



## UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

**Protocollo N.ro: 17/007395-GEN del 21/11/2017**

**EMANAZIONE DEL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO  
DEI DOCUMENTI E DEGLI ARCHIVI  
DELL'UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"**

### **IL RETTORE**

**VISTA** la Legge del 30 dicembre 2010, n. 240;

**VISTO** il DPCM del 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005", e in particolare l'articolo 5;

**VISTO** lo Statuto di Ateneo;

**VISTO** Il Regolamento Generale di Ateneo;

**VISTO** il Verbale del Consiglio di Amministrazione n. 9 del 24 ottobre 2017, e in particolare il punto 9 nel quale si prende atto del Manuale di gestione del protocollo informatico dei documenti e degli archivi;

### **DECRETA**

1. È emanato il Manuale di gestione del protocollo informatico dei documenti e degli archivi, dell'Università degli Studi di Roma "Foro Italico" allegato e facente parte integrante del presente Decreto.

2. Il presente Decreto entra in vigore dalla data di pubblicazione sul sito *web* di Ateneo.

Roma, 21 novembre 2017

F.to

Prof. Fabio Pigozzi

# Manuale di gestione del protocollo informatico, dei documenti e degli archivi

*Università degli Studi di Roma "Foro Italico"*



# INDICE

## 1. MANUALE DI GESTIONE

1.1.	Obiettivi e finalità del Manuale .....	1
1.2.	Forme di pubblicità e di divulgazione .....	2
1.3.	Acronimi e definizioni .....	2

## 2. MODELLO ORGANIZZATIVO

2.1.	Strutture organizzative .....	3
2.2.	Servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi.....	3
2.3.	Postazione di protocollazione.....	4

## 3. PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

3.1.	Obiettivi del piano di sicurezza .....	4
3.2.	Generalità .....	4
3.3.	Requisiti minimi di sicurezza .....	5
3.4.	Misure di sicurezza .....	6

## 4. IL DOCUMENTO

4.1.	Il documento amministrativo .....	7
4.1.2.	Distinzione dei documenti in base allo stato di trasmissione .....	8
4.2.	Il documento analogico .....	9
4.2.1.	Redazione/formazione del documento amministrativo analogico .....	9
4.2.2.	Documenti redatti in originale su supporto analogico .....	10
4.3.	Il documento informatico .....	10
4.3.1.	Formati.....	12
4.3.2.	Redazione/formazione del documento informatico .....	13
4.3.3.	Validazione temporale.....	14
4.4.	Redazione/formazione del documento amministrativo informatico.....	14
4.5.	Formazione dei documenti – Aspetti operativi .....	15
4.5.1.	Requisiti degli strumenti informatici di scambio .....	17
4.5.2.	Sottoscrizione dei documenti informatici .....	17
4.6.	Duplicato del documento informatico e analogico .....	18
4.7.	Copia del documento informatico e analogico: nozione.....	19
4.7.1.	Copia informatica del documento amministrativo analogico .....	19
4.8.	Estratto informatico del documento amministrativo informatico .....	20
4.9.	Copia analogica del documento amministrativo informatico .....	21
4.10.	Il documento amministrativo informatico costituito dal corpo della posta elettronica certificata (PEC) istituzionale .....	21
4.11.	Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale.....	22
4.12.	Verifica della firma digitale.....	22
4.13.	Uso della posta elettronica certificata (PEC) .....	22

4.14.	Metadati .....	23
4.14.1	Obiettivi dei metadati archivistici.....	23
4.14.2	Metadati essenziali per la registrazione del protocollo informatico.....	23

## **5. FLUSSO DOCUMENTALE E REGISTRAZIONE**

5.1.	Registrazione in entrata.....	24
5.1.1.	Ricezione dei documenti informatici sulla casella di posta elettronica certificata (PEC) istituzionale .....	25
5.1.2.	Ricezione dei documenti informatici su caselle di posta elettronica non destinate al servizio di protocollazione .....	26
5.1.3.	Ricezione dei documenti informatici su casella di posta elettronica Istituzionale .....	26
5.1.4.	Ricezione dei documenti informatici su supporti rimovibili .....	26
5.1.5.	Ricezione dei documenti cartacei a mezzo posta convenzionale.....	27
5.1.6.	Documenti cartacei ricevuti a mezzo posta convenzionale e tutela dei dati personali .....	27
5.1.7.	Errata ricezione dei documenti informatici.....	27
5.1.8.	Errata ricezione dei documenti cartacei.....	27
5.1.9.	Rilascio di ricevute attestanti la ricezione dei documenti informatici .....	27
5.1.10.	Rilascio di ricevute attestanti la ricezione dei documenti cartacei .....	28
5.1.11.	Messaggi di protocollo interoperabili.....	28
5.1.12.	Archiviazione dei documenti informatici.....	28
5.1.13.	Acquisizione delle rappresentazioni digitali dei documenti cartacei .....	28
5.2.	Flusso de documenti inviati dall'AOO.....	29
5.2.1.	Predisposizione e registrazione dei documenti da inviare .....	29
5.2.2.	Trasmissione dei documenti informatici .....	30
5.2.3.	Trasmissione dei documenti cartacei a mezzo posta .....	31
5.2.4.	Trasmissione dei documenti cartacei a mezzo telefax.....	31
5.2.5.	Inserimento delle ricevute di trasmissione del fascicolo .....	31
5.3.	Flusso dei documenti interni all'AOO .....	32
5.3.1.	Trasmissione dei documenti interni formali.....	32
5.3.2.	Trasmissione dei documenti.....	32
5.4.	Assegnazione e smistamento mediante PdP.....	32
5.5.	Modifica delle assegnazioni.....	32

## **6. ALBO ON LINE**

6.1.	Finalità dell'Albo on line .....	33
6.2.	Gestione dell'Albo on line.....	33

## **7. UNITÀ ORGANIZZATIVE COMPETENTI NELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI**

7.1.	Attività di protocollo.....	34
7.2.	Servizio archivistico .....	35
7.3.	Servizio della conservazione elettronica dei documenti .....	35
7.3.1.	Archiviazione dei documenti informatici.....	35
7.3.2.	Archiviazione ottica dei documenti analogici.....	35
7.4.	Elementi obbligatori immutabili (Registratura) .....	35
7.5.	Elementi obbligatori modificabili.....	36
7.6.	Elementi non obbligatori modificabili .....	36
7.7.	Data e ora regolate sul UTC.....	37

7.8.	Segnatura.....	37
7.9.	Per il documento informatico.....	37
7.10.	Per il documento analogico .....	37

## **8. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE**

8.1.	Documenti esclusi.....	38
8.2.	Documenti soggetti a registrazione particolare (riservata).....	38
8.3.	La registrazione di protocollo particolare.....	39
8.3.1.	Annullamento di registrazioni di protocollo particolare .....	39
8.3.2.	Accesso ai dati .....	39

## **9. FASCICOLI E ARTICOLAZIONE INTERNA**

9.1.	Apertura del fascicolo.....	40
9.2.	Fascicolazione dei documenti.....	40
9.3.	Gestione del fascicolo .....	40
9.4.	Chiusura del fascicolo .....	41
9.5.	Consultazione e movimentazione dell'archivio corrente, di deposito e storico .....	41
9.5.1.	Principi generali .....	41
9.5.2.	Consultazione ai fini giuridico-amministrativi .....	41

## **10. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO**

10.1.	Unicità del protocollo informatico .....	42
10.2.	Registro giornaliero di protocollo.....	42
10.3.	Segnatura di protocollo dei documenti.....	43
10.3.1.	Documenti informatici.....	43
10.3.2.	Documenti cartacei.....	43
10.4.	Annullamento di registrazione di protocollo.....	44
10.5.	Casi particolari di protocollo.....	44
10.5.1.	Protocollazione dei documenti fiscali previsti dalla normativa Fattura PA .....	44
10.5.2.	Protocollazione dei documenti inerenti gare di appalto .....	45
10.5.3.	Corrispondenza personale o riservata.....	45
10.5.4.	Differimento delle registrazioni.....	45
10.5.5.	Documenti in uscita con più destinatari .....	46

## **11. ACCESSO AI DOCUMENTI INFORMATICI**

11.1.	Generalità .....	46
11.2.	Abilitazioni interne per accedere ai servizi di protocollo .....	46

## **12. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA**

12.1.	Il registro di emergenza .....	47
12.2.	Modalità di apertura del registro di emergenza.....	47
12.3.	Modalità di utilizzo del registro di emergenza .....	47
12.4.	Modalità di chiusura e recupero del registro di emergenza .....	47

### **13. NORME TRANSITORIE E FINALI**

13.1.	Pubblicità del presente Manuale.....	48
13.2.	Operatività del presente Manuale.....	48

### **ALLEGATI**

	Allegato n. 1 - Riferimenti normativi .....	49
	Allegato n. 2 - Glossario .....	52

## **1. MANUALE DI GESTIONE**

### **1.1. Obiettivi e finalità del Manuale**

Il “Manuale di gestione del protocollo informatico, dei documenti e degli archivi” (di seguito Manuale) descrive il sistema di gestione dei documenti analogici e informatici, fornendo le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi dell’Università degli Studi di Roma "Foro Italico". Scopo del Manuale è quello di indicare le procedure e le istruzioni per la corretta trattazione, tenuta e conservazione sia della documentazione analogica che di quella informatica. La descrizione delle modalità di gestione dei flussi documentali e degli archivi è finalizzata all'organizzazione e alla gestione della documentazione ricevuta, inviata o comunque prodotta dall’Ateneo secondo parametri di corretta registrazione di protocollo, di assegnazione, classificazione, fascicolazione, reperimento e conservazione dei documenti informatici e analogici. Il Manuale costituisce una guida per tutto il personale coinvolto nella gestione documentale. In altre parole, esso rappresenta uno strumento per l'operatore di protocollo, affinché possa porre in essere correttamente le operazioni di gestione documentale, e per il cittadino e per le imprese, affinché possano comprendere e collaborare alla gestione documentale stessa (ad esempio utilizzando formati idonei per la formazione delle istanze).

Il Manuale è stato redatto in conformità alla normativa vigente e in particolare a quanto stabilito dall’art. 5 del DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71, del Codice dell’Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005" e tenuto conto del processo in atto verso la realizzazione di una pubblica amministrazione digitale come delineato dal 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 artt. 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".

## **1.2. Forme di pubblicità e di divulgazione**

Il Manuale 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 (UOR) delle aree organizzative omogenee dell'Ateneo, al fine di consentire la corretta diffusione delle nozioni e delle procedure documentali e di consentire la necessaria collaborazione.

## **1.3. Acronimi e definizioni**

Si riportano i seguenti acronimi utilizzati più frequentemente:

- AOO - Area Organizzativa Omogenea;
- IPA - Indice delle Pubbliche Amministrazioni; è l'archivio ufficiale degli Enti pubblici e dei Gestori di pubblici servizi, realizzato e gestito dall'Agenzia per l'Italia digitale;
- PdP - Programma di Protocollo Informatico; l'applicativo acquisito e integrato dall'Ateneo per implementare il servizio di protocollo informatico;
- RdS – Responsabile della Sicurezza; soggetto competente in merito alla definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza;
- RPA - Responsabile del Procedimento Amministrativo; soggetto che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- RSI - Responsabile dei Sistemi Informativi;
- RSP - Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi;
- UOP - Unità Organizzativa di registrazione di Protocollo (Ufficio Protocollo); rappresenta i soggetti che svolgono l'attività di registrazione a protocollo;
- UOR - Unità Organizzativa Responsabile (Coordinatore Area); un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.



## **2. MODELLO ORGANIZZATIVO**

### **2.1 Strutture organizzative**

Il sistema di gestione documentale dell'Università si basa sul modello organizzativo effettivo dell'Ateneo, interpretandolo con l'obiettivo di definire le regole di gestione della documentazione amministrativa e l'organizzazione dell'archivio.

Al fine di coordinare e controllare le operazioni connesse alla gestione e alla tenuta dei documenti la normativa ha introdotto il concetto di AOO, ovvero "un insieme di unità organizzative dell'Amministrazione che usufruiscono in modo omogeneo e coordinato degli stessi servizi per la gestione dei flussi documentali" (art. 50, comma 4 del D.P.R. 28 dicembre 2000, n. 445 e art. 3, comma 1 lettera a) del DPCM 3 dicembre 2013).

Sotto questo profilo, l'Università risulta costituita da un'unica Area Organizzativa Omogenea della quale fanno parte tutte le strutture di didattica, ricerca e tecnico-amministrative.

All'interno dell'AOO sono individuate le Unità Organizzative Responsabili, ovvero complessi di risorse umane e strumentali cui è stata affidata una competenza omogenea, nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari o procedimenti amministrativi. Le Unità Organizzative sono costituite in primo luogo dalle Direzioni dalle Aree amministrative e dai singoli Uffici, nonché dalle strutture di didattica e ricerca (Dipartimenti e Centri).

A seguito dell'istituzione dell'AOO unica sono eliminati tutti i protocolli di struttura, i protocolli multipli e più in generale i protocolli diversi dal protocollo informatico di Ateneo.

### **2.2 Servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi**

La funzione di "Servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi" prevista ai sensi dell'art. 61, comma 1 del D.P.R. 28 dicembre 2000, n. 445, è svolta dall'Ufficio Protocollo e Archivio, struttura incardinata nell'Area Affari Legali. Nello specifico, l'Ufficio svolge attività di protocollazione e funzioni di coordinamento e di presidio per tutte le componenti e i ruoli coinvolti nelle operazioni di gestione documentaria nell'ambito dell'Ateneo; sovrintende alla corretta formazione dell'archivio corrente (ovvero dei documenti relativi ad affari

in corso di trattazione, gestiti e conservati presso le strutture di didattica, ricerca e tecnico amministrative di Ateneo) e provvede inoltre alla tenuta dell'archivio di deposito e dell'archivio storico di Ateneo.

### **2.3 Postazione di protocollazione**

Nell'ambito di Ateneo è individuata una postazione principale di protocollazione operante all'interno dell'Ufficio Protocollo e Archivio e denominata per convenzione Ufficio Protocollo.

## **3. PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI**

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

### **3.1. Obiettivi del piano di sicurezza**

Il piano di sicurezza garantisce che:

1. i documenti e le informazioni trattati dall'AOO siano resi disponibili, integri e riservati;
2. i dati personali comuni, sensibili e/o giudiziari vengano gestiti nel rispetto del Regolamento, adottato dall'Ateneo con D.R. n. 165 del 12.4.2006, per il trattamento dei dati sensibili e giudiziari in attuazione del D.Lgs. 196/2003 e successive modifiche.

### **3.2. Generalità**

Il RSP ha predisposto il piano di sicurezza in collaborazione con il Responsabile dei Sistemi Informativi. Il piano di sicurezza garantisce i requisiti minimi di sicurezza, previsti dal DPCM 2013 "Regole tecniche per il protocollo informatico", e si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e/o i documenti trattati.

### 3.3. Requisiti minimi di sicurezza

L'Ateneo, ai sensi dell'art. 7 del DPCM 2013, attraverso il "Regolamento per il trattamento dei dati sensibili e giudiziari" del 12 aprile 2016 di cui al DR 165 e le procedure organizzative, oltre a quelle tecnico-informatiche, assicura:

- che il sistema di protocollo informatico garantisca: l'univoca identificazione ed autenticazione degli utenti;
  - la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
  - l'accesso alle risorse esclusivamente agli utenti abilitati;
  - la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da assicurarne l'identificazione.
1. che il sistema di protocollo informatico consenta il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
  2. che il sistema di protocollo informatico consenta il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.
  3. che il registro giornaliero di protocollo sia trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.
  4. che il sistema di protocollo informatico rispetti le misure di sicurezza previste dagli articoli del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

### 3.4. Misure di sicurezza

L'Ateneo, a norma del D.Lgs. del 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" (d'ora in poi Codice Privacy), è "titolare" dei dati personali intesi come "qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". Gli stessi vengono, poi, sotto-ripartiti in:

- *comuni identificativi*: i dati personali che permettono l'identificazione diretta dell'interessato;
- *sensibili*: i dati personali idonei a rivelare l'origine etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- *giudiziari*: i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del codice di procedura penale.

I dati personali sono contenuti nella documentazione amministrativa - in arrivo, in partenza e interna, sia informatica che analogica - di pertinenza dell'Ateneo, che, in qualità di Titolare del trattamento dei dati stessi, è responsabile per quanto riguarda le decisioni in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. In relazione alla protezione dei dati personali trattati, l'Ateneo ottempera:

- al rispetto del 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 ed al relativo consenso quando dovuto;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.

L'Ateneo garantisce il diritto degli individui e delle imprese ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche, sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

## 4. IL DOCUMENTO

### 4. 1. Il documento amministrativo

L'art. 22, comma 1, lett. d) della L. n. 241 del 7 agosto 1990 definisce documento amministrativo "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". Nel processo di gestione documentale, il documento amministrativo, in termini operativi, è riconducibile alle seguenti fattispecie

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

Il documento amministrativo, ai sensi dell'art. 1 comma 1 lettere p) e p-bis) del D. Lgs. n. 82 del 7 marzo 2005 Codice dell'Amministrazione Digitale (CAD), è definito:

- *informatico*, quando è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- *analogico*, quando è la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Ai sensi dell'art. 40 del CAD, e successive modifiche ed integrazioni, "Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'art. 71". Si intende pertanto che un documento, anche se formato con strumenti informatici, è analogico se il suo contenuto viene rappresentato su supporto cartaceo e sottoscritto con firma autografa.

#### **4.1.2. 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 arrivo;
- documenti in partenza;
- documenti interni.

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 partenza si intendono i documenti di rilevanza giuridico-probatoria prodotti dall'Amministrazione pubblica nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato ed 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 Unità Organizzative Responsabili (UOR) afferenti alla stessa Area Organizzativa Omogenea (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 all'attività svolta e alla 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.

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale - PEC. 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.

## **4.2. Il documento analogico**

Per documento analogico si intende un documento amministrativo “formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (i documenti cartacei), come le immagini su film (le pellicole mediche, i microfiches, i microfilm), come le magnetizzazioni su nastro (le cassette e i nastri magnetici audio e video) su supporto non digitale”. Si fa di seguito riferimento ad un documento amministrativo cartaceo, che può essere prodotto sia in maniera tradizionale (come una lettera scritta a mano o a macchina) sia con strumenti informatici (una lettera prodotta tramite un sistema di videoscrittura o text editor) e poi stampata. Un documento analogico può essere convertito in documento informatico.

### **4.2.1. Redazione/formazione del documento amministrativo analogico**

Nell'attività amministrativa, di norma il documento analogico è un documento formato su supporto analogico prodotto con strumenti analogici (documento scritto a mano) o con strumenti informatici (documento prodotto con un sistema di videoscrittura) e stampato su carta. L'originale analogico è il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali (sigillo, carta intestata, formulario amministrativo) e sostanziali, comprendente tutti gli elementi di garanzia e di informazione, del mittente e del destinatario e dotato di firma autografa. I documenti analogici dotati di firma autografa aventi per destinatario un ente o soggetti terzi sono di norma redatti in due esemplari: un originale per il destinatario e una minuta da conservare agli atti nel fascicolo corrispondente. Si definisce minuta l'esemplare del documento corredato di sigle, firma e sottoscrizione autografe, conservato agli atti dell'Ateneo, cioè nel fascicolo relativo al procedimento amministrativo o all'affare trattato. Il documento amministrativo analogico in uscita è redatto su carta intestata e deve, di norma, contenere la denominazione dell'Ateneo e l'indicazione di

- AOO/ UOR;
- Data;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (quando presenti);
- Oggetto;
- Destinatario;
- Testo;

- Sottoscrizione;
- Sigla eventuali istruttori;
- Elementi identificativi del responsabile del procedimento.

Il documento è sottoscritto prima di essere protocollato; di norma la data di sottoscrizione e la data di protocollazione coincidono.

#### **4.2.2. 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 (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, avanzata o digitale), sono documenti amministrativi analogici.

#### **4.3. Il documento informatico**

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. In particolare, i commi 1, 1-bis e 3 di cui all'art. 20 del CAD stabiliscono che: "Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'art. 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice. Il documento informatico è, quindi, un file, cioè una sequenza determinata di valori binari, indifferente al supporto fisico su cui è memorizzata. A differenza del documento analogico, che si caratterizza per la pluralità di forme (scrittura privata, atto pubblico, scrittura privata autenticata), che 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 appare l'autore. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità. Il documento informatico può essere sottoscritto con firma elettronica, avanzata, qualificata o digitale: il tipo di firma utilizzata differenzia il valore giuridico del documento, secondo le norme previste dalla legge. 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 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 garantiscano 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 garantiscano 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 contraria. Il documento informatico sottoscritto con firma digitale, se formato nel rispetto delle regole tecniche che garantiscano 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 contraria.

L'associazione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione; tuttavia le firme elettroniche qualificate e digitali, 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.

Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la

duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché, quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell'art. 71. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale. Ai sensi degli artt. 23, 23-bis e 23-ter del CAD è prevista l'effettuazione di copie e duplicati di documenti informatici, in formato analogico o informatico. In particolare, il comma 5 dell'art. 23-ter (modificato dalla legge Crescita 2.0) stabilisce che: "Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con linee guida dell'Agenzia per l'Italia digitale, tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità".

Il DPCM del 13 novembre 2014 art. 4 comma 2 prevede che "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". L'art. 5 del predetto DPCM prevede inoltre che "Il duplicato informatico di un documento informatico di cui all'art. 23-bis, comma 1, del Codice è prodotto mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine".

#### **4.3.1. Formati**

L'Ateneo usa per la formazione e per la gestione dei documenti informatici le seguenti tipologie di formato, 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 di un formato ne vanno valutati i seguenti parametri: l'apertura, la sicurezza, la portabilità, la funzionalità, il supporto allo sviluppo e la diffusione dello stesso. Per tale motivo, sono utilizzati i seguenti formati standard:

- Testo = Docx; Ods; Pdf/a;
- Calcolo= Xlsx; Odt;
- Immagini = Jpg, Tiff;
- Suoni = Mp3;
- Video = Avi;
- Eseguibili = Exe;
- XML;
- Archiviazione e compressione = Zip;
- Formati e-mail = RFC 2822/MIME.

#### **4.3.2. Redazione/formazione del documento informatico**

Il documento informatico è formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software: in tal caso il documento informatico assume le caratteristiche di immutabilità e di integrità con la sottoscrizione con firma digitale/firma elettronica 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;
- 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;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione;

- 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 dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

#### **4.3.3. Validazione temporale**

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 UTC (IT) (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 posta elettronica certificata.

#### **4.4. Redazione/formazione del documento amministrativo informatico**

Le amministrazioni pubbliche formano gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici in uso, oppure 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, segnatura, fascicolatura e repertoriazione. Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità con la registrazione nel registro di protocollo, nei repertori, negli albi, contenuti nel sistema di

gestione documentale. Il documento amministrativo informatico deve, di norma, contenere la denominazione dell'Ateneo e l'indicazione di

- AOO/ UOR;
- Data di sottoscrizione;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (quando presenti);
- Oggetto;
- Destinatario;
- Testo;
- Iniziali di redattore/responsabile;
- Sottoscrizione;
- 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.

#### **4.5. Formazione dei documenti – Aspetti operativi**

I documenti dell'AOO sono prodotti con sistemi informatici come previsto dalla vigente normativa. Ogni documento formato per essere inoltrato all'esterno o all'interno dell'AOO in modo formale:

- tratta un unico argomento indicato in maniera sintetica, ma esaustiva nello spazio riservato all'oggetto;
- è identificato dal numero di protocollo;
- indica il numero degli allegati, se presenti.

Le firme necessarie al perfezionamento giuridico del documento in uscita devono essere apposte prima della sua protocollazione. Le regole per la determinazione dei contenuti e della

struttura dei documenti sono definite dai responsabili delle singole UOR. Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa dell'AOO e dell'UOR che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione (via, numero, CAP, città, provincia);
- il codice fiscale dell'amministrazione;
- i numeri di telefono/fax dell'UOR;

Possono altresì essere inserite le seguenti informazioni:

- l'indirizzo PEC del referente;
- il codice univoco ufficio dell'UOR risultante dall'IPA.

#### **4.5.1. Requisiti degli strumenti informatici di scambio**

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

- integrità del messaggio;
- riservatezza del messaggio;
- il non ripudio dei messaggi;
- automazione dei processi di protocollazione e smistamento dei messaggi all'interno delle AOO;
- interconnessione tra UOR nel caso di documenti interni formali;
- certificazione di avvenuto inoltra e di ricezione;
- interoperabilità dei sistemi informativi pubblici.

Per quanto riguarda la formazione e la conservazione di documenti informatici, l'Amministrazione ottempera al DPCM 21 marzo 2013 "Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'Amministrazione Digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni".

#### **4.5.2. Sottoscrizione dei documenti informatici**

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente. Per il rilascio di certificati qualificati di firma digitale, l'AOO si avvale dei servizi di un soggetto certificatore accreditato e all'uopo autorizzato. I documenti informatici prodotti, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in PDF/A al fine di garantirne l'immodificabilità e la staticità (art. 3 comma 3 del DPCM del 13 gennaio 2004 e allegato 2 al DPCM del 13 novembre 2014).

Il formato privilegiato per la firma di documenti amministrativi gestiti dall'AOO è la busta crittografica CADES, file con estensione ".p7m". L'AOO accetta anche la busta crittografica di firma

PAdES, file con estensione “pdf”, in tutti i procedimenti amministrativi a seguito di autorizzazione rilasciata dall’Agenzia per l’Italia Digitale (Agid) id in data 29.1.2016. I documenti possono essere sottoscritti digitalmente da più soggetti: in tal caso, sono apposte firme multiple, di tipo parallelo o di tipo controfirma (c.d. firma matrioska). Con la firma di tipo parallelo due o più soggetti sottoscrivono lo stesso documento apponendo firme di uguale valore (per i contratti), con la controfirma il rapporto fra i sottoscrittori è di tipo gerarchico. Nel caso di apposizione di firme multiple, i sottoscrittori successivi al primo devono effettuare preventivamente la verifica di validità ed integrità del documento da firmare.

#### **4.6. Duplicato del documento informatico e analogico**

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. Il duplicato di un documento analogico è la riproduzione di un documento analogico originale distrutto o smarrito che lo sostituisce a tutti gli effetti legali: esempio rilascio del certificato di laurea, della carta di identità etc.



#### **4.7. Copia del documento informatico e analogico: nozione**

La copia di documento informatico è un documento informatico che, mediante processi e strumenti idonei, 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 (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 (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").

##### **4.7.1. 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 digitale del notaio o con firma digitale 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.

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 di 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 digitale o altra firma elettronica qualificata e 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.

#### **4.8. Estratto informatico del documento amministrativo informatico**

La copia che riproduce solo una parte del contenuto del documento, viene definita "estratto". L'estratto così formato, di uno o più documenti informatici, se sottoscritto con firma digitale o firma elettronica qualificata da chi effettua l'estratto hanno 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 digitale del notaio o con firma digitale 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.

#### **4.9. Copia analogica del documento amministrativo informatico**

La copia analogica del documento amministrativo informatico è, di norma, la stampa cartacea. La copia su supporto analogico di documento informatico, sottoscritto con firma elettronica avanzata, qualificata o digitale, 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.

#### **4.10. Il documento amministrativo informatico costituito dal corpo della posta elettronica certificata (PEC) istituzionale**

La posta elettronica certificata costituisce un mezzo di trasmissione che consente lo scambio di comunicazioni e documenti la cui trasmissione e ricezione 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 arrivo nel sistema di gestione documentale solo se il contenuto è rilevante al fine giuridico-probatorio.

#### **4.11. 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'Università degli Studi di Roma "Foro Italico" sono considerate sottoscritte con firma elettronica semplice e sono soggette a protocollazione solo se il contenuto è rilevante al fine giuridico-probatorio. In questo caso si procede alla conversione dell'e-mail in formato pdf/a prima di provvedere alla sua registrazione.

#### **4.12. Verifica della firma digitale**

La verifica della firma digitale avviene mediante utilizzo di applicativi appositi esterni al PdP.

#### **4.13. Uso della posta elettronica certificata (PEC)**

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045- 2049 e successive modificazioni o integrazioni. Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo. L'utilizzo della Posta Elettronica Certificata (PEC) consente di:

- conoscere in modo inequivocabile il mittente, la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica certificata dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO.

Sull'Indice delle Pubbliche Amministrazioni sono pubblicati gli indirizzi istituzionali di posta elettronica certificata associati alla AOO. La trasmissione del documento informatico tramite PEC equivale alla notificazione per mezzo di una raccomandata con avviso di ricevimento tradizionale, nei casi consentiti dalla legge. Per l'utilizzo del servizio di posta elettronica certificata (PEC), l'AOO si avvale di un gestore autorizzato presso l'Agid.

#### **4.14. Metadati**

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.

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".

##### **4.14.1. Obiettivi dei metadati archivistici**

Gli obiettivi dei metadati archivistici sono:

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

##### **4.14.2. Metadati essenziali per la registrazione nel protocollo informatico**

Gli elementi essenziali minimi sono i seguenti:

- Identificativo;
- denominazione / codice unico che individua l'Ateneo;
- corrispondente (mittente/destinatari);
- oggetto;
- numero degli allegati e descrizione degli stessi;
- numero di protocollo;
- data di registrazione a protocollo;

- indicazione dell'Unità organizzativa responsabile (UOR);
- impronta che lega il documento digitale ai metadati sopra indicati.

## 5. FLUSSO DOCUMENTALE E REGISTRAZIONE

Il flusso documentale può essere suddiviso in tre categorie di documenti:

**Documenti in entrata/arrivo** S'intendono i documenti pervenuti o comunque acquisiti dall'Università nell'esercizio delle proprie funzioni.

**Documenti in uscita/partenza** S'intendono i documenti prodotti dall'Università nell'esercizio delle proprie funzioni e inviati a soggetti pubblici e privati esterni all'Università stessa.

**Documenti interni** S'intendono i documenti prodotti e/o scambiati nell'ambito delle Unità Organizzative dell'Università. Si distinguono in:

- documenti di preminente carattere informativo
- documenti di preminente carattere giuridico-probatorio aventi rilevanza ai fini dell'attività amministrativa

### 5.1. Registrazione in entrata

La registrazione di protocollo in entrata viene effettuata di norma nel giorno del ricevimento del documento e comunque non oltre le due giornate lavorative successive, ad eccezione di quanto previsto nel caso di "Differimento delle registrazioni". I documenti informatici possono essere recapitati alla UOR sia tramite posta elettronica ordinaria sia tramite PEC, oppure mediante consegna di unità magneto-ottiche (DVD, chiavette USB, etc.).

Il ciclo dei documenti in entrata si articola nelle seguenti fasi obbligatorie:

1. registrazione di protocollo: tutti i documenti ricevuti, indipendentemente dal supporto, sono registrati tramite il PdP (salvo eccezioni). Nel caso di ricezione da parte di una UOR di un documento non di propria competenza, l'UOP provvede alla registrazione del documento stesso assegnandolo alla UOR responsabile del procedimento amministrativo cui verrà

trasmesso l'eventuale documento cartaceo originale. I requisiti obbligatori per la registrazione a protocollo sono:

- numero di protocollo e data di registrazione, generati automaticamente dal PdP in forma non modificabile;
  - mittente del documento ricevuto, registrato in forma non modificabile;
  - oggetto del documento, registrato in forma non modificabile;
  - data e numero di protocollo del documento ricevuto, se disponibili;
  - impronta del documento informatico, generata automaticamente dal PdP in forma non modificabile. Devono essere altresì indicati il tipo di supporto e il mezzo di spedizione;
2. assegnazione: il completamento della fase di protocollazione avviene mediante l'inserimento dell'assegnatario per competenza ed eventuali assegnatari per conoscenza;
  3. segnatura: al documento cartaceo dovrà essere applicata l'etichetta stampata tramite il PdP e verrà acquisita l'immagine del documento comprensiva di etichetta.

Nel caso di documento informatico la segnatura verrà apposta dal sistema. Al fine di una migliore gestione del flusso documentale è opportuna l'annotazione circa il collegamento ad altri documenti già protocollati.

#### **5.1.1. Ricezione dei documenti informatici sulla casella di posta elettronica certificata (PEC) istituzionale**

Di norma, la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale del responsabile. Quando i documenti informatici pervengono alla UOR, l'UOP procede alla registrazione a protocollo della PEC. Se il testo della PEC fa solo riferimento a un documento allegato che contiene le informazioni amministrative necessarie al procedimento, si protocolla l'allegato quale documento principale, utilizzando una specifica funzione del PdP. Se gli elementi utili ai fini dell'attività amministrativa sono contenuti esclusivamente nel testo della PEC viene protocollato il messaggio stesso.

### **5.1.2. Ricezione dei documenti informatici su caselle di posta elettronica non destinate al servizio di protocollazione**

Nel caso in cui il messaggio venga ricevuto direttamente su una casella di posta elettronica del servizio di protocollazione, il messaggio viene all'uopo inoltrato dal ricevente alla UOP.

### **5.1.3. Ricezione dei documenti informatici su casella di posta elettronica istituzionale**

Nel caso in cui venga ricevuto sulla casella istituzionale destinata al servizio di protocollazione un messaggio il cui contenuto rientra fra i documenti da protocollare l'UOP procede alla registrazione.

### **5.1.4. Ricezione dei documenti informatici su supporti rimovibili**

I documenti informatici possono essere recapitati anche tramite strumenti diversi dalla posta elettronica. L'UOR acquisisce e tratta solo i documenti informatici ricevuti su supporto rimovibile laddove decodificabili e interpretabili con le tecnologie a sua disposizione. L'UOP provvederà all'estrapolazione e registrazione del documento in presenza del consegnatario al fine di garantire la regolarità dell'operazione e a rilasciarne ricevuta su richiesta. Le UOR destinatarie sono a disposizione dell'utenza per l'indicazione dei dispositivi e formati accettati.



#### **5.1.5. Ricezione dei documenti cartacei a mezzo posta convenzionale**

I documenti pervenuti a mezzo posta, fax, telegramma o a mano, recapitati ad un indirizzo ufficiale dell'AOO o ritirati presso gli uffici postali, sono consegnati all'UOP. In caso di corrispondenza ricevuta con raccomandata o raccomandata con avviso di ricevimento la busta deve essere necessariamente allegata al documento stesso.

#### **5.1.6. Documenti cartacei ricevuti a mezzo posta convenzionale e tutela dei dati personali**

Poiché l'AOO è organizzata per ricevere documenti su carta attraverso qualsiasi UOR tutte le relative UOP preposte all'apertura della corrispondenza sono autorizzate al trattamento dei dati personali.

#### **5.1.7. Errata ricezione dei documenti informatici**

Nel caso pervengano via telematica messaggi dal contenuto espressamente riferito a terzi l'UOP provvederà a darne immediata comunicazione al mittente con la seguente segnalazione "Messaggio pervenuto per errore - non di competenza di questa Amministrazione".

#### **5.1.8. Errata ricezione dei documenti cartacei**

Nel caso in cui pervenga erroneamente all'AOO corrispondenza indirizzata ad altra AOO o persona estranea all'AOO, la corrispondenza verrà restituita all'ufficio postale.

#### **5.1.9. Rilascio dei ricevute attestanti la ricezione di documenti informatici**

Nel caso di ricezione di documenti informatici tramite posta elettronica certificata la relativa ricevuta attestante la ricezione è assicurata dal gestore del servizio utilizzato dall'AOO.

#### **5.1.10. Rilascio di ricevute attestanti la ricezione dei documenti cartacei**

Su richiesta dell'interessato l'UOP rilascerà apposita ricevuta attestante la data di avvenuta consegna.

#### **5.1.11. Messaggi di protocollo interoperabili**

Nel caso di ricezione di messaggi di protocollo tra sistemi ai sensi della circolare Agid n. 60/2013, il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvederà alla formazione e all'invio al mittente di uno dei seguenti messaggi:

- messaggio di conferma di protocollazione: un messaggio di avvenuta protocollazione del documento ricevuto;
- messaggio di notifica di eccezione: un messaggio che rileva l'anomalia del messaggio ricevuto;
- messaggio di annullamento di protocollazione: un messaggio contenente comunicazione di annullamento protocollazione di un documento già precedentemente ricevuto e protocollato;
- messaggio di aggiornamento di protocollazione: un messaggio contenente comunicazione di aggiornamento riguardante un documento protocollato ricevuto in precedenza.

#### **5.1.12. Archiviazione dei documenti informatici**

Effettuata l'operazione di registrazione e segnatura il documento informatico associato viene archiviato tramite PdP su supporto di memorizzazione in modo non modificabile.

#### **5.1.13. Acquisizione delle rappresentazioni digitali dei documenti cartacei**

Effettuata l'operazione di registrazione e segnatura il documento ricevuto in formato cartaceo è acquisito mediante scansione comprensiva di eventuali allegati. Il processo di scansione avviene mediante:

- apposizione sul documento principale dell'etichetta dal PdP;
- acquisizione delle immagini in modo tale che ad ogni documento/allegato corrisponda un unico file;
- verifica della leggibilità e della qualità delle immagini acquisite;

- collegamento delle immagini alle rispettive registrazioni di protocollo in modo non modificabile;
- generazione dell'impronta e sua registrazione.

Il documento cartaceo, dopo l'operazione di scansione e di registrazione di protocollo, è inviato all'assegnatario per competenza. In caso di rifiuto dell'assegnazione il documento cartaceo viene restituito all'UOP che ha effettuato l'errata assegnazione.

## **5.2. Flusso dei documenti inviati dall'AOO**

Si definisce protocollazione in uscita la registrazione di un documento e dei suoi eventuali allegati il cui destinatario sia un soggetto, persona fisica o giuridica, esterno all'AOO. Costituisce soggetto esterno anche il dipendente universitario al quale viene inviato sul posto di lavoro un documento "*ad personam*".

### **5.2.1 Predisposizione e registrazione dei documenti da inviare**

Il ciclo di vita in uscita si articola nelle seguenti fasi:

- **Composizione:** l'ufficio mittente provvede alla redazione del documento e della relativa minuta nel caso di documento cartaceo, e all'attribuzione dell'indice di classificazione. Il RPA e/o il Dirigente appongono la propria sigla sul documento e relativa minuta. La formalizzazione avviene mediante l'apposizione delle firme autografe del sottoscrittore sul documento e sulla minuta. Il documento, unitamente alla minuta, viene quindi consegnato all'UOP;
- **Verifica:** l'UOP esegue le verifiche di conformità della documentazione predisposta. Se la verifica dà esito positivo, il documento viene registrato sul PdP; in caso contrario è restituito al RPA con le osservazioni del caso.
- **Registrazione di protocollo:** i requisiti necessari di ciascuna registrazione di protocollo in uscita sono:
  - a) numero di protocollo e data di registrazione, generati automaticamente dal sistema in forma non modificabile;
  - b) mittente, inteso quale struttura che ha prodotto il documento, in forma non modificabile;

- c) il/i destinatario/i principale/i oltre a eventuali destinatari per conoscenza;
  - d) l'oggetto del documento, in forma non modificabile;
  - e) l'impronta del documento informatico generata automaticamente dal sistema;
  - f) il tipo di supporto;
  - g) il mezzo di spedizione.
- Classificazione e assegnazione: la fase di protocollazione si completa mediante:
    - 1) l'inserimento della classificazione indicata dal RPA o dal responsabile dell'ufficio;
    - 2) l'indicazione del nominativo del RPA o del responsabile dell'ufficio;
    - 3) l'assegnazione all'UOP mittente;
    - 4) l'annotazione circa il collegamento ad altri documenti già protocollati.

Per completare la registrazione: nel caso di documento cartaceo si appone sullo stesso l'etichetta della segnatura stampata e contestualmente si effettua la scansione del documento da inserire sul PdP; nel caso di documento informatico si carica il relativo file direttamente sul PdP.

Qualora si intenda utilizzare la trasmissione via PEC deve essere predisposto un documento contenente le informazioni utili all'attività amministrativa che dovrà essere protocollato.

### **5.2.2. Trasmissione dei documenti informatici**

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica. Per la spedizione dei documenti informatici l'UOP utilizza la casella di posta elettronica certificata o ordinaria istituzionale della propria UOR o del Dirigente. Nel caso in cui il destinatario sia un dipendente dell'Ateneo le UOP possono inviare il documento anche dalla casella di posta elettronica istituzionale ordinaria dell'UOR o tramite la funzione "Notifica" del PdP. In assenza del domicilio digitale, l'AOO può predisporre le comunicazioni a persone fisiche come documenti informatici sottoscritti con firma digitale ed inviare alle stesse, per posta ordinaria, copia analogica di tali documenti secondo la normativa vigente. Qualora sia necessaria la certezza dell'avvenuta ricezione, la trasmissione dovrà avvenire mediante raccomandata con avviso di ricevimento. Se la dimensione del documento informatico supera la dimensione massima prevista dal sistema di posta utilizzato dall'AOO, il documento viene riversato su supporto digitale rimovibile non modificabile e trasmesso al destinatario con altra modalità.

### **5.2.3. Trasmissione dei documenti cartacei a mezzo posta**

La spedizione del documento avviene di norma il giorno lavorativo in cui è stato protocollato.

### **5.2.4. Trasmissione dei documenti cartacei a mezzo telefax**

Ai sensi dell'art. 47, comma 2, lettera c) del Codice dell'Amministrazione Digitale, così come modificato dall'art. 14 della Legge n. 98 del 9 agosto 2013, la trasmissione a mezzo fax è esclusa tra pubbliche amministrazioni. Sul documento trasmesso via fax è apposta la dicitura: "La trasmissione via fax del presente documento non prevede l'invio del documento originale". Solo su richiesta del destinatario verrà trasmesso anche l'originale. Le ricevute della avvenuta trasmissione sono trattenute dall'UOR che ha formato il documento.

### **5.2.5. Inserimento delle ricevute di trasmissione nel fascicolo**

La minuta del documento cartaceo spedito, le ricevute dei messaggi telefax, le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali e gli avvisi di ricevimento delle raccomandate A.R. sono conservati all'interno del relativo fascicolo a cura dell'UOR.

### **5.3. Flusso dei documenti interni all'AOO**

Descrive il flusso di lavorazione dei documenti interni all'AOO e le modalità per la registrazione.

#### **5.3.1. Trasmissione dei documenti interni formali**

Per comunicazione formale si intende esclusivamente quella a rilevanza giuridico-probatoria; essa deve essere prodotta con strumenti informatici e sottoscritta digitalmente. Per sorgente interna dei documenti si intende qualunque UOR che invia formalmente la propria corrispondenza ad altra UOR. La registrazione del documento avviene mediante UOP da parte dell'UOR mittente che provvederà ad assegnarla all'UOR destinataria.

#### **5.3.2. Trasmissione dei documenti interni informali**

Per comunicazione informale si intende lo scambio di informazioni/documenti di cui è facoltativa la conservazione. La comunicazione informale rappresenta la tipologia prevalente di scambio tra uffici ed avviene tramite le caselle di posta elettronica istituzionale. La comunicazione informale non è soggetta a registrazione di protocollo.

### **5.4. Assegnazione e smistamento mediante PdP**

L'attività di smistamento consiste nell'invio da parte della UOP di un documento protocollato all'UOR competente che a sua volta lo trasmette al RPA contestualmente alla trasmissione dell'originale cartaceo. Il RPA assegnatario provvede alla presa in carico del documento. Le eventuali assegnazioni per conoscenza possono essere inserite direttamente dall'UOP o dal RPA.

### **5.5. Modifica delle assegnazioni**

Nel caso l'assegnatario non ritenga di propria competenza il documento lo rifiuta e, contestualmente, restituisce l'eventuale documento cartaceo all'UOP. L'UOP procederà alla nuova assegnazione sentito, se del caso, il RSP.

## **14. ALBO ON LINE**

### **6.1. Finalità dell'Albo on line**

L'Albo on line ha il compito di gestire e tutelare la pubblicazione legale di documenti dell'Ateneo per la cui efficacia è richiesta una forma di pubblicità di rilevanza giuridico-probatoria, ossia una conoscenza certa a chiunque ne abbia interesse.

In applicazione della normativa vigente, sarà attivo il repertorio dell'Albo on line, associato al protocollo dell'Amministrazione Centrale. L'indirizzo dell'Albo on line è riportato sulla pagina iniziale del sito istituzionale di Ateneo e rimanda a una sezione dedicata.

Vanno pubblicati all'Albo on line i documenti previsti dall'ordinamento e quelli da cui possono nascere diritti, doveri, aspettative o interessi legittimi di terzi e dalla cui diffusione nei confronti di una indistinta pluralità di soggetti potenzialmente interessati dipende la loro efficacia.

### **6.2. Gestione dell'Albo on line**

La gestione dell'Albo on line è affidata all'Ufficio Protocollo, mentre spettano al responsabile del procedimento amministrativo la verifica della regolarità tecnico amministrativa dell'atto, l'adozione di eventuali accorgimenti per la protezione dei dati personali e la definizione della durata della pubblicazione.

I documenti da pubblicare, redatti su carta intestata della struttura proponente e in formato pdf, dovranno essere inoltrati esclusivamente all'indirizzo e-mail dell'Ufficio Protocollo o di chi si occupa della pubblicazione dei documenti.

L'e-mail di richiesta dovrà indicare la data di inizio della pubblicazione, la durata espressa in giorni e la data di termine della pubblicazione stessa. La durata della pubblicazione è di quindici giorni consecutivi salvo diverse disposizioni legislative, regolamentari e provvedimenti. Nel caso in cui si richieda la pubblicazione per un periodo inferiore o superiore sarà necessario indicare la motivazione.

## **7. UNITÀ ORGANIZZATIVE COMPETENTI NELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI**

Per quanto riguarda l'organizzazione e la tenuta dei documenti il "Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi" di cui all'art. 61 del DPR 445/2000 è individuato nell'Ufficio Protocollo e Archivio coordinato dall'Area Affari Legali. I documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi devono essere registrati a protocollo o a repertorio.

### **7.1. Attività di protocollo**

Per registrazione di protocollo si intende l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. La registrazione 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'Ateneo, 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 immutabile. La registrazione di protocollo per ogni documento è effettuata mediante la memorizzazione di elementi obbligatori immutabili, elementi obbligatori modificabili ed elementi non obbligatori e modificabili. La registrazione degli elementi obbligatori immutabili del protocollo informatico non può essere modificata, integrata, cancellata ma soltanto annullata mediante un'apposita procedura in capo al Coordinatore della gestione documentale e a persone espressamente delegate. L'immutabilità e l'immutabilità della registrazione di protocollo devono essere garantite dal sistema di gestione documentale.

Il "Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi", è strutturato in:

- un settore Protocollo, con funzioni generali per tutto l'Ateneo, di coordinamento delle attività di registrazione a protocollo di tutte le strutture dell'AOO e di supporto per le attività di competenza esclusiva di RSP.
- L'UOP gestione dei flussi e archiviazione dei documenti di competenza delle UOR.



## **7.2 Servizio archivistico**

Il servizio archivistico è funzionalmente e strutturalmente integrato nel suddetto “Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi”.

## **7.3 Servizio della conservazione elettronica dei documenti**

Ai fini dell’organizzazione e dell’avvio del processo di conservazione a norma dei documenti digitali, in attuazione dell’art. 44 comma 1 del D.Lgs. 82/2005 s.m.i. (“Codice dell’Amministrazione Digitale”), l’Ateneo ha provveduto alla nomina del Responsabile della Conservazione in capo alla “CSA SCARL” in data 20 settembre 2016.

### **7.3.1 Archiviazione dei documenti informatici**

Secondo quanto disposto dal DPCM del 3 dicembre 2013 "Regole tecniche in materia di sistema di conservazione", il Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi assicura la trasmissione del contenuto del pacchetto di versamento, da lui prodotto, al sistema di conservazione secondo le modalità operative definite nel Manuale di conservazione.

### **7.3.2 Archiviazione ottica dei documenti analogici**

Il Responsabile del “Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi”, valutati i costi ed i benefici, può proporre l’operazione di conservazione sostitutiva dei documenti analogici su supporti di memorizzazione sostitutivi del cartaceo in conformità alle disposizioni vigenti.

## **7.4. Elementi obbligatori immutabili (Registratura)**

Gli elementi obbligatori immutabili 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 almeno sette cifre numeriche;
- data di registrazione;
- corrispondente, ovvero mittente per il documento in arrivo, destinatario per il documento

- in partenza;
- oggetto;
- impronta del documento informatico;
- numero degli allegati;
- descrizione degli allegati.

L'insieme di tali elementi è denominato registratura.

### **7.5. Elementi obbligatori modificabili**

Gli elementi obbligatori modificabili sono:

- unità organizzativa responsabile del procedimento/affare/attività (UOR);
- responsabile del procedimento amministrativo (RPA);
- classificazione archivistica;
- fascicolo.

### **7.6. Elementi non obbligatori modificabili**

Gli elementi non obbligatori modificabili sono:

- recapiti del mittente;
- collegamento ad altri documenti o a fascicoli diversi da quello d'inserimento;
- tipologia di documento;
- durata della conservazione;
- altri tipi di annotazioni (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).

### **7.7. Data e ora regolate sul UTC**

Il server 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'Istituto nazionale di ricerca metrologica - INRiM.

### **7.8. 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.

### **7.9. Per il documento informatico**

Le informazioni minime da associare al documento informatico sono:

- codice identificativo dell'amministrazione;
- codice identificativo dell'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.

### **7.10. Per il documento analogico**

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

- l'identificazione in forma sintetica o estesa dell'amministrazione e dell'AOO individuata ai fini della registrazione e della gestione del documento;

- il numero progressivo di protocollo;
- la data di protocollo nel formato GGMMAAAA;
- la classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento;
- le sigle delle Area e delle Aree coinvolte.

## **8. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE**

### **8.1. Documenti esclusi**

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del D.P.R. n. 445 del 28 dicembre 2000:

- Gazzette ufficiali, Bollettini ufficiali PA;
- Notiziari PA;
- Giornali, Riviste, Libri;
- Materiali pubblicitari;
- Note di ricezione delle circolari e altre disposizioni;
- Materiali statistici;
- Atti preparatori interni;
- Offerte o preventivi di terzi non richiesti;
- Inviti a manifestazioni;
- Documentazione già soggetta, direttamente o indirettamente, a diversa registrazione.

### **8.2. Documenti soggetti a registrazione particolare (riservata)**

All'interno dell'AOO le registrazioni particolari (riservate), sottratte a qualsiasi consultazione da parte di chi non sia espressamente abilitato, sono effettuate sul PdP esclusivamente dall'UOP dell'Area Direzionale.

La registrazione particolare di norma è riferita a:

- documenti relativi a vicende personali, a fatti privati o particolari;

- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi dell'AOO;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- altri documenti che per ragioni strettamente legate a situazioni particolari dell'Amministrazione o del mittente sono da considerarsi in situazione analoga alle tipologie di documenti descritti nei punti precedenti;
- altre tipologie di documenti individuate dalla normativa vigente (in particolare dall'art. 24 della L. n. 241 del 7 agosto 1990, dall'art. 8 del DPR n. 352 del 27 giugno 1992, dalla serie di norme collegate al D. Lgs. n. 196 del 30 giugno 2003, e dal DR n. 2386 del 17 giugno 1998 recante le regole di attuazione della citata legge n. 241 del 7 agosto 1990).

Sono altresì soggetti a registrazione particolare i certificati rilasciati dal Tribunale Ordinario, Tribunale Fallimentare, Agenzia delle Entrate, Prefettura, Ufficio Provinciale del Lavoro, INPS, INAIL e Casse edili e altri documenti analoghi riportanti situazioni giuridico/amministrative sfavorevoli all'interessato. I documenti dell'archivio particolare (riservato) sono conservati a cura della Direzione Generale o presso gli uffici dove operano gli utenti autorizzati alla registrazione particolare e divengono consultabili alla scadenza dei termini indicati dalla normativa vigente.

### **8.3. La registrazione di protocollo particolare**

Le registrazioni di protocollo particolare sono eseguite dagli utenti autorizzati secondo le usuali regole di registrazione dei documenti in entrata e in uscita. La visualizzazione delle registrazioni particolari, al pari della registrazione, è consentita solo agli utenti all'uopo autorizzati.

#### **8.3.1. Annullamento di registrazioni di protocollo particolare**

L'annullamento di registrazioni particolari può essere eseguito previa richiesta scritta motivata da inoltrare al RSP. Per le relative operazioni di annullamento valgono le regole previste per l'annullamento di una normale registrazione di protocollo.

#### **8.3.2. Accesso ai dati**

L'accesso alle informazioni collegate ai documenti particolari è consentito esclusivamente al Responsabile dell'UOR competente alla trattazione dell'affare.

## **9. FASCICOLI E ARTICOLAZIONE INTERNA**

### **9.1 Apertura del fascicolo**

L'apertura di ciascun fascicolo e la relativa gestione sarà effettuata dal RPA o dal Responsabile dell'ufficio. L'apertura di un nuovo fascicolo avviene esclusivamente al momento della registrazione di un documento relativo ad un nuovo affare/procedimento.

### **9.2 Fascicolazione dei documenti**

Tutti i documenti registrati nel sistema informatico e classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli. Ogni documento classificato viene inserito nel fascicolo di riferimento o, all'occorrenza, nel sottofascicolo o inserito, secondo l'ordine cronologico di registrazione. Il fascicolo potrà contenere documenti non soggetti a registrazione ma ritenuti utili all'attività amministrativa.

### **9.3. Gestione del fascicolo**

Qualora un documento dia luogo all'avvio di un affare e/o nuovo procedimento amministrativo, il soggetto preposto provvede all'apertura del relativo fascicolo mediante la registrazione sul PdP delle seguenti informazioni essenziali:

- ramo del titolare (cioè titolo e classe);
- numero del fascicolo generato automaticamente dal PdP;
- oggetto;
- data di apertura del fascicolo generata automaticamente dal PdP e corrispondente alla data di registrazione del primo documento;
- RPA o Responsabile dell'ufficio;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Il fascicolo viene aperto a livello della classe di titolare. I documenti originali analogici registrati confluiscono nel fascicolo cartaceo appositamente creato e gestito dal RPA.

#### **9.4. Chiusura del fascicolo**

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare. La data di chiusura corrisponde alla data dell'ultimo documento inserito. Gli elementi che individuano un fascicolo sono gestiti dal RPA.

#### **9.5 Consultazione e movimentazione dell'archivio corrente, di deposito e storico**

##### **9.5.1 Principi generali**

La richiesta di consultazione, che può comportare la movimentazione dei fascicoli, può avvenire per scopi giuridico-amministrativi.

##### **9.5.2 Consultazione ai fini giuridico-amministrativi**

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della L. n. 241 del 7 agosto 1990, e successive modifiche e integrazioni.

## **10. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO**

### **10.1. Unicità del protocollo informatico**

Nell'ambito dell'AOO il registro di protocollo informatico è unico per i documenti in entrata, per i documenti in uscita e per i documenti interni formali; la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello distribuito adottato. Sono eliminati i protocolli di struttura, i protocolli multipli e tutti i protocolli diversi da quello informatico unico. La numerazione si chiude al 31 dicembre di ogni anno e si riapre il primo gennaio dell'anno successivo. Il numero di protocollo individua un unico documento ed è costituito da otto cifre numeriche. La registrazione di protocollo in entrata deve essere effettuata di norma nel giorno del ricevimento del documento e comunque non oltre le due giornate lavorative successive. L'insieme delle registrazioni giornaliere effettuate costituisce il Registro di protocollo e si configura come atto pubblico di fede privilegiata fino a querela di falso e fa fede della tempestività e dell'effettivo ricevimento e produzione di un documento, ed è quindi idoneo a produrre effetti giuridici. L'UOP non è tenuta a controllare la completezza formale e sostanziale della documentazione in entrata ma è tenuta a registrare in ogni caso il documento ed eventuali allegati; tale verifica spetta al RPA. È fatto divieto all'UOP di registrare anticipatamente documenti in uscita o interni formali diversi dall'originale debitamente sottoscritto (bozze del documento).

### **10.2. Registro giornaliero di protocollo**

Il RSP provvede ai sensi del DPR n. 445 del 28 dicembre 2000 alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle registrazioni di protocollo effettuate nell'arco di uno stesso giorno. Ai sensi dell'art. 7, comma 5, del DPCM del 3 dicembre 2013 il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.



### **10.3. Segnatura di protocollo dei documenti**

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

#### **10.3.1. Documenti informatici**

I dati della segnatura di protocollo di un documento informatico sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML), le cui modalità tecniche ed il formato sono predisposti in relazione all'evoluzione tecnologica.

Le informazioni incluse nella segnatura sono:

- denominazione dell'AOO;
- tipologia registrazione (entrata/uscita/interno);
- data e numero di protocollo del documento.

La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.

#### **10.3.2. Documenti cartacei**

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione sulla prima pagina di una etichetta non rimovibile stampata tramite PdP sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- denominazione della AOO;
- tipologia registrazione (entrata/uscita/interno);
- data e numero di protocollo del documento;
- codice a barre contenente data e numero di protocollo.

Nell'impossibilità dell'utilizzo dell'etichetta autoadesiva viene apposto un timbro tradizionale ove riportare le informazioni sopra indicate. L'acquisizione dell'immagine dei documenti cartacei deve essere eseguita solo ad avvenuta segnatura per assicurarne la visibilità sulla scansione.

#### **10.4. Annullamento di registrazione di protocollo**

A seguito di motivata richiesta del RPA la registrazione di protocollo può essere completamente annullata esclusivamente dall'UOP Protocollo di Ateneo, tramite una specifica funzione del PdP, previa autorizzazione del RSP. Le richieste di annullamento sono riferibili a: doppia protocollazione del medesimo documento, protocollazione di un documento non soggetto a registrazione, eventuali malfunzionamenti del PdP. Non è ammessa la richiesta di annullamento al fine di integrare o modificare il contenuto di un documento già spedito. Il RSP, valutate le motivazioni, dispone per l'annullamento. In caso di rigetto della richiesta, il RSP dovrà darne motivata comunicazione al richiedente.

#### **10.5. Casi particolari di protocollo**

##### **10.5.1. Protocollazione dei documenti fiscali previsti dalla normativa Fattura PA**

Questa protocollazione si articola in:

###### Ciclo passivo

1. l'UOR riceve i documenti per il tramite del Sistema di Interscambio (intermediario) che interagisce con il PdP;
2. la protocollazione dei documenti e delle relative note di esito avviene in maniera automatica mediante acquisizione dei metadati obbligatori;
3. il RPA dà indicazione all'UOP che provvede a completare il protocollo inserendo la classificazione, la fascicolazione ed eventuali annotazioni.

###### Ciclo attivo

L'UOR trasmette via PEC al Sistema di Interscambio (SdI) il documento firmato digitalmente e protocollato dall'UOP di riferimento che provvede altresì alla registrazione delle singole ricevute provenienti via PEC dal SdI.

### **10.5.2. Protocollo dei documenti inerenti gare di appalto**

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" o simili, o dal cui involucro si evince trattarsi di partecipazione ad una gara, non deve essere aperta. Sul plico viene apposta la data e l'ora di arrivo e contestualmente si procede alla protocollazione della busta o plico o simili, all'apposizione dell'etichetta su uno spazio libero del contenitore e alla acquisizione della scansione sul PdP; terminata tale procedura il plico viene inoltrato al RPA competente. Nel bando deve essere specificata l'UOP a cui indirizzare tale corrispondenza; per motivi organizzativi il RPA competente è tenuto a informare preventivamente l'UOP ricevente cui segnalare le scadenze delle gare. Il RPA competente provvede in modo sicuro alla custodia delle buste o dei contenitori protocollati e li trasmette al Responsabile del Procedimento per la successiva detenzione e custodia sino all'espletamento della gara. Dopo l'apertura delle buste il RPA che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sul plico su tutti i documenti in esso contenuti e provvede per la relativa acquisizione digitale sul PdP, associandola al medesimo numero di protocollo.

### **10.5.3. Corrispondenza personale o riservata**

La posta indirizzata nominativamente al personale dell'Ateneo di norma non viene aperta dalla UOP, salvo autorizzazione da parte del destinatario. La corrispondenza con la dicitura "riservata" o "personale" non deve essere aperta in nessun caso e viene pertanto consegnata al destinatario il quale, presa visione del contenuto, provvede per l'eventuale protocollazione.

### **10.5.4. Differimento delle registrazioni**

Il protocollo differito è ammesso solo al fine di non recare pregiudizio a diritti o legittime aspettative di terzi, qualora nella stessa giornata lavorativa non è possibile evadere tutta la corrispondenza in arrivo causa temporaneo ed eccezionale carico di lavoro. Il protocollo differito è autorizzato dal RSP su richiesta motivata dell'UOR interessata e si applica solo per tipologie documentali omogenee. Gli estremi dell'autorizzazione rilasciata dal RSP devono essere obbligatoriamente inseriti nel campo note del PdP al momento della registrazione differita; nel campo note dovrà essere indicato il giorno di effettivo ricevimento del documento.

### **10.5.5. Documenti in uscita con più destinatari**

Qualora il medesimo documento debba essere inviato a singoli destinatari, la registrazione di protocollo è unica e comprende il documento originale, con la dicitura “Vedi elenco destinatari” in luogo del nominativo del singolo destinatario, e l’elenco dei destinatari che costituisce parte integrante del documento.

## **11. ACCESSO AI DOCUMENTI INFORMATICI**

### **11.1. Generalità**

Il controllo degli accessi è il processo che garantisce l’impiego degli oggetti e servizi del sistema informatico di protocollo esclusivamente secondo modalità prestabilite. Il processo è caratterizzato da utenti che accedono ad oggetti informatici (dati), utilizzando servizi (funzioni), mediante operazioni specifiche (aggiornamento, operatività e consultazione). Agli utenti del PdP, in base alle rispettive competenze, vengono rilasciate autorizzazioni di accesso differenziate relativamente alle tipologie di operazioni da svolgere, stabilite dall’ufficio di appartenenza. Ad ogni utente è assegnata:

- una credenziale di accesso costituita da una componente pubblica che permette l’identificazione dell’utente da parte del sistema (userID) e una privata (password) che dovrà essere modificata al primo accesso per motivi di sicurezza;
- una autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza.

Le regole di utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l’identificazione dell’UOP e del personale abilitato a vario livello allo svolgimento delle operazioni sul PdP sono costantemente aggiornate a cura del RSP.

### **11.2. Abilitazioni interne per accedere ai servizi di protocollo**

Gli utenti abilitati accedono al PdP mediante credenziali personali. Le informazioni raccolte per autorizzare l’accesso al servizio sono quelle strettamente necessarie per l’identificazione dell’utente richiedente.

## **12. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA**

### **12.1. Il registro di emergenza**

Qualora la fruibilità del PdP viene temporaneamente meno per una interruzione accidentale o programmata, l'AOO adotta il registro di emergenza cartaceo. Il registro di emergenza è unico per l'AOO ed è gestito dal RSP. Il registro di emergenza si rinnova ogni anno solare. Qualora nel corso di un anno solare il registro di emergenza non viene utilizzato, il RSP annota sullo stesso l'inutilizzo. Le operazioni di protocollo effettuate sul registro di emergenza contengono le stesse informazioni ovvero gli elementi obbligatori delle registrazioni previste dal registro di protocollo informatico.

### **12.2. Modalità di apertura del registro di emergenza**

Il RSP assicura l'utilizzo del registro di emergenza cartaceo ad ogni interruzione del servizio di PdP e ne autorizza previamente l'adozione mediante annotazione sullo stesso della data, dell'ora e della motivazione. Qualora per cause di eccezionale gravità l'interruzione del servizio di PdP si prolunghi oltre le 24 ore, il RSP autorizza la prosecuzione delle attività sul registro di emergenza per un periodo di volta in volta non superiore a 5 giorni lavorativi.

### **12.3 Modalità di utilizzo del registro di emergenza**

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro il numero totale di operazioni effettuate manualmente. La sequenza cronologica delle registrazioni di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati sul PdP. Durante il periodo di interruzione del servizio di protocollo informatico, il Responsabile dei Sistemi Informativi (RSI), o persona da lui delegata, provvede a tenere costantemente informato il RSP sui tempi di ripristino del servizio.

### **12.4. Modalità di chiusura e recupero del registro di emergenza**

Al ripristino del servizio, il RSP provvede alla chiusura del registro di emergenza indicandone la data, l'ora e il numero totale delle registrazioni effettuate. Gli operatori del Protocollo Generale di Ateneo, al ripristino delle funzionalità del programma, provvedono ad effettuare le registrazioni sul PdP riportando le informazioni dal registro di emergenza con analogia cronologia e con le modalità precedentemente indicate. La conservazione del registro di emergenza è curata dal RSP.

## **13. NORME TRANSITORIE E FINALI**

### **13.1. Pubblicità del presente Manuale**

Il presente Manuale, ai sensi dell'art. 22 della L. n. 241 del 7 agosto 1990, degli artt. 9 e 13 del D.Lgs. n. 33 del 14 marzo 2013 e s.m.i. e dell'art. 5, comma 3, del D.P.C.M. del 3 dicembre 2013 è reso disponibile alla consultazione del pubblico che può prendere visione nella home page del sito istituzionale dell'Università degli Studi di "Roma Foro Italico" (<http://www.uniroma4.it>) "Amministrazione Trasparente".

### **13.2. Operatività del presente Manuale**

Il presente "Manuale di gestione del protocollo informatico, dei documenti e degli archivi" entra in vigore dalla data di pubblicazione sul sito di Ateneo.

## **5. INDICE DEGLI ALLEGATI**

Allegato n. 1 – Riferimenti Normativi

Allegato n. 2 – Glossario

## **Allegato n. 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).
- 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, Disposizione 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.

- 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.
- 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.
- 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.
- 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

## Allegato 2. Glossario

- **DOCUMENTO AMMINISTRATIVO:** ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa. Le relative modalità di trasmissione sono quelle indicate al capo II, sezione III del presente testo unico.
- **DOCUMENTO INFORMATICO:** la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
- **DOCUMENTO DI RICONOSCIMENTO:** ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consente l'identificazione personale del titolare.
- **DOCUMENTO D'IDENTITA':** la carta di identità ed ogni altro documento munito di fotografia rilasciato, su supporto cartaceo, magnetico o informatico, dall'amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare.
- **DOCUMENTO D'IDENTITA' ELETTRONICO:** il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età.
- **CERTIFICATO:** il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione e partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche.
- **DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE:** il documento, sottoscritto dall'interessato, prodotto in sostituzione dei certificati di cui al punto 6.
- **DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETA':** il documento, sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dal presente testo unico.
- **AUTENTICAZIONE DI SOTTOSCRIZIONE:** l'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive.
- **LEGALIZZAZIONE DI FIRMA:** l'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa.
- **LEGALIZZAZIONE DI FOTOGRAFIA:** l'attestazione, da parte di una pubblica amministrazione

competente, che un'immagine fotografica corrisponde alla persona dell'interessato.

- **FIRMA DIGITALE:** il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
- **AMMINISTRAZIONI PROCEDENTI:** le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi o provvedono agli accertamenti d'ufficio.
- **AMMINISTRAZIONI CERTIFICANTI:** le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni.
- **GESTIONE DEI DOCUMENTI:** l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato; essa è effettuata mediante sistemi informativi automatizzati.
- **SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI:** l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti.
- **SEGNATURA DI PROTOCOLLO:** l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso.
- **APERTURA:** un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse.
- **SICUREZZA:** la sicurezza di un formato dipende da due elementi il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno.

- **PORTABILITA'**: la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili.
- **FUNZIONALITA'**: la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.
- **SUPPORTO ALLO SVILUPPO**: la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, etc.).
- **DIFFUSIONE**: l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione. Inoltre nella scelta dei prodotti altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili -file zippati-) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.
- **ACCESSO**: operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
- **ACCREDITAMENTO**: riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione.
- **AFFIDABILITA'**: caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
- **AGGREGAZIONE DOCUMENTALE INFORMATICA**: aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.

- **ARCHIVIO:** complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività.
- **ARCHIVIO INFORMATICO:** archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
- **AREA ORGANIZZATIVA OMOGENEA:** un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.
- **ATTESTAZIONE DI CONFORMITA' DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO:** dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
- **AUTENTICITA':** caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
- **BASE DI DATI:** collezione di dati registrati e correlati tra loro.
- **CERTIFICATORE ACCREDITATO:** soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
- **CICLO DI GESTIONE:** arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
- **CLASSIFICAZIONE:** attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati.
- **CODICE ESEGUIBILE:** insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
- **CONSERVATORE ACCREDITATO:** soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale.

- **CONSERVAZIONE:** insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione.
- **COORDINATORE DELLA GESTIONE DOCUMENTALE:** responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee.
- **COPIA ANALOGICA DEL DOCUMENTO INFORMATICO:** documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
- **COPIA DI SICUREZZA:** copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione.
- **DESTINATARIO:** identifica il soggetto/sistema al quale il documento informatico è indirizzato.
- **DUPLICAZIONE DEI DOCUMENTI INFORMATICI:** produzione di duplicati informatici.
- **ESIBIZIONE:** operazione che consente di visualizzare un documento conservato e di ottenerne copia.
- **ESTRATTO PER RIASSUNTO:** documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici.
- **EVIDENZA INFORMATICA:** una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
- **FASCICOLO INFORMATICO:** aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
- **FUNZIONALITA' AGGIUNTIVE:** le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
- **FUNZIONALITA' INTEROPERATIVE:** le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445.

- **FUNZIONALITA' MINIMA:** la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
- **FUNZIONE DI HASH:** una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
- **GENERAZIONE AUTOMATICA DI DOCUMENTO INFORMATICO:** formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
- **IDENTIFICATIVO UNIVOCO:** sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.
- **IMMODIFICABILITA':** caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
- **IMPRONTA:** la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*.
- **INSIEME MINIMO DI METADATI DEL DOCUMENTO:** complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
- **INTEGRITA':** insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
- **INOPERABILITA':** capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
- **LEGIBILITA':** insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
- **LOG DI SISTEMA:** registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
- **MANUALE DI CONSERVAZIONE:** strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione.

- **MANUALE DI GESTIONE:** strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni.
- **MEMORIZZAZIONE:** processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
- **METADATI:** insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.
- **PACCHETTI DI ARCHIVIAZIONE:** pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento.
- **PACCHETTI DI DISTRIBUZIONE:** pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
- **PACCHETTO DI VERSAMENTO:** pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.
- **PACCHETTO INFORMATIVO:** contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
- **PIANO DELLA SICUREZZA DEL SISTEMA DI CONSERVAZIONE:** documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
- **PIANO DELLA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI:** documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza.
- **PIANO DI CONSERVAZIONE:** strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.



- **PIANO GENERALE DELLA SICUREZZA:** documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
- **PRESA IN CARICO:** accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
- **PROCESSO DI CONSERVAZIONE:** insieme delle attività finalizzate alla conservazione dei documenti informatici.
- **PRODUTTORE:** persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
- **RAPPORTO DI VERSAMENTO:** documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
- **REGISTRAZIONE INFORMATICA:** insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente.
- **REGISTRO PARTICOLARE:** registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445.
- **REGISTRO DI PROTOCOLLO:** registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti.
- **REPERTORIO INFORMATICO:** registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica.
- **RESPONSABILE DELLA GESTIONE DOCUMENTALE O RESPONSABILE DEL SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI:** dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi

dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

- **RESPONSABILE DELLA CONSERVAZIONE:** soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione.
- **RESPONSABILE DEL TRATTAMENTO DEI DATI:** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
- **RESPONSABILE DELLA SICUREZZA:** soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
- **RIFERIMENTO TEMPORALE:** informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
- **SCARTO:** operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
- **SISTEMA DI CLASSIFICAZIONE:** strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
- **SISTEMA DI CONSERVAZIONE:** sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice.
- **SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI:** nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico.
- **STATICITA':** Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.
- **TRANSAZIONE INFORMATICA:** transazione informatica: particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati.
- **UFFICIO UTENTE:** riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.

- **UTENTE:** persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
- **VERSAMENTO AGLI ARCHIVI DI STATO:** operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.