC interoperante (contenente il file segnatura)

Nel caso in cui la ricezione di documenti avvenga per mezzo di PEC provenienti da si-stemi interperanti, ovvero in grado di produrre in modalità automatica il file segnatura.xml a norma della circolare 60/2013 AgID, i sistemi informativi di Corte sono in grado di estrapolare le informazioni necessarie per la protocollazione direttamente dal predetto file segnatura.xml e inviare al mittente notifica di avvenuta protocollazione.

7.2.7. Ricezione di documenti informatici da flussi informatici applicativi

Se il flusso in entrata proviene da un applicativo la lavorazione prevede i seguenti passi di massima:

- a) acquisizione dei documenti;
- b) verifica dei dati ed eventuale verifica della firma;
- c) eventuale protocollazione;
- d) inserimento nell'archivio applicativo;
- e) eventuale inserimento nell'archivio istituzionale;
- f) eventuale inserimento nell'archivio di conservazione.



7.3. Documenti in uscita indirizzati ad un soggetto pubblico (interno o esterno) o privato e anche ai propri dipendenti come persone fisiche e non nell'esercizio delle loro funzioni.

Le principali fasi di lavorazione dei documenti in uscita sono:

- a) redazione del documento;
- b) classificazione;
- c) fascicolazione;
- d) gestione del processo di validazione tramite visti/firme;
- e) protocollazione;
- f) invio del documento.

Per la redazione del documento si fa riferimento a quanto descritto nel paragrafo 3.2.

Per quanto attiene la firma dei documenti si fa riferimento a quanto indicato nel paragrafo 3.1.

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma elettronica conforme alle disposizioni dettate dalla normativa vigente (Codice di Amministrazione digitale, artt. 24-37), soddisfa il requisito della forma scritta e ha valore probatorio ai sensi dell'art. 2702 c.c..

La regole che riguardano la protocollazione sono ampiamente descritte nel CAPITOLO 6.

Per l'attività di classificazione e fascicolazione si fa riferimento a quanto riportato nell'introduzione del presente capitolo.

I documenti informatici sono trasmessi all'indirizzo di posta elettronica dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica.

Le singole UO inviano i documenti informatici in uscita tramite la casella di posta istituzionale certificata (PEC) di settore o di AOO.

In ogni modo, agli addetti alla gestione della casella istituzionale di AOO per le operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici è fatto divieto di prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto della corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche (art. 17, comma 1, del Testo Unico).

7.3.1. Invio di comunicazioni a mezzo PEC

Ai fini delle comunicazioni a mezzo PEC, il testo che si intende comunicare è trascritto nel messaggio ovvero è allegato mediante copia informatica al messaggio stesso.



L'oggetto del messaggio PEC deve contenere una stringa che sintetizzi il contenuto del messaggio stesso.

Gli atti allegati al messaggio PEC sono privi di elementi attivi e, qualora ottenuti da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti.

Per gli allegati al messaggio PEC di comunicazione o notificazione sono consentiti i seguenti formati.

In caso di documenti informatici non firmati digitalmente:

- .pdf
- .pdf/a
- .jpg

E' consentito l'utilizzo dei seguenti formati compressi, purché contenenti file nei formati indicati precedentemente:

- .zip
- .rar
- .arj

In caso di documenti informatici firmati digitalmente:

- CAdES (estensione file “p7m”)
- PAdES (estensione “pdf”).

Alle buste crittografiche CAdES che contengono a loro volta ulteriori buste crittografiche è applicata una ulteriore estensione “p7m” per ogni busta crittografica generata (es. nomefile.p7m.p7m).

L'utilizzo di firme multiple, ossia firme digitali apposte da diversi sottoscrittori allo stesso documento, quali la firma parallela e la controfirma, non comporta invece l'applicazione di ulteriori estensioni al nome del file contenente il documento firmato (es. nomefile.p7m).

Per la sottoscrizione dell'atto da parte di più soggetti dovrà essere utilizzato il criterio dell'omogeneità dei formati di firma, ovvero il solo formato CAdES o il solo formato PAdES.

Nel caso di formati compressi la firma, ove prevista, deve essere applicata digitalmente dopo la compressione.

I nomi dei file non possono contenere caratteri speciali. In caso di necessità, l'unico carattere speciale ammesso è _ (underscore). I file allegati nell'ambito di uno stesso invio devono avere nomi diversi.

Al fine di ottenere file leggibili, con un contrasto ottimale, ma di dimensioni contenute, saranno effettuate di preferenza scansioni degli allegati in forma analogica, in bianco e nero (o scala di grigio), con successiva elaborazione del documento nel formato ottimizzato PDF, con risoluzione di massimo 200 dpi.



Ciascun messaggio PEC non può avere dimensioni superiori a 30 Mb. In caso di invio del messaggio da parte della Cdc, la dimensione viene intesa come prodotto del singolo messaggio per il numero dei destinatari.

Qualora gli atti o i documenti oggetto della comunicazione o notificazione contengano dati sensibili (come definiti dal Codice in materia di protezione dei dati personali), gli stessi verranno inviati per estratto tramite PEC con contestuale messa a disposizione, su un'apposita area riservata del sito Internet, dell'atto integrale a cui potrà accedere esclusivamente il destinatario, con modalità tali da garantire l'identificazione dell'autore dell'accesso e la tracciabilità della relativa attività.

Nel caso di invio di un messaggio PEC ad un indirizzo errato, non corrispondente all'effettivo destinatario, qualora l'erroneità risulti in modo palese, il titolare della casella è tenuto a dare pronto avviso dell'anomalia al mittente a mezzo posta elettronica certificata. A tal fine, tutti i testi dei messaggi PEC contengono la seguente “Avvertenza”:

“Nel caso in cui il presente messaggio sia stato ricevuto per errore, si invita a segnalare tale circostanza all’indirizzo del mittente, al fine di evitare ulteriori disagi.”

Per le comunicazione e notificazioni a mezzo PEC nell'ambito dei giudizi dinanzi alla Corte si rinvia al Decreto Presidenziale n. 98/2015, nell'Allegato 3: Riferimenti normativi interni.

7.4. Flusso di lavorazione dei documenti interni alla Cdc

7.4.1. Flusso del documento informatico tra UO della stessa AOO

Il documento tra uffici (o interno) è quello che una UO invia ad un'altra UO della stessa AOO. Tali documenti benché non soggiacciono all'obbligatorietà della protocollazione, potrebbero essere protocollati nel caso rivestano particolare importanza giuridico-amministrativa.

7.4.2. Flusso del documento informatico tra AOO della Cdc

Il flusso dei documenti informatici tra le AOO della Cdc prevede la registrazione del protocollo in uscita per l'AOO mittente e la protocollazione in entrata per la AOO destinataria.

L'interoperabilità è garantita mediante l'uso della funzione di trasmissione/ricezione per interoperabilità disponibile nell'applicativo di protocollo informatico. Un documento trasmesso per interoperabilità si presenta con i campi obbligatori precompilati e con i dati riportati dal mittente. Tale documento è predisposto alla protocollazione: si tratta cioè un documento che può essere protocollato subito o ricercato tra i documenti in completamento e/o predisposti alla protocollazione.



7.5. Flusso di pubblicazione dei documenti sui siti web della Cdc

Il flusso di pubblicazione dei documenti sui siti web della Cdc è regolamentato dalla circolare del Segretario Generale n. 67/2015.

Il sito web istituzionale della Cdc è organizzato e gestito attraverso un sistema evoluto di gestione dei contenuti che utilizza delle strutture predefinite per la realizzazione di pagine web.

La pubblicazione di un documento sul sito prevede la partecipazione di diversi attori e fasi che vanno dalla creazione del documento fino alla pubblicazione finale.

I vari uffici/strutture della Cdc possono richiedere la pubblicazione di documenti sul sito Internet contattando l’Ufficio stampa che, come previsto dalla deliberazione n. 1/DEL/2010 relativa al “Regolamento per l’organizzazione e il funzionamento degli uffici amministrativi e degli altri uffici con compiti strumentali e di supporto alle attribuzioni della Cdc”, nella figura del proprio magistrato responsabile, cura l’immagine dell’Istituto, promuove i rapporti con gli organi di informazione, favorisce la conoscenza della Corte e delle sue funzioni attraverso la comunicazione delle pronunce adottate in sede giurisdizionale e di controllo e assume la responsabilità redazionale del sito Internet istituzionale.

L’Ufficio stampa assicura altresì l’informazione istituzionale attraverso comunicati stampa, pubblicazioni, informative, dossier, audiovisivi e strumenti telematici e contribuisce alla maggiore efficacia dell’esercizio del controllo sulla gestione, comunicando agli organi di informazione, previa autorizzazione del Presidente, i risultati del controllo medesimo nei modi e nelle forme concordate con i Presidenti delle competenti sezioni.

Le richieste di pubblicazione sul sito web possono pervenire da più soggetti (uffici centrali, uffici regionali, ufficio stampa, presidenza) e per la pubblicazione di contenuti in diversi ambiti:

- in home page e nelle pagine di interesse nazionale del sito web;
- nella sezione “Amministrazione Trasparente” del sito web;
- nelle sezioni del sito web dedicate alle attività delle sedi regionali.

A seconda dei casi, i passi da compiere sono differenti e gli attori coinvolti possono essere diversi e/o comparire in fasi del processo differenti; in ogni caso il flusso di pubblicazione è sempre implementato con l’ausilio dell’applicazione web “Scheda di pubblicazione”.

7.5.1. Flusso di pubblicazione in home page e nelle pagine di interesse nazionale

Il flusso di pubblicazione di un documento sul sito web, in home page o in qualsiasi altra sezione del sito, ad eccezione di quelle dedicate alla trasparenza e alle sezioni regionali per le quali esiste un workflow dedicato, viene innescato formulando una specifica richiesta di inserimento sul sito, ovvero modifica o cancellazione di un contenuto già esistente, attraverso la predetta “Scheda di pubblicazione”. Le richieste di pubblicazione vengono raccolte e lavorate dall’Ufficio stampa che accede all’applicazione al fine di revisionarle, completarle e approvarle. Nelle situazioni di incongruenza e/o di errore, l’Ufficio stampa può decidere

o di sospendere le attività di pubblicazione chiedendo chiarimenti all’ufficio richiedente oppure di interromperle definitivamente respingendo la richiesta di pubblicazione e dando anche in tal caso comunicazione all’ufficio richiedente (con le dovute motivazioni).

Nel caso di approvazione della richiesta, l’Ufficio stampa, dopo aver eventualmente completato le informazioni ricevute, le invia al team di pubblicazione web (Redazione tecnica DGSIA) che accede all’applicazione per il dispiegamento dei contenuti, prima off line in modalità preview a beneficio del personale dell’Ufficio stampa, successivamente, on line in caso di feedback positivo da parte di questo ufficio (o in assenza di riscontro/richiesta di preview); appena avvenuta la pubblicazione on line, l’applicazione invia automaticamente una e-mail di notifica alla segreteria del Capo di gabinetto.

Nei casi di ritorni negativi sulla preview da parte dell’Ufficio stampa, la richiesta viene opportunamente revisionata/modificata dall’Ufficio stampa e il workflow riattivato fino al dispiegamento on line del contenuto.

7.5.2. Flusso di pubblicazione nella sezione “Amministrazione trasparente”

Nel caso in cui il documento debba essere pubblicato nell’apposita sezione denominata “Amministrazione Trasparente”, il flusso è leggermente modificato, infatti la richiesta avanzata da un qualsiasi ufficio della Cdc coinvolto nella produzione di contenuti legati alla trasparenza, compreso il Responsabile della trasparenza, è specifica e vagliata dalla struttura del Responsabile della trasparenza che, attraverso l’applicazione web “Scheda di pubblicazione” la può revisionare, eventualmente completare e approvare.

Quindi il Responsabile della trasparenza la invia alla segreteria del Segretario generale. In caso di riscontro non positivo da parte del Segretario generale, il Responsabile della trasparenza revisiona la richiesta secondo le indicazioni ricevute, sospendendo le attività di pubblicazione e coinvolgendo, se necessario, l’ufficio richiedente. Viceversa in caso di riscontro positivo o in assenza di feedback da parte del Segretario generale dopo 24 ore dal momento della ricezione della comunicazione (silenzio-assenso), la struttura del Responsabile della trasparenza trasmette le informazioni al team di pubblicazione web (Redazione tecnica DGSIA) che dispiega i contenuti, prima off line in modalità preview a beneficio del personale della struttura del Responsabile della trasparenza, successivamente, on line in caso di feedback positivo da parte di questa struttura (o in assenza di riscontro/richiesta di preview).

Appena avvenuta la pubblicazione on line, l’applicazione invia automaticamente una e-mail di notifica all’Ufficio stampa.

Nei casi di ritorni negativi sulla preview da parte del Responsabile della trasparenza, la richiesta viene opportunamente revisionata/modificata dal Responsabile della trasparenza e il workflow riattivato fino al dispiegamento on line del contenuto.

Nelle situazioni di incongruenza e/o di errore, il Responsabile della trasparenza può decidere o di sospendere le attività di pubblicazione chiedendo chiarimenti all’ufficio richiedente oppure di interromperle definitivamente respingendo la richiesta di pubblicazione e dando anche in tal caso comunicazione all’ufficio richiedente (con le dovute motivazioni).



7.5.3. Flusso di pubblicazione nelle sezioni regionali

Per quanto attiene la pubblicazione di documenti nelle pagine del sito dedicate alle sezioni regionali, le richieste vengono formulate esclusivamente dagli Uffici regionali nella figura dei Referenti responsabili incaricati, i quali attraverso l'applicazione web “Scheda di pubblicazione” redigono i contenuti da pubblicare, li revisionano e li approvano (oltre che richiedere la modifica/cancellazione di quelli già esistenti); quindi, il Referente regionale invia le informazioni al team di pubblicazione web (Redazione tecnica DGSIA) per il dispiegamento dei contenuti, prima off line in modalità preview a beneficio del referente regionale e, successivamente, on line in caso di un suo feedback positivo (o in assenza di riscontro/richiesta di preview).

Appena avvenuta la pubblicazione on line, l'applicazione invia automaticamente una email di notifica alla segreteria del Capo di gabinetto e all'Ufficio stampa.

Nei casi di ritorni negativi sulla preview da parte del referente regionale, piuttosto che nelle situazioni di incongruenza e/o di errore, il team di pubblicazione web sospende le attività di pubblicazione on line dandone comunicazione all'Ufficio regionale; la richiesta viene opportunamente revisionata/modificata dall'Ufficio regionale e il workflow riattivato fino al dispiegamento on line del contenuto.

7.5.4. Flusso di pubblicazione sul sito web Biblioteca

Le richieste di pubblicazione sul sito della Biblioteca della Cdc vengono formulate esclusivamente dall'Ufficio della biblioteca e non prevedono il coinvolgimento dell'Ufficio stampa o di strutture intermedie analoghe in nessuna fase del workflow.

In questo caso, pertanto, il personale della Biblioteca accede all'applicazione web “Scheda di pubblicazione” per redigere i contenuti da pubblicare, revisionarli e approvarli (oltre che richiedere la modifica/cancellazione di quelli già esistenti) e invia le informazioni al team di pubblicazione web (Redazione tecnica DGSIA) per il dispiegamento dei contenuti, prima off line in modalità preview a beneficio del personale della Biblioteca e, successivamente, on line in caso di feedback positivo da parte di questo ufficio (o in assenza di riscontro/richiesta di preview).

Nei casi di ritorni negativi, piuttosto che nelle situazioni di incongruenza e/o di errore, il team di pubblicazione web sospende le attività di pubblicazione on line dandone comunicazione all'Ufficio della biblioteca; la richiesta viene, quindi, opportunamente revisionata/modificata dall'Ufficio della biblioteca e il workflow riattivato fino al dispiegamento on line del contenuto.

7.5.5. Flusso di pubblicazione sul sito Rivista web

Le richieste di pubblicazione sul sito della Rivista web della Cdc vengono formulate esclusivamente dalla Struttura di supporto al servizio massimario e rivista, il cui personale accede all'applicazione web “Scheda di pubblicazione” per redigere i contenuti da pubblicare, revisionarli e approvarli (oltre che richiedere la modifica/cancellazione di quelli già esistenti); quindi, le informazioni vengono inviate al team di pubblicazione web (Redazione tecnica DGSIA) per il dispiegamento dei contenuti, prima off line in modalità preview a



beneficio del personale della Struttura di supporto al servizio massimario e rivista e, successivamente, on line in caso di feedback positivo da parte di questo ufficio (o in assenza di riscontro/richiesta di preview). Appena avvenuta la pubblicazione on line, l'applicazione invia automaticamente una e-mail di notifica all'Ufficio stampa.

Nei casi di ritorni negativi sulla preview da parte della Struttura di supporto al servizio massimario e rivista, piuttosto che nelle situazioni di incongruenza e/o di errore, il team di pubblicazione web sospende le attività di pubblicazione on line dandone comunicazione alla Struttura di supporto al servizio massimario e rivista; la richiesta viene, quindi, opportunamente revisionata/modificata dalla Struttura di supporto al servizio massimario e rivista e il workflow riattivato fino al dispiegamento on line del contenuto.

7.5.6. Flusso di pubblicazione sul sito intranet

Il responsabile dei contenuti pubblicati sulla intranet della Cdc è la Redazione intranet, struttura che, ai sensi del decreto n.409/2007 del Segretario generale, è composta dal dirigente dell'Ufficio del trattamento economico del personale amministrativo e da risorse del Consiglio di Presidenza, dell'Ufficio delle relazioni sindacali e della DGSIA.

L'Ufficio stampa non interviene in alcun modo nella definizione del profilo della comunicazione da adottare sulla intranet, sebbene possa, come altri uffici (compresa la Redazione intranet stessa), richiedere la pubblicazione di uno specifico contenuto.

L'iter di pubblicazione prevede che qualsiasi ufficio della Cdc, compreso l'Ufficio stampa, può far richiesta di pubblicazione di un contenuto sulla Intranet accedendo all'applicazione "Scheda di pubblicazione" e innescando il flusso con il quale formula una specifica richiesta di inserimento, ovvero di modifica o cancellazione di un contenuto già esistente; le richieste di pubblicazione così formulate vengono elaborate dalla Redazione intranet che accede all'applicazione al fine di revisionare le richieste, completarle e approvarle.

Nelle situazioni di incongruenza e/o di errore, la Redazione intranet può decidere o di sospendere le attività di pubblicazione chiedendo chiarimenti all'ufficio richiedente, oppure di interromperle definitivamente respingendo la richiesta di pubblicazione e dando anche in tal caso comunicazione all'ufficio richiedente (con le dovute motivazioni); viceversa, nel caso di approvazione della richiesta, la Redazione intranet, dopo aver eventualmente completato le informazioni ricevute, le invia al team di pubblicazione web (Redazione tecnica DGSIA) per il dispiegamento dei contenuti, prima off line in modalità preview a beneficio del personale della Redazione intranet, successivamente, on line in caso di feedback positivo da parte di questa redazione (o in assenza di riscontro/richiesta di preview).

Nei casi di ritorni negativi sulla preview da parte della Redazione intranet, la richiesta viene opportunamente revisionata/modificata dalla Redazione intranet e il workflow riattivato fino al dispiegamento on line del contenuto.

7.5.7. Gestione delle eccezioni

Nei casi in cui il servizio di pubblicazione mediante l'applicazione web "Scheda di pubblicazione" risulti tecnicamente indisponibile, per assicurare la continuità del servizio di publishing sui siti della Cdc (sito web istituzionale – compresa sezione trasparenza e sezioni

regionali, biblioteca, Rivista web e intranet) le informazioni verranno trasmesse a mezzo posta elettronica, strutturate nel corpo della mail e tramite l'uso di allegati.

Le richieste di pubblicazione dovranno ricalcare i workflow descritti. Ad esempio, nel caso di una richiesta di pubblicazione di un contenuto nella sezione trasparenza, in caso di indisponibilità della “Scheda di pubblicazione”, la richiesta dovrà pervenire alla struttura del Responsabile della trasparenza il cui indirizzo di posta elettronica di riferimento è “trasparenza@corteconti.it”.

Le richieste di pubblicazione dovranno essere inviate con e-mail direttamente agli uffici/strutture competenti per i singoli siti:

- Per la intranet: redazione.intranet@corteconti.it;
- Per il sito web istituzionale: ufficio.stampa@corteconti.it;
- Per la sezione «Amministrazione trasparente» del sito web: trasparenza@corteconti.it;
- Per le sezioni regionali del sito web: redazione.portale@corteconti.it;
- Per il sito web della Biblioteca: redazione.portale@corteconti.it;
- Per il sito della Rivista web: redazione.portale@corteconti.it.



CAPITOLO 8. PROCEDURE PARTICOLARI

In questo capitolo sono indicate le procedure particolari che non ricadono negli standard fin qui descritti.

8.1. Gestione delle gare d'appalto

8.1.1. Gare e procedure negoziate gestite in modalità telematica

I documenti inerenti le gare svolte mediante portale telematico o pervenuti in modalità elettronica possono essere soggetti a registrazione di protocollo e comunque sono inseriti nel sistema di gestione documentale.

Qualora il portale non abbia possibilità di riversare i file della documentazione di gara o procedura negoziata nel sistema di gestione documentale, la UO provvede a inserirli nelle rispettive registrazioni di protocollo o, in base alla natura del documento, come documenti non protocollati.

8.2. Gestione di concorsi e selezioni

La domanda di partecipazione deve essere presentata esclusivamente per via telematica. Per la presentazione della domanda i candidati devono essere in possesso di un indirizzo di posta elettronica certificata personalmente intestato al candidato e devono registrarsi al Portale concorsi all'indirizzo: <https://concorsionline.corteconti.it> e seguire la procedura ivi indicata. In caso di prolungata e significativa indisponibilità del sistema informativo l'Amministrazione si riserva di informare i candidati, al ripristino delle attività, circa le eventuali determinazioni da adottare al riguardo, mediante avviso pubblicato sul portale dedicato.

La documentazione deve essere allegata, in formato digitale, secondo le modalità illustrate sul portale dedicato. Nel caso in cui il candidato non disponga della versione digitale della documentazione da esibire può inviare gli originali cartacei secondo le modalità definite nel bando di concorso. La medesima documentazione può essere presentata a mano al Segretariato generale della Cdc nei termini definiti dal bando di concorso. Non si tiene conto delle domande spedite a mezzo raccomandata.

Per la consegna degli allegati analogici, occorre tenere traccia della data di ricezione, in base alla vigente normativa.

8.3. Fatture elettroniche (Fattura PA)

La fattura elettronica destinata alla Pubblica Amministrazione rispetta i requisiti di formato e contenuto prescritti dal Decreto Ministeriale 3 aprile 2013, n. 55 (e successive modifiche), e viene trasmessa e ricevuta attraverso il Sistema di interscambio (SdI).

È obbligatorio emettere fatture elettroniche nei confronti di tutte le Pubbliche Amministrazioni italiane (ciclo attivo e passivo).



Non si accettano più fatture cartacee emesse in data pari o successiva al 31 marzo 2015, salvo per i soggetti non tenuti a rispettare l'obbligo di fatturazione elettronica (es. fornitori esteri, persone fisiche o giuridiche senza partita IVA).

Le fatture cartacee che avrebbero dovuto essere emesse in formato elettronico vanno restituite al mittente utilizzando lo stesso canale di comunicazione, in piena simmetria delle forme.

Le fatture cartacee pervenute a mezzo PEC emesse a far data dal 31 marzo 2015 in poi devono essere annullate con la seguente motivazione: "Ai sensi della Legge 24 dicembre 2007, art. 1 commi 209-214, le fatture emesse nei confronti dell'Ente in data pari o successiva al 31 marzo 2015 devono essere trasmesse in forma elettronica secondo il formato di cui all'allegato A "Formato della fattura elettronica" del Decreto Ministeriale 3 aprile 2013, n. 55". Il mittente riceverà la notifica di annullamento, comprensiva di motivazione, a mezzo PEC.

La fattura PA non è prevista per i fornitori non residenti in Italia che dovranno attendere l'emanazione di uno specifico decreto. In tal caso la fattura andrà gestita come qualsiasi documento analogico: protocollata, assegnata e fascicolata.

La fattura elettronica perviene in formato XML, come previsto dalla normativa in materia, attraverso lo SdI sul Sistema Informativo per la gestione integrata della contabilità economica e finanziaria (SICOGE), realizzato da SOGEI per la Ragioneria Generale dello Stato (RGS).

Le fatture elettroniche, recapitate dallo SdI all'Amministrazione, vengono singolarmente protocollate, in modo automatico, da SICOGE in fase di ricezione. Il sistema attribuisce un numero, progressivo nell'ambito dell'Amministrazione ricevente, e una data coincidente con quella di ricezione. Viene inoltre creato un fascicolo elettronico, che contiene la fattura, il riferimento al lotto e gli allegati eventualmente inviati dal fornitore. Al fascicolo viene assegnato un numero identificativo.

La data di protocollo fa fede quale termine iniziale dei 15 giorni entro cui la fattura va accettata o rifiutata con motivazione (la mancata notifica di rifiuto entro 15 giorni equivale ad accettazione), nonché dei 30 giorni previsti dalla legge decorsi i quali, in assenza di pagamento, iniziano automaticamente a decorrere gli interessi moratori (D.Lgs. 192/2012, art. 1, comma 1, lett. d).

Le fatture elettroniche possono essere rifiutate in due diverse modalità:

- se non sono decorsi i 15 giorni, è possibile rifiutare una fattura all'interno del sistema SICOGE, dunque per il tramite dello SdI;
- se sono decorsi 15 giorni dall'arrivo e dunque la fattura è stata accettata automaticamente nel sistema, per poter procedere al rifiuto della stessa, è necessario inviare una PEC al fornitore, nella quale verrà specificato il motivo del rifiuto.

Le fatture Sogei per oneri a rimborso vengono acquisite sul Sistema Informativo Gestione Iniziative (SIGI) e successivamente protocollate e archiviate. E' implementato il processo di validazione delle fatture (workflow approvativo) che prevede l'apposizione della firma del referente per l'esecuzione del servizio e l'autorizzazione al pagamento.



Le fatture elettroniche trasmesse dai fornitori alle PA (ciclo passivo), così come quelle emesse dall'Amministrazione (ciclo attivo), sono obbligatoriamente conservate in modalità elettronica, secondo quanto espressamente disposto dalla legge¹⁹.

8.4. DURC on-line

Ai sensi dell'art. 4 della Legge 78/2014, la verifica della regolarità contributiva avviene con modalità esclusivamente telematiche. In caso di Documento Unico di Regolarità Contributiva (DURC) già disponibile, questi avrà durata pari a quanto indicato nel documento stesso, in caso di non disponibilità del documento il sistema ne comunicherà la data di disponibilità. Il documento così ottenuto avrà validità di 120 giorni dalla data di emissione. Per le verifiche immediatamente disponibili on-line, si procede acquisendo l'immagine come documento non protocollato all'interno del sistema di gestione documentale.

Per i DURC richiesti, ma non immediatamente disponibili, occorre attendere la ricezione dell'avviso di disponibilità del documento che perviene a mezzo PEC. Anche questo avviso è acquisito come documento non protocollato. A questo punto è possibile consultare il sistema del DURC on-line e procedere come per i DURC immediatamente disponibili.

8.5. Certificati di malattia

I certificati di malattia sono consultati sulla banca dati dell'INPS con apposite credenziali rilasciate ai dipendenti incaricati. I certificati di malattia sono una tipologia di documenti esclusa dalla registrazione di protocollo.

Nei casi in cui il dipendente debba richiedere istituti particolari che richiedono copia cartacea della certificazione (disponibile solo all'interessato in quanto contiene dati sensibili su diagnosi e prognosi) questa deve essere inviata o consegnata all'ufficio di appartenenza, che provvederà all'inserimento nel fascicolo in SIAP (Sistema Informativo Amministrazione del Personale).

8.6. Documenti del portale degli acquisti della Pubblica Amministrazione

Gli strumenti messi a disposizione sulla piattaforma di *e-Procurement* gestita da Consip per conto del Ministero dell'economia e delle finanze sono:

- Il *Mercato Elettronico della P.A.* (MePA), ai sensi dell'art. 11 del D.P.R. 101/2002, mediante il quale le Pubbliche Amministrazioni possono acquistare beni e servizi offerti dai fornitori abilitati presenti sui diversi cataloghi del sistema, il cui importo deve essere inferiore alla soglia comunitaria.
- Le *Convenzioni* contratti quadro stipulati da Consip ai sensi dell'art. 26 della Legge 488/99, nell'ambito dei quali i fornitori aggiudicatari di gare - esperite in modalità tradizionale o smaterializzata a seguito della pubblicazione di bandi - si impegnano ad accettare ordinativi di fornitura emessi dalle singole Amministrazioni che hanno

¹⁹ DM MEF 17 giugno 2014.

effettuato l'abilitazione al sistema Acquisti in rete. Gli *Accordi quadro*, aggiudicati da Consip a più fornitori a seguito della pubblicazione di specifici Bandi, definiscono le clausole generali che, in un determinato periodo temporale, regolano i contratti da stipulare. Nell'ambito dell'Accordo quadro, le Amministrazioni che hanno effettuato l'abilitazione al sistema Acquisti in Rete, attraverso la contrattazione di "Appalti Specifici", provvedono poi a negoziare i singoli contratti, personalizzati sulla base delle proprie esigenze.

- Il *Sistema Dinamico di Acquisizione della P.A.* (SDAPA) è un processo di acquisizione interamente elettronico, aperto per tutto il periodo di validità dello stesso a qualsivoglia operatore economico che soddisfi i criteri di selezione.

Per l'aggiudicazione nell'ambito di un Sistema dinamico di acquisizione, le Amministrazioni aggiudicatrici seguono le norme della procedura ristretta. Tutti i candidati che soddisfano i criteri di selezione sono ammessi al sistema e tutti i partecipanti ammessi sono invitati a presentare un'offerta per ogni specifico appalto nell'ambito del sistema dinamico di acquisizione.

Il Sistema dinamico è caratterizzato da una procedura bifasica:

- Fase 1 - pubblicazione da parte di Consip di un bando istitutivo per una o più categorie merceologiche a cui i fornitori possono abilitarsi.
- Fase 2 - indizione e aggiudicazione di appalti specifici in cui le Amministrazioni, definendo i quantitativi, il valore e le caratteristiche specifiche dell'appalto, invitano tutti i partecipanti ammessi a presentare un'offerta.

Di seguito vengono descritte le procedure di acquisto d'uso più frequente alla data di stesura del Manuale, in attesa delle regole di attuazione del nuovo Codice degli Appalti:

- Affidamenti diretti → MePA;
- Adesioni → Convenzioni;
- Negoziazioni → MePA.

8.6.1. Affidamenti diretti sulla piattaforma MePA (OdA)

Nei casi previsti dalla normativa e dai regolamenti vigenti, si fa ricorso ad un ordine diretto, che consiste nel selezionare l'articolo di proprio interesse fra quelli presenti nel catalogo dei fornitori e nell'effettuare l'Ordine di Acquisto (OdA) al fornitore che è in grado di fornire l'articolo al prezzo più conveniente per l'Amministrazione.

Il processo può essere così brevemente schematizzato: il punto istruttore effettua una bozza dell'ordine attraverso la piattaforma e la invia al punto ordinante. Il punto ordinante, cioè la persona che dispone di potere di spesa e del dispositivo di firma elettronica, controlla la bozza, genera attraverso la piattaforma il file pdf/a che costituisce il documento d'ordine, lo scarica localmente, lo firma elettronicamente, lo registra nel sistema di protocollo e lo ricarica a sistema. La piattaforma MePA chiede il numero di protocollo come campo obbligatorio per procedere nella registrazione. Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l'emissione del corrispondente documento gestionale. Nel caso sia un documento di tipo "ordine", questo può essere tra-



smesso al sistema di gestione documentale dove si genera una bozza per la protocollazione e la fascicolatura. Nel caso invece sia un documento di tipo “contratto” dal sistema contabile può essere richiamato il numero di protocollo assegnato all’ordine emesso sulla piattaforma MePA.

8.6.2. Adesioni – Convenzioni (OdA)

Quando l’articolo che si intende acquistare è presente in una delle convenzioni Consip attive, l’Amministrazione aderisce a tale convenzione ed effettua un ordine al fornitore che è vincitore della gara precedentemente espletata da Consip.

Il processo può essere così brevemente schematizzato: il punto istruttore seleziona la convenzione, effettua una bozza dell’ordine attraverso la piattaforma e la invia al punto ordinante. Il punto ordinante controlla la bozza, genera attraverso la piattaforma il file pdf/a che costituisce il documento d’ordine (OdA), lo scarica localmente, lo firma elettronicamente, lo registra nel sistema di protocollo e lo ricarica a sistema. La piattaforma MePA chiede il numero di protocollo per procedere nella registrazione. Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l’emissione del corrispondente documento gestionale. Nel caso sia un documento di tipo “ordine”, questo può essere trasmesso al sistema di gestione documentale dove è generata una bozza per la protocollazione e la fascicolatura. Nel caso invece sia un documento di tipo “contratto” dal sistema contabile può essere richiamato il numero di protocollo assegnato all’ordine emesso sulla piattaforma MePA.

8.6.3. Procedure negoziate (RdO) - MePA

Nei casi previsti dalla normativa e dai regolamenti vigenti, si fa ricorso ad un Richiesta di Offerta (RdO), che consiste nell’espletamento di una gara telematica con gli strumenti offerti dalla piattaforma MePA. Si può fare inoltre ricorso alla RdO per effettuare indagini di mercato finalizzate a una procedura di affidamento diretto.

Nell’esecuzione dell’iter che conduce alla creazione della RdO, è possibile allegare dei documenti prodotti dall’Amministrazione, sia di carattere amministrativo che tecnico-economico, al fine di supportare i fornitori nella predisposizione dell’offerta. Esempi di tali documenti sono il disciplinare di gara, il capitolato tecnico, ecc..

Le buste arrivate sulla piattaforma MePA possono essere aperte solo alla scadenza della gara telematica con una seduta pubblica web.

Nel caso lo strumento dell’RdO sia utilizzato per una procedura negoziata i documenti di gara saranno salvati localmente dal punto ordinante e registrati sul sistema di gestione documentale come documenti non protocollati. Al momento della stipula del contratto con il fornitore aggiudicatario, si genera tramite la piattaforma il file pdf/a che costituisce il documento di stipula. Il punto ordinante salva il documento di stipula localmente, lo firma elettronicamente lo registra nel sistema di protocollo e lo ricarica a sistema.

Nel caso lo strumento dell’RdO sia utilizzato per effettuare un’indagine di mercato ai fini di una procedura di affidamento diretto verranno salvati localmente dal punto ordinante solo i documenti relativi all’aggiudicatario.



8.7. Gestione del secondo esemplare

Per essere certi che si tratti di un secondo originale di un documento già protocollato, è necessario verificare l'esatta corrispondenza tra i due esemplari, inclusi gli allegati, in tutte le loro parti (firme, date, segnature di protocollo, ecc.). Per i documenti sottoscritti con firma elettronica è necessario verificare anche che la data e l'ora di firma coincidano.

Una volta appurata la perfetta identità tra i due documenti, si agirà diversamente nel trattamento a seconda della modalità di ricezione del secondo esemplare.

Nel caso di entrata mediante PEC o altro sistema informatico (*e-mail* semplice, ecc.) si effettua una registrazione come “Documento non protocollato”, riportandovi tutti i dati già inseriti nella registrazione di protocollo del primo esemplare (oggetto, mittente, RPA, classificazione, fascicolo, ecc.). Si inserisce, inoltre, la “Nota/Annotazione” in modo immodificabile del tipo “*Il documento non è stato protocollato in quanto trattasi di secondo esemplare del documento già pervenuto e registrato col prot. n. 000 del gg/mm/aaaa*”. Nella registrazione di protocollo del primo esemplare andrà invece inserita un'annotazione del tipo “*Pervenuto secondo esemplare via PEC (o altro mezzo) – vedi id. n. 000*”.

8.8. Documenti anonimi

La *ratio* che deve governare il comportamento di un operatore durante la fase di registrazione di un documento in entrata deve essere improntata all'avalutatività. In altre parole, l'operatore di protocollo deve attestare che un determinato documento, così come si è registrato, è pervenuto. Si tratta di una delicata competenza di tipo certificativo, attestante la certezza giuridica di data, forma e provenienza per ogni documento.

Le lettere anonime, pertanto, sono soggette a registrazione di protocollo. Se il documento anonimo è pervenuto a mezzo PEC si lascia come mittente l'indirizzo PEC.



CAPITOLO 9. IL SISTEMA INFORMATICO

Il sistema informatico è l'insieme di hardware, software, mezzi di comunicazione e procedure informatiche utilizzate dalle Amministrazioni per la gestione di documenti e dati in formato digitale. In particolare, il sistema di gestione informatica dei documenti attiene alla gestione dei documenti digitali (cfr. DPR 445/2000, art.1, lettera r).

La gestione dei flussi documentali è un insieme di funzionalità che consentono di trattare e di organizzare la documentazione prodotta (in entrata, in uscita e interna) dalle Amministrazioni.

Il Coordinatore della gestione documentale, d'intesa con il Responsabile della sicurezza (CSO - Chief Security Officer), individua le misure di sicurezza da adottare secondo quanto stabilito dalle normative vigenti valide per tutte le AOO presenti nell'Amministrazione.

Qualora emergessero esigenze specifiche da parte di una o più AOO, queste ultime dovranno individuare particolari misure di sicurezza da adottare d'intesa con il Coordinatore della gestione documentale.

9.1. Il modello organizzativo

I servizi di *Information and Communication Technology (ICT)* per il supporto all'attività istituzionale e amministrativa sono curati dal Servizio per la Gestione del Centro Unico dei Servizi (SGCUS), struttura appartenente alla Direzione Generale dei Sistemi Informativi Automatizzati (DGSIA).

Il SGCUS si occupa della gestione dei sistemi e cura il supporto per l'erogazione dei servizi IT presso tutte le sedi centrali e regionali della Cdc. Svolge azioni di coordinamento e promozione nell'ambito dei referenti informatici.

Il Servizio è responsabile della progettazione, realizzazione, implementazione e gestione dell'infrastruttura IT e della sua connessione al Sistema Pubblico di Connattività (SPC). Propone e realizza accordi di cooperazione infrastrutturale con altre Amministrazioni con particolare attenzione alla creazione di specifiche soluzioni di tipo Cloud.

Definisce e cura l'implementazione delle politiche di sicurezza sui sistemi informativi della Cdc e garantisce la collaborazione istituzionale con le altre PP.AA. e in particolare con l'Agenzia per l'Italia Digitale (AgID). Assicura altresì la condivisione delle esperienze maturate in medesimi ambiti con le strutture tecniche di SOGEI, nell'ambito della specifica Convezione in essere.

Nel dettaglio il Servizio svolge i seguenti compiti:

- cura l'organizzazione e il corretto funzionamento dei data center della Cdc;
- gestisce gli strumenti tecnologici e l'infrastruttura, rendendo disponibili i vari ambienti (sviluppo, test, collaudo, pre-produzione, produzione, manutenzione, formazione) su cui poggiano e di cui necessitano i singoli sistemi applicativi, assicura la condivisione di tali strumenti e delle risorse strumentali ad essi afferenti, promuove e favorisce le attività di interconnessione e integrazione architetturale e tecnologica



tra i vari sistemi applicativi, fornendo le strutture di competenza organizzativa e tecnica a supporto;

- provvede all'esame e alla selezione dei servizi offerti dai diversi Cloud Service Provider;
- provvede alla progettazione, implementazione e gestione delle architetture dei sistemi applicativi e delle infrastrutture IT, adottando il paradigma “Cloud first, Mobile first”;
- redige studi di fattibilità, analizza, progetta e implementa progetti ITC di natura innovativa e/o progetti che introducano tecnologie innovative all'interno del contesto infrastrutturale e tecnologico della Cdc;
- elabora, di concerto con il Servizio per la gestione e il coordinamento dei servizi informatici e telematici presso le sedi regionali, le linee guida sulle politiche di sicurezza informatica dell'Amministrazione;
- gestisce le architetture, le infrastrutture, le componenti di accesso, terminazione e virtualizzazione dei servizi SOA e non SOA, nonché la dislocazione dei relativi processi;
- cura la progettazione e implementazione del sistema centralizzato di gestione documentale e dei sistemi di collaborazione, assicurandone la loro massima diffusione e integrazione con tutti i sistemi applicativi;
- attende al coordinamento delle attività dei referenti informatici, dislocati nelle varie sedi centrali e periferiche dell'Amministrazione;
- assicura l'assistenza agli utenti dei sistemi IT della Corte tramite l'help desk di I e II livello, fornendo un unico punto di accesso alle richieste di supporto per tutte le sedi della Cdc. L'help desk fornisce assistenza per le postazioni di lavoro (fisse e mobili) su software di base, software di produttività individuale, servizi di rete, sistemi applicativi, banche dati e malfunzionamenti hardware sia in modalità diretta che mediando e monitorando l'intervento di ulteriori servizi interni ed esterni;
- introduce e diffonde le best practices ITIL (Information Technology Infrastructure Library) in tutti i processi di gestione IT, con particolare riguardo al ciclo di vita dei servizi, del governo e del monitoraggio della disponibilità, della continuità di servizio, delle procedure di dimensionamento, del monitoraggio dei livelli di servizio;
- coordina e partecipa con proprio personale al CAB di supporto al Change Manager per l'applicazione delle best practices ITIL, nell'ambito della stesura di appositi accordi di servizio con i singoli sistemi informativi.

Il Servizio è impegnato nella concretizzazione di quanto contenuto nella direttiva di II° livello emanata dalla DGSIA, che a sua volta implementa quanto disposto dalla Direttiva per l'azione amministrativa annuale emanata dal Presidente della Cdc. Inoltre dà attuazione e cura il costante monitoraggio del rispetto della Direttiva per l'utilizzo delle risorse informatiche coerentemente con quanto in essa specificato, esamina e valuta le richieste di forniture di materiale informatico provenienti da tutti gli uffici dell'Amministrazione e provvede ad istruire le pratiche per le assegnazioni del materiale hardware e software.



Con propri ordini di servizio il Dirigente, d'intesa con il Dirigente generale, organizza la struttura in funzione delle esigenze di miglior funzionalità della stessa, individua i diversi settori in cui questa si articola e i relativi responsabili amministrativi e assegna i compiti al personale sulla base dei carichi di lavoro previamente definiti nell'ambito della struttura. Provvede, inoltre, alla gestione delle risorse umane e strumentali assegnate al Servizio.

Nell'ambito della gestione documentale, l'Amministrazione ha acquisito la piattaforma MS SharePoint che attualmente è usufruita sia in modalità on premise che con una soluzione di tipo *Software as a Service* (SaaS): le funzionalità del programma sono rese disponibili attraverso un sito web, il cui accesso è subordinato a un processo di autenticazione informatica effettuato mediante il sistema centralizzato dell'Istituto.

Attualmente il sistema informatico della Cdc è dislocato in due data center on premise (Baiamonti e Carucci); in essi è collocata l'infrastruttura ICT sulla base della quale vengono erogati i servizi IT fruiuti dagli utenti finali (apparati, apparecchiature di rete, server, dispositivi IT, software di base, software applicativo, ecc.). La Cdc utilizza delle estensioni logiche dei data center on premise dislocate su cloud pubblico Microsoft Azure e Amazon AWS.

Inoltre vi è da rilevare che il data center on premise Baiamonti sarà migrato e consolidato presso il data center Carucci, gestito da Sogei.

9.2. La conduzione operativa

La conduzione operativa delle apparecchiature presenti nei data center on premise e nelle estensioni logiche degli stessi attualmente è curata da un fornitore²⁰ attraverso un apposito contratto per l'acquisizione di figure professionali per la conduzione dei sistemi della Cdc.

Al fornitore indicato, in virtù del contratto richiamato, sono demandati gli oneri di installazione, manutenzione, gestione, aggiornamento, monitoraggio di tutte le componenti fisiche e logiche infrastrutturali, di verifica della correttezza operativa delle funzioni applicative e dell'integrità delle basi di dati in conformità a quanto previsto dalla normativa vigente in materia di sicurezza e di protezione dei dati, di Continuità Operativa (CO) e di Disaster Recovery (DR).

9.3. Sicurezza del sistema informatico

La sicurezza dei dati, delle informazioni e dei documenti informatici memorizzati (poi archiviati) nel sistema di gestione documentale è garantita dall'utilizzo della piattaforma MS SharePoint adottata dall'Amministrazione, sia on premise che on cloud (definita SharePoint on line).

Il piano della sicurezza informatica relativo a formazione, gestione, trasmissione, interscambio, accesso, memorizzazione dei documenti informatici, ivi compresa la gestione delle copie di sicurezza nel rispetto delle misure minime di sicurezza previste nel disciplinare tec-

²⁰ Attualmente il Lotto 2 – Servizi di conduzione è affidato al RTI HP Enterprise Services Italia Srl – Open System Srl.

nico descritto nell'Allegato B del D.Lgs. 30 giugno 2003, n. 196 e successive modificazioni è in corso di redazione da parte del SGCUS, che avrà anche il compito di mantenerlo aggiornato con frequenza annuale.

9.3.1. Il sistema di gestione documentale

Il sistema di gestione documentale è costituito dall'insieme delle tecnologie presenti presso i *data center* on premise e presso i sistemi e le componenti dislocate in cloud, nonché da tutti i dispositivi e i programmi presenti presso le varie sedi operative dell'Amministrazione che permettono l'utilizzo del sistema.

In particolare, sono parte integrante dell'infrastruttura i cablaggi e gli apparati di rete presenti presso le sedi dell'Amministrazione e necessari per la connettività verso la rete SPC, i sistemi informatici e le componenti software sottese al sistema di autenticazione dell'Amministrazione e tutte le postazioni di lavoro utilizzate dagli utenti del sistema di gestione documentale inclusi i dispositivi mobili.

Le misure di sicurezza fisica e logica specifiche e le procedure comportamentali adottate per la protezione dell'infrastruttura del sistema di gestione documentale, delle informazioni e dei dati sono riportate nei paragrafi seguenti. In essi è data evidenza di quali ambiti siano gestiti e curati dal Raggruppamento Temporaneo di Imprese (RTI) che si occupa della conduzione operativa, quali siano curati dal SGCUS della DGSIA e quali invece rimangano in carico esclusivo a ogni specifica AOO.

Resta comunque inteso che le indicazioni su quali documenti siano riportate, e quindi reperibili, le informazioni relative alla sicurezza anche in relazione alla CO sono a carico del SGCUS. Per tutto quello che si riferisce all'attivazione e alla gestione del registro di emergenza si rimanda a quanto descritto nel CAPITOLO 6.

Il sistema di gestione documentale è concepito come un servizio trasversale a tutte le applicazioni esistenti, che permette alla Cdc di centralizzare tutti i processi di gestione documentale, nonché tutto il patrimonio documentale esistente. Tale architettura consente di costituire un sistema di gestione elettronica documentale i cui servizi siano usufruibili dai sistemi applicativi, creando un'unica base informativa che venga alimentata da tutti gli applicativi gestionali e che, a sua volta, si renda disponibile ad altri soggetti (persone e applicativi) per mezzo di canali diversi (es. il canale "mobile"), in modo da costituire uno strumento messo "a fattor comune" fra tutti i possibili utilizzatori.

Il sistema di gestione documentale è strutturato in tre componenti logici:

- Agorà, che contiene i documenti ufficiali dell'Amministrazione;
- Docs, dedicato ad ospitare i documenti di preminente utilizzo dei sistemi applicativi;
- Domos, dedicato alla documentazione personale di ogni utente.

Tutti i documenti dovranno essere allocati in una di tali componenti.

Avendo l'Amministrazione deciso di utilizzare a supporto della gestione documentale la piattaforma MS SharePoint, i file server e tutti gli altri supporti informatici (hard disk, chia-

vette usb, ecc.) non vengono considerati componenti del sistema di gestione documentale e dunque non possono essere adoperati per la memorizzazione dei documenti.

9.3.2. Sicurezza fisica dei data center

Le misure di sicurezza fisica in carico all'Amministrazione sono descritte di seguito.

I sistemi server e gli apparati di rete sono ospitati in ambienti che presentano i seguenti livelli minimi di sicurezza fisica:

- locali dedicati esclusivamente a ospitare gli apparati server e i dispositivi di rete;
- impianto di videosorveglianza;
- sistema di controllo e tracciatura degli accessi;
- sistema di estinzione degli incendi;
- alimentazione elettrica protetta da dispositivi di stabilizzazione e continuità della tensione (UPS);
- impianto di climatizzazione automatico opportunamente dimensionato in grado di mantenere una temperatura ambientale non superiore ai 25°.

I locali non devono:

- essere soggetti ad allagamenti e devono disporre delle eventuali protezioni specifiche necessarie;
- ospitare apparecchiature pericolose o che aumentino il rischio di allagamenti, incendi o inagibilità dei locali stessi;
- essere utilizzati per stivare materiali infiammabili o essere utilizzati come deposito di materiale e attrezzi.

Eventuali interventi di qualsiasi natura (anche non informatica) nei locali ospitanti gli apparati server e gli apparati di rete devono sempre avvenire in presenza di personale autorizzato.

E' da precisare che, anche al fine di aumentare la sicurezza fisica e logica complessiva, la Cdc ha in programma la dislocazione del data center on premise Baiamonti presso il centro di Carucci, gestito da Sogei, dotato di migliori servizi di facility management (impianti di climatizzazione, antiincendio, videosorveglianza, controllo e tracciatura accessi, sicurezza perimetrale, ecc.).

Per quanto attiene le informazioni relative alla CO, al DR, ai punti di ripristino (*Restore Point Objective* - RPO), al tempo di ripristino dei servizi (*Recovery Time Objective* - RTO) e alle misure di messa in sicurezza di dati e applicazioni, si rimanda ai piani DRP (Disaster Recovery Plan) e BCP (Business Continuity Plan) redatti e manutenuti dal SGCUS.



9.3.3. La manutenzione e la continuità operativa degli impianti elettrici

Gli impianti elettrici devono essere monitorati da sistemi automatici di allarme in grado di allertare i tecnici di manutenzione in caso di anomalie e permetterne l'intervento entro il tempo di protezione garantito dai sistemi *UPS*.

9.3.4. Rete dati

L'utilizzo del sistema di gestione documentale è garantito dalla rete dati dell'Amministrazione e dalla rete SPC, sistema al quale la Cdc aderisce.

Il Centro Unico dei Servizi, in qualità di amministratore della rete, assicura in modo esclusivo e tempestivo la gestione, il monitoraggio, l'aggiornamento e l'ampliamento della rete dati (cablaggio e parte attiva), sia sotto l'aspetto fisico che logico, fino alla presa utente compresa.

L'amministratore della rete registra – in appositi *file* di *log* – i dati relativi all'accesso alla rete dell'Amministrazione e all'accesso a internet o al traffico telematico in generale (escluso il contenuto della trasmissione dati).

I dati registrati nei *file* di *log* sono raccolti, memorizzati e conservati in conformità alla normativa vigente. Le informazioni contenute nei *file* di *log* possono essere messe a disposizione dell'autorità giudiziaria, la quale può richiedere la non cancellazione e la conservazione per un periodo più lungo di quanto disposto dalla legge.

Ciascun dirigente o preposto di AOO è responsabile dei dispositivi collegati alla rete dell'Amministrazione e utilizzati per l'accesso al sistema di gestione documentale e deve riferirsi all'amministratore della rete per ogni violazione o sospetto di violazione della sicurezza informatica. Inoltre, ogni AOO opera secondo le direttive e le procedure stabilite dall'amministratore della rete, nel rispetto delle norme previste dall'Amministrazione, garantendone altresì il rispetto, per quanto di propria competenza, da parte dell'utenza gestita e adottando tempestivamente i provvedimenti previsti.

9.3.5. Le postazioni di lavoro

Le postazioni di lavoro degli utenti dell'Amministrazione sono gestite dal SGCUS che si occupa anche di fornire e manutenere gli strumenti inerenti l'utilizzo del sistema di gestione documentale.

Per postazioni di lavoro si intendono i pc desktop in dotazione agli utenti, notebook, ultrabook, smartphone e tablet.

SGCUS verifica il coerente utilizzo delle postazioni di lavoro, da tavolo o portatili, o degli strumenti comunque funzionalmente assimilabili e predisponde la necessaria dotazione di dispositivi (*hardware*) e programmi (*software*) tali da consentire il corretto funzionamento e il mantenimento in condizioni di sicurezza ai fini del regolare svolgimento dell'attività lavorativa.

Le postazioni di lavoro soddisfano i criteri minimi di sicurezza, in particolare:

- il sistema operativo è costantemente aggiornato e aggiornabile;
- tutti gli aggiornamenti di sicurezza sono applicati attraverso un processo definito e condiviso;
- gli applicativi installati e i loro componenti software aggiuntivi (ad es., *plug-in*) sono aggiornati e aggiornabili;
- sono dotate di un programma antivirus con funzionalità automatica di aggiornamento periodico;
- l'accesso al sistema operativo della postazione di lavoro è protetto da *password* di adeguata complessità, cambiata con cadenza regolare;
- sono dotate di tutti i programmi necessari per lo svolgimento delle attività lavorative nonché della suite di produttività Microsoft Office 2013/2016;
- sono dotate dell'Enhanced Mitigation Experience Toolkit (EMET), un'utilità che consente di prevenire le vulnerabilità del software di cui un malintenzionato potrebbe approfittare, utilizzando tecnologie per l'attenuazione a livello di sicurezza che funzionano come protezioni speciali e ostacoli che un autore dannoso deve abbattere per sfruttare le vulnerabilità del software presente;
- l'utente può utilizzare OneDrive, dislocato sul cloud MS Azure, per gestire e collocare i propri dati, soprattutto documenti;
- possono raggiungere la piattaforma di gestione documentale, sia quella dislocata on premise che quella collocata on cloud;
- salvo motivate e documentate eccezioni, su di esse non è permessa la connessione remota dall'esterno della Rete Dati dell'Amministrazione (*RDP, SSH, VNC*, ecc.);
- la connessione da remoto ad esse dall'interno della Rete Dati dell'Amministrazione, ove attivata, viene effettuata esclusivamente mediante protocolli di comunicazione sicuri ed è consentita solo previo consenso dell'utente che in quel momento sta utilizzando l'elaboratore.

E' da rilevare che in Cdc vi sono operativi anche i desktop virtuali, erogati attraverso specifiche piattaforme tecnologiche; tali desktop virtuali, qualora messi a disposizione degli utenti, anche per un periodo di tempo limitato e definito, devono essere considerati alla stregua dei corrispondenti desktop erogati da postazioni di lavoro o dispositivi fisici.

9.4. Sicurezza dei documenti informatici

L'accesso al sistema di gestione documentale di ogni utente dell'Amministrazione è gestito centralmente ed è subordinato all'abilitazione da parte del Coordinatore della gestione documentale.

Le identità digitali utilizzate per l'accesso al sistema di gestione documentale sono costituite da *nome utente* e *password*. L'identificazione informatica dell'utente, cioè la validazione dell'identità digitale, è operata attraverso un'infrastruttura di autenticazione centralizzata basata su Microsoft Active Directory (*AD*).

Inoltre in Cdc è presente il meccanismo denominato Microsoft Active Directory Federation Services (*ADFS*), che è una soluzione di accesso alle identità che consente ai client basati su browser (interni o esterni alla rete) di utilizzare una singola procedura semplificata per accedere a una o più applicazioni aperte su Internet e protette, anche se gli account utente e le applicazioni si trovano in reti o organizzazioni completamente diverse.

L'accesso al sistema di gestione documentale da parte di soggetti esterni all'Amministrazione è consentito attraverso procedure tecniche specificatamente definite e dietro autorizzazione del coordinatore della Gestione documentale.

Il sistema di gestione documentale rispetta le misure di sicurezza previste dagli artt. 31-36 e dal disciplinare tecnico di cui all'allegato B del D.Lgs. 30 giugno 2003, n. 196.

I dati sono resi disponibili e accessibili a chiunque ne abbia diritto; si individuano, a tal proposito, i soggetti preposti al trattamento dei dati:

- *Titolare del trattamento* – È il destinatario delle norme, ossia la persona fisica e/o giuridica, l'Amministrazione pubblica o altro Ente a cui compete decidere finalità, modalità del trattamento dei dati personali e strumenti utilizzati, compresa la sicurezza;
- *Responsabile del trattamento* – La persona fisica, giuridica, l'Amministrazione pubblica o altro Ente designato, facoltativamente, dal titolare a trattare i dati compreso il profilo relativo alla sicurezza;
- i Direttori Generali per gli Uffici di staff o per unità di lavoro trasversali alla direzioni generali presenti all'interno dell'Amministrazione;
- i Dirigenti per le Aree dirigenziali dell'Amministrazione Centrale;
- i Responsabili della gestione documentale di ogni AOO, qualora nominati;
- il Coordinatore della gestione documentale.
- *Responsabile esterno del trattamento* – in coerenza con il modello organizzativo adottato dell'Amministrazione per la conduzione del sistema di gestione documentale, al RTI indicato in precedenza è conferito il ruolo di Responsabile esterno del trattamento; in virtù di tale ruolo è il RTI che, per le attività di conduzione del sistema, gestione applicativa e assistenza, provvede alla nomina dell'amministratore di sistema, ne assolve i compiti e conseguenti adempimenti.
- *Incaricato del trattamento* – La persona fisica autorizzata a compiere operazioni di trattamento dati dal Titolare o dal Responsabile.

I Responsabili del trattamento designano, con provvedimento espresso, gli Incaricati del trattamento dei dati operanti all'interno della struttura di competenza.

Nello svolgimento dei compiti è fatto divieto agli Incaricati di comunicare e/o di divulgare qualsivoglia dato sensibile e/o personale. Tale obbligo di riservatezza è esteso anche al periodo successivo alla scadenza dell'incarico, fino a quando le suddette informazioni non vengano divulgate a opera del Titolare, oppure divengano di dominio pubblico in base al procedimento amministrativo di riferimento.

L'applicazione delle normative sulla privacy e sulla sicurezza dei dati è in carico agli Incaricati nominati dai Responsabili del trattamento di cui al Decreto Presidenziale n. 56 del

07/12/2011 (riguardante l'individuazione dei responsabili del trattamento dei dati personali gestiti nell'ambito degli uffici amministrativi centrali della Cdc).

9.4.1. Accesso e profili di abilitazione ai dati e ai documenti informatici

Il sistema adottato dall'Amministrazione garantisce:

- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso ai documenti, alle informazioni e ai dati esclusivamente agli utenti abilitati;
- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;
- la registrazione delle attività svolte da ciascun utente anche rilevanti ai fini della sicurezza, in modo tale da garantirne l'identificazione;
- l'immodificabilità dei contenuti e, comunque, la loro tracciabilità.

Attraverso una *ACL* il sistema di gestione documentale permette l'assegnazione differenziata dei profili di abilitazione, intervento, modifica e visualizzazione dei documenti in rapporto alle funzioni e al ruolo svolto dagli utenti e garantisce la protezione dei dati personali e dei dati sensibili.

I diritti di accesso prevedono genericamente i seguenti privilegi:

- Lettura
- Modifica
- Scrittura
- Controllo completo

Per gestire situazioni particolari di visibilità (ad es. gruppi di lavoro) possono essere creati dei ruoli ad hoc.

I suddetti ruoli hanno abilitazioni diverse sui documenti/fascicoli della AOO gestite dal responsabile della gestione documentale.

Il Responsabile della gestione documentale di ciascuna AOO autorizza le nuove abilitazioni, le modifiche e ha l'onere di comunicare tempestivamente la cessazione dei diritti sugli applicativi di competenza.

Il controllo degli accessi è assicurato dall'utilizzo di credenziali di autenticazione con differenti profili di autorizzazione in relazione ai diversi ruoli di ciascun utente. I trattamenti associabili a ciascun profilo, preventivamente individuati dal Coordinatore della gestione documentale di concerto con i Responsabili del trattamento dei dati e i Responsabili della gestione documentale delle diverse AAO, sono in sintesi:

- *inserimento* dei dati per effettuare una registrazione;
- *modifica* dei dati di una registrazione;



- *annullamento* di una registrazione;
- *ricerca* di informazioni registrate ai fini della visualizzazione o consultazione;
- *visualizzazione e consultazione*;
- *download* dei documenti associati alla registrazione;
- *upload* dei documenti associati alla registrazione.

Periodicamente, e comunque almeno annualmente, è verificata a cura del Coordinatore della gestione documentale di concerto con i Responsabili delle strutture della conduzione operativa e i Responsabili della gestione documentale, la sussistenza delle condizioni per il mantenimento dei profili di autorizzazione per tutte le AOO.

Quando l'accesso ai dati e agli strumenti informatici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni volte a individuare chiaramente le modalità con le quali il Titolare può assicurare la disponibilità di dati o di strumenti informatici in caso di prolungata assenza o di impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

In tal caso, la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente e attraverso specifiche procedure i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'Incaricato dell'intervento effettuato.

Le stesse credenziali non possono essere assegnate a persone diverse, neppure in tempi diversi, in quanto le credenziali stesse sono strettamente personali. Ciò vale per qualunque forma di credenziali si adoperi per l'accesso e l'utilizzo del sistema di gestione documentale.

Ciascun utente ha la possibilità di cambiare la propria *password* in qualsiasi momento attraverso una specifica procedura codificata e posta a conoscenza degli utenti; è auspicabile che ciò avvenga nel caso in cui si presume che essa abbia perso il requisito della segretezza; comunque la procedura impone un cambio periodico.

Le postazioni di lavoro, i dispositivi mobili e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà dall'Amministrazione a vario titolo messi a disposizione del personale, sono da considerarsi un particolare strumento di lavoro e il loro utilizzo è finalizzato allo svolgimento delle attività professionali e istituzionali dell'Amministrazione stessa. Ogni utente deve adottare comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza dei sistemi informatici, rispettando quanto stabilito dalla direttiva inerente l'utilizzo delle risorse informatiche.

In ogni caso, l'utilizzo delle risorse informatiche dell'Amministrazione, non deve pregiudicare il corretto adempimento della prestazione lavorativa, ostacolare le attività operative o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici e istituzionali.

Gli utenti a cui sono affidate le postazioni di lavoro dell'Amministrazione, sono soggetti a tutte le responsabilità dettate dalla normativa vigente e applicabile.

Si sottolineano le seguenti responsabilità:

- l'utente è responsabile per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui ha accesso; qualora sulle postazioni di lavoro siano memorizzati dati sensibili o giudiziari, il responsabile della postazione stessa deve attuare le misure idonee previste dall'Allegato B al D.Lgs. 30 giugno 2003, n. 196;
- l'utente è tenuto a segnalare immediatamente ai referenti informatici e al Coordinatore della gestione documentale ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
- in caso di cessazione del rapporto di lavoro, l'utente deve restituire all'Amministrazione qualsiasi risorsa informatica assegnata e mettere a disposizione ogni informazione di interesse istituzionale al fine di non intralciare il normale processo operativo e i vari procedimenti amministrativi che riguardavano l'utente stesso.

Sulle postazioni di lavoro non è ammesso:

- installare programmi o software di ogni genere che siano tutelati ai sensi della convenzione sulla protezione delle opere letterarie e artistiche, nonché le banche dati che, per la scelta o per la disposizione del materiale, costituiscono una creazione intellettuale dell'autore, se non in possesso delle relative licenze d'uso;
- installare o utilizzare modem o dispositivi similari per l'accesso da o verso l'esterno della rete dell'Amministrazione, se non preventivamente autorizzati;
- installare programmi, librerie di codici o manufatti software compilati di qualsiasi genere non inerenti all'attività lavorativa e/o privi di licenze d'uso;
- utilizzare qualsiasi supporto e/o tecnologia per un uso improprio dei dati la cui titolarità è della Cdc.

E' consentito, invece, utilizzare dispositivi mobili quali punti di accesso verso il dominio interno dell'Amministrazione, secondo le politiche di BYOD (*Bring Your Own Device*) appositamente stilate dal settore SGCUS. E' inoltre possibile utilizzare tali dispositivi per usufruire dei servizi esterni al dominio stesso.

Per adempiere al proprio dovere di diligenza e vigilanza nell'utilizzo dei beni e strumenti assegnati, il dipendente ha l'obbligo di impedire ad altri utilizzi indebiti della propria apparecchiatura informatica.

L'utente è tenuto a bloccare o a spegnere il *personal computer* o la postazione di lavoro assegnata e in dotazione, in caso di sospensione o di termine dell'attività lavorativa, assicurandosi di evitarne l'utilizzo improprio da parte di terzi, mediante inserimento di apposite credenziali di accesso.

Le stazioni di lavoro, da tavolo e portatili, i dispositivi di lavoro mobili o gli strumenti comunque funzionalmente assimilabili, messi a disposizione del personale, non devono essere lasciati incustoditi.

Al termine dell'orario di servizio, i *computer* devono essere spenti prima di lasciare gli uffici. In caso di allontanamento temporaneo, l'utente deve attivare il salvaschermo con sblocco tramite *password*.

In linea generale è fortemente raccomandato di evitare la memorizzazione di dati sensibili o giudiziari su dispositivi mobili (*palmari, notebook, tablet, smartphone, penne USB, dischi rigidi esterni, memory card*, ecc.). Quando, per giustificati motivi, ciò si rendesse necessario, è fatto obbligo di adottare le misure idonee prescritte dal già citato allegato B al D.Lgs. 30 giugno 2003, n. 196.

Le credenziali di accesso (generalmente, *nome utente e password*) sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime. Per la disciplina riguardante l'utilizzo delle credenziali, per la segretezza e per la protezione delle *password* è fatto riferimento espresso alle disposizioni contenute nel D. Lgs. 30 giugno 2003, n. 196, e, in particolare, agli artt. 4 comma 3 lett. d) e 34.



CAPITOLO 10. ALLEGATI

In questo capitolo vengono riportati gli allegati al presente documento.

10.1. Allegato 1: Riferimenti normativi

- Legge 7 agosto 1990, n. 241, *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*
- Decreto del Presidente della Repubblica 4 aprile 2002, n. 101, *Regolamento recante criteri e modalità per l'espletamento da parte delle Amministrazioni pubbliche di procedure telematiche di acquisto per l'approvvigionamento di beni e servizi*
- Direttiva del Ministro per l'innovazione e le tecnologie 9 dicembre 2002, *Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali*
- Decreto legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*
- Legge 9 gennaio 2004, n. 4, *Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici*
- Decreto legislativo 22 gennaio 2004, n. 42, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*
- Decreto legislativo 7 marzo 2005, n. 82, *Codice dell'Amministrazione digitale*
- Legge 24 dicembre 2007, n. 244, *Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008)*
- Decreto legge 29 novembre 2008, n. 185, *Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale*
- Legge 3 marzo 2009, n. 18 Ratifica ed esecuzione della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, con Protocollo opzionale, fatta a New York il 13 dicembre 2006 e istituzione dell'Osservatorio nazionale sulla condizione delle persone con disabilità
- Legge 18 giugno 2009, n. 69, *Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile*
- Decreto legislativo 27 ottobre 2009, n. 150, *Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle Pubbliche Amministrazioni*
- Deliberazione del Garante per la protezione dei dati personali 2 marzo 2011, n. 88, *Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web*
- Decreto Legge n. 9 febbraio 2012, n. 5 coordinato con la Legge di conversione 4 aprile 2012, n. 35, *Disposizioni urgenti in materia di semplificazione e di sviluppo*
- Legge 17 dicembre 2012, n. 221, *Conversione in legge, con modificazioni, del Decreto Legge 18 ottobre 2012, n. 179 recante ulteriori misure urgenti per la crescita del Paese*
- Circolare dell'Agenzia per l'Italia Digitale – AIPA 23 gennaio 2013, n. 60 *Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni - Revisione della Circolare AIPA del 7 maggio 2001, n. 28 relativa agli standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le Pubbliche Amministrazioni e associate ai*



documenti protocollati, ai sensi dell'art. 18, comma 2, del D.P.C.M. 31 ottobre 2000 di cui al D.P.R. 28 dicembre 2000, n. 445

- DPCM 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*
- Circolare interpretativa del Ministero dell'Economia e Finanze numero 1/DF del 9 marzo 2015 *in tema di fatturazione elettronica*
- Circolare dell'Agenzia per l'Italia Digitale 29 marzo 2013, n. 61, *Disposizioni del Decreto legge n. 79 del 18 ottobre 2012 in tema di accessibilità dei siti web e servizi informatici. Obblighi delle Pubbliche Amministrazioni*
- Decreto del Ministro dell'Economia e delle Finanze 3 aprile 2013, n. 55, *Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle Amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244*
- DPCM 3 dicembre 2013, *Regole tecniche in materia di sistema di conservazione degli archivi digitali*
- DPCM 3 dicembre 2013, *Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005*
- Deliberazione del Garante per la protezione dei dati personali 15 maggio 2014, n. 243, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*
- Decreto del Ministro dell'Economia e delle Finanze 17 giugno 2014, *Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005*
- Regolamento del Parlamento e del Consiglio dell'Unione europea 23 luglio 2014, n. 910, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (eIDAS)*
- Decreto legge 24 aprile 2014, n. 66, *Misure urgenti per la competitività e la giustizia sociale*
- Legge 16 maggio 2014, n. 78, *Conversione in legge, con modificazioni, del decreto legge 20 marzo 2014, n. 34, recante disposizioni urgenti per favorire il rilancio dell'occupazione e per la semplificazione degli adempimenti a carico delle imprese*
- DPCM 13 novembre 2014, *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle Pubbliche Amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005*
- Decreto del Ministero del lavoro e delle politiche sociali 30 gennaio 2015, *Semplificazione in materia di documento unico di regolarità contributiva (DURC)*
- Deliberazione del Garante per la protezione dei dati personali 19 marzo 2015, n. 161, *Linee guida in materia di trattamento di dati personali per profilazione on line*
- Decreto legislativo 18 aprile 2016, n. 50 *Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture*



- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (Regolamento generale sulla protezione dei dati).

10.2. Allegato 2: AOO – UO

Le AOO della Cdc comprendenti uffici sono complessivamente 110.

AOO UFFICI CENTRALI

1. PRESIDENZA

- Gabinetto
- Ufficio Stampa
- Ufficio Legale e documentazione
- Ufficio Affari internazionali

2. ORGANISMO DI VALUTAZIONE DELLA PERFORMANCE

3. CONSIGLIO DI PRESIDENZA

- Ufficio Segreteria
- Ufficio studi e documentazione

4. SEGRETARIO GENERALE

- Segreteria del Segretario generale
- Servizio ispettivo
- Servizio contenzioso del lavoro
- Servizio controllo di gestione
- Servizio statistica
- Servizio per il trattamento economico e quiescenza dei magistrati
- Servizio relazioni sindacali
- Ufficio relazioni con il pubblico
- Biblioteca
- Struttura di supporto agli organi di valutazione della dirigenza di II fascia
- Consiglio di Amministrazione
- Collegio dei revisori

5. SEMINARIO DI FORMAZIONE PERMANENTE

6. SERVIZIO MASSIMARIO E RIVISTA



7. DIREZIONE GENERALE GESTIONE AFFARI GENERALI

- Segreteria della direzione generale gestione affari generali
- Segreteria tecnica
- Servizio affari amministrativi ed attività negoziale
- Servizio prevenzione e sicurezza
- Ufficio del cassiere
- Ufficio del consegnatario
- Servizio provveditorato gestione finanziaria e patrimoniale delle strutture regionali
- Servizio tecnico

8. DIREZIONE GENERALE GESTIONE RISORSE UMANE E FORMAZIONE

- Segreteria della direzione generale gestione risorse umane e formazione
- Struttura protocollo centrale Segretariato generale
- Servizio formazione ed aggiornamento del personale
- Servizio accessi, mobilità e dotazioni organiche
- Servizio disciplina del rapporto di lavoro
- Servizio trattamento economico del personale amministrativo
- Servizio per i procedimenti disciplinari
- Struttura di gestione del personale ausiliario e di supporto

9. DIREZIONE GENERALE PROGRAMMAZIONE E BILANCIO

- Segreteria della direzione generale programmazione e bilancio
- Servizio bilancio e contabilità
- Servizio di controllo di regolarità amministrativa e contabile

10. DIREZIONE GENERALE SISTEMI INFORMATIVI AUTOMATIZZATI

- Segreteria della direzione generale sistemi informativi automatizzati
- Servizio per la gestione degli acquisti, gare e contratti
- Servizio per la gestione dei progetti applicativi
- Servizio per la gestione del centro unico dei servizi
- Servizio per la gestione ed il coordinamento dei servizi informatici e telematici presso le sedi regionali



- 11. SEZIONI RIUNITE IN SEDE GIURISDIZIONALE, DELIBERANTE E CONSULTIVA**
- 12. SEZIONI RIUNITE IN SEDE CONTROLLO**
- 13. UFFICIO DEL RUOLO GENERALE GIUDIZI APPELLO**
- 14. I SEZIONE CENTRALE D'APPELLO**
- 15. II SEZIONE CENTRALE D'APPELLO**
- 16. III SEZIONE CENTRALE D'APPELLO**
- 17. PROCURA GENERALE**
- 18. SEZIONE CENTRALE DI CONTROLLO LEGITTIMITÀ'**
 - Segreteria della Sezione centrale di controllo legittimità
 - Ufficio controllo atti Presidenza del Consiglio, Ministero giustizia e Ministero affari esteri
 - Ufficio controllo atti Ministero interno e Ministero difesa
 - Ufficio controllo atti Ministero economia e finanza
 - Ufficio controllo atti Ministero sviluppo economico e Ministero politiche agricole
 - Ufficio controllo atti Ministero infrastrutture e Ministero ambiente
 - Ufficio controllo atti Ministero istruzione, Ministero beni e attività culturali, Ministero salute e Ministero lavoro
- 19. SEZIONE CENTRALE DI CONTROLLO SULLA GESTIONE**
 - Segreteria della Sezione centrale di controllo gestione
 - Ufficio controllo sulla gestione Ministeri istituzionali
 - Ufficio controllo sulla gestione Ministeri economico-finanziari
 - Ufficio controllo sulla gestione Ministeri attività produttive
 - Ufficio controllo sulla gestione Ministeri infrastrutture ed assetto del territorio
 - Ufficio controllo sulla gestione Ministeri alla persona e beni culturali
 - Collegio di controllo sulle entrate
- 20. COLLEGIO DI CONTROLLO SULLE SPESE ELETTORALI E FONTI**
- 21. FINANZIAMENTO**
- 22. SEZIONE CONTROLLO ENTI**
- 23. SEZIONE DELLE AUTONOMIE**

24. SEZIONE DI CONTROLLO AFFARI COMUNITARI E INTERNAZIONALI

AOO SEDE REGIONALE LAZIO

25. SEZIONE GIURISDIZIONALE

26. PROCURA REGIONALE

27. SEZIONE REGIONALE CONTROLLO

AOO DELLA SEDE DELLA REGIONE SARDEGNA

28. SERVIZIO AMMINISTRATIVO UNICO REGIONALE

29. SEZIONE GIURISDIZIONALE

30. PROCURA REGIONALE

31. SEZIONE REGIONALE CONTROLLO

- Ufficio controllo legittimità Amministrazioni statali (ufficio I)
- Ufficio controllo legittimità Amministrazioni regionali (ufficio II)
- Ufficio controllo gestione enti locali (ufficio III)

32. SEZIONI RIUNITE

AOO DELLA SEDE DELLA REGIONE SICILIANA

33. SERVIZIO AMMINISTRATIVO UNICO REGIONALE

34. SEZIONE GIURISDIZIONALE

35. SEZIONE GIURISDIZIONALE D'APPELLO

36. PROCURA GENERALE

37. PROCURA REGIONALE

38. SEZIONE REGIONALE CONTROLLO

- Ufficio controllo legittimità Amministrazioni statali (ufficio I)
- Ufficio controllo legittimità Amministrazioni regionali (ufficio II)
- Ufficio controllo gestione enti locali (ufficio III)

39. SEZIONI RIUNITE

AOO DELLE SEDI DI TRENTO E BOLZANO

40. AMMINISTRAZIONE ATTIVA I. SEZIONE GIURISDIZIONALE

41. PROCURA REGIONALE



42. SEZIONE REGIONALE CONTROLLO

AOO DELLE ALTRE SEDI REGIONALI

(Abruzzo, Basilicata, Calabria, Campania, Emilia Romagna, Friuli Venezia Giulia, Liguria, Lombardia, Marche, Molise, Piemonte, Puglia, Toscana, Umbria, Valle d'Aosta, Veneto)

43. SERVIZIO AMMINISTRATIVO UNICO REGIONALE

44. SEZIONE GIURISDIZIONALE

45. PROCURA REGIONALE

46. SEZIONE REGIONALE CONTROLLO



10.3. Allegato 3: Riferimenti normativi interni

Struttura emanante	Oggetto	Data e protocollo	Tipologia
Segretariato Generale	Nuove modalità di pubblicazione sui siti web della Cdc		Allegato tecnico
Segretariato Generale	Nuove modalità di pubblicazione sui siti web della Cdc	10/12/2015 (0000067-10/12/2015-CIRC-UOPROT-P)	Circolare
Presidente	Periodi di conservazione dei documenti nell'archivio di deposito	19/02/2016 (0000011-19/02/2016-DECP-UOPROT-P)	Decreto Presidenziale
Presidente	Prime regole tecniche ed operative per l'utilizzo della posta elettronica certificata nei giudizi dinanzi alla Cdc	28/10/2015 (0000098-21/10/2015-DECP-UOPROT-P)	Decreto Presidenziale
Segretariato Generale	Posta elettronica certificata	31/01/2012 (0000008-31/01/2012-CIRC-UOPROT-P)	Circolare
Segretariato Generale	Normalizzazione denominazione caselle PEC conseguente all'applicazione dei DP 98/2015 e 9/2016. Istituzione caselle PEC per Segreterie	17/06/2016 (0000031-17/06/2016-CIRC-UOPROT-P)	Circolare
Segretariato Generale	Pubblicazione delle prime regole tecniche e delle relative istruzioni tecnico-operative per l'utilizzo della posta elettronica certificata nei giudizi dinanzi alla Cdc – Conseguenti adempimenti	30/10/2015 (0000052-30/10/2015-CIRC-UOPROT-P)	Circolare
Presidente	Definizione delle AOO	22/05/2014 (0000024-22/05/2014-DECP-UOPROT-P)	Decreto Presidenziale
DGSIA	L'utilizzo delle casella istituzionale di posta elettronica ordinaria	04/07/2013 (0000036-04/07/2013-CIRC-UOPROT-P)	Circolare
Presidente	Norme sul funzionamento dell'Archivio Generale e aggiornamento regole di scarto	14/1987	Determinazione Presidenziale
Presidente	Norme sul funzionamento dell'Archivio Generale e regole di scarto	375/1981	Determinazione Presidenziale



10.4. Allegato 4: Titolario

Di seguito sono elencati i titolari di classificazione attualmente in uso.

10.4.1. Titolario Amministrazione attiva

Il seguente titolario è in uso presso i SAUR regionali e presso le seguenti AOO Centrali per la documentazione amministrativa:

- Procura Generale
- Procura Regionale Lazio
- Controllo Lazio
- Sezione Giurisdizionale Lazio
- Ruolo Generale dei Giudici di appello
- Sezione Giurisdizionale I di Appello
- Sezione Giurisdizionale II di Appello
- Sezione Giurisdizionale III di Appello

Qualche sede ha richiesto qualche nodo di quarto livello aggiuntivo per dettagliare meglio una particolare materia.

Titolario Amministrazione Attiva				
1				Organizzazione
1	10			Direzione
1	10	10		Comunicazioni
1	20			Decreti e disposizioni
1	20	10		Ordini di Servizio/Direttive/Decreti/Circolari
1	20	20		Gruppi di Studio
1	20	30		Commissioni
1	30			Direttive generali e circolari del Consiglio di Presidenza
1	30	10		Convocazioni - Sintesi e Deliberazioni
1	30	20		Procedure concorsuali e conferimenti di incarico
1	40			Commissione di vigilanza e scarto sugli archivi
1	50			Direttive - decreti - circolari dei vertici della Corte dei conti
1	50	10		Presidente Corte dei conti
1	50	20		Segretario Generale
1	50	30		Dirigenti generali
1	60			Consulenti Tecnici
1	70			Direttive e decreti - circolari della Procura Generale
1	70	10		Comunicazioni e Note del Procuratore Generale
1	80			Cerimoniale
1	90			L. 241/90



1	90	10		Accesso documenti
1	90	20		Altri adempimenti
1	100			Trattamento dati personali
1	110			Comunicati stampa
1	130			Servizi comuni
1	130	10		Ausiliari - autisti
1	130	20		Auto di servizio e permessi sosta
1	130	30		Biblioteca
1	130	40		Telefonia
1	130	50		Gestione immobili
1	130	50	10	Richiesta intervento
1	130	50	20	Inventario provincia
1	140			Convenzioni
1	140	10		Banche - Università - altre
1	150			Richiesta Informazioni
1	160			L.89/2001 (Legge Pinto Equariparazione)
1	160	10		Accesso documenti
1	160	20		Altri adempimenti
2				Pianificazione-Programmazione-Rendicontazione
2	10			Controllo di Gestione
2	20			Pianificazione e rendicontazione annuale
2	30			Monitoraggio e Statistiche
2	30	10		Amministrativo
2	30	20		Magistratuale
2	40			OIV
3				Gestione Risorse Umane
3	10			Stato Giuridico
3	10	10		Trasferimenti Mobilità Pensioni
3	10	20		Assunzioni e Riassunzioni in servizio
3	10	30		Comandi e Distacchi
3	10	40		Part-time
3	10	50		Percorsi qualificazione
3	10	60		Valutazioni
3	10	70		Incarichi
3	10	80		Dimissioni e Cessazione dal servizio
3	20			Stato Economico
3	20	10		Competenze e recuperi stipendiali
3	20	20		Trattamenti accessori
3	20	30		Missioni
3	20	40		Buoni pasto (personale amministrativo)
3	20	50		Detrazioni e assegni familiari



3	20	60		Assistenza Fiscale
3	30			Gestione delle presenze e assenze
3	30	10		Presenze
3	30	100		Ferie e riposi compensativi
3	30	110		Altre assenze (malattia, art.18 CCNL1995, art.4 L.53-2000, donazione sangue, ecc)
3	30	20		Assenze
3	30	30		Permessi (diritto allo studio, permessi elettorali)
3	30	40		Congedi (congedi parentali, malattie del figlio, maternità, allattamento)
3	30	50		Aspettative
3	30	60		Scioperi
3	30	70		Legge 104/92
3	30	80		Visite fiscali
3	30	90		Permessi sindacali
3	40			Personale di magistratura
3	40	10		Assegnazioni
3	40	20		Incarichi
3	40	30		Corsi
3	40	40		Missioni
3	40	50		Congedi
3	40	60		Istanze
3	40	70		Buoni pasto
3	50			Tessere di riconoscimento
3	60			Contenzioso del lavoro
3	70			Corsi di aggiornamento e formazione
3	70	10		Corsi organizzati dalla Corte dei conti
3	70	20		Corsi organizzati dalla Provincia di Bolzano
3	80			Attestati di servizio
3	90			Fascicoli personali
3	100			Fascicoli dei Magistrati
4				Acquisizione Risorse Strumentali e spesa
4	10			Titolare Centro di Spesa
4	10	10		Preventivi
4	10	20		Contratti
4	10	30		Richiesta accreditamento/riduzione fondi
4	10	40		Previsione annuale di spesa
4	10	50		Rendiconti
4	10	60		Modelli 32 C.G.
4	20			Acquisti di beni e servizi
4	20	10		Spese di funzionamento
4	20	20		Spese per mezzi di trasporto

4	20	30		Spese per la sicurezza
4	20	40		Spese per manutenzione immobili
4	20	50		Spese per mobili, arredi e attrezzature
4	20	60		Spese per dotazioni librerie
4	20	70		Schede di rilevazione
4	30			Spese Postali
4	40			Spese di Giustizia (rimborsi ufficiali giudiziari per spese di notifica)
4	50			Spese per C.T.U.
4	60			Direttive- decreti- circolari
4	70			Comunicazioni Banca D'Italia
5				Gestione Risorse Strumentali
5	10			Gestione beni servizi e lavori
5	10	10		Richieste
5	10	20		Assegnazioni
5	10	30		Comunicazioni
5	10	40		Servizi e beni informatici
5	10	50		Gestione sede
6				Gestione beni mobili
6	10			Inventario
6	10	10		Modelli 130
6	10	15		Beni di facile consumo
6	10	20		Beni patrimoniali di I categoria (valore > €500,00)
6	10	30		Beni durevoli di I categoria (valore <= €500,00)
6	10	40		Beni patrimoniali di II categoria
6	10	50		Beni durevoli di II categoria
6	10	60		Modelli 98
6	10	70		Discarico Contabile
6	10	80		Fuori uso
6	20			Approvvigionamento materiali e stampati CDC
6	30			Note
7				Prevenzione e Sicurezza
7	10			Delegato del Datore di Lavoro (Regionale)
7	10	10		Sorveglianza sanitaria
7	10	20		Gestione infortuni
7	10	30		Formazione - Informazione
7	10	40		Comunicazioni al RLS
7	20			Servizio di Prevenzione e Protezione
7	20	10		Gestione della prevenzione
7	30			Riunioni periodiche sicurezza
8				Relazioni Sindacali
8	10			Contrattazioni



8	20		Elezioni RSU
8	30		Comunicazioni
8	40		Riunioni
9			Comunicazioni Istituzionali
9	10		Modalità esposizione bandiera
9	20		Variazioni denominazione e indirizzi
9	30		Erronea competenza
9	40		Conferenza permanente
9	50		Albi e ordini professionali

10.4.2. Titolario Sezioni controllo regionali

Il seguente titolario è in uso presso tutte le Sezioni di controllo regionali.

Qualche nodo relativo ad una materia specifica di una determinata sede è nascosto alle altre sedi (ad es. i nodi 80.10 e 80.20 sono visibili esclusivamente e rispettivamente alle sede di Trento. e Bolzano).

Titolario Sezioni Controllo regionali			
Controllo sulla gestione			
10	10		Indagini
10	20		Deferimenti
10	30		Attività e programmi della Sezione Regionale
10	40		Attività e programmi di altre Sezioni Centrali e Regionali
10	50		Altre forme di collaborazione previste dalla L.131/2003
10	60		Rilievi
20			Controllo di regolarità contabile L. 266/2005 (L. F. 2006) art. 1, co. 166 e ss. e L. 213/2012
20	10		Linee guida Enti Locali e Regione
20	10	10	Bilanci di previsione
20	10	10	Province
20	10	20	Comuni
20	10	30	Regione
20	10	20	Consuntivo
20	10	20	Province
20	10	20	Comuni
20	10	20	Regione
20	10	30	Inottemperanza
20	20		Linee guida Sanità
20	20	10	Bilanci economici di previsione
20	20	20	Consuntivo (Bilanci di esercizio)
20	20	30	Inottemperanza
20	30		Attività e programmi di altre Sezioni Centrali e Regionali
20	40		Deferimenti
20	35		Attività di verifica del rendiconto generale della provincia di Trento
20	37		Attività di verifica del rendiconto generale della regione T. AA



20	50			Attività di verifica del rendiconto generale della provincia di Bolzano
20	60			Rilievi
30				Controllo di legittimità preventivo e successivo
30	10			Controllo Preventivo
30	10	10		DAR
30	10	20		Incarichi dirigenziali
30	10	30		Contratti attivi
30	10	40		Contratti passivi lavori, forniture e servizi, locazioni
30	10	50		PROVVEDIMENTI COMMISSARIALI
30	10	45		Riconoscimento di debito
30	10	80		Atti amministrativi, a carattere generale e particolare, adottati dal Governo Regionale e dall'Amministrazione Regionale in adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'EU
30	10	90		Atti derivanti dall'attuazione dei fondi FAS
30	20			Controllo successivo di legittimità
30	20	10		Pensioni
30	20	20		Contabilità di tesoreria
30	20	30		Rendiconti Funzionari Delegati (mod. 27 CG)
30	20	40		Provvedimenti di cui all'art. 10, comma 1, D. Lgs. n. 123/2011
30	30			Rilievi
30	30	10		Controllo Preventivo di legittimità
30	30	20		Controllo successivo di legittimità
30	60			Deferimenti
30	60	10		Controllo Preventivo di legittimità
30	60	20		Controllo successivo di legittimità
30	70			Attività di altre Sezione Centrali e Regionali - Coordinamento
30	80			Note d'incompetenza
40				Pareri
40	10			Richiesti in base alla legge 131/2003
40	20			Comunicati da altre Sezioni Regionali di controllo
40	30			Comunicazioni Presidente Corte dei conti, Sezioni Riunite, Sezione delle Autonomie, Ufficio di Coordinamento
40	50			Note di inammissibilità e improcedibilità (pareri palesemente inammissibili per cause diverse)
45				Ordinanze/Decreti della Sezione Regionale di Controllo
45	20			Decreti
45	30			Ordinanze istruttorie
50				Convocazioni della Sezione regionale di controllo
55				Delibere della Sezione regionale di controllo
55	10			Inoltro programma di controllo
60				Convocazioni della Sezione delle Autonomie
70				Coordinamento delle Sezioni regionali di controllo
80				Certificazione dei contratti collettivi del personale regionale dirigenziale e amministrativo
80	10			Certificazione dei contratti collettivi del personale regionale dirigenziale della Provincia di Trento
80	20			Certificazione dei contratti collettivi del personale regionale dirigenziale della Provincia di Bolzano
90				Adempimenti specifici introdotti dalle L.F. e collegati
90	10			Controllo Regolamenti dei servizi di Enti Locali ex art.89 TUEL (art. 3, co.56 e



			57 L.F. 2008)
90	20		Incarichi, consulenze e spese sup. 5.000 (art.1, co. 173, L.F. 2006)
90	30		Relazioni a consuntivo annuale sui piani triennali finalizzati alla razionalizzazione dell'utilizzo delle risorse (art. 2, co. 597, L. F. 2008)
90	40		Verifica rispetto divieti introdotti dalla L. F. 2008 (art. 1, co. 7 D.L. 93/2008 e succ.)
90	50		Verifica veridicità delle certificazioni inoltrate dai comuni al Ministero dell'Interno in tema di riduzione degli introiti ICI (art.2, co.7, D.L. 154/2008)
90	60		Segnalazioni su inadempimenti nel trasferimento risorse ad organismi partecipati (art. 3, co. 32 L.F. 2008)
90	70		Verifica emolumenti o retribuzioni nell'ambito di rapporti di lavoro dipendente o autonomo con pubbliche amministrazioni statali ex (art.3, co. 44 e 53 L.F. 2008)
90	65		Mantenimento, variazione e dismissioni partecipazioni societarie degli EE.II.
90	68		Razionalizzazione delle spese per l'utilizzo dei beni ex art. 2 commi 594 e seguenti L. 244/2007
90	80		Referti Servizi Controllo di Gestione Enti Locali (art.198-bis TUEL)
90	90		Delibere in materia di assunzione ovvero di mantenimento di partecipazioni societarie ex art. 19, comma 2, del D.L. 1° luglio 2009 n. 78, conv. in L. 102/2008
90	100		Comunicazioni delle Ragionerie ai sensi dell'art. 14 , co. 6, 7 e 8 D. Lgs. 123/2011 (in materia di procedimento di controllo dei rendiconti)
90	110		Relazione sulla realizzazione degli interventi delegati (art. 15 D. Lgs. 123/2011)
90	120		Relazione annuale delle Ragionerie sugli esiti del controllo (art. 18 D. Lgs. 123/2011)
90	130		Prospetti spese di rappresentanza- art. 16 co. 26 D.L. 138/2011 e DM dell'Interno del 23.01.2012
90	135		Riconoscimento debito fuori bilancio
90	140		Referti semestrali dei sindaci e dei presidenti delle province sulla regolarità della gestione e sull'efficacia e adeguatezza del sistema dei controlli interni, adottato sulla base delle linee guida della Sezione delle Autonomie (art. 148 D.lgs 267/2000, e
90	140	10	Comuni con popolazione superiore a 15000 abitanti e Province
90	140	20	Comuni con popolazione inferiore a 15000 abitanti
90	150		Relazione di fine legislatura regionale e relazioni di fine mandato provinciali e comunali (artt. 1 e 4 del D.lgs 149/2011 e s.m.i.)
90	160		Controllo spese elettorali EE.II di cui all'art. 12 L. 115/1993 e art. 13 comma 6 lett. B L. 96/2012
95			Adempimenti specifici introdotti dalle L.R. e collegati
95	10		Relazioni semestrali (art.13 L.R. 2/2007)
110			Adempimenti specifici introdotti dal DL 174/2012
110	10		Relazione semestrale della Corte dei conti sulle coperture finanziarie e sulle tecniche di quantificazione degli oneri conseguenti all'approvazione delle leggi regionali di spesa (art. 1, comma 2, del D.L. 174/2012 convertito, con modificazioni, nella legge 213)
110	20		Relazione annuale del Presidente della Regione sulla regolarità della gestione e sull'efficacia e sull'adeguatezza del sistema dei controlli interni (art. 1, comma 6, del D.L. 174/2012, convertito con modificazioni, nella legge 7 dicembre 2012 n. 213)
110	30		Controllo sui rendiconti dei gruppi consiliari regionali (art. 1, comma 9, del D.L. 174/2012 convertito, con modificazioni, nella legge 7 dicembre 2012 n. 213);
110	40		Procedura di riequilibrio finanziario pluriennale di cui agli articoli 243-bis e seguenti del D.Lgs. n. 267/2000.
120			Esposti, Segnalazioni, Rapporti, Verifiche Contabili (segnalazioni di



			morosità, . . .)
120	10		Verifiche di cassa
120	20		Verifiche ispettive MEF
130			Nomine consegnatari, Funzionari Delegati e firme di traenza
130	10		Consegnatari inadempienti
130	20		Nomina e sostituzioni Consegnatari e Funzionari Delegati Regione
140			Contabilità mensile di Tesoreria e Rendiconti Funzionari Delegati (mod. 27 CG)
140	10		Funzionari delegati inadempienti
140	20		Consegnatari inadempienti
145			Conti Consuntivi Università
150			Rapporti con le altre amministrazioni
160			Comunicazioni (da privati e amministrazioni pubbliche) non altrimenti classificabili
160	10		Deposito firma
160	20		Esecuzioni sentenze, Ordinanze e Decisioni della Sezione Giurisdizionale
170			Dichiarazione di affidabilità sul rendiconto della Regione
180			Parifica sul rendiconto generale della Regione
183			Parifica sul rendiconto generale della Provincia di Trento
185			Parifica sul rendiconto generale della Provincia di Bolzano
190			Certificazione dei contratti collettivi

10.4.3. Titolario Segreterie dei Presidenti delle Sezioni di Controllo regionali

Il seguente titolario è in uso presso le Segreterie dei Presidenti delle Sezioni di Controllo regionali.

10			ORGANIZZAZIONE
20			TRATTAMENTO DATI PERSONALI
30			AFFARI GENERALI
40			MAGISTRATI
40	10		Assegnazioni
40	20		Incarichi
40	30		Corsi
40	40		Missioni
40	50		Congedi
40	60		Istanze
40	70		Buoni pasto
40	80		Relazioni per passaggio di grado
40	90		Fascicoli dei magistrati
50			CORRISPONDENZA RISERVATA
60			MONITORAGGIO E STATISTICHE



10.4.4. Titolario Segreterie dei Presidenti delle Sezioni di Giurisdizionali regionali

ORGANIZZAZIONE			
1	1		Decreti
1	2		Direttive annuali
1	3		Disposizioni Organizzative
1	4		Carichi di lavoro ed autorelazioni
1	5		Consiglio di Presidenza (note e risposte)
1	6		Altri Adempimenti
TRATTAMENTO DATI PERSONALI			
2	1		Personale Amministrativo
2	2		Personale di Magistratura
2	3		Nomina Responsabile
LEGGE PINTO EQUA RIPARAZIONE			
AFFARI GENERALI			
4	1		Relazioni esterne
4	2		Cerimoniale
4	3		Comunicazioni calendario udienze
4	4		Cambi di indirizzo
4	5		Deleghe generiche
4	6		Attestazioni di presenza in udienza
MAGISTRATI			
5	1		Assegnazioni
5	2		Incarichi
5	3		Corsi
5	4		Missioni
5	5		Congedi
5	6		Istanze
5	7		Buoni pasto
5	8		Relazioni per passaggio di grado
5	9		Fascicoli dei magistrati
CORRISPONDENZA RISERVATA			

10.4.5. Titolario Procuratori regionali

ATTI CORTE CENTRALE			
10	10		COMUNICAZIONI
10	20		INDIRIZZI DI COORDINAMENTO
10	30		CONSIGLIO DI PRESIDENZA
10	30	10	COMUNICAZIONI
10	30	20	CIRCOLARI
10	30	30	SINTESI E DECRETI CONSIGLIO DI PRESIDENZA
10	30	40	RICHIESTE
10	40		SENTENZE ED ISCRIZIONI A RUOLO SEZIONI RIUNITE
10	50		CONVOCAZIONI
10	50	10	CONSIGLIO DI PRESIDENZA
10	50	20	CONSIGLIO PROCURATORI REGIONALI



10	60			PROCURA GENERALE
10	60	10		COMUNICAZIONI
10	60	20		RICHIESTE
20				ATTI PROCURATORE GENERALE
20	10			CONFERENZE E CONVEGNI
30				FASCICOLI PERSONALI
40				INCARICHI
50				INAUGURAZIONE ANNO GIUDIZIARIO
60				COMUNICAZIONI RISERVATE

10.4.6. Titolario Segretariato Generale

Tale titolario include le competenze dei seguenti uffici che appartengono alla AOO del Segretario Generale:

- Segretario generale
- Ufficio Relazioni con il Pubblico
- Biblioteca
- Servizio Controllo di Gestione
- Servizio statistica
- Servizio ispettivo
- Servizio contenzioso
- Relazioni sindacali
- Trattamento economico dei magistrati

1				Segretario generale
1	10			Rapporti con gli organi istituzionali interni
1	10	1		Presidente
1	10	1	1	documenti
1	10	1	2	direttive
1	10	2		Consiglio di Presidenza
1	10	2	1	verbali - sintesi - odg
1	10	2	2	convegni
1	10	3		Procuratore generale
1	10	4		Consiglio di Amministrazione
1	10	5		Collegio dei revisori
1	10	6		Comitato per l'Informatica
1	20			Rapporti con le strutture interne all'amministrazione
1	20	1		Ufficio Stampa
1	20	2		Ufficio ispettivo
1	20	3		Ufficio statistica
1	20	4		Ufficio analisi e sviluppo processi decisionali ed organizzativi



1	20	5			Relazioni sindacali
1	20	5	1		Rappresentanze e organismi sindacali interni
1	20	5	2		Rappresentanze sindacali esterne - Aran
1	20	6			Seminario permanente sui controlli
1	20	6	1		documenti
1	20	6	2		convegni
1	20	7			Ufficio legale
1	20	8			Servizio controllo della gestione
1	20	9			Comitato pari opportunità
1	20	10			Biblioteca
1	20	11			Nucleo Carabinieri
2					Attività amministrative e di affari generali
2	10				Gestione, pianificazione ed organizzazione
2	10	10			Gestione risorse umane
2	10	10	1		Contenzioso
2	10	10	2		Rapporti di lavoro - mobilità
2	10	10	3		Formazione del personale
2	10	10	4		Dotazioni organiche
2	10	10	5		Trattamento economico personale amm.vo
2	10	10	6		Trattamento economico personale magistratura
2	10	10	7		Accessi personale
2	10	10	8		Dirigenti
2	10	10	10		Concorsi/selezioni/assunzioni
2	10	10	20		Sorveglianza sanitaria
2	10	10	20	10	Infermità o lesioni dipendenti da causa di servizio
2	10	10	20	20	Equo indennizzi
2	10	10	20	30	Visite mediche/collegiali/periodiche
2	10	10	20	40	Idoneità al servizio
2	10	10	20	50	Sicurezza e prevenzione
2	10	10	30		Gestione presenze/assenze
2	10	10	30	10	Assenze per missioni
2	10	10	30	20	Permessi/congedi
2	10	10	30	30	Legge 104/92
2	10	10	40		Stato giuridico
2	10	10	40	10	Incarichi interni ed esterni
2	10	10	40	20	Trasferimenti
2	10	10	40	30	Valutazioni
2	10	10	40	40	Part-time
2	10	10	40	50	Dimissioni e cessazioni dal servizio
2	10	10	50		Stato economico
2	10	10	50	10	Trattamento accessorio
2	10	10	50	20	Posizioni organizzative
2	10	10	50	30	Straordinari
2	10	10	50	40	Quote disagiate
2	10	10	50	50	Premio di produttività collettivo
2	10	10	50	60	Premio di collettività individuale
2	10	10	50	70	Missioni
2	10	10	50	80	Buoni pasto personale amministrativo



2	10	10	50	90	Trattamento fiscale
2	10	20			AFFARI GENERALI
2	10	20	1		Amministrazione
2	10	20	2		Prevenzione e sicurezza
2	10	20	3		Archivio e protocollo
2	10	20	4		Gestione patrimoniale centrale
2	10	20	5		Gestione patrimoniale periferica
2	10	20	6		Consegnatario
2	10	20	7		Urp
2	10	20	8		Ausiliari e di supporto
2	10	20	9		Contratti
2	10	30			BILANCIO
2	10	30	1		documenti
2	10	30	2		bilancio corte conti
2	10	40			CONTROLLO INTERNO
2	10	50			Gestione amministrativo/finanziaria
2	10	50	10		Bilancio di previsione
2	10	50	20		Consuntivazione
2	10	50	30		Fatturazione spesa
2	10	60			Gestione risorse strumentali
2	10	60	10		Attrezzature tecniche
2	10	60	20		Acquisizione gestione beni mobili
2	10	60	30		Acquisto beni
2	10	60	40		Materiale di facile consumo
2	10	70			Pianificazione e organizzazione
2	10	70	10		Programmi attività e progetti
2	10	70	20		Consuntivi attività
2	10	70	30		Direzione
2	10	70	40		Decreti
2	10	70	50		Disposizioni
2	10	70	60		Ordini di Servizio
2	10	70	70		Commissioni e gruppi di lavoro
2	10	70	80		Convegni
2	10	70	90		Direttive e circolari
2	10	70	100		Valutazione
2	10	70	110		Organizzazione ufficio
2	10	70	110	10	Informazione e comunicazione
2	20				Sistemi Informativi Automatizzati
2	20	1			Gestione e manutenzione dei sistemi informativi
2	20	1	1		SIAP - SIAM - Giurisdizione - Procure - SIPA - Biblioteca
2	20	2			Progetti informatici
2	20	2	1		P.I. - F.D. - M.I. - SIIAC - processo telematico - Sicurezza informatica - Ced
2	20	3			Sviluppo
2	20	4			Attività contrattuale
2	20	5			Piano triennale
2	20	6			Formazione
3					Attività con i SAUR



4				Attività con le Procure
4	10			PROCURE REGIONALI
4	10	1		procura regionale Abruzzo
4	10	2		procura regionale Basilicata
4	10	3		procura regionale Calabria
4	10	4		procura regionale Campania
4	10	5		procura regionale Emilia Romagna
4	10	6		procura regionale Friuli Venezia Giulia
4	10	7		procura regionale Lazio
4	10	8		procura regionale Liguria
4	10	9		procura regionale Lombardia
4	10	10		procura regionale Marche
4	10	11		procura regionale Molise
4	10	12		procura regionale Piemonte
4	10	13		procura regionale Puglia
4	10	14		procura regionale Sardegna
4	10	15		procura regionale Sicilia
4	10	16		procura regionale Toscana
4	10	17		procura regionale Sicilia
4	10	18		procura regionale Trentino A. Adige - Bolzano
4	10	19		procura regionale Trentino A. Adige - Trento
4	10	20		procura regionale Umbria
4	10	21		procura regionale Valle d'Aosta
4	10	22		procura regionale Veneto
5				Attività con le Sezioni Giurisdizionali
5	10			SSRR
5	10	10		sede giurisdizionale Ufficio ruolo generale giudizi d'appello
5	10	20		in sede controllo
5	10	30		in sede deliberante e consultiva
5	20			Sezioni centrali d'appello
5	20	1		I Sezione centrale d'appello
5	20	2		II Sezione centrale d'appello
5	20	3		III Sezione centrale d'appello
5	30			Sezioni giurisdizionali regionali
5	30	1		sezione giurisdizionale Abruzzo
5	30	2		sezione giurisdizionale Basilicata
5	30	3		sezione giurisdizionale Calabria
5	30	4		sezione giurisdizionale Campania
5	30	5		sezione giurisdizionale Emilia Romagna
5	30	6		sezione giurisdizionale Friuli Venezia Giulia
5	30	7		sezione giurisdizionale Lazio
5	30	8		sezione giurisdizionale Lombardia
5	30	9		sezione giurisdizionale Marche
5	30	10		sezione giurisdizionale Molise
5	30	11		sezione giurisdizionale Piemonte
5	30	12		sezione giurisdizionale Puglia
5	30	13		sezione giurisdizionale Sardegna



5	30	14		sezione giurisdizionale Sicilia
5	30	15		sezione giurisdizionale appello Sicilia
5	30	16		sezione giurisdizionale Toscana
5	30	17		sezione giurisdizionale Trentino Alto Adige - Bolzano
5	30	18		sezione giurisdizionale Trentino Alto Adige - Trento
5	30	19		sezione giurisdizionale Umbria
5	30	20		sezione giurisdizionale Valle d'Aosta
5	30	21		sezione giurisdizionale Veneto
6				Attività con le Sezioni di Controllo
6	10			Sezione centrale
6	10	10		legittimità
6	10	20		gestione
6	20			Sezione enti
6	30			Sezione autonomie
6	30	1		Referto
6	30	2		Coordinamento sezioni regionali di controllo
6	40			Sezioni regionali controllo
6	40	1		sezione regionale controllo Abruzzo
6	40	2		sezione regionale controllo Basilicata
6	40	3		sezione regionale controllo Calabria
6	40	4		sezione regionale controllo Campania
6	40	5		sezione regionale controllo Emilia Romagna
6	40	6		sezione regionale controllo Friuli Venezia Giulia
6	40	7		sezione regionale controllo Lazio
6	40	8		sezione regionale controllo Lombardia
6	40	9		sezione regionale controllo Marche
6	40	10		sezione regionale controllo Molise
6	40	11		sezione regionale controllo Piemonte
6	40	12		sezione regionale controllo Puglia
6	40	13		sezione regionale controllo Sardegna
6	40	14		sezione regionale controllo Sicilia
6	40	15		sezione regionale controllo Toscana
6	40	16		sezione controllo Trentino Alto Adige - Bolzano
6	40	17		sezione controllo Trentino Alto Adige - Trento
6	40	18		sezione controllo Veneto
6	50			Uffici controllo legittimità
6	50	10		Ministeri istituzionali
6	50	20		Ministeri economico - finanziari
6	50	30		Ministeri attività produttive
6	50	40		Ministeri infrastrutture e assetto del territorio
6	50	50		Ministeri servizi alla persona e beni culturali
6	50	60		Collegio di controllo spese elettorali
6	60			Uffici controllo gestione
6	60	10		Ministeri istituzionali
6	60	20		Ministeri economico - finanziari
6	60	30		Ministeri attività produttive
6	60	40		Ministeri infrastrutture e assetto del territorio
6	60	50		Ministeri servizi alla persona e beni culturali



7				Rapporti istituzionali con organismi internazionali
7	10			Corte conti europea
7	20			UE
7	30			ONU
7	40			NATO
8				Rapporti istituzionali con organi costituzionali
8	10			Ministeri
8	10	10		Ministeri istituzionali
8	10	20		Ministeri economico - finanziari
8	10	30		Ministeri attivita produttive
8	10	40		Ministeri infrastrutture e assetto del territorio
8	10	50		Ministeri servizi alla persona e beni culturali
8	20			Presidenza consiglio
8	30			Parlamento
8	40			Avvocatura Stato
8	50			Consiglio di Stato
8	60			Corte Costituzionale
8	70			SSPA
9				Rapporti con Enti ed Associazioni
9	10			interni
9	10	10		Associazione Dipendenti Corte dei conti
9	10	20		Associazione Magistrati
9	10	30		Associazione avvocati difensori dinanzi alla Corte dei conti
9	10	40		Associazione di mutua assistenza e previdenza del personale della Corte dei conti
9	20			nazionali
9	20	10		INPDAP
9	20	20		ENEA
9	20	30		ISTAT
9	20	40		INAIL
9	20	50		INPS
9	20	60		BANCA d'ITALIA
9	20	70		Guardia di Finanza
9	30			locali
9	30	10		Regioni
9	30	20		Comuni
10				Rapporti con istituti di credito
10	10			Banche
10	10	1		Uncredito Banca
11				Rapporti con Autority
11	10			Editoria
11	20			LL.PP.
11	30			Privacy
11	40			Antitrust
11	50			Telecomunicazioni
12				Rapporti con Agenzie
12	10			Agenzie viaggi
12	10	10		CIT



20				Struttura di Supporto agli organi di valutazione della dirigenza
20	10			SUPPORTO AGLI ORGANI DI VALUTAZIONE DELLA DIRIGENZA DI II FASCIA
20	10	10		Consuntivo
20	10	20		Valutazione
20	10	30		Contraddittorio
20	10	40		Controllo della Gestione
20	10	50		Elementi conoscitivi vertici istituzionali
20	10	60		Comunicazioni varie
20	20			SUPPORTO AGLI ORGANI DI VALUTAZIONE DEL PERSONALE AMMINISTRATIVO NON DIRIGENZIALE
20	20	10		Consuntivo
20	20	20		Valutazione
20	20	30		Contraddittorio
20	20	40		Controllo della Gestione
20	20	50		Elementi conoscitivi vertici istituzionali
20	20	60		Comunicazione varie
20	30			Direttiva annuale
30				Ufficio Relazioni con il Pubblico
30	10			Relazioni sindacali
30	10	10		Comunicazioni
30	20			Comunicazioni istituzionali
30	20	10		Variazione denominazione e indirizzi
30	20	20		Erronea competenza
30	30			Gestione badge esterni
40				Biblioteca
40	10			Gestione pubblicazioni
40	10	10		Acquisto monografie
40	10	20		Acquisto periodici
40	10	30		Richiesta doni
40	10	40		Ringraziamenti
40	10	50		Rilegatura pubblicazioni
40	20			Gestione prestiti e sale di lettura
40	20	10		Disposizioni regolamentari
40	20	20		Comunicazioni (avvisi e solleciti)
40	20	30		Comunicazioni varie
40	30			Contabilità
40	30	10		Fatture
40	30	20		Preventivi
40	30	30		Note di credito
40	30	40		Tracciabilità finanziaria fornitori
40	40			Statistiche attività
50				Servizio Controllo di Gestione
50	10			Controllo di gestione
50	10	10		Programmazione
50	10	20		SAL I semestre
50	10	30		SAL II semestre
50	10	40		Supporto valutazione e contraddittorio dirigenti
50	10	40	10	Supporto valutazione dirigenti



50	10	40	20		Contraddittorio dirigenti
50	10	50			Supporto valutazione pos. org.
50	10	60			Comunicazioni Bilancio CO.AN. Statistica
50	20				Comunicazioni Istituzionali
50	20	10			Report
50	20	20			Relazioni
50	20	30			Osservazioni
50	20	40			Note metodologiche
50	20	50			Comunicazioni esterne
60					Servizio statistica
70					Servizio ispettivo
80					Servizio contenzioso
90					Relazioni sindacali
100					Trattamento economico dei magistrati



10.5. Allegato 5: Registri e Repertori Informatici

10.5.1. Repertorio - Nozione

Per repertorio si intende il registro in cui sono annotati con numerazione progressiva i documenti per i quali è prevista la registrazione particolare. I documenti repertoriati costituiscono una serie di documenti di una stessa tipologia cui è associata una numerazione specifica.

La numerazione di repertorio si rinnova ogni anno solare: inizia il 1° gennaio e termina il 31 dicembre di ogni anno. Ogni repertorio è collegato ad una specifica tipologia documentale oppure ad una AOO dell'Amministrazione.

10.5.2. Repertori attivi

I repertori attualmente attivi sono relativi alle delibere e alle ordinanze delle Sezioni centrali e delle sezioni regionali. Di seguito l'elenco:

Repertorio	Descrizione
Delibere SS.RR. Controllo CSIC	Delibere Sezioni Riunite in sede di controllo Sicilia
Decreti Presidente CLAZ	Decreti Presidente Controllo Lazio
Decreti Presidenziale CABR	Decreti Presidente Controllo Abruzzo
DECRETO CSAR	Decreti Controllo Sardegna
DECRETO SSRR_SAR	Decreto Sezioni Riunite Sardegna
Delibera Reg.	Delibere Sezioni regionali di Controllo (con contatore associato ad AOO)
Delibere SS.RR. Consultiva CSIC	Delibera Sezione Riunite in sede di Consultiva Sicilia
DELIBERA SSRRCO	Delibera Sezione Riunite in sede di Controllo
ORDINANZA COLLEGIALE SCCLA	ORDINANZA COLLEGIALE (Segreteria Sezione centrale di controllo di legittimità)
ORDINANZA PRESIDENZIALE SCCLA	ORDINANZA PRESIDENZIALE (Segreteria Sezione centrale di controllo di legittimità)
Ordinanza Reg.	Ordinanze Sezioni regionali di Controllo (con contatore associato ad AOO)
Ordinanza SS.RR Consultiva CSIC	Ordinanza Sezioni Riunite in sede consultiva Sicilia
Ordinanza SS.RR. Controllo CSIC	Ordinanza Sezioni Riunite in sede controllo Sicilia
Ordinanza SSRR_SAR	Ordinanza Sezioni Riunite Sardegna

10.5.3. Repertorio dei fascicoli

È il registro in cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno del titolario. I fascicoli hanno un codice univoco all'interno della AOO costituito dal codice del titolario, anno di creazione e progressivo associato al particolare nodo di titolario.

