

**UNIVERSITA' DEGLI STUDI DI BERGAMO**

## **MANUALE DI GESTIONE DOCUMENTALE**

**(Testo Unico n. 445 del 28 dicembre 2000. Codice dell'Amministrazione Digitale D.lgs. n.82 del 7 marzo 2005. Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale entrate in vigore dal 10 settembre 2020. Comunicato di adozione pubblicato su G.U. n. 259 del 19.10.2020)**

Emanato con Decreto del Direttore Generale protocollo n. \_\_\_\_\_ del  
\_\_\_\_\_ (rep. \_\_\_\_\_)

adottato ai sensi del Testo n. 445 del 28 dicembre 2000; del codice dell'Amministrazione Digitale D.Lgs. n.82 del 7 marzo 2005; delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale entrate in vigore il 10 settembre 2020 (Comunicato di adozione pubblicato su G.U. n. 259 del 19.10.2020)

## SOMMARIO

### CAPITOLO 1. IL MANUALE DI GESTIONE DOCUMENTALE

1.1.	Finalità.....	9
1.2.	Oggetto.....	9
1.3.	Modalità di redazione.....	11
1.4.	Forme di pubblicità e divulgazione.....	11
1.5.	Principi e tutela dei dati personali.....	12

### CAPITOLO 2. QUADRO ORGANIZZATIVO ISTITUZIONALE

2.1.	Sistema di gestione informatica del flusso documentale.....	13
2.2.	<i>Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti.....</i>	13
2.3.	<i>Il responsabile della gestione documentale.....</i>	13
2.4.	<i>Area organizzative omogenea e unità organizzativa responsabile.....</i>	14
2.5.	Profili di abilitazione di accesso interno ed esterno alle informazioni documentali.....	15
2.6.	Posta elettronica istituzionale.....	15
2.7.	PEC istituzionale.....	15
2.8.	Piano di eliminazione dei registri di protocollo diversi dal protocollo informatico.....	15
2.9.	Il sistema di conservazione dei documenti informatici: ruoli e compiti.....	15
2.11.	In particolare i compiti del responsabile della conservazione.....	17

### CAPITOLO 3. IL DOCUMENTO: DEFINIZIONI E TIPOLOGIE – PROCESSI DI FORMAZIONE E DI DEMATERIALIZZAZIONE DEI DOCUMENTI

3.1.	Il documento e il documento amministrativo: definizioni e caratteristiche.....	20
3.2.	Documenti amministrativi: in arrivo, in partenza, interni e da registrare in repertori.....	21
3.3.	Il documento analogico: definizione e disciplina.....	22
3.4.	Il documento informatico: definizione e disciplina giuridica.....	23
3.5.	Il documento amministrativo informatico: definizione e disciplina giuridica.....	24
3.6.	In particolare: la formazione del documento amministrativo analogico.....	25
3.7.	Documenti redatti in originale su supporti analogico.....	25

3.8. In particolare: la formazione del documento informatico.....	26
3.9. Copie per immagine su supporto informatico di documento analogico.....	27
3.10. Duplicati, copie ed estratti informatici di documenti informatici.....	28
3.11. Formazione del documento amministrativo informatico.....	29
3.12. Copie su supporto informatico di documenti amministrativi analogici.....	30
3.13. Il documento amministrativo informatico costituito dal corpo della posta elettronica istituzionale.....	31
3.14. Metadati.....	31
3.15. Obiettivi dei metadati archivistici.....	31
3.16. Metadati essenziali per la registrazione del protocollo informatico.....	32
3.17. Validazione temporale.....	32
3.18. Formati.....	33

## **CAPITOLO 4. IL FASCICOLO**

4.1. Il fascicolo: definizione e funzione.....	34
4.2. Il fascicolo analogico: formazione, implementazione e gestione.....	35
4.3. Il fascicolo informatico: formazione, implementazione e gestione.....	35
4.4. I fascicoli annuali ripetitivi.....	36
4.5. Il fascicolo ibrido.....	37
4.6. Metadati del fascicolo informatico.....	37
4.7. Il repertorio dei fascicoli informatici.....	38
4.8. Raccogliitore.....	38

## **CAPITOLO 5. LA GESTIONE DELL'ARCHIVIO CORRENTE**

5.1. Definizione.....	39
5.2. Buone prassi per la gestione dell'archivio corrente.....	39
5.3. Gli strumenti dell'archivio corrente.....	40
5.3.1. Registro di protocollo.....	40

5.3.2. Titolario (piano di classificazione).....	41
5.3.3. Repertorio di fascicoli.....	41
5.3.4. I repertori.....	42
5.3.5. Massimario di selezione.....	42
5.4. Spostamento di un archivio corrente analogico.....	43

## **CAPITOLO 6. IL PROTOCOLLO INFORMATICO**

6.1. Registratura.....	44
6.1.1. Elementi obbligatori immutabili (registratura).....	45
6.1.2. Elementi obbligatori modificabili.....	45
6.1.3. Elementi non obbligatori modificabili.....	45
6.2. Data e ora regolate sul UTC.....	46
6.3. Segnatura.....	46
6.3.1. Per il documento informatico.....	46
6.3.2. Per il documento analogico.....	47
6.4. Modalità di produzione e di conservazione delle registrazioni.....	47
6.5. La registrazione differita (o “protocollo differito”).....	48
6.6. La ricevuta di avvenuta registrazione.....	48
6.6.1. Per il documento analogico.....	49
6.6.2. Per il documento informatico.....	49
6.7. Documenti esclusi dalla registrazione di protocollo.....	49
6.8. Il registro giornaliero di protocollo.....	50
6.9. Il registro di emergenza.....	50

## **CAPITOLO 7. REGISTRI E REPERTORI INFORMATICI**

7.1. Repertorio – nozioni.....	52
7.2. Repertori attivi.....	52
7.3. repertorio dei fascicoli.....	52

## **CAPITOLO 8. FLUSSO DI LAVORAZIONE DEI DOCUMENTI**

8.1. Flusso di lavorazione del documento informatico.....	53
8.2. Ricezione di documenti informatici nella casella elettronica istituzionale.....	53
8.3. Ricezione dei documenti informatici tramite la casella di posta elettronica certificata (PEC) istituzionale.....	54
8.4. Ricezione di documenti informatici su supporti rimovibili.....	55
8.4.1. Documenti informatici prodotti da banche dati dell'Ateneo o prodotti da banche dati di terzi.....	55
8.5. Priorità alla registrazione dei documenti informatici in arrivo.....	55
8.6. Flusso del documento analogico.....	56
8.7. Apertura delle buste.....	56
8.7.1. Conservazione ed eliminazione delle buste.....	57
8.8. Priorità della registrazione dei documenti analogici in arrivo.....	57
8.9. Protocollo particolare/riservato.....	58
8.9.1. Procedure del protocollo particolare/riservato.....	58
8.10. L'archivio particolare/riservato.....	58
8.11. Annullamento di una registrazione.....	59
8.12. Corresponsabilità di un documento e di un fascicolo.....	60
8.13. Documenti scambiati tra uffici non soggetti a registrazione di protocollo	61
8.14. Casi di rigetto.....	61
8.15. Flusso del documento informatico in partenza.....	61
8.16. Flussi del documento informatico tra UOR della stessa AOO.....	62
8.17. Utilizzo delle firme elettroniche: firma elettronica semplice avanzata, firma elettronica qualificata, firma digitale.....	63

## **CAPITOLO 9. CASISTICA E COMPORAMENTI**

9.1. Gestione delle gare d'appalto.....	64
9.1.1. Gare e procedura negoziata gestite in modalità analogica.....	64
9.1.2. Gare e procedura negoziata gestite in modalità tematica.....	64
9.2. Gestione di concorsi e selezioni.....	64
9.3. Atti giudiziari.....	65
9.4. Documenti informatici con oggetto multiplo.....	66

9.5. Fatture elettroniche (Fattura PA).....	66
9.6. DURC on-line.....	67
9.7. Denunce di infortuni.....	68
9.8. Certificati di malattia.....	68
9.9. Documenti del portale degli acquisti della pubblica amministrazione.....	68
9.9.1. Affidamenti diretti della piattaforma MePA.....	69
9.9.2. Adesioni-Convenzioni (OdA).....	69
9.9.3. Procedure negoziate (RdO) – MePA.....	69
9.10. Documenti pervenuti via PEC.....	70
9.11. Gestione di due documenti diversi trasmessi via PEC.....	71
9.12. Gestione di soli allegati pervenuti via PEC e di documenti costituiti dal solo corpo della PEC.....	71
9.13. Documenti pervenuti a mezzo e-mail semplice (non certificata).....	71
9.13.1. Rapporti con terzi esterni.....	71
9.13.2. Rapporti tra diverse AOO.....	72
9.14. Gestione del secondo esemplare.....	72
9.15. Documenti anonimi.....	72
9.16. Documenti scambiati tra UOR della stessa AOO.....	72

**CAPITOLO 10. ALBO on-line – Pubblicazioni su sito istituzionale dell’AOO – Ateneo (rinvio)73**

**CAPITOLO 11. DALL’ARCHIVIO CORRENTE ALL’ARCHIVIO DI DEPOSITO**

11.1. Archivio di deposito.....	74
11.2. Trasferimenti dei fascicoli cartacei.....	76
11.3. Trasferimenti dei fascicoli informatici.....	77
11.4. Trasferimento delle serie archivistiche.....	77
11.5. Ordinamento archivistico.....	78
11.6. Servizio di ricerca documentale e movimentazione dei fascicoli (record delivery)79	
11.7. Conservazione.....	79

## **CAPITOLO 12. Il sistema informatico**

12.1. Obiettivi e piani di sicurezza.....	81
12.2. Il modello organizzativo.....	81
12.3. Sicurezza del sistema informatico.....	82
12.3.1. Il sistema di gestione documentale.....	82
12.3.2. Sicurezza fisica dei data center.....	82
12.3.3. La manutenzione e la continuità operativa degli impianti elettrici.....	83
12.3.4. Rete dati.....	83
12.3.5. Le postazioni di lavoro.....	83
12.4. Sicurezza dei documenti informatici.....	84
12.4.1. Accesso ai dati e ai documenti informatici.....	85
12.4.2. Le procedure comportamentali ai fini della protezione dei documenti.....	85
12.5. Il sistema informatico (software, produzione e conservazione delle registrazioni sul prodotto di protocollo).....	87
12.6. Il sistema degli accessi.....	87

Allegati:

- 1) Delibera di approvazione del Manuale;
- 2) Funzionigramma con nomina del DPO e altre nomine;
- 3) Registrazioni particolari;
- 4) Piano di classificazione/titolario;
- 5) Piano di fascicolazione;
- 6) Massimario di scarto/Piano di conservazione:
  - 6/1) Massimario o elenco descrittivo della documentazione da conservare perennemente oppure da scartare;
  - 6/2) si fa riferimento al Massimario di selezione dei documenti inerenti al fascicolo di studente universitario – Quaderni UNIDOC;
  - 6/3) si fa riferimento al Massimario di selezione dei documenti inerenti al fascicolo del personale universitario – UNIDOC .
- 7) Manuale di Conservazione del Conservatore esterno – Cineca -;
- 8) Piano per la sicurezza informatica;
- 9) Regolamento di Ateneo sulla disciplina del diritto di accesso;
- 10) Appendice normativa;
- 11) Glossario,
- 12) Elenco dei documenti che non serve protocollare;
- 13) Regolamento in materia di pubblicazione dei documenti all'albo di Ateneo.

## **CAPITOLO 1. IL MANUALE DI GESTIONE DOCUMENTALE**

### **1.1. Finalità**

Il manuale di gestione è uno strumento operativo che descrive il sistema di produzione e di gestione documenti, come previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, capitolo 3 “Gestione documentale”, paragrafo 5 “Manuale di gestione documentale, 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”.

Serve a indicare le procedure e a fornire le istruzioni per la corretta formazione, gestione, tenuta e conservazione della documentazione analogica e digitale.

Esso descrive, altresì, le modalità di gestione dei flussi documentali e degli archivi, in modo tale da organizzare e governare la documentazione ricevuta, inviata o comunque prodotta dall’amministrazione secondo parametri di corretta registrazione di protocollo, smistamento, assegnazione, classificazione, fascicolatura, reperimento e conservazione dei documenti.

Il manuale di gestione costituisce una guida per l'operatore di protocollo e per il cittadino e per le imprese. Al primo, per porre in essere le corrette operazioni di gestione documentale, agli ultimi due per comprendere e per collaborare nella gestione documentale stessa (ad es., utilizzando formati idonei per la formazione delle istanze, ecc.).

### **1.2. Oggetto**

Il presente Manuale disciplina la gestione di tutti i documenti, prodotti o ricevuti dall'unica Area Organizzativa Omogenea istituita nell'ambito dell'Università degli Studi di Bergamo, e dalle sue relative articolazioni interne quali definite ai sensi del presente Manuale e risultanti dallo Statuto nonché dagli atti formali di organizzazione emanati dall'Ateneo.

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

Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

Il presente Manuale di gestione – ai sensi delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, capitolo 3 “Gestione documentale”, paragrafo 5 “Manuale di gestione documentale, 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”. descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Nel Manuale di Gestione Documentale sono riportati, in particolare:

1. Relativamente agli aspetti organizzativi:

- a) Le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi ed all'esterno dell'AOO, applicando le modalità di trasmissione indicate nell'allegato 6 delle Linee Guida AgiD "Comunicazione tra AOO di Documenti Amministrativi Protocollati";
- b) L'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno dell'AOO;
- c) L'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;
- d) I criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno dell'Amministrazione, al sistema di gestione informatica dei documenti;

2) relativamente ai formati dei documenti:

- a) l'individuazione dei formati utilizzati per la produzione del documento informatico, come introdotti nel paragrafo 3.6 (delle Linee Guida indicati nell'allegato 2) "Formati di file e riversamento";
- b) La descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi che sono individuati nell'Allegato 2 (Linee Guida) "Formati di file e riversamento";
- c) Le procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento previste come indicato al paragrafo 3.7 e nell'Allegato 2 (Linee Guida) "Formati di file e riversamento";

3) relativamente al protocollo informatico e alle registrazioni particolari:

- a) Le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;
- b) La descrizione completa e puntuale delle modalità di utilizzo della componente "sistema di protocollo informatico" del sistema di gestione informatica dei documenti;
- c) Le modalità di utilizzo del registro di emergenza ai sensi dell'art.63 del TUDA, inclusa la funzione di recupero dei dati protocollati manualmente;
- d) L'elenco dei documenti esclusi dalla registrazione di protocollo, per cui è prevista registrazione particolare ai sensi dell'art.53, comma 5, del TUDA.
- e) Determinazione dei metadati da associare ai documenti soggetti a registrazione particolare individuati, assicurando almeno quelli obbligatori previsti per il documento informatico dall'Allegato 5 (Linee Guida);
- f) I registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, riconosciuti da una norma;

4) relativamente alle azioni di classificazione e selezione:

- a) Il piano di classificazione adottato dall'Amministrazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative, ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;

5) relativamente alla formazione delle aggregazioni documentali:

- a) Le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;

6) relativamente ai flussi di lavorazione dei documenti in uso:

- a) La descrizione dei flussi di lavorazione interni all'Amministrazione, anche mediante la rappresentazione formale dei processi attraverso l'uso dei linguaggi indicati da AgID, applicati per la gestione dei documenti ricevuti, inviati o ad uso interno;

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

- a) Le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia dei dati personali;

8) relativamente alla conservazione:

- a) Per le Pubbliche Amministrazioni il piano di conservazione è allegato al manuale di gestione documentale, con l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate.

### **1.3. Modalità di redazione**

La redazione del manuale di gestione deve contemperare l'assolvimento dell'obbligo normativo e le esigenze concrete dell'amministrazione.

Per tale motivo è stato redatto previa verifica e analisi del modello organizzativo e delle procedure amministrative.

Per la pubblicazione di questo Manuale sono state seguite le indicazioni della Soprintendenza Archivistica della Lombardia.

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

Il manuale di gestione è reso pubblico mediante la diffusione sul sito istituzionale,

come previsto dalle Linee Guida Agid, cap. III par.5.

E' prevista infine, un'attività di formazione continua e permanente in materia di gestione documentale per tutte le unità organizzative responsabili dell'Ateneo.

## **1.5 Principi e tutela dei dati personali**

L'amministrazione titolare dei dati di protocollo e dei dati personali – comuni, sensibili e/o giudiziari – contenuti nella documentazione amministrativa di propria pertinenza dà attuazione, con atti formali aventi rilevanza interna ed esterna, alla vigente normativa in materia di protezione delle persone fisiche con particolare riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 e relativo Decreto Legislativo n. 101 del 10 agosto 2018 di attuazione di detto Regolamento UE, modificativo del Codice Privacy approvato con D.Lgs. del 30 giugno 2003 n. 196).

Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri secondo quanto previsto nel presente Manuale risultano incaricati dal titolare dei dati e, dai responsabili del trattamento dei dati personali come individuati a norma del regolamento di ateneo emanato in attuazione della suddetta normativa nazionale e dell'Unione Europea.

Relativamente agli adempimenti esterni, l'amministrazione si è organizzata per garantire che i certificati e i contenuti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente.

In relazione alla protezione dei dati personali trattati al proprio interno l'amministrazione dichiara di aver ottemperato a quanto previsto dalla suddetta normativa vigente in materia, con particolare riferimento:

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

## CAPITOLO 2. QUADRO ORGANIZZATIVO ISTITUZIONALE

### 2.1. Sistema di gestione informatica del flusso documentale

Il presente Manuale come richiesto dalle linee Guida AgiD descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

<b>Testo adottato all'uso con Decreto Direttoriale 199/2021</b>	<b>Testo modificato con Decreto Direttoriale 23/2022</b>
<p><b>2.2. Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti</b></p> <p>Nell'Università degli Studi di Bergamo nell'ambito dell'Area Affari Generali e Legali vi è l'Unità Organizzativa Omogenea "Supporto Organi e Protocollo" con funzioni di servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, come previsto dal DPR 445/2000, art. 61.</p> <p>Alla UOR è attribuita la competenza di tenuta del sistema di gestione analogica e informatica dei documenti, dei flussi documentali e degli archivi, nonché il coordinamento degli adempimenti previsti dalla normativa vigente.</p> <p>L'Ufficio Supporto Organi e Protocollo garantisce la corretta gestione, tenuta e tutela dei documenti, vigila sull'osservanza della corretta applicazione della normativa in materia di gestione documentale durante l'intero ciclo di vita dei documenti, oltre a ulteriori specifici compiti attribuiti dalla legge o dall'ordinamento interno dell'Ateneo.</p> <p>L'Ateneo è organizzato in un'unica A.O.O. allegato 2, ha un proprio servizio per la tenuta del protocollo informatico, della gestione documentale, individuato tra il personale in possesso di idonei requisiti professionali o di professionalità tecnico</p>	<p><b>2.2. Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti</b></p> <p>Nell'Università degli Studi di Bergamo nell'ambito dell'Area Affari Generali e Legali vi è l'Unità Organizzativa Omogenea "<b>Servizio Protocollo</b>" con funzioni di servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, come previsto dal DPR 445/2000, art. 61.</p> <p>Alla UOR è attribuita la competenza di tenuta del sistema di gestione analogica e informatica dei documenti, dei flussi documentali e degli archivi, nonché il coordinamento degli adempimenti previsti dalla normativa vigente.</p> <p>L'Ufficio <b>Servizio Protocollo</b> garantisce la corretta gestione, tenuta e tutela dei documenti, vigila sull'osservanza della corretta applicazione della normativa in materia di gestione documentale durante l'intero ciclo di vita dei documenti, oltre a ulteriori specifici compiti attribuiti dalla legge o dall'ordinamento interno dell'Ateneo.</p> <p>L'Ateneo è organizzato in un'unica A.O.O. allegato 2, ha un proprio servizio per la tenuta del protocollo informatico, della gestione documentale, individuato tra il personale in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi</p>

<p>archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente, art. 61, comma 2, DPR 445/2000.</p>	<p>di formazione definiti secondo le procedure prescritte dalla disciplina vigente, art. 61, comma 2, DPR 445/2000.</p>
--	---

### **2.3. Il responsabile della gestione documentale**

Il responsabile della gestione documentale è preposto al servizio di cui all'art. 61 del TUDA e predispone:

- il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione;

Tale manuale conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:

- misure di sicurezza predisposte dall'Agid e dagli altri organismi preposti;
- delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.

I provvedimenti di nomina del responsabile della gestione documentale e, ove diverso, del responsabile della conservazione, indicano:

- a) La denominazione del servizio;
- b) Il nominativo del responsabile;
- c) Il possesso dei requisiti di professionalità anche di tipo archivistico ed informatico previsti dalla normativa vigente;
- d) La descrizione dei compiti assegnati al responsabile che deve comprendere tutte le attribuzioni che la normativa vigente attribuisce sia al responsabile del servizio di cui al citato art.61 T.U. sia quelle previste per il ruolo di Responsabile della gestione documentale (Linee Guida Agid)

### **2.4. Area organizzativa omogenea e unità organizzativa responsabile**

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

L'unità organizzativa responsabile (UOR) è, all'interno della AOO, un complesso organizzato 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, attività e procedimenti amministrativi.

L'Università è organizzata come descritto nell'allegato 2 Funzionigramma, come previsto dalla legge 7 agosto 1990, n. 241 (artt. 4-6), dal DPR 28 dicembre 2000, n. 445 e dalle Linee Guida Agid.

Le AOO e le UOR sono descritte, unitamente alle altre informazioni richieste, nell'indice delle Pubbliche Amministrazioni – IPA. E' compito del Referente IPA dell'ente provvedere all'accreditamento, alla trasmissione delle informazioni richieste dalla legge e all'aggiornamento senza ritardo dei dati nel sito IPA

## **2.5. Profili di abilitazioni di accesso interno ed esterno alle informazioni documentali**

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

Il Responsabile della gestione documentale riceve dai responsabili delle UOR dell'Amministrazione e dai responsabili delle strutture didattiche, scientifiche e di servizio richiesta scritta (tramite e-mail) di abilitazione per ciascun utente, concordando, caso per caso, le tipologie di abilitazione.

Il profilo di ogni utente è generato mediante la personalizzazione di modelli predefiniti.

## **2.6. Posta elettronica istituzionale**

Ciascuna UOR è dotata della casella istituzionale di posta elettronica.

La casella viene denominata in modo da rendere facilmente individuabile la UOR di riferimento.

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

## **2.7. PEC Istituzionale**

L'Università degli Studi di Bergamo ha attivato le caselle di PEC per l'Amministrazione Centrale ed i Presidi di Ateneo.

## **2.8. Piano di eliminazione dei registri di protocollo diversi dal protocollo informatico**

Il registro di protocollo dell'Ateneo è unico. A far data dal 30.03.2001 sono cessati di fatto e di diritto tutti i cosiddetti protocolli interni (cioè di settore, di divisione, protocolli multipli, protocollo del telefax, etc.) o altri sistemi di registrazione dei documenti diversi dal protocollo unico. Qualsiasi registrazione eventualmente effettuata su registri non autorizzati è nulla di diritto e non può produrre alcun effetto giuridico-probatorio.

## **2.9. Il sistema di conservazione dei documenti informatici: ruoli e compiti e funzioni**

Il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell'art.44, comma 1 – bis, del CAD:

- a) I fascicoli informatici chiusi e le serie informatiche chiuse trasferendoli dall'archivio corrente o dall'archivio di deposito;
- b) I fascicoli informatici e le serie non ancora chiuse trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'ente, con particolare attenzione per i rischi di obsolescenza tecnologica.

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

- a) I documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
- b) Le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/2000 e art.44, comma 1- bis, CAD;
- c) Gli archivi informatici con i metadati associati.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e della normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e della normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Il sistema di conservazione è almeno logicamente distinto dal sistema di gestione informatica dei documenti.

Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili.

Il processo di conservazione è realizzato ai sensi dell'art. 34, comma 1 – bis, del CAD, fatte salve le competenze del Ministero per i beni le attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n.42.

Il processo di conservazione può essere pertanto svolto all'interno o all'esterno della struttura organizzativa dell'ente.

I requisiti del processo di conservazione, le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione, e le loro modalità di interazione sono formalizzate nel manuale di conservazione del titolare dell'oggetto della conservazione e nelle specifiche del contratto di servizio o dell'accordo. Tali modalità trovano riscontro anche nel manuale di conservazione del conservatore.

Al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, i fornitori di servizi di conservazione devono possedere requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001 (*Information security management systems – Requirements*) del sistema di gestione della sicurezza delle informazioni nel dominio, logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione e ISO 14721 OAIS (*Open Archival Information System – Sistema informatico aperto per l'archiviazione*), e alle raccomandazioni ETSI TS 101 533 – 1v. 1.2.1, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

L'Università degli Studi di Bergamo ha optato per affidamento della conservazione a soggetto accreditato come conservatore presso l'Agid: il Cineca.

Nel caso di affidamento a soggetto esterno, il responsabile interno della conservazione (RIC) mantiene il compito di vigilare sulla corretta esecuzione del contratto nel rispetto della normativa e delle regole tecniche o linee guida vigenti.

Il responsabile interno della conservazione ed eventualmente il responsabile del servizio di conservazione esterno all'ateneo opereranno d'intesa con il Responsabile del trattamento dei dati personali e con il Responsabile della sicurezza, oltre che con il Responsabile della gestione documentale.

## **2.10. In particolare i compiti del responsabile della conservazione**

I compiti del responsabile della conservazione dei documenti informatici previsti dall'art. 44 comma 1-bis del CAD - sono definiti dal Codice dell'Amministrazione Digitale e dalle relative Linee Guida AgID e, all'atto dell'emanazione del presente Manuale, risultano i seguenti:

- a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
- b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

- c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia.

Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.

In particolare, il responsabile della conservazione:

- a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentario degli archivi;
- g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, adotta analoghe misure con riguardo all'obsolescenza dei formati;
- h) provvede alla duplicazione o copia dei documenti in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- i) predisporre le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11 (Linee Guida AgiD);
- j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

- k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art.41, comma 1, del Codice dei beni culturali;
- m) predisporre il manuale di conservazione di cui al par. 4.7 (Linee Guida AgiD) e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore esterno, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing delle PA.

## CAPITOLO 3.

### IL DOCUMENTO: DEFINIZIONI E TIPOLOGIE - PROCESSI DI FORMAZIONE E DI DEMATERIALIZZAZIONE DEI DOCUMENTI

#### 3.1. Il documento e il documento amministrativo: definizioni e caratteristiche.

Per documento amministrativo si intende – in generale - la rappresentazione comunque formata di atti, fatti o dati giuridicamente rilevanti, dalla quale possono nascere diritti, doveri o legittime aspettative di terzi, completa dei suoi elementi sostanziali e formali relativi al soggetto che lo forma e sottoscrive con firma autografa, firma elettronica, firma elettronica avanzata, firma elettronica qualificata e firma digitale.

I documenti così definiti:

- sono scritti a mano o con l'ausilio di strumenti informatici;
- con riferimento al tipo di supporto sul quale sono prodotti, i documenti si distinguono in analogici ed informatici;
- sono soggetti ad obbligo di registrazione a protocollo ad esclusione *“delle gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari ed altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni”* come stabilito dalla normativa ad oggi in vigore ed alla quale si rimanda;
- sono gestiti e prodotti in modo da tutelare la riservatezza dei dati personali e dei dati sensibili in essi contenuti;
- contengono caratteristiche oggettive di qualità, sicurezza, integrità, immodificabilità, staticità, leggibilità, accessibilità, autenticità dell'origine, certezza giuridica, idoneità della conservazione a norma;
- sono gestiti, tenuti, reperiti, tutelati, destinati a conservazione, sottoposti ad eventuale procedura di scarto.

Una particolare tipologia di documenti è costituita dai documenti amministrativi che sono i documenti detenuti da una Pubblica Amministrazione ed utilizzati per fini amministrativi, ed ai quali il presente manuale farà riferimento.

In particolare l'art. 22 comma 1 lettera d) della Legge 241/1990 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”*.

### **3.2. Documenti amministrativi: in arrivo, in partenza, interni e da registrare in repertori**

Per documenti dell'Università degli studi di Bergamo, ai fini del presente Manuale, si intendono quelli prodotti ed acquisiti nello svolgimento della propria attività o nell'esercizio delle proprie funzioni amministrative da tutte le UOR di cui si compone l'AOO-Ateneo.

Con riferimento al tipo di supporto con cui sono prodotti essi possono essere analogici e informatici.

Secondo quanto previsto dall'art. 40 comma 1 del CAD *“le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici, secondo le disposizioni di cui al presente codice e le Linee guida”*.

Nel seguito si intende che un documento anche se formato con strumenti informatici è analogico se il suo contenuto viene rappresentato su supporto cartaceo e sottoposto a firma autografa da parte del sottoscrittore.

Per evitare conflitti di notazione, il documento amministrativo informatico sottoscritto con firma digitale sarà di seguito denominato documento digitale.

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

- Documenti in arrivo;
- Documenti in partenza;
- Documenti interni (scambiati tra UOR);
- Documenti da registrare in repertori

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 “*documenti 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 “*documenti da registrare in repertori*” si intendono i documenti privi di destinatario o con destinatario generale, che presentano gli stessi elementi formali, indipendentemente dal loro contenuto (documenti uguali per forma ma diversi per contenuto) quali, ad esempio, le circolari, i decreti o le determine degli organi monocratici, i verbali degli organi collegiali, i contratti o le convenzioni, ecc.

L’elenco completo delle tipologie documentali soggette a registrazione mediante registrazione a repertorio è riportato nell’allegato 3.

La creazione di nuovi repertori o la modifica dei repertori esistenti viene effettuata dagli amministratori del sistema informatico di protocollo a seguito di disposizione del Direttore Generale.

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 pur potendo essere acquisite sul sistema di gestione documentale come “bozze” ossia come documenti non protocollati

### **3.3. Il documento analogico: definizione e disciplina giuridica**

Il CAD, all’art. 1 comma 1 lett. p-bis) definisce documento analogico “*la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*”.

Qualsiasi documento non informatico (ad es. un documento cartaceo) è, dunque, un documento analogico. Pertanto sono documenti analogici i documenti formati utilizzando una grandezza fisica (quali ad esempio: le tracce su carta, le immagini contenute nei film e la magnetizzazione su nastro).

Nell’attività amministrativa, di norma il documento analogico è un documento formato su supporto analogico prodotto con strumenti analogici (ad es., documento scritto a mano) o con strumenti informatici (ad es., documento prodotto con un sistema di videoscrittura) e stampato su carta.

Di seguito nel presente Manuale faremo riferimento al documento amministrativo analogico nella sua forma cartacea, che può essere prodotto sia nella sua forma tradizionale (scritto cioè a mano o a macchina sia con strumenti informatici e poi stampato). In tal caso

si definisce “*originale*” il documento cartaceo nella sua redazione definitiva, perfetta ed autentica, negli elementi sostanziali e formali, comprendente tutti gli elementi di garanzia e di informazione del mittente e del destinatario, stampato su carta intestata e dotato di firma autografa.

### **3.4. Il documento informatico: definizione e disciplina giuridica**

Il CAD, all’art. 1 comma 1 lett. p), definisce documento informatico “*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*”.

Il documento informatico è, quindi, un *file*, cioè una sequenza determinata di valori binari indifferente al supporto fisico su cui è memorizzata.

Ai sensi dell’art. 46 del Regolamento UE e-Ideas “*ad un documento elettronico non sono negati gli effetti giuridici e l’ammissibilità come prova in giudizio per il solo motivo della sua forma elettronica*”

I documenti informatici ed i loro aggregati formati nel rispetto delle regole tecniche in vigore devono soddisfare caratteristiche di: qualità, sicurezza, immodificabilità, staticità, leggibilità, accessibilità, interoperabilità, diffusione, riutilizzabilità, idoneità alla conservazione.

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.

A norma dell’art. 20 del CAD, così come modificato con il Decreto Legislativo 217/2017, il documento informatico soddisfa il requisito della forma scritta e ha l’efficacia prevista dall’art. 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato previa identificazione del suo autore, attraverso un processo avente i requisiti fissati dall’AgID tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta, la sua riconducibilità all’autore.

In tutti gli altri casi l'idoneità del documento a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di qualità, sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida definite dall'AgID.

L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica salvo che questi ne dia prova contraria.

Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa, anche regolamentare, in materia di processo telematico.

Il documento informatico – ai sensi delle Linee Guida AgiD, capitolo 2, in materia di formazione dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle Pubbliche Amministrazioni - assume la caratteristica di immodificabilità se prodotto in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

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.

### **3.5. Il documento amministrativo informatico: definizione e disciplina giuridica**

L'art. 22 comma 1 lettera d) della Legge n. 241 del 7 agosto 1990 e s.m.i. 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”*.

Il successivo comma 2 dello stesso art. 22 legge 241/90 prevede che *“l'accesso ai documenti amministrativi, attese le sue rilevanti finalità di pubblico interesse, costituisce principio generale dell'attività amministrativa al fine di favorire la partecipazione e di assicurare l'imparzialità e la trasparenza”*.

Il documento amministrativo può assumere la forma di documento informatico.

L'AOO-Ateneo forma gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici ovvero acquisendo le istanze, le dichiarazioni e le comunicazioni previste dalla legge, CAD.

Gli atti formati dall'AOO-Ateneo con strumenti informatici, nonché i dati e i documenti informatici detenuti dalla stessa, 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 anche con la registrazione nel registro di protocollo unico dell'AOO, nei repertori e negli albi contenuti nel sistema di gestione documentale. E' compito del responsabile della gestione documentale verificare con la ditta fornitrice del software di gestione del protocollo informatico e con gli amministratori di sistema e/o di procedura le misure necessarie a rendere effettiva l'immodificabilità e l'integrità dei documenti contenuti nel sistema di gestione documentale adottato.

### **3.6. In particolare: la formazione del documento amministrativo analogico**

L'originale analogico è il documento nella sua redazione definitiva, perfetta ed autentica negli elementi essenziali 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 un soggetto terzi, sono di norma redatti in più originali in un numero di esemplari pari al numero dei destinatari e in una minuta da conservare agli atti nel fascicolo corrispondente.

Per "*originale*" si intende il documento analogico destinato all'invio, mentre si definisce "*minuta*" l'esemplare del documento corredato da sigle, firma e sottoscrizione autografe, conservato agli atti dell'Ateneo, cioè nel fascicolo relativo al procedimento amministrativo, affare o attività cui il documento si riferisce.

Il documento amministrativo analogico in partenza e interno è redatto su carta intestata e deve, di norma contenere la denominazione e il logo dell'Ateneo e l'indicazione di:

- AOO/UOR;
- data;
- classificazione;
- indicazione atte a individuare il fascicolo di competenza;
- numero di allegati (indicare 0 zero se non presenti);
- oggetto;
- destinatario;
- testo;
- sottoscrizione (firma del responsabile del provvedimento amministrativo o suo delegato o responsabile dell'affare o dell'attività);
- sigla di eventuali istruttori e dell'RPA;
- elementi identificativi del responsabile del procedimento (nominativo dell'RPA, UOR di appartenenza, telefono ed indirizzo istituzionale di posta elettronica della UOR/RPA).

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

### **3.7. Documenti redatti in originale su supporto analogico**

Ai sensi del DPCM 21 marzo 2013, per particolari tipologie di documenti analogici originali unici, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato.

Per documenti originali unici si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta (ad es., i verbali di una riunione o di un'assemblea). Pertanto, tutti i documenti su cui vengono apposti manualmente dati di registrazione a protocollo, sigle e firma autografa (che non sono sottoscritti con firma elettronica, semplice, avanzata o digitale), sono documenti amministrativi analogici.

### **3.8. In particolare: la formazione del documento informatico**

Il documento informatico - ai sensi delle Linee Guida AgiD, paragrafo 4, è formato mediante una delle seguenti modalità:

Il documento informatico è formato mediante una delle seguenti modalità:

- a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2, Linee Guida AgiD;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso modulo formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico deve essere identificato in modo univoco e persistente. Nel caso della Pubblica Amministrazione, l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento. L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di *hash* che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle Linee Guida AgiD, nella tabella 1 del paragrafo 2.2

regole di processamento.

Il documento informatico è immutabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immutabilità ed integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera b) l'immutabilità ed integrità sono garantite da una o più delle seguenti operazioni mediante:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo le sopracitate lettere c) e d) le caratteristiche di immutabilità e di integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata
- registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
- produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

La certezza dell'autore è la capacità di poter associare in maniera certa e permanente il soggetto che ha sottoscritto al documento stesso.

Al momento della formazione del documento informatico immutabile, devono essere

generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati del documento informatico è definito nell'allegato 5 "Metadati", Linee Guida AgiD. Potranno essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

### **3.9. Copie per immagine su supporto informatico di documenti analogici**

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, 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.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo", delle Linee Guida AgiD.

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'art. 22, commi 4 e 5 del CAD.

### **3.10. Duplicati, copie ed estratti informatici di documenti informatici**

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".doc" in un documento ".pdf". L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le

copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo", delle Linee Guida AgiD.

Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

Fatto salvo quanto previsto dall'art. 23bis comma 2 del CAD nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

### **3.11. Formazione del documento amministrativo informatico**

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

- AOO/UOR;
- Data di sottoscrizione;
- Classificazione;
- Indicazione atte a individuare il fascicolo di competenza;
- Numero di allegati (indicare 0 se non presenti);
- Oggetto;
- Destinatario;
- Testo;
- Iniziali di redattore/responsabile;
- Sottoscrizione (firma del responsabile del provvedimento amministrativo o suo delegato o responsabile dell'affare o dell'attività);

- Elementi identificativi del responsabile del procedimento (nominativo dell'RPA, UOR di appartenenza, telefono ed indirizzo istituzionale di posta elettronica della UOR/RPA).

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.

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico, salvo quanto specificato.

La Pubblica Amministrazione forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 -bis, 40 -bis e 65 del CAD.

Il documento amministrativo informatico è identificato e trattato nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD sono identificate e trattate come i documenti amministrativi informatici. Se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto sono memorizzate in specifici archivi informatici dettagliatamente descritti nel manuale di gestione documentale.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui al paragrafo 2.1.1 delle Linee Guida AgiD, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA, nonché i metadati relativi alla

classificazione, ai sensi dell'articolo 56 del TUDA, e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.

Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, secondo quanto previsto dall'Allegato 5 alle presenti Linee guida.

Sarà cura dell'Amministrazione individuare ulteriori metadati (ad es. metadati relativi al Registro giornaliero di protocollo ecc.) da associare a particolari tipologie di documenti amministrativi informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

Sono inclusi i documenti soggetti a registrazione particolare, come identificati nel manuale di gestione documentale, che comunque devono contenere al proprio interno o avere associati l'insieme minimo dei metadati previsti per il documento amministrativo informatico.

In applicazione dell'art.23-ter comma 5-bis del CAD, i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

### **3.12. Copie su supporto informatico di documenti amministrativi analogici**

L'attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dalla Pubblica Amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato.

### **3.13. Il documento amministrativo informatico costituito dal corpo della posta elettronica 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 Bergamo sono considerate sottoscritte con firma elettronica semplice e sono soggette a protocollazione solo se il contenuto è rilevante ai fini giuridico-probatori. In questo caso la e-mail istituzionale viene associata alla registrazione di protocollo quale documento in arrivo nel suo formato nativo (eml) oppure in formato pdf A/3 comprendente anche i relativi allegati. Trattandosi di un documento informatico nativo non si procederà alla stampa e apposizione tramite timbro della segnatura prima della registrazione e protocollo.

### **3.14. Metadati**

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

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

### **3.15. Obiettivi dei metadati archivistici**

Gli obiettivi dei metadati sono:

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

### **3.16. Metadati essenziali per la registrazione del protocollo informatico**

Gli elementi essenziali minimi sono i seguenti:

- Identificativo;
- Denominazione/codice unico che individua l'Ateneo;
- (mittente/destinatario);
- 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.

### **3.17. Validazione temporale**

Costituiscono validazione temporale:

- i riferimenti temporali realizzati dai certificatori accreditati mediante marche temporali;
- i riferimenti temporale 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;
- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica.

### **3.18. 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:

- Testo = Docx; Ods; Pdf/a;
- Calcolo = Xlsx; Odt;
- Immagini = Jpg; Tiff; DWG DXF;
- Suoni Mp3; WAV;
- Video = Avi; H.264/MPEG-4AVC (mime type: video/mp4);
- Eseguibili = Exe;
- XML;
- Archiviazione e compressione = Zip;
- Formati e-mail = RFC 2822/MIME.

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

## **CAPITOLO 4. IL FASCICOLO**

### **4.1. Il fascicolo: definizione e funzione**

Il fascicolo è l'unità di base dell'archivio corrente. Ogni fascicolo contiene documenti che ineriscono a uno stesso affare, attività o procedimento e sono classificati in maniera omogenea, in base al contenuto e secondo il grado divisionale attribuito dal titolare (o piano di classificazione), salvo alcune eccezioni, come il fascicolo di persona (e le rispettive tipologie, di personale, di studente etc.) e il fascicolo di fabbricato.

All'interno di ciascun fascicolo i documenti sono inseriti secondo l'ordine cronologico di registrazione e la loro sedimentazione avviene in modo tale che si individui subito il documento più recente.

L'ordine di sedimentazione è rispettato anche all'interno dei sottofascicoli se istruiti. L'obbligo di fascicolatura dei documenti riguarda sia i documenti contraddistinti dalla segnatura di protocollo sia i documenti procedurali non registrati.

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

Si possono distinguere cinque tipologie di fascicolo:

- **affare:** conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata. Per gli affari non esiste un termine per la conclusione previsto da norme;
- **Attività:** conserva i documenti relativi a una competenza proceduralizzata per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque prevista l'adozione di un provvedimento finale;
- **Procedimento amministrativo:** conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un atto finale;
- **Persona fisica:** conserva i documenti relativi a diversi procedimenti amministrativi distinti per affari o per attività, ma legati da un vincolo

archivistico interno, relativo ad una persona fisica determinata. La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'ente;

- Persona giuridica: conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica.
- Il fascicolo può essere ulteriormente suddiviso in sottofascicoli e inserti. Queste suddivisioni sono identificate grazie a un'ulteriore sequenza numerica progressiva (detta anche "catena numerica"), gerarchicamente posta al di sotto del numero di fascicolo o del sottofascicolo. Il sottofascicolo può essere chiuso prima del fascicolo, ma non viceversa, in quanto di norma trattasi di un subprocedimento o di un endoprocedimento stesso.

#### **4.2. Il fascicolo analogico: formazione, implementazione e gestione**

Per ogni procedimento, affare e attività, l'Ateneo ha l'obbligo di conservare in un fascicolo cartaceo gli atti, i documenti e i dati da chiunque formati su supporto analogico, cioè un documento nativo su supporto cartaceo deve essere conservato in originale su tale supporto all'interno dell'apposito fascicolo. Ovviamente un fascicolo analogico può contenere anche copie analogiche di documenti nativi digitalmente.

Ogni fascicolo deve essere contraddistinto dai seguenti elementi, atti a determinarne l'identificazione all'interno del sistema documentale:

- Anno di apertura (o istruzione);
- Numero di fascicolo, cioè un numero sequenziale all'interno dell'ultimo grado divisionale, da 1 a n con cadenza annuale;
- L'oggetto del fascicolo, cioè una stringa di testo per descrivere compiutamente un affare, una pratica, un dossier, una cartella, un procedimento amministrativo o più di questi insieme. Per convenzione, il titolo va scritto in numeri romani, mentre gli altri gradi, divisionali vanno scritti in cifre arabe (titolo I; classe3; sottoclasse 5; categoria 2; sottocategoria 6). L'anno va separato dal titolo da un trattino ( - ); il titolo va separato dagli altri gradi divisionali da una barretta ( / ); gli altri gradi divisionali, invece, vanno separati dal numero del fascicolo da un punto ( . ); l'oggetto del fascicolo va scritto tra virgolette caporali " " (esempio: 2016 – IX/1.6 "Costruzione della nuova sede degli uffici").

Il fascicolo raccoglie i documenti, creati e ricevuti, fino al termine della pratica. La chiusura della pratica comporta la chiusura del fascicolo. I fascicoli chiusi sono conservati presso l'Ufficio produttore per un limite minimo di un anno al fine di consentire l'eventuale reperimento dei documenti necessari allo svolgimento delle attività giornaliere. Non si forniscono limiti massimi di giacenza dei fascicoli chiusi presso l'archivio corrente poiché i tempi possono risultare diversi a seconda della natura della pratica e dell'attività d'ufficio. In ogni caso, i responsabili di UOR non devono mantenere i fascicoli di attività cessate non più consultati e che non hanno più alcuna utilità diretta presso gli uffici per evitare un eccessivo ingombro e una conseguente difficoltà nella gestione dei fascicoli aperti e attivi. Il trasferimento dei fascicoli chiusi dall'archivio corrente all'archivio di deposito avviene secondo le modalità descritte al paragrafo 11.2.

### 4.3. Il fascicolo informatico: formazione, implementazione e gestione

Ai sensi delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate entrate in vigore il 10 settembre 2020:” nelle pubbliche amministrazioni l’AOO gestisce i flussi documentali mediante fascicoli informatici predisposti secondo il piano di classificazione e relativo piano di organizzazione delle aggregazioni documentali ai sensi dell’art. 64 del TUDA, anche con riferimento a fascicoli non afferenti a procedimenti.”

Per ogni affare, attività e procedimento, l’Ateneo ha l’obbligo di conservare in un fascicolo informatico gli atti i documenti e i dati da chiunque formati su supporto informatico; cioè un documento nativo su supporto informatico deve essere conservato in originale su tale supporto all’interno dell’apposito fascicolo. Ovviamente un fascicolo informatico può contenere anche copie di qualunque tipo di documenti nativi cartacei.

Il fascicolo informatico reca le seguenti indicazioni:

- Amministrazione titolare del procedimento;
- Altre amministrazioni partecipanti;
- Nominativo del responsabile del procedimento;
- Oggetto del procedimento;
- Elenco dei documenti contenuti;
- Indice di classificazione (titolo, classe, etc.);
- Numero del fascicolo, identificativo di una catena numerica relativamente alla classe e al titolo di riferimento dell’anno di creazione;
- Data di apertura e di chiusura del fascicolo.

Il fascicolo informatico è creato dal responsabile del procedimento o da una persona incaricata all’interno del sistema di gestione documentale “Titulus” ed è visualizzabile con possibilità di intervento da parte degli utenti abilitati ad operare sui documenti della UOR responsabile.

Istruendo i fascicoli è necessario evitare la frammentazione delle pratiche, l’accorpamento eccessivo di documenti all’interno della stessa unità, la tendenza a costruire fascicoli intestati ai destinatari invece che basati sull’analisi di processi e funzioni. Se necessario, i fascicoli possono essere rinominati. Se il contenuto è costituito da documenti esclusivamente informatici questa attività è sufficiente; se è costituito da documenti informatici e documenti cartacei bisogna rinominare anche la camicia del fascicolo cartaceo.

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

Titulus è un software di gestione documentale. CINECA ha inteso, tramite l’acquisizione di Titulus, iniziare un percorso finalizzato a proporre agli Atenei Italiani un sistema di gestione documentale. Titulus nasce come software di gestione dell’archivio corrente, garantendo tutte le operazioni di condivisione e fascicolazione dei documenti, nel rispetto dei requisiti di legge per la gestione del protocollo informatico. Garantisce una gestione multi AOO, può quindi gestire un numero di registri di protocollo pari al bisogno dell’Ateneo (solitamente uno per ogni centro di costo: presidio, centro, etc.) al tempo stesso - attraverso la funzione interoperabilità

– dà la possibilità di scambiare automaticamente informazioni tra i registri di uno stesso Ateneo.

Titulus integra un modulo di workflow attraverso il quale si possono automatizzare i passaggi di un iter di approvazione, inoltre integra il modulo Titulus Organi per la gestione completa del processo di approvazione della delibera da parte degli Organi collegiali: dalla formulazione delle proposte passando per l'iter approvativo, la formulazione dell'Ordine del Giorno fino ad arrivare all'approvazione del verbale e dell'emanazione delle delibere.

#### **4.4. I fascicoli annuali ripetitivi**

E' possibile prevedere la possibilità di aprire automaticamente fascicoli annuali ripetitivi. L'indicazione della UOR e del RPA concorrono all'identificazione del fascicolo e alla individuazione del responsabile. La UOR e il RPA devono essere gli stessi di ciascun documento, del fascicolo e degli eventuali sottofascicoli. Ogni qualvolta cambia il RPA il fascicolo informatico deve essere immediatamente trasferito per competenza al nuovo responsabile del procedimento. I fascicoli informatici saranno trasferiti in conservazione, mediante pacchetto di versamento a cura del Responsabile della conservazione d'intesa con il Coordinatore/Responsabile della gestione documentale o dal suo vicario, dopo la loro chiusura e nelle modalità previste dal Manuale di conservazione.

#### **4.5. Il fascicolo ibrido**

Il fascicolo inteso come unità logica, può conservare documenti affissi su diverse tipologie di supporto. Tale problematica, particolarmente sentita negli odierni sistemi di gestione documentale, produce il cosiddetto fascicolo ibrido. Si tratta di un fascicolo composto da documenti formati su supporto cartaceo e su supporto informatico, e tale duplicità dà origine a due unità archivistiche fisiche di conservazione differenti.

L'unitarietà del fascicolo è comunque garantita dal sistema di classificazione mediante gli elementi identificativi del fascicolo (anno di istruzione, titolo/classe, numero del fascicolo, oggetto) e dal contenuto dei documenti. Il risultato è che un fascicolo di tale natura occuperà due luoghi distinti (un faldone e un file system) e questa caratteristica permane per tutta la vita del fascicolo, dal momento della sua istruzione al momento del trasferimento nell'archivio di deposito e, infine, per il versamento all'archivio storico. Tale peculiarità rende più complessa la gestione del fascicolo e dei documenti che vi afferiscono: entrambi vanno gestiti correttamente rispettando le caratteristiche proprie del supporto su cui il documento è stato prodotto e deve essere conservato.

Qualora si ravvisi l'utilità di avere tutti i documenti presenti in un determinato formato, si suggerisce di privilegiare il fascicolo informatico e creare le opportune copie per immagine dei documenti nativi analogici; è possibile inserire all'interno del fascicolo, qualora lo si ritenga necessario, anche documenti di carattere strumentale non soggetti a registrazione di protocollo, mediante la modalità denominata "non protocollato" prevista dal sistema di gestione informatica dei documenti Titulus. Questa pratica non esenta dalla conservazione dell'originale cartaceo nel fascicolo di pertinenza.

#### **4.6. Metadati del fascicolo informatico**

I metadati sono un insieme di dati associati a un fascicolo informatico per identificarlo e descrivere il contesto, il contenuto e la struttura, nonché per permettere la gestione nel tempo nel sistema di conservazione. I metadati minimi del fascicolo informatico e della aggregazione documentale informatica rispettando la codifica di caratteri ISO-8859-1.

I metadati minimi del fascicolo informatico sono:

- Identificativo univoco e persistente rappresentato da sequenza di caratteri alfanumerici associata in modo univoco e permanente al fascicolo in modo da consentirne l'identificazione;
- AOO;
- UOR responsabile del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- Responsabile del procedimento: cognome e nome;
- Eventuali amministrazioni partecipanti al procedimento;
- Oggetto: metadato funzionale a riassumere brevemente il contenuto del fascicolo comunque a chiarirne la natura;
- Elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità;
- Data di apertura del fascicolo;
- Data di chiusura del fascicolo.

#### **4.7. Il repertorio dei fascicoli informatici**

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

- Anno e numero progressivo del fascicolo;
- Classificazione nell'ambito del titolario adottato;
- Oggetto dell'affare/procedimento/attività;
- UOR responsabile dell'affare/procedimento/attività;
- Nominativo del responsabile dell'affare/procedimento/attività;
- Date di apertura e chiusura del fascicolo;
- Numero dei documenti contenuti nel fascicolo;
- Dati relativi alla movimentazione del fascicolo;
- Stato: chiuso/aperto.

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

#### **4.8. Raccoglitore**

Il raccoglitore non è un fascicolo, ma un contenitore che raggruppa documenti relativi a uno stesso argomento e afferenti a procedimenti diversi e quindi a fascicoli diversi, privi di una classificazione e una numerazione propria.

In buona sostanza, si tratta di un *dossier* a uso e consumo del responsabile del procedimento amministrativo per propria memoria e autodocumentazione, di norma, non destinato alla conservazione.

## **CAPITOLO 5. – LA GESTIONE DELL’ARCHIVIO CORRENTE**

### **5.1. Definizione**

Per archivio corrente si intende il complesso dei documenti relativi ad affari, ad attività e a procedimenti amministrativi in corso di istruttoria e di trattazione o, comunque, verso i quali sussista un interesse non ancora esaurito. L’organizzazione dell’archivio deve rispondere a criteri di efficienza ed efficacia al fine di garantire la certezza dell’attività giuridico amministrativa dell’Ente e la conservazione stabile della memoria nel tempo. L’archivio corrente è, quindi il primo elemento gestionale per il corretto funzionamento del sistema documentale. Il responsabile del procedimento amministrativo è tenuto alla corretta gestione, conservazione e custodia dei documenti e dei fascicoli, siano essi di natura analogica, digitale o ibrida, relativi ai procedimenti di propria competenza; a esso è quindi affidata l’attuazione delle disposizioni contenute in questo manuale in merito al corretto funzionamento dell’archivio corrente di propria pertinenza. La UOR che crea il fascicolo mantiene la responsabilità amministrativa dei documenti creati durante la fase corrente e la fase di deposito; quindi per la fase corrente e di deposito viene garantito il proprio accesso, da parte delle sole UOR che hanno la titolarità dei documenti, attraverso il sistema di gestione documentale. Durante la fase di deposito all’Archivio Generale di Ateneo passa la gestione dei fascicoli, ma non la responsabilità. Nel caso di documenti cartacei, per la movimentazione dei fascicoli, viene effettuata una richiesta di accesso da parte delle UOR.

### **5.2. Buona prassi per la gestione dell’archivio corrente**

Il responsabile del procedimento amministrativo, come si è detto sopra, è incaricato della corretta gestione dell'archivio corrente di sua pertinenza e ciò comporta in primo luogo la corretta creazione dei fascicoli e inserimento dei relativi documenti; in secondo luogo il responsabile del procedimento è tenuto alla corretta gestione dei fascicoli stessi e tale incombenza varia a seconda del supporto con cui vengono creati. I fascicoli analogici devono essere creati secondo le indicazioni fornite nel paragrafo 4.2. e successivamente conservati all'interno di appositi faldoni o cartelle nell'archivio corrente situato presso gli uffici di ciascuna UOR. Il faldone, per consentire l'agevole e immediato reperimento dei fascicoli deve riportare sul dorso le seguenti informazioni:

- L'ufficio produttore;
- L'oggetto;
- Gli estremi cronologici;
- Gli estremi identificativi dei fascicoli contenuti (indice di classificazione e numero progressivo di repertorio).

Laddove una pratica avesse dimensioni tali da occupare singolarmente più di un faldone, questi andranno contrassegnati con le medesime indicazioni esterne e con una numerazione progressiva, a partire da uno, così da risultare immediata la comprensione del legame tra le unità di conservazione. I fascicoli restano collocati presso ogni singola struttura (AOO/UOR) per la propria responsabilità e competenza nel trattamento dell'affare fino al momento del loro trasferimento nell'archivio di deposito. Il trasferimento è effettuato a cura del Responsabile della gestione documentale secondo le modalità illustrate nel presente manuale al paragrafo 11.2. I documenti creati nel corso dell'attività d'ufficio sono soggetti a fascicolazione obbligatoria ai sensi del DPR 445/2000, art.64, comma 4, indipendentemente da supporto su cui sono creati. Inserire i documenti nell'apposito fascicolo permette la costituzione di un archivio organizzato essendo essi le unità logiche del sistema di gestione documentale e, di conseguenza, consente il facile e veloce reperimento dei documenti di un determinato procedimento permettendo il rispetto del principio di trasparenza e dell'istituto del diritto di accesso. La fascicolazione deve essere effettuata in maniera continuativa e sistematizzata da parte di tutte le unità organizzative responsabili costituenti l'amministrazione. Un'attività secondaria, ma molto utile da un punto di vista di gestione corrente delle unità di archivio, è lo sfoltimento dei fascicoli. Lo sfoltimento è l'operazione preliminare e propedeutica a una corretta conservazione documentale: al momento della chiusura del fascicolo, oppure prima del trasferimento dello stesso all'archivio di deposito, il carteggio di carattere transitorio e strumentale deve essere selezionato ed estratto dal fascicolo da parte dell'operatore incaricato del trattamento della pratica. Si tratta, cioè, di estrarre dal fascicolo le copie e i documenti che hanno appunto carattere strumentale e transitorio, utilizzati dall'operatore incaricato o dal responsabile del procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad esempio appunti, promemoria, copie di normativa e documenti di carattere generale). Questa operazione riguarda principalmente i fascicoli cartacei.

### **5.3. Gli strumenti dell'archivio corrente**

Il trattamento dell'intero sistema documentale dell'Ateneo comporta la predisposizione di strumenti di gestione dell'archivio corrente che permettano una efficiente organizzazione e consultazione della documentazione, a prescindere dai supporti dei documenti.

### **5.3.1. Registro di protocollo**

Il registro di protocollo è lo strumento finalizzato all'identificazione univoca e certa dei documenti ricevuti e spediti mediante la registrazione di determinati elementi che caratterizzano ogni singolo documento. Il registro di protocollo svolge quindi una fondamentale funzione giuridico probatoria attestando l'esistenza di un determinato documento all'interno del sistema di gestione documentale e garantendone l'autenticità. Il registro di protocollo è un atto pubblico di fede privilegiata.

### **5.3.2. Titolario (piano di classificazione)**

Il titolare è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (titolo/classe/eventuale sottoclasse) stabilite sulla base delle funzioni dell'ente. Ciascun documento, registrato in modalità arrivo, partenza, interno, anche non protocollato, è classificato in ordine alla corrispondenza tra il suo contenuto e la relativa voce attribuibile, desunta dal titolare e successivamente fascicolato. La classificazione, necessaria e fondamentale, è prodromica all'inserzione di un documento all'interno di un determinato fascicolo. La relazione tra i documenti (vincolo archivistico) di un'unità archivistica è garantita dalla segnatura archivistica completa (anno di istruzione, classificazione, numero del fascicolo). Il titolare può essere corredato da un'appendice denominata voci di indice. Si tratta di un ulteriore strumento, correlato al titolare, che agevola le operazioni di classificazione. In esso sono presenti le possibili varianti lessicali, trattate e riportate in modo analitico, che possono essere incontrate nel contenuto del documento. Il titolare e, di conseguenza, il prontuario delle voci di indice sono inseriti nel sistema di gestione documentale. Possono essere soggetti a revisione periodica, qualora ciò si renda necessario a seguito di modifiche di carattere normativo e/o statutario in questo caso, essi sono adottati a partire dal primo gennaio dell'anno successivo a quello di approvazione. Il sistema di gestione documentale garantisce che le voci del titolare siano storicizzate, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolare vigente al momento della loro registrazione. Il titolare è sottoposto, altresì, all'approvazione della Direzione Generale Archivi del Ministero per i Beni Culturali e del Turismo e comunicato alla Soprintendenza Archivistica per la Regione Lombardia. Il titolare unico valido per l'AOO dell'Università degli Studi di Bergamo, è predisposto all'interno del progetto Procedamus e approvato (con nota prot. n. 218707 in data 14.12.2012) della Direzione Generale degli Archivi, Servizio II, Tutela e conservazione del patrimonio, è descritto nell'allegato n.4.

### **5.3.3. Repertorio dei fascicoli**

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

### **5.3.4. Repertori**

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

### **5.3.5. Massimario di selezione**

Il massimario di selezione è uno strumento da utilizzare durante la fase di deposito dell'archivio, come previsto dall'art. 68 del DPR 445/2000. Il massimario di selezione è lo strumento con cui l'ente individua le disposizioni di massima e definisce i criteri e le procedure attraverso cui i documenti non rivestendo interesse storico ai fini della conservazione permanente e avendo esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della Soprintendenza Archivistica, i sensi del D.lgs. 22 gennaio 2004, n. 42, art. 21. Il massimario individua le tipologie documentali in rapporto ai procedimenti che le costituiscono e, a partire da tali tipologie, si applicano i criteri e le disposizioni atti ad individuare i termini di conservazione: distinzione oggetto ed atto esercitato sull'oggetto; inoltre, è uno strumento indirizzato sia alla conservazione che all'eliminazione, detto in altri termini il massimario consente la selezione che ha come conseguenze o la conservazione o la distruzione. Del massimario è parte integrante il prontuario di scarto, nel quale sono menzionati i tempi di conservazione in relazione alle tipologie documentarie. Le operazioni di selezione, necessarie a garantire la corretta gestione e la conservazione del complesso documentale dell'ente, avvengono nella fase di deposito, in modo tale da sedimentare solo la documentazione ritenuta rilevante ai fini della conservazione a lungo termine. La proposta di scarto formulata su apposito modulo cioè

*“l’elenco di scarto”* in cui sono indicate le tipologie documentarie, gli estremi cronologici, il volume (espresso in metri lineari o in chilogrammi, solo per i documenti analogici) e le motivazioni dell’eliminazione, corredata da disposizione dirigenziale, inviata alla Soprintendenza Archivistica della Lombardia nelle modalità concordate. L’attività è soggetta ad autorizzazione della Soprintendenza Archivistica ai sensi del D.lgs. 42/2004 art.21. A seguito dell’autorizzazione, l’Ateneo avvia il procedimento per individuare il soggetto legittimato al ritiro del materiale e alla eliminazione fisica dei documenti, la ditta affidataria individuata effettua le operazioni di ritiro e macero della documentazione con rilascio di relativo verbale di esecuzione.

Per i fascicoli informatici la proposta di scarto segue lo stesso iter per quanto riguarda l’autorizzazione della Soprintendenza e il Responsabile della gestione documentale invierà un documento informatico trasmesso digitalmente. Il fascicolo inerente al procedimento di scarto è a conservazione illimitata

#### **5.4. Spostamento di un archivio corrente analogico**

Qualora una UOR dovesse spostare la documentazione corrente, a seguito di mutamento della sede operativa o per altra ragione, dovrà darne informazione tempestiva al Responsabile della gestione documentale, producendo un apposito elenco dei fascicoli soggetto di spostamento. Inoltre, l’Archivio Generale di Ateneo provvederà a effettuare un sopralluogo per verificare l’idoneità degli spazi e la correttezza della collocazione del nuovo archivio, rimanendo in ogni caso a disposizione per eventuali chiarimenti o consigli sulle modalità di spostamento della documentazione. Lo spostamento dell’archivio corrente non necessita di alcuna autorizzazione preventiva da parte della Soprintendenza archivistica pertinente.

## **CAPITOLO 6. IL PROTOCOLLO INFORMATICO**

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

Il registro di protocollo ha cadenza annuale: inizia il 1° gennaio e termina il 31 dicembre di ogni anno ed è unico per l'AOO dell'Università degli Studi di Bergamo.

### **6.1. Registratura**

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

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'Ateneo, ossia i cui destinatari sono esterni all'ente e tutti i documenti informatici, ad eccezione di quelli espressamente esclusi dalla normativa vigente (DPR 445/2000, art.53, comma 5) e altri documenti informatici già soggetti a registrazione particolare.

Per registrazione di protocollo si intende l'apposizione o l'associazione del documento o l'associazione al documento in forma permanente, 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 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 registratura degli elementi obbligatori immodificabili del protocollo informatico non può essere modificata, integrata, cancellata ma soltanto annullata mediante un'apposita procedura in capo al Responsabile della gestione documentale o a persone espressamente delegate.

L'inalterabilità e l'immodificabilità della registrazione di protocollo devono essere garantite dal sistema di gestione documentale.

### **6.1.1. Elementi obbligatori immodificabili (Registratura)**

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

Essi sono:

- Numero di protocollo progressivo e costituito da 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 denominata registratura.

### **6.1.2. Elementi obbligatori modificabili**

Gli elementi obbligatori modificabili sono:

- Unità organizzativa responsabile del procedimento/affare/attività (UOR);
- Responsabile del procedimento amministrativo (RPA);
- Classificazione archivistica;

- Fascicolo.

### **6.1.3. Elementi non obbligatori modificabili**

Gli elementi non obbligatori modificabili sono:

- Recapiti del mittente;
- Collegamento di altri documenti o a fascicoli diversi da quello d'inserimento;
- Tipologia di documento;
- Durata della conservazione;
- Altri tipi di annotazioni (ad es., si può annotare l'arrivo in data successiva di un secondo esemplare dello stesso documento precedentemente ricevuto e protocollato, previa verifica della sua conformità al primo).

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

Il 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.

## **6.3. Segnatura**

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

### **6.3.1 Per il documento informatico**

Le informazioni minime da associare al documento informatico sono:

- Codice identificativo dell'amministrazione;
- Codice identificativo 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 titolare di classificazione adottato e vigente al momento della registrazione del documento;
- Codice identificativo dell'ufficio a cui il documento è assegnato;

- Ogni altra informazione utile o necessaria, già disponibile al momento della registrazione.

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

La firma digitale, infatti, produce un file, definito “busta crittografica” che racchiude al suo interno il documento originale, l’evidenza informatica, della firma e la chiave per la verifica della stessa, che, a sua volta, è contenuta nel certificato emesso a nome del sottoscrittore.

Nel caso in cui si debba riportare sul documento annotazioni successive alla sottoscrizione (quali i dati della segnatura di protocollo), il documento dovrà essere predisposto per contenere dei campi testo ove sia possibile inserire delle informazioni successivamente alla firma senza invalidare la stessa in coerenza con quanto previsto dalle regole tecniche di cui al DPCM del 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”.

### **6.3.2. 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 di forma sintetica o estesa dell’amministrazione e dell’AOO individuata ai fini della registrazione e della gestione del documento;
- Il numero progressivo di protocollo;
- Il numero di protocollo nel formato GGMMAAAA;
- La classificazione in base al titolare di classificazione adottato e vigente al momento della registrazione del documento;
- La sigla dell’UOR/RPA e delle UOR/RPA a cui il documento è assegnato per competenza e responsabilità;
- Le eventuali sigle della UOR/RPA o delle UOR/RPA in copia conoscenza.

Gli elementi della segnatura devono essere presenti sia nei documenti prodotti da registrare in partenza, sia nei documenti scambiati tra le UOR della medesima AOO (protocollo tra uffici).

### **6.4. Modalità di produzione e di conservazione delle registrazioni**

Ogni registrazione di protocollo produce un record nel sistema di gestione documentale che viene accodato in una base dati accessibile esclusivamente all’amministratore del sistema. Ogni operazione di inserimento e modifica viene

registrata inoltre su un file di log corredato da codici di controllo in grado di evidenziare eventuali tentativi di manipolazione. Da esso l'amministratore del sistema è in grado di ottenere l'elenco delle modifiche effettuate su una data registrazione, permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione (smistamento, invio per conoscenza, restituzione, fascicolatura ecc.), ottenendo in dettaglio:

- Nome dell'utente;
- Data e ora;
- Postazione di lavoro;
- Tipo di operazione (inserimento/visualizzazione/cancellazione);
- Valore dei campi soggetti a modifica.

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

#### **6.5. La registrazione differita (o “protocollo differito”)**

E' possibile effettuare la registrazione differita di protocollo nel caso di temporaneo, eccezionale e imprevisto carico di lavoro e qualora dalla mancata registrazione di un documento nell'ambito del sistema nel medesimo giorno lavorativo di ricezione, possa venire meno un diritto di terzi.

La registrazione differita di protocollo informatico è possibile esclusivamente per i documenti in arrivo.

Per “protocollo differito” si intende la registrazione di documenti in arrivo autorizzata con provvedimento motivato del Responsabile della gestione documentale o da persona espressamente delegata, in cui sono indicati nello specifico la data alla quale si differisce la registrazione del documento stesso e la causa che ne ha determinato il differimento.

Per i documenti ricevuti dall'Ufficio Protocollo il differimento opera su iniziativa del Responsabile della gestione documentale, o da suo delegato, che ne cura la registrazione differita corredata della motivazione.

Per i documenti ricevuti direttamente dalla UOR competente la registrazione differita avviene su richiesta motivata della stessa UOR al Responsabile della gestione documentale o suo delegato, in cui è indicata anche la data di effettivo ricevimento.

La registrazione differita non si applica per i documenti informatici pervenuti via PEC, in quanto la PEC ha lo stesso valore giuridico della raccomandata AR e quindi fa fede la data di invio della PEC allo stesso modo del timbro postale di invio della raccomandata AR.

#### **6.6. la ricevuta di avvenuta registrazione**

La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo deve riportare i seguenti dati:

- Il numero e la data di protocollo;
- L'indicazione dell'AOO che ha acquisito il documento;
- Il mittente;
- L'oggetto;
- Numero e descrizione degli allegati se presenti;
- L'operatore di protocollo che ha effettuato la registrazione.

#### **6.6.1. Per il documento analogico**

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è cura di chi effettua la protocollazione rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal sistema di gestione documentale.

La ricevuta può essere altresì ritirata dall'interessato o da persona espressamente delegata nei giorni successivi.

#### **6.6.2. Per il documento informatico**

Qualora il documento informatico sia pervenuto tramite PEC, la ricevuta di protocollazione è rilasciata direttamente dal sistema di gestione documentale.

Se il documento è pervenuto tramite e-mail, la ricevuta, se richiesta, sarà generata in formato pdf o pdf/a e inviata via e-mail al mittente.

L'Ufficio Protocollo non è autorizzato a rilasciare a terzi copie dei documenti protocollati in entrata.

#### **6.7. Documenti esclusi dalla registrazione di protocollo**

Sono esclusi per legge dalla registrazione di protocollo:

- Le gazzette ufficiali;
- I bollettini ufficiali P.A.;
- I notiziari P.A.;
- Le note di ricezione delle circolari;

- Le note di ricezione di altre disposizioni;
- I materiali statistici;
- Gli atti preparatori interni;
- I giornali;
- Interviste;
- I libri;
- I materiali pubblicitari;
- Gli inviti a manifestazioni.

Sono parimenti esclusi dalla registrazione di protocollo:

- I certificati medici dei dipendenti. Se pervenuti via PEC essi sono registrati ma non protocollati.

## 6.8. Il registro giornaliero di protocollo

Il registro giornaliero di protocollo è prodotto in maniera automatica dal software di gestione documentale entro il giorno lavorativo seguente, mediante la generazione o il raggruppamento delle informazioni registrate secondo una struttura logica predeterminata e memorizzato in forma statica, immutabile e integra.

Attualmente, in base allo stato dell'arte delle tecnologie e dei formati, è utilizzato il formato XML ai sensi della normativa vigente.

Gli elementi memorizzati del registro giornaliero sono i seguenti:

- Identificativo univoco e persistente, espresso in Codice IPA, AOO, anno, mese e giorno (8 cifre);
- Data di chiusura (data di creazione del registro);
- Impronta del documento informatico;
- Responsabile della gestione documentale (Nome, Cognome);
- Oggetto (descrizione della tipologia di registro, ad es., "Registro giornaliero di protocollo");
- Codice identificativo del registro;
- Numero progressivo del registro;
- Numero della prima registrazione effettuata sul registro;
- Numero dell'ultima registrazione effettuata sul registro;

Il registro giornaliero è trasmesso al Sistema di conservazione entro la giornata lavorativa successiva alla produzione.

## 6.9. Il registro di emergenza

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

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

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le 24 ore, per cause di eccezionale gravità, il Responsabile della gestione documentale autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

Sul registro di emergenza devono essere riportati gli estremi del provvedimento di autorizzazione. La sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea.

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

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

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

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.

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

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

Al termine dell'emergenza, il Responsabile della gestione documentale, chiude il registro e dà contestuale comunicazione della revoca dell'emergenza.

Il registro di emergenza è conservato con le stesse modalità del registro ufficiale come descritto al paragrafo 6.4.

## **CAPITOLO 7. REGISTRI E REPERTORI INFORMATICI**

### **7.1. Repertorio – Nozione**

Le regole tecniche attuative del CAD definiscono repertorio informatico *“un registro 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”* nel sistema di gestione documentale.

Ai sensi del presente manuale si intende per repertorio il registro in cui sono annotati, con numerazione progressiva, i documenti, prevalentemente interni, per i quali è prevista una registrazione particolare. Trattasi di documenti uguali per forma ma diversi per contenuto e che assumono la connotazione di “serie archivistiche”.

Sono un esempio la registrazione di circolari, decreti/determine di organi monocratici, verbali/deliberazioni di organi collegiali, contratti e convenzioni, etc..

Il complesso dei documenti registrati a repertorio per forma omogenea costituisce una serie (es serie dei decreti, dei contratti, delle deliberazioni, ecc).

I documenti sono comunque inseriti nel fascicolo archivistico di loro pertinenza per la loro minuta e in originale (o in copia conforme) nel repertorio.

La numerazione di repertorio si rinnova ogni anno solare: inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Ogni repertorio è collegato al registro di protocollo dell’AOO-Ateneo. I documenti annotati nel repertorio e trasferiti contestualmente nel protocollo generale recano, quindi, due numeri: quello progressivo annuale del repertorio corrispondente e quello del registro unico di protocollo.

### **7.2. Repertori attivi**

L’elenco dei repertori attivi presso l’AOO dell’Università degli studi di Bergamo all’atto dell’emanazione del presente Manuale è descritto nell’allegato 3 ,

### **7.3. Repertorio dei fascicoli**

E' il registro in cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno dei gradi divisionali del titolare.

## **CAPITOLO 8. FLUSSO DI LAVORAZIONE DEI DOCUMENTI**

### **8.1. Flusso del documento informatico in arrivo**

L'Ufficio protocollo registra in modo avalutativo i documenti che rivestono un valore giuridico-probatorio.

La documentazione da protocollare viene registrata, classificata e smistata alla UOR competente. Il Responsabile della UOR, a sua volta, assegna al documento (e di conseguenza al procedimento amministrativo cui si riferisce) il RPA. L'informativa alla registrazione è resa immediatamente disponibile in due modalità:

- Attraverso un messaggio *e-mail* che il sistema di gestione documentale invia automaticamente alla casella di posta elettronica indicata dal responsabile della UOR;
- Attraverso l'accumulo nella vaschetta del menù principale del sistema di gestione documentale.

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

- Tramite posta elettronica convenzionale (e-mail);
- Tramite posta elettronica certificata (PEC);
- Su supporto rimovibile (Cd, ROM, DVD, ecc.) con consegna diretta o trasmesso a mezzo servizio postale o corriere;
- O altre banche dati.

### **8.2. Ricezione di documenti informatici nella casella di posta elettronica istituzionale**

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

Si possono avere i seguenti casi:

- Documento che arriva alla casella di posta elettronica istituzionale dell'Ufficio Protocollo;
- Documento allegato alla e-mail istituzionale con PDF creator<sup>13</sup> si crea il PDF/a e lo si associa al sistema di gestione documentale procedendo alla registrazione in arrivo con le consuete modalità. Sarà cura del RPA dell'UOR competente verificarne la provenienza e valutare se accettare o meno la firma elettronica leggera;
- Documento costituito dal corpo della mail: con PDF creator si crea il PDF/A e lo si associa al sistema di gestione documentale procedendo alla registrazione in arrivo con le consuete modalità. Sarà cura del RPA della UOR competente verificarne la provenienza e valutare se accettare o meno la firma elettronica leggera. I documenti informatici così pervenuti saranno protocollati a cura dell'Ufficio Protocollo, di norma entro le 24 ore lavorative dal giorno di arrivo;
- Documento che arriva alla casella di posta elettronica istituzionale di una UOR diversa dall'Ufficio Protocollo. La UOR ricevente gira l'*e-mail* con *forward* corredata degli eventuali allegati alla casella di posta elettronica istituzionale dell'Ufficio Protocollo che converte il file in pdf/a registra nel protocollo informatico e associa il file con estensione pdf/a alla registrazione;
- Il mittente è l'autore della *e-mail* e non la UOR che ha inoltrato il file all'Ufficio Protocollo. Nel caso di e-mail da cui non sia possibile desumere l'indicazione di nome e cognome il documento sarà trattato come Anonimo (cfr. paragrafo 9.15).

E' in capo al RPA verificare la provenienza del documento pervenuto via *e-mail* ed eventualmente chiedere al mittente un documento informatico firmato digitalmente e inviato via PEC. In questo caso sarà un nuovo protocollo e non un secondo esemplare, in quanto quest'ultimo è sottoscritto. I documenti informatici così pervenuti saranno protocollati a cura dell'Ufficio Protocollo entro le 24 ore dal giorno di arrivo. Analogamente se un dipendente riceve nella propria casella di posta fornita dall'Amministrazione documenti concernenti affari o procedimenti amministrativi dell'Amministrazione è tenuto a inoltrare tempestivamente il messaggio e-mail alla casella istituzionale dell'Ufficio protocollo.

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

La PEC è un vettore attraverso il quale è spedito/ricevuto un documento informatico che può essere allegato o incorporato nel corpo stesso.

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

La prima operazione consiste nell'identificazione del mittente che non sempre coincide con il proprietario della PEC. Se il documento informatico è privo di firma va evidenziato in un campo imm modificabile con la dicitura *firma mancante*.

La verifica della validità della firma digitale è a cura del RPA del documento.

Qualora il documento ricevuto non sia pdf o pdf/a (con o senza firma digitale) e venga comunque registrato al protocollo, spetta al responsabile del procedimento valutare se

accettare il documento informatico assegnato non sottoscritto o non conforme agli standard o richiedere il documento al mittente.

Una registrazione di documenti sia in arrivo che in partenza via PEC, non permette di modificare i file informatici associati ad essa. Il sistema di gestione documentale genera tutte le ricevute previste dalla normativa in materia di posta elettronica certificata.

#### **8.4. Ricezione di documenti informatici su supporti rimovibili**

I documenti digitali possono pervenire anche in modalità diverse dalla posta elettronica o dalla posta elettronica certificata e quindi su supporti diversi.

L'Ufficio Protocollo verifica la leggibilità dei dati contenuti nel supporto informatico e provvede alla registrazione solo in caso di esito positivo. E' cura della UOR responsabile verificarne le caratteristiche e la provenienza certa.

I documenti informatici così pervenuti sono protocollati, di norma, entro le 2 ore lavorative successive al giorno in arrivo.

##### **8.4.1. Documenti informatici prodotti da banche dati dell'Ateneo o prodotti da banche dati di terzi**

I documenti inseriti e convalidati da banche dati dell'ateneo o prodotti da banche dati di terzi che arrivano nel sistema di gestione documentale possono essere trattati in due modi:

- Essere gestiti in automatico dal sistema che li protocolla, attribuisce loro la classificazione, li inserisce nel fascicolo di pertinenza, li assegna alla UOR e al RPA di competenza;
- Essere gestiti come bozze.

Ad esempio, ordini e fatture attive in formato Fattura PA destinati a pubbliche amministrazioni generati sul sistema di contabilità *U-GOV* e trasferiti automaticamente al sistema di gestione documentale sono gestiti come bozze. I documenti relativi al fascicolo studente, i verbali d'esame e i verbali di laurea sono gestiti automaticamente dal sistema gestione carriere studenti – ESSE 3 a *Titulus*.

Prima di attivare una procedura automatica, il Responsabile della gestione documentale, in collaborazione con il RPA e con il Responsabile dei sistemi informativi, dovrà stabilire le modalità del flusso e le condizioni per la protocollazione automatica che devono comprendere la valutazione della possibilità o meno di trattare adeguatamente dati sensibili.

Per motivi organizzativi, le UOR sono tenute ad informare preventivamente l'Ufficio Protocollo di scadenze massive (gare, bandi, valutazioni comparative, immatricolazioni alle scuole di specializzazione, dottorati di ricerca, etc.) scrivendo, di norma, almeno una settimana prima di tali scadenze, una mail alla sua casella istituzionale.

### **8.5. Priorità alla registrazione dei documenti informatici in arrivo**

Indipendentemente dal mezzo telematico di arrivo, è data priorità nella registrazione a protocollo:

- Atti giudiziari notificati;
- Documenti del Ministero;
- Documenti di rilevanza finanziario-contabile (MEF-Corte dei Conti, etc.);
- Documenti ricevuti direttamente dalla segreteria del Rettore;
- Documenti ricevuti direttamente dalla Segreteria del Direttore Generale;
- Documenti ricevuti direttamente dall'ufficio Legale;
- Fatture passive pervenute con PEC al di fuori del sistema di interscambio (es. le fatture in formato elettronico provenienti da fornitori esteri).

E' data inoltre priorità ai documenti pervenuti con PEC in considerazione del fatto che il sistema rilascia automaticamente al mittente la ricevuta di avvenuta consegna del documento.

Tale casistica è soltanto indicativa ed è suscettibile di variazione in concomitanza con altre priorità che si dovessero presentare (scadenze bandi di concorso, gare, etc.).

### **8.6. Flusso del documento analogico**

La corrispondenza analogica in arrivo perviene all'Ufficio Protocollo secondo le seguenti modalità:

- Posta pervenuta per il tramite di Poste italiane spa e di altri gestori autorizzati;
- Posta pervenuta direttamente alle UOR e da queste recapitate all'Ufficio Protocollo;
- Posta recapitata personalmente, *brevi manu*.

### **8.7. Apertura delle buste**

Tutte le buste vanno aperte a cura dell'Ufficio Protocollo, fanno eccezione e pertanto non vanno aperte le buste:

- Riportanti le seguenti diciture, riservato, personale, confidenziale, spm/sgm (sue proprie mani/sue gentilissime mani), etc. o dalla cui confezione si evinca il carattere di corrispondenza privata (ad es. busta particolare);
- Riportanti le seguenti diciture “offerta”, “gara d’appalto” “non aprire” o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara (ad es., il CIG).
- Le altre buste indirizzate nominativamente al personale nella convinzione che nessun dipendente utilizzi l’Amministrazione come fermoposta o casella postale privata. Chiunque riceva tramite corrispondenza privata, documenti concernenti affari o procedimenti amministrativi dell’Amministrazione è tenuto a farli pervenire tempestivamente all’Ufficio Protocollo.

### 8.7.1. Conservazione ed eliminazione delle buste

Le buste pervenute tramite posta raccomandata, corriere o altra modalità per la quale si renda rilevante evidenziare il mezzo di trasmissione e il timbro postale (ad es., una fattura passiva proveniente da un fornitore estero arrivata in prossimità del termine di scadenza per il pagamento), sono spillate assieme al documento e trasmesse alla UOR.

Le altre buste sono conservate a parte in plichi quotidiani per trenta giorni. Trascorso tale termine sono eliminate senza formalità.

### 8.8. Priorità nella registrazione dei documenti analogici in arrivo

Indipendentemente dal mezzo di trasmissione è data priorità nella registrazione a protocollo a:

- Atti giudiziari notificati;
- Documenti del Ministero;
- Documenti di rilevanza finanziario-contabile (MEF-Corte dei Conti, etc.);
- Documenti ricevuti direttamente dalla segreteria del Rettore;
- Documenti ricevuti direttamente dalla segreteria del Direttore Generale;
- Documenti ricevuti direttamente dall’Ufficio Legale;
- Fatture passive pervenute al di fuori del Sistema di interscambio (es. le fatture di fornitori esteri);
- Documenti relativi a procedimenti ispettivi;
- Documenti di trasmissione di assegni o altri valori di debito/credito;
- Documenti consegnati *brevi manu*: si protocolla subito e si rilascia la ricevuta di avvenuta protocollazione.

Tale casistica è soltanto indicativa ed è suscettibile di variazione in concomitanza con altre priorità che si dovessero presentare (scadenze, bandi di concorso, gare etc.)

Di norma si procede all'apertura e alla registrazione di protocollo nella stessa giornata di consegna e comunque di norma, entro le 24 ore lavorative successive alla ricezione.

Nel caso in cui non sia possibile l'immediata protocollazione di un documento consegnato a mano (ad es., per momentanea indisponibilità del sistema informatico) viene concordato l'invio telematico della ricevuta di protocollo all'indirizzo mail fornito da chi consegna il documento. In casi eccezionali, si rilascia la fotocopia nel frontespizio del documento col timbro di protocollo.

## **8.9. Protocollo particolare/riservato**

Sono previste particolari forme di riservatezza e di accesso controllato al protocollo unico per:

- Documenti di indirizzo di competenza del Rettore o del Direttore Generale che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- Tipologie di documenti individuati dalla normativa vigente relativamente a dati sensibili i c. *sensibilissimi*;
- Documenti legati a vicende di persone o a fatti privati e, in particolare, i documenti riportanti dati sensibili e dati giudiziari.

### **8.9.1. Procedure del protocollo particolare/riservato**

Le tipologie di documenti da registrare nel protocollo particolare sono individuate dal Responsabile della gestione documentale, in collaborazione con gli Organi monocratici e d'intesa con i Responsabili delle UOR.

Ogni documento reca un numero di protocollo.

Per i documenti in arrivo analogici particolarmente voluminosi, viene fotoriprodotta la lettera accompagnatoria con l'apposizione della dicitura "I documenti integrati sono consultabili presso l'Ufficio Protocollo.

## **8.10. L'Archivio particolare/riservato**

Il complesso dei documenti registrati col protocollo particolare costituisce l'archivio particolare.

A protezione dei dati personali e sensibili, il documento analogico viene trasmesso direttamente al RPA in busta chiusa, sigillata e firmata sui lembi di chiusura. Al Rettore, al Direttore Generale e agli altri eventuali destinatari in copia conoscenza viene inoltrata una copia del documento analogico sempre in busta chiusa, sigillata e firmata sui lembi di chiusura.

Per il documento informatico soggetto a registrazione di protocollo particolare/riservato saranno gli organi monocratici a definirne l'utilizzo in collaborazione con il Responsabile della gestione documentale.

## **8.11. Annullamento di una registrazione**

Ai sensi delle Linee Guida AgiD, capitolo 3 paragrafo 1.5:

Il protocollo informatico deve assicurare il tracciamento e la storicizzazione di ogni operazione, comprese le operazioni di annullamento, e la loro attribuzione all'operatore. Il sistema di protocollo informatico assicura che:

- le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista dall'art. 54 del TUDA;
- le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
- le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
- per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema storicizzi tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili, nel rispetto di quanto previsto dall'art. 54, comma 2 del TUDA.

E' consentito l'annullamento di una registrazione di protocollo per motivate e verificare ragioni.

Solo il Responsabile della gestione documentale e le persone espressamente delegate sono autorizzate ad annullare la registrazione.

L'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo.

I motivi per i quali è richiesto l'annullamento possono essere:

- Errore di inserimento delle informazioni registrate in forma immodificabile nel caso che dette informazioni non siano generate o assegnate automaticamente dal sistema;
- Il documento registrato deve essere sostituito per rettifica del destinatario, dell'oggetto purché il documento non sia stato già diffuso;
- La motivazione per cui il documento è stato prodotto è venuta meno purché il documento non sia stato già diffuso.

Nel caso in cui il documento da annullare sia sostituito da una nuova registrazione, negli estremi del provvedimento di autorizzazione all'annullamento si indica che il documento è stato correttamente registrato con protocollo n.\_del\_.

La registrazione annullata resta visibile all'interno del sistema di gestione documentale e della sequenza numerica con la dicitura "Annullato".

Il documento analogico annullato riporta gli estremi dell'annullamento e viene conservato. La richiesta di annullamento, inviata a mezzo *e-mail* alla casella istituzionale dell'Ufficio Protocollo, sarà associata alla registrazione di protocollo del documento annullato a cura del Responsabile della gestione documentale o dalle persone espressamente delegate.

In *Titulus* i documenti annullati possono essere inseriti nei rispettivi fascicoli o, nel caso di documenti non inerenti a specifici procedimenti, in un fascicolo annuale.

Se il documento analogico o informatico costituisce una tipologia documentale soggetta a registrazione particolare (ad es. un contratto) per la quale è prevista la conservazione perenne, lo stesso sarà conservato nel proprio repertorio con la dicitura "annullato" assieme alla richiesta di annullamento.

In tema di annullamento dei provvedimenti occorre far riferimento alle disposizioni di cui alla L. 241/1990 in merito agli strumenti di autotutela.

Nella registrazione di protocollo appaiono in forma ben visibile, oltre agli elementi già indicati, anche la data, il cognome e nome dell'operatore che ha effettuato l'annullamento.

Le informazioni relative al protocollo rimangono comunque memorizzate nel registro informatico per essere sottoposte alle elaborazioni previste dalla procedura, comprese le visualizzazioni e le stampe, nonché la data, l'ora, l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo.

Non si annulla mai un documento informatico trasmesso con PEC in quanto il destinatario è già in possesso del documento stesso.

Si può procedere con la redazione di un nuovo documento che annulla e sostituisce il precedente (in questo caso o è necessario citare il riferimento del protocollo) è protocollato e inviato via PEC.

## **8.12. Corresponsabilità di un documento e di un fascicolo**

La corresponsabilità di un documento e/o di un fascicolo è la partecipazione al procedimento amministrativi di:

- Più UOR della stessa AOO (corresponsabilità di servizi interna);
- Più AOO dello stesso ente (corresponsabilità esterna di 1° livello);
- Più AOO di enti diversi (corresponsabilità di servizi esterna di 2° livello);

Nella corresponsabilità di servizi interna pur essendo la responsabilità amministrativa tra più UOR e di conseguenza tra più RPA, la responsabilità della tenuta dei documenti in originale (per quelli analogici), cioè nel fascicolo, spetta esclusivamente alla UOR che ha la competenza prevalente sul procedimento amministrativo e che l'Ufficio Protocollo ha inserito per prima nella registrazione e prima riportata nella registrazione di protocollo.

Spetta pertanto alla prima UOR indicata ad aprire il fascicolo e poi renderlo disponibile alle altre UOR coinvolte nella corresponsabilità di servizi.

La corresponsabilità di servizi esterna di 1° livello (tra più AOO dello stesso ente) e la corresponsabilità di servizi esterna di 2° livello (tra AOO di enti diversi) non sono utilizzate.

## **8.13. Documenti scambiati tra uffici non soggetti a registrazione di protocollo**

- Richieste di servizio di pulizie;
- Richieste di facchinaggio;
- Richieste di fornitura di cancelleria;
- Richieste di piccole manutenzioni;
- Richieste di sopralluoghi e servizi tecnici;
- Richieste di sopralluoghi archivistici,
- Richieste di fascicoli conservati nell'archivio di deposito per attività istituzionale;
- Richieste di accesso ai locali destinati all'archivio analogico.

## **8.14. Casi di rigetto**

Per rigetto si intende la segnalazione di una UOR all'Ufficio Protocollo della erronea assegnazione di competenza su un determinato documento ricevuto in smistamento. Pertanto il rigetto avviene solo per i documenti in arrivo.

Prima del rigetto la UOR deve riportare nella registrazione una annotazione motivando e indicando la UOR competente.

Il documento originale analogico deve essere sempre conservato (salvo diversa indicazione nel campo ANNOTAZIONE di Titulus) a cura della UOR assegnataria del protocollo.

In caso di conflitto di competenza tra UOR, è il Dirigente/Direttore, su proposta del responsabile della gestione documentale, che determina lo smistamento definitivo.

Sono ammessi solo due rigetti prima dell'assegnazione d'autorità.

Nessun documento analogico e/o informatico, può rimanere in carico all'Ufficio Protocollo, soprattutto se pervenuto con PEC.

### **8.15. Flusso del documento informatico in partenza**

Il documento informatico prodotto deve essere redatto preferibilmente nel formato Pdf/a o per casi particolari, secondo gli altri formati stabiliti in precedenza (cfr. paragrafo 3.20) e in base alla tipologia di documento informatico, deve avere i seguenti requisiti minimi di forma e contenuto per poter essere registrato al protocollo:

- a) Documento informatico formato attraverso l'acquisizione della copia per immagine su supporto informatico di un documento analogico:
  - Sigillo;
  - Data completa (luogo, giorno, mese, anno) scritta per esteso;
  - Indicazione dell'indirizzo PEC o e-mail del destinatario;
  - Il nominativo dell'RPA;
  - Numero di protocollo;
  - Numero degli allegati;
  - Sottoscrizione autografa (nei casi previsti dalla normativa deve essere corredato da dichiarazione di conformità sottoscritta con firma digitale).
- b) Redazione tramite l'utilizzo di appositi strumento software:
  - Sigillo;
  - Data completa (luogo, giorno, mese, anno) scritta per esteso;
  - Indicazione dell'indirizzo PEC o e-mail del destinatario;
  - Il nominativo del RPA;
  - Numero degli allegati;
  - Firma digitale;

- Il numero di protocollo può essere inserito solo nel caso si adottino particolari accorgimenti nella formazione del documento e si utilizzi il formato PAdES per la sottoscrizione digitale.
- Può essere predisposto un flusso all'interno del sistema gestionale per i visti eventualmente richiesti all'interno dell'amministrazione prima della protocollazione del documento firmato digitalmente. Il documento informatico protocollato può essere trasmesso via e-mail e a mezzo PEC.

#### **8.16. Flusso del documento informatico tra UOR della stessa AOO**

Il documento tra uffici (o interno) è quello che una UOR invia ad un'altra UOR della stessa AOO.

Trattandosi di documenti endoprocedimentali, possono essere prodotti in pdf/a e la registrazione a protocollo costituisce firma elettronica avanzata.

#### **8.17. Utilizzo delle firme elettroniche: firma elettronica semplice, firma elettronica avanzata, firma elettronica qualificata, firma digitale**

*Firma elettronica*: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ed altri dati elettronici, utilizzati come metodo di identificazione informatica.

*Firma elettronica semplice*: la cosiddetta “*firma debole*” intesa come l'insieme dei dati in forma elettronica, riconducibili all'autore (anche di tipo: *log identificativo, indirizzo, mail, ecc*), allegati o connessi ad atti o fatti giuridicamente rilevanti contenuti in un documento informatico, utilizzati come metodo di identificazione informatica. Può essere utilizzata per i documenti interni.

*Firma elettronica avanzata*: intesa come insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati su mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati. Le *annotazioni* sulle registrazioni del sistema di gestione documentale sono considerate firma elettronica avanzata e vengono utilizzate per l'attestazione di regolare esecuzione del servizio/fornitura e l'autorizzazione al pagamento delle fatture elettroniche.

*Firma elettronica qualificata*: una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. Ai sensi dell'art.25, comma3, del Regolamento del

Parlamento e del Consiglio dell'Unione Europea 23 luglio 2014, n. 910 corrisponde alla firma digitale italiana. Utilizzata per tutti i documenti per cui viene richiesto dalla normativa.

## **CAPITOLO 9. CASISTICA E COMPORTAMENTI**

### **9.1. Gestione delle gare d'appalto**

#### **9.1.1. Gare e procedure negoziate gestite in modalità analogica**

Le buste sigillate riportanti le seguenti diciture: «offerta», «gara d'appalto» o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara d'appalto o a una procedura negoziata non vanno aperte e si registrano a protocollo per garantire la data certa di acquisizione. La segnatura va apposta sulla busta. Inoltre, per le offerte consegnate nel giorno di scadenza, l'ufficio deputato alla ricezione apporrà sulla busta anche l'ora di consegna. Se la registrazione avviene dopo l'ora fissata per la consegna o se la consegna avviene dopo la scadenza fissata dal bando di gara, a protocollo viene inserita anche una annotazione immodificabile del tipo: "documento pervenuto/consegnato alle ore hh.mm del giorno gg/mm/aaaa come risulta dall'indicazione riportata sulla busta che si digitalizza".

Nell'oggetto si riporta la descrizione della gara/offerta così come è riportata sulla busta,

Gli uffici che indicano le procedure possono dare disposizione di apporre sulla busta una dicitura, ad es., "Non aprire: offerta per la procedura negoziata per la realizzazione di... - CIG: ... - CUP: ...".

### **9.1.2. Gare e procedure negoziate gestite in modalità telematica**

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

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

### **9.2. Gestione di concorsi e selezioni**

Se le istanze di partecipazione a concorsi e procedure di selezione sono inviate in formato analogico, tenuto conto che sono spesso corredate di allegati numerosi e, in alcuni casi, anche voluminosi, alla registrazione di protocollo può essere associata la sola scansione dell'istanza e non quella degli allegati. Sarà cura del servizio di registrazione indicare nel sistema di protocollo ciascun allegato ricevuto, inserendo una "Annotazione" immodificabile in cui si dà contezza del fatto che non si procede alla scansione, del tipo: "Non si procede alla scansione ... (ad es. delle pubblicazioni)".

.Nei casi in cui l'istanza viene prima esaminata dalla UOR e gli allegati trattenuti, è possibile trasmettere all'Archivio Generale di Ateneo solo l'istanza dei candidati, avendo cura di annotare a penna o mediante timbro sul documento il numero degli allegati trattenuti, sottoscrivendo la nota.

In alternativa la UOR trasmette insieme all'istanza l'elenco degli allegati, che viene scansionato e unito alla registrazione. Nella registrazione di protocollo si riporta: come numero di allegati l'effettiva quantità pervenuta e indicata sul documento dalla UOR ricevente; nel campo allegati la dicitura "N. ... allegati trattenuti dal Servizio/Ufficio ...".

La documentazione per la partecipazione a concorsi, selezioni, etc., per cui non sia stato possibile procedere alla registrazione a protocollo nella giornata di ricezione, deve essere protocollata con provvedimento di differimento della registrazione alla data di ricezione.

Non è ammessa la consegna della domanda in busta sigillata: l'Ufficio Protocollo apre il plico e registra le domande nella loro completezza, ferma restando la possibilità di non provvedere alla scansione degli allegati voluminosi.

Se le istanze di partecipazione a concorsi e procedure di selezione sono inviate in modalità telematica, a mezzo PEC, gli allegati saranno automaticamente associati alla registrazione.

### **9.3. Atti giudiziari**

Ai fini dell'identificazione del corrispondente di atti e/o note inerenti a contenzioso, occorre tener presente la differenza tra la notifica (effettuata direttamente all'Amministrazione) e altri tipi di comunicazione.

La notifica avviene con la consegna dell'atto eseguita dall'ufficiale giudiziario, nelle mani proprie del destinatario o a soggetto rappresentante dell'amministrazione autorizzato a ricevere l'atto, o da altro soggetto abilitato tramite servizio postale, a mezzo PEC o nelle altre modalità stabilite dalla legge.

Se l'atto è notificato a mano si considera come data di notifica quella indicata nella referta di notifica del documento; se è notificato con raccomandata si considera il giorno in cui si ritira la raccomandata.

Ai sensi dell'art. 149-bis cpc, la copia estratta dal documento originale deve essere firmata digitalmente dall'ufficiale giudiziario e, se non è fatto espresso divieto dalla legge, la notificazione può eseguirsi a mezzo posta elettronica certificata, anche previa estrazione di copia informatica del documento analogico. In questo caso, l'ufficiale giudiziario trasmette copia informatica dell'atto sottoscritta con firma digitale all'indirizzo di posta elettronica certificata del destinatario risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni.

La notifica si intende perfezionata nel momento in cui il gestore rende disponibile il documento informatico nella casella di posta elettronica certificata del destinatario.

Per mittente si intende la parte istante, cioè il legale/avvocato delegato mediante procura alle liti che agisce in nome e per conto del soggetto interessato e che ha richiesto la notifica dell'atto. Anche un sindacato o un'associazione non riconosciuta, può essere mittente, nel caso in cui agisca in nome e per conto di un lavoratore in una controversia sindacale. Il mittente del documento non è l'organo giudiziario indicato generalmente sul frontespizio dell'atto (ad es., Tribunale, Corte di Appello), ma colui che ha richiesto la notificazione, generalmente il legale a cui il ricorrente/attore che ha conferito mediante mandato la procura alle liti (quindi il corrispondente apposto di norma sulla prima pagina dell'atto in alto a destra).

Quando l'atto è notificato presso l'Avvocatura Distrettuale o Generale dello Stato, in quanto soggetto che assicura la difesa in giudizio dell'Amministrazione, l'Avvocatura stessa generalmente procede alla trasmissione dell'atto all'Ateneo, dandone informativa, quindi il mittente da indicare nella registrazione di protocollo è l'Avvocatura. In tal caso si tratta di una comunicazione, non di una notifica, il cui mittente da indicare nella registrazione di protocollo è appunto l'Avvocatura, come per tutte le comunicazioni dalla stessa provenienti.

Diverse sono poi le comunicazioni (quali quelle consistenti in avvisi di deposito di note o di fissazione di udienza) che provengono direttamente dalla cancelleria dell'autorità giudiziaria (Tribunale, Corte di appello, ecc.) innanzi a cui pende il giudizio. In questi casi il mittente è sicuramente l'autorità giudiziaria medesima. Le comunicazioni che provengono dalla cancelleria dell'autorità giudiziaria arrivano tramite l'applicativo del processo civile telematico – PTC, sono conservate nella casella PEC, rilasciata dall'ordine professionale a cui è iscritto l'avvocato che ha in carico la pratica.

Si noti che nei procedimenti giuslavoristici (cause di lavoro) contestuale al ricorso introduttivo del giudizio si trova il pedissequo decreto di fissazione di udienza, in calce al ricorso stesso. In tal caso si è in presenza, contestuale di un atto di parte e di un atto prodotto dall'organo giurisdizionale.

Lettere, diffide, solleciti, messe in mora e similari sono da considerarsi e da trattarsi come le comunicazioni e non come le notifiche.

#### **9.4. Documenti informatici con oggetto multiplo**

Nel caso di documenti in arrivo che trattano più argomenti di competenza di UOR diverse tra loro, concretando il caso del cosiddetto "oggetto multiplo", il documento viene registrato redigendo l'oggetto in maniera esaustiva con tutte le informazioni necessarie a comprendere i vari argomenti. La classificazione del documento riguarderà l'argomento prevalente o comunque individuato come tale e smistato alla UOR competente sullo stesso.

Compatibilmente con la funzionalità del sistema di gestione documentale, ciascuna UOR corresponsabile potrà (dovrà) creare la propria copia informatica al fine di proseguire con la gestione e la fascicolatura.

Nel caso di documento in partenza è compito della UOR responsabile verificare che il documento prodotto tratti un solo argomento, chiaramente espresso nel campo "oggetto".

## **9.5. Fatture elettroniche (Fattura PA)**

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

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

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

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

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

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

La fattura elettronica perviene in formato XML via PEC, agli indirizzi dichiarati dall'ente e registrati sull'indice IPA nel corrispondente servizio di fatturazione.

La fattura così pervenuta è automaticamente protocollata, assegnata alla UOR competente - che provvede alla classificazione e alla fascicolatura - e trasmessa al sistema di contabilità dove dovrà essere presa in carico per la verifica di correttezza e conformità. Sul sistema contabile si provvede alla registrazione della stessa sul registro delle fatture, entro 10 giorni dal ricevimento (DL 66/2014 art. 42).

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

Per inoltrare e ricevere le fatture elettroniche è stato integrato il sistema documentale con il sistema di contabilità. Nel sistema di protocollo sono utilizzati più indirizzi di posta elettronica certificata e più codici IPA specificamente destinati alla ricezione delle fatture elettroniche (Allegato 6).

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

## **9.6. DURC on-line**

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

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

## **9.7. Denunce di infortuni**

Il datore di lavoro è tenuto a denunciare all'INAIL gli infortuni da cui siano colpiti i dipendenti prestatori d'opera, indipendentemente da ogni valutazione circa la ricorrenza degli estremi di legge per l'indennizzabilità.

Le denunce di infortunio sono inviate esclusivamente in modalità telematica accedendo al portale dell'INAIL con apposite credenziali rilasciate ai dipendenti incaricati. L'invio delle denunce tramite PEC è consentito solo in caso di malfunzionamento del sistema.

Considerato che il sistema per l'invio telematico della denuncia prevede l'inserimento obbligatorio di dati ulteriori rispetto a quelli presenti sul certificato del pronto soccorso, è onere del lavoratore consegnare la dichiarazione di infortunio sul lavoro compilata in ogni sua parte. Il delegato alle denunce che ricevesse tale modulo compilato in modo incompleto dovrà chiederne tempestivamente l'integrazione all'infortunato. Il funzionario attesta la data certa e la piena conoscenza dell'infortunio sottoscrivendo e datando il documento. Questa procedura sostituisce il protocollo in arrivo del documento, quindi le denunce di infortunio sono una tipologia di documenti esclusa dalla registrazione di protocollo.

## **9.8. Certificati di malattia**

I certificati di malattia sono acquisiti consultando la banca dati dell'INPS con apposite credenziali rilasciate ai dipendenti incaricati. Dopo averli visualizzati sono stampati o salvati come file e inseriti nel fascicolo personale. I certificati di malattia sono una tipologia di documenti esclusa dalla registrazione di protocollo.

## **9.9. Documenti del portale degli acquisti della pubblica amministrazione**

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

Il Mercato Elettronico della P.A. (MePA), ai sensi dell'art. 11 del D.P.R. 101/2002, mediante il quale le Pubbliche Amministrazioni possono acquistare beni e servizi offerti dai fornitori abilitati presenti sui diversi cataloghi del sistema, il cui importo deve essere inferiore alla soglia comunitaria.

Le Convenzioni contratti quadro stipulati da Consip ai sensi dell'art. 26 della Legge 488/99) nell'ambito dei quali i fornitori aggiudicatari di gare esperite in modalità tradizionale o smaterializzata a seguito della pubblicazione di bandi si impegnano ad accettare ordinativi di fornitura emessi dalle singole Amministrazioni che hanno effettuato l'abilitazione al sistema Acquisti in rete. Gli Accordi quadro, aggiudicati da Consip a più fornitori a seguito della pubblicazione di specifici Bandi, definiscono le clausole generali che, in un determinato periodo temporale, regolano i contratti da stipulare. Nell'ambito dell'Accordo quadro, le Amministrazioni che hanno effettuato l'abilitazione al sistema Acquisti in Rete, attraverso la contrattazione di "Appalti Specifici", provvedono poi a negoziare i singoli contratti, personalizzati sulla base delle proprie esigenze.

Si descrivono le procedure di acquisto d'uso più frequente:

- Affidamenti diretti à MePA (Mercato Elettronico Pubblica Amministrazione)
- Adesioni a Convenzioni
- Negoziazioni à MePA (Mercato Elettronico Pubblica Amministrazione).

### **9.9.1. Affidamenti diretti sulla piattaforma MePA (OdA)**

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

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

### **9.9.2. Adesioni – Convenzioni (OdA)**

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

Il processo può essere così brevemente schematizzato: il punto istruttore seleziona la convenzione, effettua una bozza dell'ordine attraverso la piattaforma e la invia al punto ordinante.

Il punto ordinante controlla la bozza, genera attraverso la piattaforma il file pdf/a che costituisce il documento d'ordine (Ordine di Acquisto OdA), lo scarica localmente, lo firma digitalmente, lo registra nel sistema di protocollo e lo ricarica a sistema. La piattaforma MePA chiede il numero di protocollo per procedere nella registrazione. Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l'emissione del corrispondente documento gestionale. Nel caso sia un documento di tipo "ordine", questo può essere trasmesso al sistema di gestione documentale dove è generata una bozza per la registrazione a protocollo e la fascicolatura. Nel caso invece sia un documento di tipo "contratto" dal sistema contabile può essere richiamato il numero di protocollo assegnato all'ordine emesso sulla piattaforma Me- PA.

### **9.9.3. Procedure negoziate (RdO) – MePA**

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

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

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

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

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

### **9.10. Documenti pervenuti via PEC**

Le caselle di PEC istituzionali dell'Università degli Studi di Bergamo sono "chiuse" quindi possono ricevere messaggi e documenti solo da altri vettori qualificati (altre caselle di PEC). In questo caso, al fine di rendere efficace la natura giuridico-probatoria del messaggio di PEC, si procede con la protocollazione o con la registrazione del documento come "non protocollato".

La ricezione via PEC di un documento comprova il fatto che lo stesso ha raggiunto il destinatario.

In ogni caso sono soggetti a registrazione di protocollo:

- il messaggio;

- i file allegati.

Per quanto riguarda la corretta identificazione del mittente, bisogna tener presente che la PEC è solo un vettore, il mittente è colui che sottoscrive il documento allegato o, nel caso di testo nel corpo del messaggio (body message) senza allegato, colui che lo trasmette.

Nel caso in cui con uno stesso messaggio PEC pervengano documenti di firmatari diversi, senza alcun documento con funzione di lettera di trasmissione, è prodotta una registrazione distinta per documento, corredata di annotazioni esplicative. In alternativa è lasciato l'indirizzo così come pervenuto e nell'oggetto è scritto: "Trasmissione di documenti con firmatari diversi". Oppure, se si evince che l'indirizzo PEC è riconducibile in mondo certo a uno dei firmatari dei documenti trasmessi, si indica nell'oggetto: "Cognome Nome trasmette per sé e per ...".

La regola generale da seguire, in base al principio di simmetria delle forme, è che a un documento pervenuto con PEC si risponde con un documento trasmesso con PEC, utilizzando lo stesso canale di comunicazione.

Qualora il messaggio di posta elettronica pervenga a una casella di PEC dello stesso ente, ma diversa da quella competente, si annulla il documento in entrata e nella causale si indica l'AOO corretta e il relativo indirizzo PEC. Il mittente riceve il messaggio e ha quindi la possibilità di inoltrare il messaggio PEC alla casella corretta.

### **9.11. Gestione di due documenti diversi trasmessi via PEC**

Se con un unico messaggio pervengono due o più documenti, si provvede alla registrazione dei singoli documenti e non del messaggio, quindi con tante registrazioni quanti sono i documenti pervenuti provvedendo ad inserire opportune annotazioni di richiamo tra le registrazioni.

### **9.12. Gestione di soli allegati pervenuti via PEC e di documenti costituiti dal solo corpo della PEC**

Qualora pervengano a mezzo PEC documenti identificabili come allegati e il documento principale si limita all'oggetto del messaggio, presentato dal protocollo informatico come oggetto nell'apposito campo in fase di registrazione, l'oggetto proposto rimane inalterato e si redige la seguente annotazione: «*Considerato che nessuna [istanza /lettera di accompagnamento /altro] è pervenuta tramite questa PEC e che il documento allegato è (descrizione allegato/i), si deduce che la richiesta sia rappresentata da quanto descritto nel campo oggetto dal mittente. Si è pertanto proceduto con la protocollazione*».

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

### **9.13. Documenti pervenuti a mezzo e- mail semplice (non certificata)**

#### **9.13.1. Rapporti con terzi esterni**

Se richiesto dal responsabile del procedimento, o da suo delegato, si registrano a protocollo anche le e-mail semplici, limitatamente ai casi in cui il loro contenuto sia rilevante nell'ambito di un procedimento, valutando caso per caso. Per richiesta si intende l'inoltro della e-mail alla casella di posta elettronica istituzionale associata all'Archivio Generale di Ateneo.

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

Le richieste di informazioni su orari di apertura e sul funzionamento di procedure (anche provenienti dall'estero) non sono soggette a registrazione di protocollo e ad esse si può rispondere a mezzo e-mail non protocollata. Invece lamentele, doglianze, comunicazioni di disservizi devono essere valutate caso per caso. Nei casi di particolare gravità e rilevanza, si procede alla registrazione a protocollo.

### **9.13.2. Rapporti tra diverse AOO**

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

### **9.14. Gestione del secondo esemplare**

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

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

Se il secondo esemplare perviene in formato analogico, si appone su di esso la segnatura di protocollo e l'indicazione "Secondo esemplare". Nella registrazione di protocollo si inserisce la "Annotazione" in modo immutabile "Pervenuto secondo esemplare mediante raccomandata a/r" al fine di poter recuperare tutti gli esemplari pervenuti nel caso si debba, ad es., modificare la UOR indicata nella segnatura di protocollo.

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

### **9.15. Documenti anonimi**

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

Le lettere anonime, pertanto, non sono soggette a registrazione di protocollo a meno che il documento anonimo non sia pervenuto a mezzo PEC; in tal caso si lascia come mittente l'indirizzo PEC.

### **9.16. Documenti scambiati tra UOR della stessa AOO**

Per documenti interni si intendono i documenti scambiati tra le diverse UOR della medesima AOO.

I documenti informatici prodotti a seguito della protocollazione e scansione di documenti originali cartacei trasmessi tra le UOR di ciascuna AOO sono inoltrati in formato digitale tramite il sistema di protocollo informatico senza procedere all'inoltro dell'originale analogico, che resta nella disponibilità della UOR mittente, che procederà alla sua gestione e fascicolatura.

Le comunicazioni informali tra uffici non sono soggette a registrazione di protocollo in base al principio di non aggravio del procedimento, ma a cura delle UOR interessate possono essere acquisite nel sistema di protocollo come documento non protocollato

## **CAPITOLO 10. ALBO ON-LINE - PUBBLICITA' LEGALE - PUBBLICAZIONI SUL SITO WEB ISTITUZIONALE DELL'AOO-ATENEIO (rinvio)**

La disciplina relativa all'Albo on-line, il valore della pubblicazione all'albo on line, le modalità di pubblicazione dei documenti all'albo on line, i formati per la pubblicazione e per la conservazione, le modalità di pubblicazione dei documenti nel repertorio dell'albo on line nonché i contenuti e le modalità di pubblicazione di documenti nelle altre sezioni del sito web di ateneo e nei siti web delle strutture (UOR) che compongono l'AOO-Ateneo sono fissati nel regolamento di Ateneo.

## **CAPITOLO 11. DALL'ARCHIVIO CORRENTE ALL'ARCHIVIO DI DEPOSITO**

### **11.1. Archivio di deposito**

L'archivio di deposito è la fase intermedia del processo di tenuta dei documenti prodotti dall'Ateneo nel corso della propria attività e si colloca temporalmente tra l'archivio corrente e l'archivio storico. Il suo carattere di transitorietà e l'introduzione dell'informatizzazione degli archivi ha condotto alla sottovalutazione di un momento gestionale che ha, prima di tutto, una dimensione logica e un'importanza funzionale rilevanti. L'archivio di deposito è il momento di decantazione dei documenti e delle informazioni relative, organizzati in fascicoli inerenti ad affari, ad attività e a procedimenti conclusi, per i quali non risulta più necessaria la trattazione corrente o verso i quali sussista solo un interesse sporadico.

Le attività che connotano questa fase d'archivio sono definite dal DPR 445/2000, artt.67, 68 e 69, e riguardano l'obbligo della periodicità dei trasferimenti di documenti dall'archivio corrente, la conservazione ordinata delle unità archivistiche e la disponibilità dei mezzi di corredo per assicurare le funzioni di controllo e di ricerca del materiale (registri di protocollo, piani di classificazione repertori dei fascicoli, etc.).

I documenti sono conservati con le modalità indicate dal Responsabile della gestione documentale e di archivio, rispettando l'organizzazione che essi avevano nell'archivio corrente.

La produzione e gestione informatica di dati e di documenti comporta una diversificazione delle procedure di gestione durante la fase di deposito determinata dalla peculiarità del supporto. Ciononostante non cambia il ruolo e la funzione concettuale svolta dall'archivio di deposito nella tenuta del sistema documentale. Si tratta, in ogni caso, di una

fase di sedimentazione della documentazione, ossia di un periodo in cui i documenti esauriscono nel tempo le proprie funzioni rilevando la propria natura temporanea o permanente, a seconda del valore delle informazioni in essi contenute. I documenti nativi digitali sono caratterizzati dalla predeterminazione dei termini di conservazione. Ciò significa che la durata della vita di un documento è determinata nel momento stesso in cui il documento viene creato. Si tratta di una forma di impostazione della selezione a priori dei documenti, attività che avviene anche per i documenti analogici, ma che è messa in atto solo in un secondo momento, durante la fase di deposito.

L'archivio di deposito analogico è gestito e conservato a cura dell'Archivio Generale di Ateneo, che si occupa di organizzare i seguenti servizi e attività:

- Attività preliminari finalizzate alla creazione di locali d'archivio a norma:
  - Trasferimenti periodici dei documenti dagli uffici e acquisizione delle unità da parte dell'archivio di deposito: preparare annualmente il trasferimento dei fascicoli relativi ad affari conclusi con la predisposizione di appositi elenchi di consistenza;
  - Concentrazione ordinata dei documenti, mantenendo le aggregazioni (serie e fascicoli) create nella fase di formazione e procedere alla revisione degli elenchi di trasferimento: effettuare una schedatura sommaria delle unità trasferite in archivio attribuendo una numerazione univoca, continua e progressiva che determina la progressione logica e fisica delle unità nell'elenco di consistenza e nel locale d'archivio;
  - Selezione della documentazione sulla base dei Massimari di selezione adottati dall'Ateneo;
  - Campionatura di determinate tipologie documentali da non destinare integralmente alla conservazione a lungo termine;
  - Scarto della documentazione;
  - Riordinamento e ricostituzione delle serie originarie (rispetto del vincolo archivistico - piano di fascicolazione – Titolare di classificazione – successione cronologica annuale, cioè le serie sono chiuse per anno);
  - Conservazione adeguata dei documenti: sostituzione delle unità di condizionamento laddove danneggiate o non adatte alla conservazione a medio o lungo termine, mantenimento delle condizioni ambientali ottimali etc.;
  - Versamento della documentazione all'archivio storico: predisposizione degli elenchi di versamento e aggiornamento dell'elenco di consistenza;
  - Servizio di ricerca documentale (recupero dei documenti/unità richieste – consultazione – creazione di copie semplici o conformi);

- Predisposizione di statistiche sia per le attività di trasferimento e versamento che di consultazione: consente un'adeguata programmazione degli spazi e ottimizzazione dei servizi;
- Elaborazione e aggiornamento del piano di conservazione degli archivi.
- Attività straordinaria – in caso di necessari interventi di recupero del pregresso:
  - Ricognizione, censimento o mappatura della documentazione presente nel locale adibito a deposito e della documentazione impropriamente conservata presso gli uffici produttori;
  - messa in sicurezza del locale di deposito e spostamento di tutto ciò che non è documento;
  - schedatura delle unità documentale;
- Selezione della documentazione e redazione di:
  - Elenco di scarto, contenente la descrizione della documentazione da distruggere;
  - Elenco di versamento dell'archivio storico, contenente la descrizione della documentazione da conservare senza limiti di tempo;
  - Elenco di consistenza dell'archivio di deposito, contenente la descrizione della documentazione rimasta dopo lo scarto ed il versamento in archivio storico;
  - Procedura di scarto.

## **11.2. Trasferimento dei fascicoli cartacei**

Periodicamente e comunque una volta all'anno, il RPA trasferisce, per la conservazione nell'archivio di deposito al Responsabile della gestione documentale, i fascicoli relativi ad affari, attività e a procedimenti amministrativi conclusi e non più necessari ad una trattazione corrente.

Per il trasferimento viene predisposto a cura del RPA l'elenco dei fascicoli trasferiti indicando, nell'intestazione l'ufficio di provenienza della documentazione, e per ogni unità trasferita la classificazione, il numero progressivo di repertorio del fascicolo, l'oggetto e gli estremi cronologici.

Il trasferimento dei fascicoli comporta il passaggio della sola responsabilità gestionale all'Archivio Generale di Ateneo, mentre la titolarità amministrativa dei documenti rimane in capo alla UOR che ha creato i documenti; solo con il versamento nell'archivio storico l'Archivio Generale di Ateneo acquisisce la piena titolarità dei documenti a esso affidati.

I fascicoli sono trasferiti rispettando l'ordine dei documenti all'interno dei fascicoli. Qualora i responsabili delle UOR si trovassero nelle condizioni di dovere trasferire fascicoli o documenti prodotti e chiusi da molto tempo, oppure i cui RPA non siano più in servizio, essi dovranno essere trasferiti nelle condizioni in cui si trovano, senza operare interventi sull'ordinamento degli stessi e redigendo l'elenco di consistenza. Nei casi in cui ciò non sia possibile, i responsabili delle UOR concorderanno le modalità opportune di trasferimento, caso per caso, con il Responsabile della gestione documentale. Prima del trasferimento i RPA provvedono anche a verificare che i fascicoli risultino chiusi anche nel sistema informatico di gestione documentale.

Alla ricezione dei fascicoli il Responsabile della gestione documentale verifica la corrispondenza dell'elenco di consistenza con il verbale di trasferimento, sottoscritto insieme all'elenco anche dal RPA al momento della consegna dei fascicoli.

La non corrispondenza, anche parziale tra l'elenco di consistenza e il materiale documentale effettivamente versato è oggetto di dichiarazione a cura del Responsabile della gestione documentale e sarà informata la struttura versante con invito a provvedere entro 10 giorni alla regolarizzazione.

### **11.3. Archivio informatico. Trasferimento dei fascicoli informatici**

Ai sensi delle Linee Guida AgiD: Ai fini di una corretta organizzazione dei documenti informatici, dei fascicoli informatici e delle serieinformatiche, nella Pubblica Amministrazione il manuale di gestione documentale definisce la struttura dell'archivio all'interno del sistema di gestione informatica dei documenti.

L'archivio informatico - formato ai sensi del capo IV "Sistema di gestione informatica dei documenti" del DPR 445/2000 - deve essere progettato in modo da assicurare certezza e trasparenza all'attività giuridico amministrativa.

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

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

A titolo di esempio, per tutti i documenti informatici a rilevanza fiscale occorre rispettare le tempistiche previste dal D.M. 17 giugno 2014 quindi, nel caso in esame, delle fatture elettroniche attive e passive, inserite nel fascicolo della procedura di acquisto, si dovrà procedere al versamento anticipato in conservazione secondo le regole previste nel manuale di conservazione e gli specifici accordi di versamento stipulati con il soggetto esterno cui è affidato il processo di conservazione.

#### **11.4. Trasferimento delle serie archivistiche**

Le serie archivistiche (contratti, decreti, verbali, ecc.) sono trasferite all'archivio di deposito nella loro unitarietà, secondo un termine che può variare da serie a serie.

Le modalità di trasferimento sono le medesime previste per i fascicoli cartacei e informatici.

Se la serie archivistica è ibrida, cioè composta sia da documenti analogici che da documenti digitale, si procederà nel seguente modo:

- Il repertorio digitale nel sistema di gestione documentale conterrà tutti i documenti informatici in formato nativo e la copia per immagine dei documenti analogici associata alla registratura;
- Il repertorio analogico sarà composto dagli originali analogici dei documenti e dalla copia analogica conforme all'originale informatico dichiarata dal Responsabile del procedimento amministrativo;
- Il documento originale deve essere fascicolato. Il documento è unico ma collocato sia nel repertorio che nel fascicolo. Analogamente per i documenti nativi analogici: due originali, uno a repertorio e il secondo nel fascicolo della pratica relativa o, in alternativa copia conforme.

#### **11.5. Ordinamento archivistico**

L'ordinamento delle unità archivistiche nell'archivio di deposito avviene nel rispetto del principio di provenienza e dell'ordine originario. In particolare, per i fascicoli, l'ordine è quello stabilito dal repertorio dei fascicoli.

Il titolario di classificazione è parte integrante del presente Manuale ed è applicabile solo ai documenti prodotti/ricevuti dopo la sua adozione. Ciò significa che il piano di classificazione non ha mai efficacia retroattiva. I fascicoli prodotti in precedenza, quindi, vengono archiviati sulla base dei titolari/piani di classificazione in vigore al momento della produzione dei documenti afferenti, specificatamente nell'anno di chiusura del fascicolo. L'ordinamento, infatti, comporta la ricostruzione delle serie originarie e si lavora per serie chiuse per anno considerando come data di riferimento la data di chiusura della pratica. Pertanto, il dato cronologico è fondamentale perché per ogni anno si ricostruiscono le serie di fascicoli sulla base della classificazione attribuita ai fascicoli e desumibile dal repertorio dei fascicoli. Se il fascicolo è pluriennale e il suo periodo di attività cade a cavallo di una modifica del titolario verrà inserito, in base alla sua classificazione, nella serie dell'ultimo

anno di vita della pratica, annotando la doppia classificazione di parte della documentazione causata dalla modificazione o aggiornamento del piano di classificazione.

Fascicoli e documenti analogici, prodotti senza l'applicazione di un titolario o piano di classificazione, sono ordinati dopo una adeguata analisi degli stessi, al fine di un ordinamento secondo criteri condivisi e orientati ad essere perduranti nel tempo. Gli interventi su questa documentazione vanno comunque valutati insieme alla Soprintendenza Archivistica della Lombardia.

#### **11.6. Servizio di ricerca documentale e movimentazione dei fascicoli (record delivery)**

L'Archivio Generale di Ateneo è titolare e responsabile del servizio documentale, effettuato su richiesta degli uffici dell'Ateneo o di altri soggetti autorizzati. Il servizio, ove necessario, viene effettuato con la collaborazione degli uffici produttori o interessati.

Il servizio è di norma erogato tramite comunicazione delle informazioni richieste o con la trasmissione di copia della documentazione pertinente. Solo ove richiesto o necessario si ricorre al prelievo dal deposito e alla trasmissione della documentazione originale.

E' consentito il richiamo temporaneo di uno o più fascicoli, già trasferiti all'archivio di deposito da parte della UOR produttrice o altra UOR autorizzata. E' vietata l'estrazione di documenti in originale dal fascicolo, che va mantenuto nell'ordine di sedimentazione derivante dall'archivio corrente, rispettando il vincolo archivistico (cioè l'appartenenza di ogni documento alla rispettiva unità o sottounità archivistica).

Il richiamo di uno o più fascicoli è consentito per il tempo necessario alla UOR richiedente per l'esaurimento della pratica.

Un fascicolo chiuso e trasferito all'archivio di deposito non può essere riaperto se non dopo che il RPA si sia consultato con il Responsabile della gestione documentale, al fine di valutare la correttezza di tale operazione o se invece sia opportuna la creazione di un nuovo fascicolo per il nuovo procedimento, indipendente dal fascicolo richiamato.

Il Responsabile della gestione documentale (o suo delegato) tiene traccia delle richieste di prelievo dei fascicoli dall'archivio di deposito in un apposito registro di carico e scarico. Il registro riporta, oltre ai dati identificativi del fascicolo, l'unità organizzativa richiedente, il nominativo del richiedente, la motivazione, la data della richiesta, la data di evasione della richiesta, la data della effettiva restituzione ed eventuali note sulla documentazione consegnata.

## **11.7. Conservazione**

Il Responsabile della gestione documentale attua tutte le iniziative finalizzate alla corretta conservazione della documentazione, sia in ambito analogico che digitale.

Per la conservazione della documentazione analogica, il Responsabile della gestione documentale verifica che nei depositi d'archivio siano rispettati i criteri che garantiscano la sicurezza della documentazione (ordinamento, sicurezza dei locali con sistemi antincendio e antintrusione, il controllo di temperatura e umidità relativa, prevenzione dall'intrusione di agenti patogeni, ordinaria manutenzione e pulizia, spolveratura periodica), in collaborazione con i servizi preposti alle attività tecniche e ai servizi generali.

Il Responsabile della gestione documentale provvede anche ad attuare interventi di restauro, nei casi in cui si rendessero necessari.

Per la conservazione digitale il Responsabile della gestione documentale concorderà i criteri con il Responsabile della conservazione (art.21, 29 – 31, D.Lgs. 42/2004.)

## **CAPITOLO 12. II SISTEMA INFORMATICO**

Il sistema informatico è l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti (DPR 445/2000, art. 1 lettera r).

La gestione dei flussi documentali è un insieme di funzionalità che consentono di trattare e di organizzare la documentazione prodotta (in arrivo, in partenza e interna) delle amministrazioni. La AOO di Ateneo individua le misure di sicurezza da adottare secondo quanto stabilito dalle normative vigenti.

### **12.1. Obiettivi e Piani di sicurezza**

Obiettivo delle politiche di sicurezza adottate dall'Amministrazione è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.

Dette regole sono elaborate in sede di redazione ed approvazione del "Piano generale della sicurezza" che è il 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'Amministrazione.

Nel contesto del Piano generale della sicurezza va redatto un documento che descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.

### **12.2. Il modello organizzativo**

I servizi *di information and communication technology* per il supporto all'attività amministrativa e per le esigenze della didattica e della ricerca dell'Ateneo sono curati dal Servizio "Servizi ICT".

Nell'ambito della gestione documentale, l'Ateneo ha acquisito – secondo il modello *in house providing* – dal Consorzio Cineca l'applicativo "Titulus" con una soluzione di tipo *Software as a Service* (SaaS: le funzionalità del programma sono rese disponibili attraverso un sito web, il cui accesso è subordinato ad un processo di autenticazione informatica effettuato mediante il sistema centralizzato dell'Ateneo).

La conduzione operativa del sistema è curata direttamente dal Consorzio Cineca, a cui, in virtù di un'apposita convenzione, sono demandati gli oneri di installazione, manutenzione, gestione, aggiornamento, monitoraggio di tutte le componenti fisiche e logiche infrastrutturali di verifica della correttezza delle funzioni applicative e dell'integrità delle basi di dati in conformità a quanto previsto dalla normativa vigente in materia di sicurezza e di protezione dei dati e di continuità operativa.

### **12.3. Sicurezza del sistema informatico**

La sicurezza dei dati, delle informazioni e dei documenti informatici memorizzati (poi archiviati) nel sistema di gestione documentale è garantita dall'applicazione informatica adottata dall'Ateneo.

Il piano della sicurezza informatica relativo a formazione, gestione, trasmissione, interscambio, accesso, memorizzazione dei documenti informatici ivi compresa la gestione delle copie di sicurezza nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico descritto nell'Allegato 8 del D.lgs. 30 giugno 2003, n. 196 e successive modificazioni è predisposto e aggiornato annualmente dal Consorzio Cineca.

#### **12.3.1. Il sistema di gestione documentale**

Il sistema di gestione documentale è costituito dall'insieme delle tecnologie presenti presso il *data center* del Consorzio Cineca e da tutti i dispositivi e i programmi presenti presso le sedi dell'Ateneo che permettono l'utilizzo del sistema.

In particolare sono parte integrante dell'infrastruttura i cablaggi e gli apparati di rete presenti presso le sedi dell'Ateneo e necessari per la connettività verso il Consorzio Cineca per mezzo della rete GARR, i sistemi informatici e le componenti software sottese al sistema di autenticazione dell'Ateneo e tutte le postazioni di lavoro utilizzate dagli utenti del sistema di gestione documentale.

Le misure di sicurezza fisica e logica specifiche e le procedure comportamentali adottate per la protezione dell'infrastruttura del sistema di gestione documentale, delle informazioni e dei dati sono riportate nei paragrafi seguenti. In essi è data evidenza di quali ambiti sono gestiti e curati dal Consorzio Cineca, e quali invece sono curati dal Servizio "Servizi ITC" dell'Ateneo.

Per tutto quello che si riferisce all'attivazione e alla gestione del registro di emergenza si rimanda a quanto descritto al paragrafo 6.9.

#### **12.3.2 Sicurezza fisica dei data center**

Le misure adottate per garantire un adeguato livello di sicurezza fisica del *data center* del Consorzio Cineca sono descritte nell'allegato tecnico *Servizio di Hosting* della Convenzione. Esso illustra le misure per la protezione fisica dei locali tecnici finalizzate a garantire l'integrità e la disponibilità degli apparati di rete, dei server e delle applicazioni, nonché le misure adottate per la protezione dei dati e le caratteristiche del servizio di *Disaster Recovery* per il quale è dichiarato un punto di ripristino (*Restore Point Objective – RPO*) pari a 24 H.

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

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

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

Eventuali interventi di qualsiasi natura (anche non informatica) nei locali ospitanti gli apparati server e apparati di rete avvengono sempre in maniera coordinata tra Servizio ICT e Settore Acquisizioni Edilizia e Sicurezza.

### **12.3.3. La manutenzione e la continuità operativa degli impianti elettrici**

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

### **12.3.4. Rete dati**

L'utilizzo del sistema di gestione documentale è garantito dalla rete dati di Ateneo e dalla rete GARR.

L'accesso alla rete dati di Ateneo è effettuato in conformità alle regole definite nella *Acceptable Use Policy – AUP* stabilite dal *Consortium* GARR.

Il servizio "Servizi ICT", in qualità di amministratore della rete di Ateneo, assicura in modo coordinato con il Settore Acquisizione Edilizia e sicurezza la gestione, il monitoraggio, l'aggiornamento e l'ampliamento della rete dati di Ateneo (cablaggio e parte attiva), sia sotto l'aspetto fisico che logico, fino alla presa utente compresa.

L'amministratore della rete di Ateneo – registra – in appositi *file* di *log* – i dati relativi all'accesso alla rete universitaria e all'accesso ad internet o al traffico telematico in generale (escluso il contenuto della trasmissione dati). I dati registrati nei *file* di *log* sono raccolti, memorizzati e conservati in conformità alla normativa vigente. Le informazioni contenute nei *file* di *log* possono essere messe a disposizione dell'autorità giudiziaria, la quale può richiedere la non cancellazione e la conservazione per un periodo più lungo di quanto disposto dalla legge.

Ciascun utente è responsabile dei dispositivi collegati alla rete di Ateneo e utilizzati dallo stesso per l'accesso al sistema di gestione documentale e deve riferirsi all'amministratore della rete di Ateneo per ogni violazione o sospetto di violazione della sicurezza informatica. Inoltre, ogni AOO opera secondo le direttive e le procedure stabilite dall'amministratore della rete, nel rispetto delle norme previste dall'Ateneo, garantendone altresì il rispetto, per

quanto di propria competenza, da parte dell'utenza gestita e adottando tempestivamente i provvedimenti previsti.

### 12.3.5. Le postazioni di lavoro

La gestione e la manutenzione delle postazioni di lavoro per l'utilizzo del sistema di gestione documentale è competenza del servizio "Servizi ICT".

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

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

- Il sistema operativo è aggiornato e aggiornabile;
- Gli applicativi installati e i loro componenti software aggiuntivi (ad es. *plug-in*) sono aggiornati e aggiornabili;
- Sono dotate di un programma antivirus con funzionalità automatica di aggiornamento periodico;
- L'accesso al sistema operativo della postazione di lavoro è protetto da *password* di adeguata complessità, che deve essere cambiata con cadenza regolare;
- Salvo motivate e documentate eccezioni, sulle postazioni di lavoro non è permessa la connessione remota dall'esterno della rete di dati di Ateneo (*RDP, SSH, VNC, ecc.*);
- La connessione da remoto alle postazioni di lavoro dall'interno della Rete dati dell'Ateneo, ove attivata, viene effettuata esclusivamente mediante protocolli di comunicazione sicuri ed è consentita solo previo consenso dell'utente che in quel momento sta utilizzando l'elaboratore.

### 12.4. Sicurezza dei documenti informatici

L'accesso al sistema di gestione documentale di ogni utente di tutte le AOO dell'Ateneo è gestito centralmente ed è subordinato all'abilitazione a cura del Responsabile della gestione documentale. Le identità digitali utilizzate per l'accesso al sistema di gestione documentale sono costituite da *nome utente* e *password*. L'identificazione informatica dell'utente, cioè la validazione dell'identità digitale, è operata attraverso una infrastruttura e autenticazione centralizzata (IDP).

L'accesso al sistema di gestione documentale da parte di soggetti esterni all'Ateneo non è consentito.

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

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

- *Titolare del trattamento* – è il destinatario delle norme, ossia la persona fisica e/o giuridica, l'amministrazione pubblica o altro ente a cui compete decidere finalità, modalità del trattamento dei dati personali e gli strumenti utilizzati, compresa la sicurezza;

- *Responsabile del trattamento* – La persona fisica, giuridica, l'amministrazione pubblica o altro ente designato, facoltativamente, dal titolare a trattare i dati compreso il profilo relativo alla sicurezza:
  - I Direttori dei Dipartimenti, Centri servizi, Centri speciali, Scuole;
  - Il Direttore Generale per gli Uffici di staff;
  - I Dirigenti per le Aree dirigenziali dell'Amministrazione centrale;
  - I Responsabili della gestione documentale di ogni AOO.
- Responsabile esterno del trattamento in coerenza con il modello organizzativo adottato dall'Ateneo per la conduzione del Sistema di gestione documentale, al Consorzio Cineca è conferito il ruolo di responsabile esterno del trattamento; in virtù di tale ruolo è il Consorzio che, per le attività di conduzione del sistema, gestione applicativa e assistenza, provvede alla nomina dell'amministratore di sistema, ne assolve i compiti e i conseguenti adempimenti.
- *Incaricato del trattamento* – la persona fisica autorizzata a compiere operazioni di trattamento dati dal Titolare o dal Responsabile.

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

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

#### **12.4.1. Accesso ai dati e ai documenti informatici**

Il sistema adottato dall'Ateneo garantisce:

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

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

- *Inserimento* dei dati per effettuare una registrazione;
- *Modifica* dei dati di una registrazione;
- *Annullamento* di una registrazione;
- *Ricerca* di informazioni registrate ai fini della visualizzazione o consultazione;
- *Visualizzazione* o consultazione;
- *Download* dei documenti associati alla registrazione.

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

Quando l'accesso ai dati e agli strumenti informatici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, in caso di prolungata assenza o impedimento dell'incaricato l'accesso ai dati è assicurato mediante l'organizzazione interna alla UOR che necessariamente prevede la ridondanza di operatori incaricati sulle medesime procedure.

Le stesse credenziali non possono essere assegnate a persone diverse, neppure in tempi diversi, quindi le credenziali sono strettamente personali.

Ciascun utente ha la possibilità di cambiare la propria *password* in qualsiasi momento ed il titolare è tenuto a comunicare al Servizio ICT lo smarrimento delle stesse.

#### **12.4.2. Le procedure comportamentali ai fini della protezione dei documenti.**

Le postazioni di lavoro, da tavolo o portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà dell'Ateneo a vario titolo messi a disposizione del personale, sono uno strumento di lavoro e il loro utilizzo è finalizzato allo svolgimento delle attività professionali e istituzionali dell'Ateneo. Ogni utente adotta comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza dei sistemi informativi.

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

Gli utenti a cui sono affidate le postazioni di lavoro dell'Ateneo, sono soggetti a tutte le responsabilità dettate dalla normativa vigente e applicabile. Si sottolineano le seguenti responsabilità:

- L'utente è responsabile per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui ha accesso: qualora sulle postazioni di lavoro siano memorizzati dati sensibili o giudiziari, il responsabile della postazione stessa deve attuare le misure idonee previste dall'Allegato B al D.Lgs. 30 giugno 2003, n.196;
- L'utente è tenuto a segnalare immediatamente ai referenti informatici ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
- In caso di cessazione del rapporto di lavoro, l'utente deve restituire all'Ateneo qualsiasi risorsa informatica assegnata e mettere a disposizione ogni informazione di interesse istituzionale;

Sulle postazioni di lavoro non è ammesso:

- Installare programmi per elaboratore tutelati ai sensi della convenzione sulla protezione delle opere letterarie e artistiche, nonché le banche dati che, per la scelta o per la disposizione del materiale, costituiscono una creazione intellettuale dell'autore se non in possesso delle relative licenze d'uso;
- Installare modem per l'accesso da o verso l'esterno della rete dell'Ateneo, se non preventivamente autorizzati;
- Utilizzare dispositivi mobili quali punti di accesso da/all'esterno la rete dell'Ateneo, se non preventivamente autorizzati;
- Installare programmi non inerenti all'attività lavorativa e/o privi di licenze d'uso;
- Copiare dati la cui titolarità è dell'Università degli Studi di Bergamo su dispositivi esterni personali.

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

L'utente è tenuto a bloccare o a spegnere il *personal computer* in caso di sospensione o di termine dell'attività lavorativa, assicurandosi di evitare l'utilizzo improprio da parte di terzi, mediante inserimento di apposite credenziali di accesso. Le stazioni di lavoro, da tavolo o portatili, o gli strumenti comunque funzionalmente assimilabili, messe a disposizione del personale, non devono essere lasciati incustoditi. Al termine dell'orario di servizio, i *computer* devono essere spenti prima di lasciare gli uffici, in caso di allontanamento temporaneo, l'utente deve attivare il salvaschermo con sblocco tramite *password*.

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

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

## **12.5. Il sistema informatico (software, produzione e conservazione delle registrazioni sul Prodotto di Protocollo)**

È compito del RSI provvedere al salvataggio dei dati (backup), alla loro verifica, al trasferimento su supporto rimovibile ed all'eventuale ripristino in caso di caduta del sistema.

Le modalità di gestione di tali supporti sono definite e regolamentate direttamente dal RSI.

I dati contenuti su tali supporti sono conservati con le modalità previste dalla normativa vigente.

## **12.6. Il sistema degli accessi**

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (nome utente e password) ed un sistema di autorizzazione basato sulla profilazione degli utenti.

Le password di accesso al sistema di protocollo, conformemente alla legge 196/2003 dovranno avere le seguenti caratteristiche:

- lunghezza non inferiore ad otto caratteri;
- durata non superiore a sei mesi per gli utenti che trattano dati personali;
- durata non superiore a tre mesi per gli utenti che trattano dati sensibili e/o giudiziari;
- scadenza dopo un periodo di inutilizzo prolungato.

La profilazione preventiva adottata dall'Università degli Studi di Bergamo (vedi tabella allegata) definisce delle classi di utenti e consente di definire le abilitazioni che possono essere rilasciate ad un utente del servizio di protocollo e gestione documentale.

Ciascun utente del SdP può accedere solamente ai documenti che sono stati assegnati a lui, e/o al suo ufficio ed agli uffici ad esso subordinato.

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

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di protocollo esclusivamente secondo modalità prestabilite.

Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).

Gli utenti del servizio di protocollo, in base agli UU di appartenenza, ovvero in base alle rispettive competenze (UOP, UOR, UU) hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza.

Ad ogni utente è assegnata:

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

I diversi livelli di autorizzazione sono assegnati agli utenti dal RSP, che si avvale di un utente così detto privilegiato (amministratore).

Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione degli UU e del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'AOO, sono costantemente aggiornate a cura del Responsabile Servizio Protocollo.