

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO

Entrato in vigore il 01/10/2021

Terza versione: adeguato al Reg. UE 679/2016 – cd GDPR secondo le indicazioni fornite dal DPO/RPD

Sommario

CAPITOLO 1. IL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO.....	7
1.1. Che cos'è, a cosa serve e a chi serve	7
1.2. Modalità di redazione.....	7
1.3. Forme di pubblicità e di divulgazione	7
CAPITOLO 2. QUADRO ORGANIZZATIVO ISTITUZIONALE	7
2.1. Area organizzativa omogenea e unità organizzativa responsabile	7
2.2. Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti.....	8
2.3. Il Responsabile della gestione documentale	9
2.4. Profili di abilitazioni di accesso interno ed esterno alle informazioni documentali.....	9
2.5. Posta elettronica istituzionale	9
2.6. PEC istituzionale	9
2.7. Piano di eliminazione dei registri di protocollo diversi dal protocollo informatico	10
2.8. Responsabile della conservazione	10
CAPITOLO 3. IL DOCUMENTO.....	10
3.1. Documento informatico e analogico: definizione e disciplina giuridica	10
3.2. Redazione/formazione del documento informatico	12
3.2.1. Validazione temporale	12
3.2.2. Formati	13
3.3. Redazione/formazione del documento amministrativo informatico.....	13
3.4. Redazione/formazione del documento amministrativo analogico	14
3.5. Documenti redatti in originale su supporto analogico	15
3.6. Il documento amministrativo informatico costituito dal corpo della PEC istituzionale	15
3.7. Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale	15
3.8. Distinzione dei documenti in base allo stato di trasmissione (arrivo, partenza, scambiati tra UOR, scambiati tra AOO dello stesso ente, fax, PEC, e-mail).....	16
3.9. Duplicato del documento informatico e analogico	16
3.10. Copia del documento informatico e analogico: nozione.....	17
3.11. Copia informatica del documento amministrativo analogico	17
3.12. Estratto informatico di documento amministrativo informatico	18
3.13. Copia analogica di documento amministrativo informatico	18
3.14. Metadati	18
3.14.1. Obiettivi dei metadati archivistici.....	19
3.14.2. Metadati essenziali per la registrazione nel protocollo informatico.....	19

CAPITOLO 4. IL FASCICOLO.....	19
4.1. Il fascicolo: definizione e funzione	19
4.2. Il fascicolo analogico: formazione, implementazione e gestione.....	20
4.3. Il fascicolo informatico: formazione, implementazione e gestione	21
4.4. I fascicoli annuali ripetitivi	22
4.5. Il fascicolo ibrido.....	22
4.6. Metadati del fascicolo informatico.....	22
4.7. Il repertorio dei fascicoli informatici	23
4.8. Raccoglitore	23
CAPITOLO 5. LA GESTIONE DELL'ARCHIVIO CORRENTE.....	23
5.1. Definizione.....	23
5.2. Buone prassi per la gestione dell'archivio corrente	24
5.3. Gli strumenti dell'archivio corrente.....	25
5.3.1. Registro di protocollo	25
5.3.2. Titolario (piano di classificazione)	25
5.3.3. Repertorio dei fascicoli.....	26
5.3.4. Repertori	26
5.3.5. Massimario di selezione	26
5.4. Spostamento di un archivio corrente analogico.....	27
CAPITOLO 6. IL PROTOCOLLO INFORMATICO.....	27
6.1. Registratura	27
6.1.1. Elementi obbligatori immodificabili (Registratura).....	28
6.1.2. Elementi obbligatori modificabili	28
6.1.3. Elementi non obbligatori modificabili	28
6.2. Data e ora regolate sul UTC	28
6.3. Segnatura.....	29
6.3.1. Per il documento informatico	29
6.3.2. Per il documento analogico.....	29
6.3.3. Ragioni della scelta di un timbro meccanico.....	30
6.4. Modalità di produzione e di conservazione delle registrazioni.....	30
6.5. La registrazione differita (o "protocollo differito")	31
6.6. La ricevuta di avvenuta registrazione	31
6.6.1. Per il documento analogico.....	31
6.6.2. Per il documento informatico	31
6.7. Documenti esclusi dalla registrazione di protocollo	32

6.8. Il registro giornaliero di protocollo.....	32
6.9. Il registro di emergenza.....	33
CAPITOLO 7. REGISTRI E REPERTORI INFORMATICI	33
7.1. Repertorio - Nozione	33
7.2. Repertori attivi.....	34
7.3. Repertorio dei fascicoli.....	34
CAPITOLO 8. FLUSSO DI LAVORAZIONE DEI DOCUMENTI	34
8.1. Flusso del documento informatico in arrivo.....	34
8.2. Ricezione di documenti informatici nella casella di posta elettronica istituzionale.....	34
8.3. Ricezione dei documenti informatici tramite la casella di posta elettronica certificata (PEC) istituzionale	35
8.4. Ricezione di documenti informatici su supporti rimovibili.....	35
8.4.1. Documenti informatici prodotti da banche dati dell'Ateneo o prodotti da banche dati di terzi	36
8.5. Priorità nella registrazione dei documenti informatici in arrivo	36
8.6. Flusso del documento analogico	36
8.7. Apertura delle buste.....	37
8.7.1. Conservazione ed eliminazione delle buste	37
8.8. Priorità nella registrazione dei documenti analogici in arrivo.....	37
8.9. Protocollo particolare/riservato	38
8.9.1. Procedure del protocollo particolare/riservato	38
8.10. L'archivio particolare/riservato	38
8.11. Annullamento di una registrazione	38
8.12. Corresponsabilità di un documento e di un fascicolo	39
8.13. Documenti scambiati tra uffici non soggetti a registrazione di protocollo	39
8.14. Casi di rigetto.....	40
8.15. Flusso del documento informatico in partenza.....	40
8.16. Flusso del documento informatico tra UOR della stessa AOO	41
8.17. Flusso del documento informatico tra AOO dell'Ateneo	41
8.18. Utilizzo delle firme elettroniche: firma elettronica semplice, firma elettronica avanzata, firma elettronica qualificata, firma digitale	41
CAPITOLO 9. CASISTICA E COMPORTAMENTI.....	42
9.1. Gestione delle gare d'appalto	42
9.1.1. Gare e procedure negoziate gestite in modalità analogica.....	42
9.1.2. Gare e procedure negoziate gestite in modalità telematica	42
9.2. Gestione di concorsi e selezioni.....	42

9.3. Atti e comunicazioni giudiziarie.....	43
9.4. Documenti informatici con oggetto multiplo	44
9.5. Fatture elettroniche (Fattura PA)	44
9.6. DURC on-line.....	45
9.7. Denunce di infortuni.....	45
9.8. Certificati di malattia	46
9.9. Documenti del portale degli acquisti della pubblica amministrazione	46
9.9.1. Affidamenti diretti sulla piattaforma MePA (OdA)	46
9.9.2. Adesioni – Convenzioni (OdA).....	47
9.9.3. Procedure negoziate (RdO) - MePA	47
9.10. Documenti pervenuti via PEC	48
9.11. Gestione di due documenti diversi trasmessi via PEC	48
9.12. Gestione di soli allegati pervenuti via PEC e di documenti costituiti dal solo corpo della PEC	48
9.13. Documenti pervenuti a mezzo <i>e- mail</i> semplice (non certificata)	48
9.13.1. Rapporti con terzi esterni.....	48
9.13.2. Rapporti tra diverse UOR	49
9.14. Gestione del secondo esemplare	49
9.15. Documenti anonimi	49
9.16. Documenti scambiati tra UOR della stessa AOO	50
CAPITOLO 10. ALBO ON-LINE	50
CAPITOLO 11. DALL’ARCHIVIO CORRENTE ALL’ARCHIVIO DI DEPOSITO	50
11.1 Archivio corrente	50
11.2 Archivio di deposito analogico	50
11.3 Trasferimento dei fascicoli cartacei all’archivio di deposito	50
11.4 Trasferimento dei fascicoli informatici.....	51
11.5. Trasferimento delle serie archivistiche	51
11.6 Ordinamento archivistico	52
11.7. Elenco di consistenza per l’archivio di deposito analogico	52
11.8. Servizio di ricerca documentale e movimentazione dei fascicoli (<i>record delivery</i>).....	52
11.9. Conservazione	53
CAPITOLO 12. SISTEMA INFORMATICO	53
12.1. Il modello organizzativo.....	53
12.2. Sicurezza del sistema informatico	54
12.2.1. Il sistema di gestione documentale	54
12.2.2. Sicurezza fisica dei data center	54

12.2.3. La manutenzione e la continuità operativa degli impianti elettrici	55
12.2.4. Rete dati	55
12.2.5. Le postazioni di lavoro	55
12.3. Sicurezza dei documenti informatici	56
12.3.1. Accesso ai dati e ai documenti informatici	56
12.3.2. Le procedure comportamentali ai fini della protezione dei documenti	57

Allegato n. 1 -Riferimenti normativi

Allegato n. 2 - Passaggio ad Area Organizzativa Omogenea unica di Ateneo

Allegato n. 3 - Nomina del responsabile della gestione documentale

Allegato n. 4 - Nomina responsabile della conservazione

Allegato n. 5 - Linee guida per l'utilizzo del servizio di posta elettronica

Allegato n. 6 - Linee guida per l'utilizzo delle caselle PEC e loro elenco

Allegato n. 7 - Titolario di classificazione unico in vigore dal 1° marzo 2014

Allegato n. 8 - Elenco repertori

Allegato n. 9 - Regolamento per la pubblicazione dei documenti all'albo on line di ateneo

Allegato n. 10 – Acceptable Use Policy

CAPITOLO 1. IL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO

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

Il manuale di gestione è uno strumento operativo che descrive il sistema di produzione e di gestione documenti (tradizionali e digitali), come previsto dall'art. 3 e dall'art. 5 del DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del Codice dell'Amministrazione digitale di cui al decreto legislativo n.82 del 2005".

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. Modalità di redazione

La redazione del manuale di gestione deve contemperare l'assolvimento dell'obbligo normativo e le esigenze concrete dell'Amministrazione (cfr. **l'Appendice normativa descritta nell'allegato 1**).

Per tale motivo è stato redatto previa verifica e analisi del modello organizzativo e delle procedure amministrative. Nell'Università degli Studi di Brescia le procedure e i processi più rilevanti sono stati descritti nel Manuale delle procedure, pubblicato sul portale istituzionale di Ateneo (www.unibs.it) nella sezione "Statuto e Regolamenti".

Per la redazione di questo Manuale è stato utilizzato il modello proposto dal Gruppo di lavoro nell'ambito del progetto Procedamus per gli atenei aderenti (www.procedamus.it).

1.3. Forme di pubblicità e di divulgazione

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

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

CAPITOLO 2. QUADRO ORGANIZZATIVO ISTITUZIONALE

2.1. 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 nel Funzionigramma e Organigramma generale, pubblicati sul sito istituzionale di Ateneo nella sezione "Ateneo/Amministrazione/Unità Organizzative", come previsto dalla legge 7 agosto 1990, n. 241 (artt. 4-6), dal DPR 28 dicembre 2000, n. 445 e dal DPCM 3 dicembre 2013, art. 3, comma 1, lett.a.

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

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

Nell'Università degli Studi di Brescia è istituita la U.O.C. Flussi Documentali 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.

Alla U.O.C. 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.

L'Ateneo è organizzato in A.O.O. unica a far data dal 1 luglio 2019, con Disposizione del Direttore Generale repertorio 260/2019 prot. n.153492 del 11/06/2019, come descritto **nell'allegato 2**. ha un proprio servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi e un responsabile della gestione documentale, individuato tra il personale in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.

Con Disposizione del Direttore generale repertorio 349/2019 prot. n. 204941 del 24/07/2019, è stato individuato il Responsabile della gestione documentale e il rispettivo vicario, come previsto dal DPCM 3 dicembre 2013, art. 3, lett. b) e c) e come descritto **nell'allegato 3**.

La U.O.C. Flussi Documentali 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. In particolare il servizio cura:

- il livello di autorizzazione (*Acces Control List* - ACL) per l'accesso al sistema di gestione documentale – protocollo informatico - degli utenti secondo i profili distinti in ruoli abilitati alla mera consultazione, inserimento o modifica delle informazioni, sulla base delle richieste provenienti dal Responsabile UOR. In tal caso il Responsabile di UOR invierà richiesta al Responsabile della gestione documentale scrivendo un messaggio all'indirizzo mail istituzionale della U.O.C. Flussi documentali;
- la correttezza delle operazioni di registrazione, segnatura, gestione dei documenti e dei flussi documentali;
- notifica ai Responsabili delle UOR di Ateneo l'eventuale indisponibilità del sistema e l'attivazione del registro di emergenza secondo quanto disposto al § 6.9;
- le autorizzazioni di annullamento delle registrazioni di protocollo;
- l'adeguamento del sistema di gestione documentale alle eventuali modifiche dell'organigramma e funzionigramma dell'Ateneo.

2.3. Il Responsabile della gestione documentale

È compito del Responsabile della gestione documentale:

- definire e assicurare criteri uniformi di trattamento dei documenti e di classificazione e archiviazione;
- predisporre e mantenere aggiornato il manuale di gestione;
- predisporre, di concerto con il Responsabile della Conservazione, il Responsabile dei sistemi informativi, il Responsabile della Protezione dei Dati (RPD) e gli eventuali Referenti di Dipartimento, il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici secondo quanto dettagliato al capitolo 12;
- produrre, insieme al Responsabile della Conservazione, il pacchetto di versamento e assicurare il trasferimento del suo contenuto al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione predisposto dal Responsabile della Conservazione.

Il Responsabile della gestione documentale è coadiuvato dal referente dei sistemi informatici documentali e della sicurezza informatica e dal referente della protezione dei dati personali relativamente al sistema documentale come previsto dal D.Lgs. 7 marzo 2005, n. 82.

2.4. 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.

2.5. 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.

L'utilizzo della casella istituzionale di posta elettronica è regolamentato da linee guida descritte nell'allegato 5.

2.6. PEC istituzionale

L'Università degli Studi di Brescia ha attivato le caselle di PEC per l'Amministrazione Centrale, i Dipartimenti di Ateneo e la "Facoltà di Medicina" e le caselle di posta elettronica certificata per la gestione della fatturazione elettronica.

L'utilizzo delle PEC dell'Ateneo sono regolate da linee guida cui all'allegato 6 il quale riporta elenco di tali caselle e loro modalità di utilizzo.

2.7. Piano di eliminazione dei registri di protocollo diversi dal protocollo informatico

Il registro di protocollo dell'Ateneo è unico.

A far data dal 31 marzo 2014 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.

2.8. Responsabile della conservazione

Il sistema di conservazione opera secondo modelli organizzativi espliciti, definiti e distinti dal sistema di gestione documentale.

Qualora la conservazione sia svolta all'esterno dell'Ateneo, all'interno della struttura organizzativa è nominato un Responsabile della conservazione che fornisce le indicazioni utili alla definizione delle politiche del sistema di conservazione e alla predisposizione del manuale di conservazione.

Il Responsabile della conservazione opera d'intesa con il Responsabile dei sistemi informativi, il Responsabile della Protezione dei Dati (RPD) e gli eventuali Referenti di Dipartimento oltre che con il Responsabile della gestione documentale.

Con Disposizione del Direttore Generale 5 giugno 2014, prot. n. 14006, è stato nominato il Responsabile della conservazione (allegato 4).

CAPITOLO 3. IL DOCUMENTO

3.1. Documento informatico e analogico: definizione e disciplina giuridica

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

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

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

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

L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono valutabili in giudizio tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immutabilità. Il documento informatico assume la caratteristica di immutabilità se prodotto in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

Il documento informatico può essere sottoscritto con firma elettronica, avanzata, qualificata o digitale: il tipo di firma utilizzata differenzia il valore giuridico del documento, secondo le norme previste dalla legge.

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

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

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

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

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

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

Se stipulate sotto forma di documento informatico, devono essere sottoscritte a pena di nullità, salvo i casi di firma autenticata, con firma elettronica qualificata, con firma elettronica qualificata o digitale le scritture private relative ai seguenti tipi di contratti:

- i contratti che trasferiscono la proprietà di beni immobili;
- i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta;
- i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti;
- i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione;
- gli atti di rinuncia ai diritti indicati dai numeri precedenti;
- i contratti di affrancazione del fondo enfiteutico;
- i contratti di anticresi;
- i contratti di locazione di beni immobili per una durata superiore a nove anni;
- i contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato;
- gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite dello Stato;
- gli atti di divisione di beni immobili e di altri diritti reali immobiliari;
- le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti;

- contratti di locazioni e di comodato immobiliare.

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

3.2. Redazione/formazione del documento informatico

Il documento informatico è formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software: in tal caso il documento informatico assume le caratteristiche di immodificabilità e di integrità con la sottoscrizione con firma digitale/firma elettronica qualificata o con l'apposizione di una validazione temporale o con il trasferimento a soggetti terzi con PEC con ricevuta completa o con la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza o con il versamento ad un sistema di conservazione;
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

3.2.1. Validazione temporale

Costituiscono validazione temporale:

- i riferimenti temporali realizzati dai certificatori accreditati mediante marche temporali;
- i riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato secondo la scala di tempo UTC (IT) (INRIM) con una differenza non superiore ad un minuto primo;

- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata;
- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica.

3.2.2. 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;
- Suoni = Mp3;
- Video = Avi;
- 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 dello stesso.

3.3. Redazione/formazione del documento amministrativo informatico

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

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

Le amministrazioni pubbliche formano gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici, di cui al § 3.1 ovvero acquisendo le istanze, le dichiarazioni e le comunicazioni previste dalla legge. Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria e originale da cui è possibile effettuare duplicazioni e copie.

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

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità oltre che nei modi di cui al § 3.2 anche con la registrazione nel registro di protocollo unico per ciascuna Area organizzativa omogenea (AOO), nei repertori, negli albi, contenuti nel sistema di gestione documentale.

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

- AOO/ UOR;
- Data di sottoscrizione;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (indicare 0 zero se non presenti);
- Oggetto;
- Destinatario;
- Testo;
- Iniziali di redattore/responsabile;
- Sottoscrizione;
- Elementi identificativi del responsabile del procedimento.

Il documento è sottoscritto prima di essere protocollato. Le informazioni relative alla classificazione atte a identificare il fascicolo di competenza, la data di sottoscrizione, il numero di allegati sono inserite prima della sottoscrizione del documento. Di norma, la data di sottoscrizione e la data di protocollazione coincidono.

3.4. Redazione/formazione del documento amministrativo analogico

Per documento analogico si intende un documento formato utilizzando una grandezza fisica (ad es., le tracce su carta, le immagini contenute nei film e le magnetizzazioni 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. L'originale analogico è il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali (sigillo, carta intestata, formulario amministrativo) e sostanziali, comprendente tutti gli elementi di garanzia e di informazione, del mittente e del destinatario e dotato di firma autografa.

I documenti analogici dotati di firma autografa aventi per destinatario un ente o un soggetto terzi, sono di norma redatti in due esemplari, un originale per il destinatario e una minuta da conservare agli atti nel fascicolo corrispondente.

Si definisce *minuta* l'esemplare del documento corredato di sigle, firma e sottoscrizione autografe, conservato agli atti dell'Ateneo, cioè nel fascicolo relativo al procedimento amministrativo o all'affare trattato.

Il documento amministrativo analogico in uscita è redatto su carta intestata e deve, di norma, contenere la denominazione dell'Ateneo e l'indicazione di

- AOO/ UOR;
- Data;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (indicare 0 zero se non presenti);
- Oggetto;
- Destinatario;
- Testo;
- Sottoscrizione;
- Sigla eventuali istruttori;

- Elementi identificativi del responsabile del procedimento.

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

3.5. Documenti redatti in originale su supporto analogico

Ai sensi del DPCM 21 marzo 2013, per particolari tipologie di documenti analogici originali unici, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato. Per documenti originali unici si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta (ad es., i verbali di una riunione o di un'assemblea).

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

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

La posta elettronica certificata costituisce un mezzo di trasmissione che consente lo scambio di comunicazioni e documenti la cui trasmissione e ricezione sono giuridicamente rilevanti. Tale modalità di trasmissione dei documenti viene utilizzata nei casi in cui è necessario avere prova opponibile dell'invio e della consegna del messaggio di posta.

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

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

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

Di norma, si dovrebbe usare la PEC per trasmettere e/o ricevere un documento informatico, ma può accadere che la comunicazione/istanza ricevuta sia costituita dal mero corpo della *e-mail*. In questo caso si procede alla registrazione del messaggio in arrivo nel sistema di gestione documentale solo se il contenuto è rilevante al fine giuridico-probatorio.

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

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

Le *e-mail* inviate da una casella istituzionale dell'Università degli Studi di Brescia sono considerate sottoscritte con firma elettronica semplice e sono soggette a protocollazione solo se il contenuto è rilevante al fine giuridico-probatorio. In questo caso si procede alla conversione dell'*e-mail* in formato pdf/a prima di provvedere alla sua registrazione. Trattandosi di un documento informatico nativo non si procederà alla stampa e apposizione tramite timbro della segnatura prima della registrazione a protocollo.

3.8. Distinzione dei documenti in base allo stato di trasmissione (arrivo, partenza, scambiati tra UOR, scambiati tra AOO dello stesso ente, fax, PEC, e-mail)

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

- documenti in arrivo;
- documenti in partenza;
- documenti interni (scambiati tra UOR);

I documenti scambiati tra AOO dell'Ateneo sono documento in arrivo e in partenza.

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

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

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

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

Per documenti scambiati tra AOO dello stesso Ente si intendono documenti di preminente carattere giuridico probatorio sottoposti alla protocollazione in partenza per la AOO mittente, e alla protocollazione in arrivo per la AOO ricevente.

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale – PEC – accessibile all'Unità Organizzativa responsabile della protocollazione in arrivo per la AOO di appartenenza.

Il documento informatico trasmesso tramite casella di posta elettronica certificata – PEC si intende spedito dal mittente se inviato al proprio gestore e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

3.9. Duplicato del documento informatico e analogico

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

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

Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originali (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro

perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

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

3.10. Copia del documento informatico e analogico: nozione

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

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

La copia di un documento analogico è la trascrizione o riproduzione dell'originale. Si distingue in copia semplice, imitativa e conforme. La copia semplice è la pura trascrizione dell'originale senza riguardo agli elementi formali. La copia imitativa riproduce sia il contenuto che la forma (es. fotocopia). La copia conforme è la copia certificata come conforme all'originale da un pubblico ufficiale autorizzato ad eseguire tale attestazione nell'esercizio delle sue funzioni (copia "autentica").

3.11. Copia informatica del documento amministrativo analogico

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

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

Per copia informatica di un documento analogico si intende:

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

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

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

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

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

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

3.12. Estratto informatico di documento amministrativo informatico

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

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

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

3.13. Copia analogica di documento amministrativo informatico

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

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

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 metadati può essere associato a tre categorie funzionali:

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

3.14.1. Obiettivi dei metadati archivistici

Gli obiettivi dei metadati archivistici sono:

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

3.14.2. Metadati essenziali per la registrazione nel protocollo informatico

Gli elementi essenziali minimi sono i seguenti:

- Identificativo;
- denominazione / codice unico che individua l'Ateneo;
- corrispondente (mittente/destinatari);
- oggetto;
- numero degli allegati e descrizione degli stessi;
- numero di protocollo;
- data di registrazione a protocollo;
- indicazione dell'Unità organizzativa responsabile (UOR);
- impronta che lega il documento digitale ai metadati sopra indicati

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 titolario (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 cronologico 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 previsto 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 a 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 di 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; classe 3; 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 presentate al § 11.2.

4.3. Il fascicolo informatico: formazione, implementazione e gestione

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 a 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 costituire 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 di 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 e 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: facoltà, dipartimenti, centri, ecc...); 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 delle delibere 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 all'emanazione delle delibere.

4.4. I fascicoli annuali ripetitivi

È 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 fascicolo 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 descriverne 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 rispettano la codifica di caratteri ISO-8859-1.

I metadati minimi del fascicolo informatico sono:

- identificativo univoco e persistente rappresentato da una sequenza di caratteri
- 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 libero accesso, da parte delle sole UOR che hanno la titolarità dei documenti, attraverso il sistema di gestione documentale.

5.2. Buone 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 § 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 1, 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 parte di propria responsabilità e competenza nel trattamento dell'affare, fino al momento del loro trasferimento nell'archivio di deposito.

I documenti creati nel corso dell'attività d'ufficio sono soggetti a fascicolazione obbligatoria ai sensi del DPR 445/2000, art. 64, c. 4, indipendentemente dal 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 responsabile 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 es., 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 un'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, strettamente 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 d'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 1° 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, predisposto all'interno del progetto Procedamus e approvato (con nota prot.n. 218708 in data 14.12.2012) dalla Direzione Generale degli Archivi, Servizio II, Tutela e conservazione del

patrimonio archivistico, è unico e valido per tutte le AOO dell'Università degli Studi di Brescia ed è descritto **nell'allegato n. 7**.

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 tali 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 i quali i documenti, non rivestendo interesse storico ai fini della conservazione permanente e avendo esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della Soprintendenza archivistica, ai 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, è 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.

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, la U.O.C. Flussi Documentali 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 per territorio (in base al D.Lgs. 42/2004 art. 21 c.3).

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 o 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 ciascuna delle AOO dell'Università degli Studi di Brescia.

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

La registrazione di protocollo per ogni documento è effettuata mediante la memorizzazione di elementi obbligatori immutabili, elementi obbligatori modificabili ed elementi non obbligatori e modificabili.

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

6.1.1. Elementi obbligatori immutabili (Registratura)

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

Essi sono:

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

L'insieme di tali elementi è denominato *registratura*.

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

Quando il documento è indirizzato ad altre amministrazioni ed è sottoscritto con firma 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 in 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 in forma sintetica o estesa dell'amministrazione e dell'AOO individuata ai fini della registrazione e della gestione del documento;
- il numero progressivo di protocollo;
- la data di protocollo nel formato GGMMAAAA;
- la classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento;
- la sigla della UOR/RPA o 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).

6.3.3. Ragioni della scelta di un timbro meccanico

La segnatura su un documento cartaceo si appone mediante un timbro meccanico a inchiostro indelebile che riporta gli elementi normalizzati della registrazione, trascritti dall'operatore di protocollo a penna blu all'interno degli spazi predisposti.

Vanno evitati dispositivi di segnatura meccanizzati (esempio etichettatrici, *printpen*, *barcode* e simili) per la scarsa maneggevolezza e per la frequente necessità di integrare la segnatura con trascrizioni e aggiunte, che possono essere soltanto manuali.

Più in dettaglio, l'etichetta adesiva ha una colla la cui composizione chimica (acida o basica) provoca il danneggiamento irreversibile del supporto cartaceo, con la perdita delle informazioni. Col tempo, infatti, avviene il distacco dell'etichetta dal documento o un danneggiamento del documento (solitamente un foro).

La *printpen*, invece, obbliga l'operatore a intervenire per integrare gli scarni dati visto che questo strumento consente la contestuale segnatura della registrazione di norma solo per il codice struttura, data e numero di protocollo. Le informazioni di natura gestionale, titolo, classe, anno e numero del fascicolo, nonché le indicazioni di UOR, RPA e CC, non sono immediatamente consultabili in quanto non vengono riportate nella segnatura. Inoltre è poco immediata anche la lettura della data e del numero di protocollo. Nel caso del protocollo in arrivo differito la *printpen* non evidenzia le due date, cioè quella della registrazione e quella del differimento, bensì solo la prima. I successivi interventi sul cambio di UOR e/o aggiunte di altre UOR, persone fisiche o organi, in copia conoscenza non si evincono mai dai dati stampati con la *printpen*. L'utilizzo di *barcode*, oltre agli inconvenienti già elencati, non è di immediata intelligibilità, e necessita sempre di un dispositivo di lettura.

L'uso di un timbro meccanico, pertanto, consente di raccogliere in forma sintetica gli estremi utili e necessari alla gestione del documento, anche grazie a una chiara e immediata lettura delle informazioni relative al documento.

6.4. Modalità di produzione e di conservazione delle registrazioni

Ogni registrazione di protocollo informatico produce un *record* nel sistema di gestione documentale che viene accodato in una base dati accessibile esclusivamente all'amministratore del sistema. Ogni operazione di inserimento e modifica viene registrata inoltre 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/modifica/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”)

È 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 dalla U.O.C. Flussi Documentali 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 informatico è pervenuto tramite *e-mail*, la ricevuta, se richiesta, sarà generata in formato pdf o pdf/a e inviata via *e-mail* al mittente.

La U.O.C. Flussi Documentali non è autorizzata 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;
- le riviste;
- 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.

Sono esclusi su disposizione dell'Ateneo:

- le richieste di ferie;
- le richieste di permessi retribuiti;
- le comunicazioni da parte di enti diversi di bandi di concorso (fatta eccezione dei bandi di mobilità di altri enti universitari o di bandi di consorzi interuniversitari che vengono pubblicati all'albo on line);
- i DURC.

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, imm modificabile e integra.

Attualmente, in base allo stato dell'arte delle tecnologie e dei formati, è utilizzato il formato XML, a mente del DPCM 3 dicembre 2013.

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 provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

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

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

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

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 § 6.4.

CAPITOLO 7. REGISTRI E REPERTORI INFORMATICI

7.1. Repertorio - Nozione

Per repertorio si intende il registro in cui sono annotati con numerazione progressiva i documenti per i quali è prevista la registrazione particolare. I documenti sono inseriti nel fascicolo archivistico di loro pertinenza per la loro minuta e in originale (o in copia conforme) nel repertorio. Il complesso dei documenti registrati a repertorio per forma omogenea costituisce una serie.

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.

7.2. Repertori attivi

L'elenco dei repertori attivi in Titulus attivi presso l'Università degli Studi di Brescia è descritto nell'allegato 8.

7.3. Repertorio dei fascicoli

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

CAPITOLO 8. FLUSSO DI LAVORAZIONE DEI DOCUMENTI

8.1. Flusso del documento informatico in arrivo

La U.O.C. Flussi Documentali 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 della 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 menu 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;
- da 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 della U.O.C. Flussi Documentali;
- documento allegato alla e-mail istituzionale: con *PDF creator*¹³ si crea il PDF/a e lo si associa al sistema di gestione documentale procedendo alla registratura 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;
- 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 registratura 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 della U.O.C. Flussi Documentali, di norma, entro le 24 ore lavorative dal giorno di arrivo;

- documento che arriva alla casella di posta elettronica istituzionale di una UOR diversa dalla U.O.C. Flussi Documentali. La UOR ricevente gira l'*e-mail* con *forward* corredata degli eventuali allegati alla casella di posta elettronica istituzionale della U.O.C. Flussi Documentali 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 alla U.O.C. Flussi Documentali. Nel caso di e-mail da cui non sia possibile desumere l'indicazione di nome e cognome il documento sarà trattato come "Anonimo" (cfr. § 9.15);

È 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 della U.O.C. Flussi Documentali di norma 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 è tenuto ad inoltrare tempestivamente il messaggio e-mail ricevuto alla relativa PEC istituzionale di Ateneo ai fini della protocollazione.

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 immodificabile 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.

La U.O.C. Flussi Documentali verifica la leggibilità dei dati contenuti nel supporto informatico e provvede alla registrazione solo in caso di esito positivo. È cura della UOR responsabile verificarne le caratteristiche e la provenienza certa.

I documenti informatici così pervenuti sono protocollati, di norma, entro le 24 ore lavorative successive dal giorno di 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 di gestione carriere studenti – *ESSE3 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 a informare preventivamente la U.O.C. Flussi Documentali 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 nella registrazione dei documenti informatici in arrivo

Indipendente dal mezzo telematico di arrivo, 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 in formato elettronico provenienti da fornitori esteri).

È 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 alla U.O.C. Flussi Documentali 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 questa recapitata alla U.O.C. Flussi Documentali
- posta recapita personalmente, *brevi manu*;

8.7. Apertura

Tutte le buste vanno aperte a cura della U.O.C. Flussi Documentali; 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 vanno aperte 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 U.O.C. Flussi Documentali.

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 30 giorni. Trascorso tale termine sono eliminate senza formalità.

8.8. Priorità nella registrazione dei documenti analogici in arrivo

Indipendente 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 del frontespizio del documento col timbro del protocollo.

8.9. Protocollo particolare/riservato

Sono previste particolari forme di riservatezza e di accesso controllato al protocollo riservato 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 cd. *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 integrali sono consultabili presso".

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 col Responsabile della gestione documentale.

8.11. Annullamento di una registrazione

È consentito l'annullamento di una registrazione di protocollo per motivate e verificate 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 già stato 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 della U.O.C. Flussi Documentali, 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 documento non inerenti a specifici procedimenti, in un fascicolo annuale.

Se il documento analogico o informatico annullato 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 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 amministrativo 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 del fascicolo, spetta esclusivamente alla UOR che ha la competenza prevalente sul procedimento amministrativo e che la U.O.C. Flussi Documentali ha inserito per prima nella registrazione e prima riportata nella registrazione di protocollo.

Spetta pertanto alla prima UOR indicata 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;
- Richiesta di piccole manutenzioni;
- Richiesta di sopralluoghi ai servizi tecnici;
- Richieste di sopralluoghi archivistici;
- Richiesta 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 alla U.O.C. Flussi Documentali 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 informatico ritorna così in carico alla U.O.C. Flussi Documentali che potrà immediatamente inoltrarlo alla UOR competente.

I documenti possono comunque essere riassegnati direttamente nel caso di UOR appartenenti allo stesso Servizio.

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 competenze 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 alla U.O.C. Flussi Documentali, 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 (cfr. Capitolo 9), secondo gli altri formati stabiliti in precedenza (cfr. § 3.2) 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 del 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 strumenti 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. Flusso del documento informatico tra AOO dell'Ateneo

Il flusso dei documenti informatici tra le AOO dell'Ateneo prevede la registrazione del protocollo in partenza per l'AOO mittente e la protocollazione in arrivo per la AOO destinataria.

L'interoperabilità è garantita mediante l'uso della PEC.

Dal 1 luglio 2019 l'Università degli Studi di Brescia è articolata in un'unica Area Organizzativa Omogenea.

8.18. 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 ad 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 con 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, comma 3, 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.

I verbali d'esame e i verbali di laurea (processo interamente dematerializzato) sono firmati con firma digitale in formato XAdES.

I libri contabili previsti dalla normativa per cui l'ateneo ha dematerializzato il processo di produzione e conservazione sono firmati con firma digitale in formato CADES.

Le fatture elettroniche in formato PA (XML) destinate a pubbliche amministrazioni italiane, i contratti stipulati in forma pubblica amministrativa, i contratti stipulati mediante scrittura privata, i contratti stipulati (scambio di lettera commerciale) sulla piattaforma Consip per il mercato elettronico della pubblica amministrazione (MePA), gli accordi tra pubbliche amministrazioni sono firmati con firma digitale in formato CADES.

Nei casi in cui sia richiesto per norma di legge o opportuno inserire annotazioni successivamente alla sottoscrizione digitale è necessario utilizzare una firma digitale in formato PAdES.

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 alla U.O.C. Flussi Documentali 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, se coincidesse con la scadenza dei termini di presentazione, deve essere protocollata con provvedimento di differimento della registrazione alla data di ricezione.

Non è ammessa la consegna della domanda in busta sigillata: la U.O.C. Flussi Documentali apre il plico e a 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.

Attualmente l'Università degli Studi di Brescia ha introdotto una piattaforma informatica per la gestione delle iscrizioni ai concorsi di assunzione di personale in qualsiasi ruolo dell'Ateneo (PICA). Per ogni bando viene garantita una procedura ad hoc che rispetta tutti i requisiti di ammissibilità, la presentazione della documentazione richiesta, l'apertura e la chiusura automatica delle varie fasi previste. Le domande presentate vengono automaticamente protocollate dal sistema di protocollo informatico che fornisce riscontro immediato. Per ogni bando è disponibile un servizio di supporto anche telefonico.

La piattaforma è integrata con i gestionali dell'Ateneo e consente oltre che la dematerializzazione del processo di iscrizione dei candidati, anche la gestione dei processi interni relativi alle commissioni valutatrici.

9.3. Atti e comunicazioni giudiziarie

La notifica, quando non è disposto diversamente, 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, tramite servizio postale, a mezzo PEC o nelle altre modalità stabilite dalla legge. La notifica tramite il servizio postale o a mezzo Pec può essere eseguita anche da avvocati e procuratori legali autorizzati (ai sensi della L.53/94 e dell'art. 55 L.69/2009).

Se l'atto è notificato a mano si considera come data di notifica quella indicata nella relata di notifica, posta ordinariamente in fondo al documento. Se è notificato con raccomandata si considera come data di notifica il giorno in cui si riceve la raccomandata, facendo fede il timbro del servizio postale del giorno di effettiva consegna.

Se l'atto è notificato a mezzo PEC, ai sensi dell'art. 149-bis cpc, la copia estratta dal documento originale deve essere firmata digitalmente dall'ufficiale giudiziario o dall'avvocato/procuratore autorizzato e, se non è fatto espresso divieto dalla legge, la notificazione può eseguirsi anche previa estrazione di copia informatica del documento analogico. L'ufficiale giudiziario o l'avvocato/procuratore autorizzato 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 relata di notifica deve essere redatta su documento informatico separato, sottoscritto con firma digitale. La notifica si intende perfezionata nel momento in cui il gestore rende disponibile il documento informatico nella casella di posta elettronica certificata del destinatario.

In tutti i casi su esposti, per mittente si intende l'avvocato/procuratore istante, munito di apposita 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 il soggetto che ha richiesto la notificazione, generalmente il legale a cui il ricorrente/attore che ha conferito mediante mandato la procura alle liti.

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: il mittente da indicare nella registrazione di protocollo è l'Avvocatura. In tal caso si tratta infatti di una semplice 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.

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 attive vengono firmate dal responsabile del Servizio che le ha emesse.

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. 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: MePA (Mercato Elettronico Pubblica Amministrazione)
- Adesioni: Convenzioni
- Negoziazioni: 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 (Acquisti in rete PA) 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 MePA.

9.9.3. Procedure negoziate (RdO) - MePA

Nei casi previsti dalla normativa e dai regolamenti vigenti, si fa ricorso ad una 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, ove possibile, 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 Brescia sono "aperte", ossia possono ricevere anche messaggi di posta elettronica semplice. Nel caso di comunicazioni rilevanti da acquisire agli atti, si procede con la registrazione a protocollo dell'e-mail.

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.

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, 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 alla U.O.C. Flussi Documentali.

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 UOR

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 segnature di protocollo e l'indicazione "Secondo esemplare". Nella registrazione di protocollo si inserisce la "Annotazione" in modo imm modificabile "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 segnature 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 "Nota/ Annotazione" in modo imm modificabile 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 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, sono soggette a registrazione di protocollo. Se il documento

anonimo è pervenuto a mezzo PEC 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

Si rinvia al Regolamento per la pubblicazione dei documenti all'Albo on-line di Ateneo emanato con D.R. repertorio n.208 prot. n. 118980 del 21/03/2019, in vigore dal 1 aprile 2019, descritto [nell'allegato 9](#).

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

11.1 Archivio corrente

Il RPA è responsabile della corretta tenuta dei fascicoli della propria UOR, cioè dell'archivio corrente di propria competenza della UOR stessa.

Il responsabile si attiene alle indicazioni che vengono fornite a livello generale dal coordinatore e/o dal responsabile della gestione documentale e da quanto espressamente indicato nel presente Manuale di gestione del protocollo informatico.

Per la documentazione/fascicoli analogici 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.

11.2 Archivio di deposito analogico

Presso l'archivio di deposito analogico sono conservati tutti i fascicoli e i documenti relativi a procedimenti conclusi, per i quali non risulta più necessaria la trattazione corrente o verso i quali può sussistere solo un interesse sporadico. Tali documenti sono conservati con le modalità indicate dal coordinatore o dal responsabile della gestione documentale, rispettando l'organizzazione che essi avevano nell'archivio corrente.

11.3 Trasferimento dei fascicoli cartacei all'archivio di deposito

Periodicamente il Responsabile del procedimento amministrativo trasferisce, per la conservazione nell'archivio di deposito, 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.

I fascicoli vengono trasferiti rispettando l'ordinamento 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 dei flussi documentali. Prima del trasferimento i RPA provvedono anche a verificare che i fascicoli risultino chiusi anche nel sistema informatico di gestione documentale.

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

11.4 Trasferimento dei fascicoli informatici

Il Coordinatore/Responsabile della gestione documentale provvede, d'intesa con il Responsabile della conservazione, a generare e trasmettere dei pacchetti di versamento al sistema di conservazione, secondo le regole previste nel manuale di conservazione, avvalendosi anche di processi di automazione disponibili nel sistema di gestione documentale.

Qualora, per determinate tipologie di procedimenti o di documenti, si rendesse necessario predisporre l'attivazione della procedura di conservazione con tempistiche particolari, il RPA interessato dall'esigenza deve darne tempestiva comunicazione al coordinatore/responsabile della gestione documentale, al fine di valutare congiuntamente con il Responsabile della conservazione e con il Responsabile dei sistemi informativi le modalità più idonee per dare attuazione a tale esigenza. Ne costituisce un esempio la conservazione delle fatture elettroniche attive e passive. Queste devono essere tassativamente fascicolate nei rispettivi fascicoli informatici a cura del Responsabile del procedimento.

11.5. 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 digitali, 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.

11.6 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 classificazioni 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 un'adeguata analisi degli stessi, al fine di un ordinamento secondo criteri condivisi e orientati a essere perduranti nel tempo.

Gli interventi su questa documentazione vanno comunque valutati insieme alla Soprintendenza Archivistica della Lombardia.

11.7. Elenco di consistenza per l'archivio di deposito analogico

Il personale addetto all'archivio di deposito, ricevuti i fascicoli e le serie archivistiche, li dispone nei locali di deposito rispettando l'ordinamento archivistico loro proprio, provvedendo a integrare e aggiornare l'elenco di consistenza con i trasferimenti effettuati dagli uffici.

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

La U.O.C. Flussi Documentali è titolare e responsabile del servizio di ricerca 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.

È consentito il richiamo temporaneo di uno o più fascicoli, già trasferiti all'archivio di deposito, da parte della UOR produttrice o altra UOR autorizzata. È 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 flusso della ricerca documentale deve essere esclusivamente digitale.

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 costituito da un documento informatico in formato xlsx. 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.

11.9. 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.

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. 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) dalle amministrazioni.

12.1. 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 a 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.

12.2. 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 di quanto previsto dall'art. 32 del Regolamento UE 2016/679, dal D.lgs 196/03, come novellato dal D.lgs 101/2018 e da ogni altra disposizione in materia di protezione dei dati personali, è predisposto e aggiornato annualmente dal Consorzio Cineca.

12.2.1 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 ICT" dell'Ateneo.

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

12.2.2 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 24H.

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.

12.2.3 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*.

12.2.4 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* consultabili attualmente all'indirizzo: <http://www.garr.it/utenti/regole-di-accesso/acceptable-use-policy-aup> e nel Regolamento di utilizzo dei Servizi Informatici e di Rete.

Il servizio "Servizi ICT", in qualità di amministratore della rete di Ateneo, assicura in modo coordinato con il Settore Acquisizioni 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.

12.2.5. 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 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.

12.3. 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 di 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 di quanto previsto dall'art. 32 del Regolamento UE 2016/679, dal D.lgs 196/03, come novellato dal D.lgs 101/2018 e da ogni altra disposizione in materia di protezione dei dati personali.

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 della Protezione dei Dati (RPD)* – ovvero la persona fisica o giuridica, deputata alla sorveglianza della normativa privacy all'interno dell'organizzazione del Titolare del trattamento ed eventuali Referenti di Dipartimento;
- *Responsabile 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 allanomina dell'amministratore di sistema, ne assolve i compiti e conseguenti adempimenti.
- *Incaricato del trattamento* – La persona fisica autorizzata a compiere operazioni di trattamento dati dal Titolare o dal Responsabile.

Il Titolare del trattamento designa, con provvedimento espresso, gli Incaricati del trattamento dei dati operanti all'interno della struttura di competenza.

In carenza di provvedimento espresso, gli autorizzati al trattamento sono individuati anche mediante il criterio tacito della afferenza/preposizione alla struttura di operatività, come risultante dalla pubblicazione sulla rete di Ateneo.

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.

12.3.1. 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 l'RPD e gli eventuali Referenti di Dipartimento sono in sintesi:

- *inserimento* dei dati per effettuare una registrazione;
- *modifica* dei dati di una registrazione;
- *annullamento* di una registrazione;
- *ricerca* di informazioni registrate ai fini della visualizzazione o consultazione;
- visualizzazione e consultazione;
- *download* dei documenti associati alla registrazione.

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. Per quanto riguarda la garanzia di immodificabilità dei contenuti si rimanda a quanto illustrato al § 6.8.

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.

12.3.2. Le procedure comportamentali ai fini della protezione dei documenti

Le postazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà dall'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'art.32 del Regolamento UE 2016/679, dal D.lgs 196/03, come novellato dal D.lgs 101/2018 e da ogni altra disposizione in materia di protezione dei dati personali
- 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 Brescia 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 evitarne l'utilizzo improprio da parte di terzi, mediante inserimento di apposite credenziali di accesso. Le stazioni di lavoro, da tavolo e 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 art. 32 del Regolamento UE 2016/679, dal D.lgs 196/03, come novellato dal D.lgs 101/2018 e da ogni altra disposizione in materia di dati personali. Le credenziali di accesso (generalmente, *nome utente* e *password*) sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime. Per la disciplina riguardante l'utilizzo delle credenziali, per la segretezza e per la protezione delle *password* è fatto riferimento espresso alle disposizioni contenute nell'art. 32 del Regolamento UE 2016/679, dal D.lgs 196/03, come novellato dal D.lgs 101/2018 e da ogni altra disposizione in materia di dati personali D.lgs 30 giugno 2003, n. 196, e, in particolare, agli artt. 4 comma 3 lett. d) e 34.