Manuale di gestione documentale

a cura dell'Area Affari generali – Ufficio Affari generali e gestione documentale
adottato con disposizione della Direttrice Generale del 24/10/2023

Sapienza Università di Roma
Area Affari generali
CF 80209930587 PI 02133771002
P.le Aldo Moro, 5, 00185, Roma
www.uniroma1.it

SOMMARIO

PREMESSA: PRINCIPI GENERALI DELLA GESTIONE DOCUMENTALE

La gestione documentale, secondo quanto riportato dalle Linee guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale (d'ora in poi "Linee guida"), "*è un processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti*".

Riguarda quindi l'intera vita del documento che, tipicamente, possiamo suddividere in tre fasi principali: formazione, gestione e conservazione.

Ciascuna di queste fasi comporta una serie di attività più o meno complesse, cui sono associati approcci metodologici e prassi operative specifiche.

Il sistema di gestione informatica dei documenti affinché possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolga la vita del documento ed effettuata secondo i principi generali applicabili in materia di trattamento dei dati personali.

Dal punto di vista archivistico, si distinguono tre fasi di gestione:

- l'archivio corrente, che riguarda i documenti necessari alle attività correnti;
- l'archivio di deposito, che riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- l'archivio storico, che riguarda i documenti storici selezionati per la conservazione permanente.

Una corretta gestione dei documenti sin dalla loro fase di formazione rappresenta la migliore garanzia per il corretto adempimento degli obblighi di natura amministrativa, giuridica e archivistica tipici della gestione degli archivi pubblici.

L'impostazione di una corretta gestione documentale risponde, inoltre, all'esigenza di conferire certezza all'attività giuridico-amministrativa e di conservarne stabilmente la memoria.

Nella fase di formazione devono essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza alle regole tecniche che presidiano la formazione dei documenti informatici, tenendo in debito conto le esigenze e i bisogni pratici del lavoro quotidiano.

Allo stesso modo, anche i processi e le attività che governano la fase di formazione dei documenti informatici devono essere sottoposti a un costante lavoro di valutazione e monitoraggio.

La gestione dei documenti informatici prosegue con il trasferimento in un sistema di conservazione da realizzarsi in ottemperanza a quanto disposto dal Codice dell'amministrazione digitale (d'ora in poi "CAD") e dalle Linee guida.

La conservazione dei documenti è tipicamente svolta all'interno di un sistema di conservazione dedicato a questa funzione.

Tuttavia, l'attenzione al profilo conservativo deve essere posta fin dal momento della formazione del documento.

L'adozione del Manuale di gestione documentale, oltre a rappresentare un preciso obbligo normativo, rappresenta una formidabile opportunità per definire le politiche che l'Ateneo fissa nell'ambito della gestione documentale rispetto a tutti i vari aspetti che la compongono.

In un contesto in continua trasformazione, il Manuale di gestione quindi va inteso come uno strumento in continuo divenire.

CAPITOLO 1 – IL MANUALE DI GESTIONE

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

Il Manuale di gestione è un documento informatico che raccoglie "*l'insieme delle norme, direttive o procedure interne che stabiliscono le modalità operative di formazione, utilizzo e conservazione dei documenti, definiscono le responsabilità per la gestione dei documenti nell'ambito dell'ente considerato e forniscono le informazioni necessarie a un efficiente trattamento dei documenti*."[1]

Serve ad organizzare e a 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.

Rappresenta una guida: per l'operatore di protocollo e, più in generale, per tutto il personale, al fine di porre in essere le corrette operazioni di gestione documentale; per il cittadino e per le imprese, per comprendere e collaborare alla gestione documentale stessa (ad esempio, utilizzando formati idonei per la formazione delle istanze, etc.).

1.2. Modalità di redazione

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

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

Questo Manuale è stato redatto utilizzando 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 divulgazione

La Pubblica Amministrazione è tenuta a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale.

La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'articolo 9 del D.Lgs. 33/2013.

Il Manuale deve, inoltre, essere capillarmente divulgato alle unità organizzative responsabili (UOR) delle aree organizzative omogenee (AOO) dell'Ateneo, al fine di consentire la corretta diffusione delle nozioni e delle procedure documentali in essere.

[1] P. Carucci – M. Guercio, *Manuale di archivistica*, Roma 2021, p.348.

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

La Legge 7 agosto 1990, n. 241, il DPR 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa; d'ora in poi "TUDA") e le Linee guida prevedono che l'ente si organizzi in Aree Organizzative Omogenee (AOO) e, all'interno della medesima AOO, in Unità Organizzative Responsabili (UOR).

L'Area Organizzativa Omogenea (AOO) è l'insieme di funzioni e di strutture individuate dall'amministrazione cui sono assegnate le funzioni omogenee.

L'Unità Organizzativa Responsabile (UOR) è, all'interno della AOO, il 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'Ateneo ha individuato, nell'ambito del proprio ordinamento, 110 Aree Organizzative Omogenee (d'ora in poi AOO) e le relative Unità Organizzative Responsabili da considerare ai fini della gestione unica o coordinata dei documenti, assicurando criteri uniformi di gestione (es. classificazione, fascicolazione, trasmissione etc.), nonché di comunicazione interna tra le UOR stesse.

L'Amministrazione centrale costituisce una unica AOO mentre ciascuna struttura esterna (facoltà, dipartimento, centro, scuola, etc.) rappresenta un'ulteriore singola AOO.

L'organigramma completo, AOO e UOR, è riportato sul portale di Ateneo: https://www.uniroma1.it/it

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

Presso l'AOO Amministrazione centrale il servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, come previsto dal DPR 445/2000, art. 61, è gestito dal Settore Protocollo, gestione e conservazione documentale (d'ora in poi "Settore Protocollo").

Al Settore Protocollo è attribuita la competenza di tenuta del sistema di gestione informatica e analogica dei documenti, dei flussi documentali e degli archivi, nonché il coordinamento degli adempimenti previsti dalla normativa vigente.
Il Settore Protocollo è incardinato nell'Ufficio Affari generali e gestione documentale.
Il Responsabile dell'Ufficio Affari generali e gestione documentale è anche Coordinatore della gestione documentale, ai sensi delle Linee guida, art. 3.1.2. lettera C).
Ogni altra AOO (facoltà, dipartimenti, centri, scuole, etc.) 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.
In difetto di nomina espressa, il Responsabile coincide con il Responsabile Amministrativo Delegato della Struttura.
Con Disposizione Direttoriale n. 3863 del 05/10/2023 sono stati individuati il Coordinatore e i Responsabili della gestione documentale previsti dalle Linee guida, art. 3.1.2. lettere B e C.
Il Settore Protocollo garantisce la corretta gestione, tenuta e tutela dei documenti; vigila sull'osservanza della corretta applicazione della normativa in materia di gestione documentale durante l'intero ciclo di vita dei documenti; attende a ulteriori specifici compiti attribuiti dalla legge o dall'ordinamento interno dell'Ateneo.
In particolare, il Settore cura:

- il livello di autorizzazione (Access 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 di AOO/UOR. In tal caso il Responsabile di AOO/UOR invierà apposita richiesta al Coordinatore della gestione documentale alla mail istituzionale del Settore Protocollo;
- la correttezza delle operazioni di registrazione, segnatura, gestione dei documenti e dei flussi documentali;
- la notifica ai Responsabili della gestione documentale di ciascuna AOO dell'eventuale indisponibilità del sistema e dà loro disposizioni per l'attivazione del registro di emergenza secondo quanto disposto al capitolo 6.9;
- le autorizzazioni e le operazioni di annullamento delle registrazioni di protocollo per l'AOO Amministrazione centrale;

- l'adeguamento del sistema di gestione documentale alle eventuali modifiche dell'organigramma e del funzionigramma di Sapienza Università di Roma.

2.3. Il Coordinatore della gestione documentale e i Responsabili della gestione documentale

Il Coordinatore della gestione documentale e i Responsabili della gestione documentale, per le rispettive AOO di competenza, sono preposti al servizio di cui all'art. 61 del TUDA.

Il Coordinatore della gestione documentale, d'intesa con il Responsabile della conservazione e con il Responsabile per la transizione digitale di cui all'articolo 17 del CAD, acquisito il parere del Responsabile della protezione dei dati personali, di cui agli articoli 37 ("Designazione del responsabile della protezione dei dati") e 39 ("Compiti del responsabile della protezione dei dati") del Regolamento UE 679/2016, predispone e mantiene aggiornato il Manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali.

È compito del Coordinatore della gestione documentale e dei Responsabili della gestione documentale produrre il pacchetto di versamento e assicurare il trasferimento del suo contenuto al sistema di conservazione.

Il Coordinatore della gestione documentale e i Responsabili della gestione documentale verificano l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

2.4. Profili di abilitazioni di accesso interno ed esterno alle informazioni documentali

Il sistema di gestione documentale prevede 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.

Il Responsabile del Settore Protocollo riceve dai responsabili delle UOR dell'Amministrazione centrale e dai Responsabili della gestione documentale delle altre AOO richiesta scritta (tramite e-mail) di abilitazione per ciascun utente, concordando, caso per caso, le tipologie di abilitazione.

Al di là di casi specifici che prevedono abilitazioni particolari, da concordare con il Coordinatore della gestione documentale, presso l'Ateneo sono attivi i profili riportati nell'allegato 2 al presente Manuale.

2.5. Posta elettronica istituzionale

Ogni AOO e ciascuna UOR sono dotate di una casella istituzionale di posta elettronica.

La casella viene denominata in modo da rendere facilmente individuabile l'AOO/UOR di riferimento.

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

L'utilizzo della casella istituzionale di posta elettronica, assegnata a ciascun dipendente, è disciplinato dall'apposito regolamento, emanato con Decreto Rettorale n. 3283 del 18 dicembre 2017 e disponibile al seguente *link*: https://www.uniroma1.it/sites/default/files/field_file_allegati/regolamento_posta_elettronica.pdf

2.6. PEC istituzionale

L'Ateneo ha attivato una casella di PEC per ciascuna AOO.

La gestione della posta elettronica certificata è integrata nel sistema di protocollo informatico Titulus.

Tutti gli utenti abilitati a registrare documenti in partenza possono pertanto inviare le PEC direttamente da Titulus e verificarne lo stato tramite la lettura delle ricevute, che sono associate in automatico al numero di protocollo.

Il personale addetto alla registrazione dei documenti in arrivo procede giornalmente alla lettura della corrispondenza ivi pervenuta e adotta gli opportuni metodi di registrazione e conservazione, in relazione alle varie tipologie di messaggi.

L'elenco degli indirizzi PEC di Sapienza, uno per ciascuna AOO, è pubblicato sull'Indice delle Pubbliche Amministrazioni (IPA) e sulle pagine web dell'Università.

Il settore Protocollo gestisce la casella istituzionale di PEC - Posta elettronica certificata dell'AOO Amministrazione centrale (protocollosapienza@cert.uniroma1.it).

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

È istituito un registro di protocollo per ciascuna AOO dell'Ateneo.

A far data dal 1° gennaio 2006 sono cessati di fatto e di diritto tutti i cosiddetti protocolli interni (cioè di settore, di ufficio, di area, protocolli multipli, protocollo del telefax, etc.) o altri sistemi di registrazione dei documenti diversi dal protocollo associato a ciascuna AOO.

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.

Il Responsabile della conservazione, pertanto, può coincidere con il Coordinatore della 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 del trattamento dei dati personali, con il Responsabile della sicurezza e con il Responsabile dei sistemi informativi, oltre che con il Coordinatore della gestione documentale nel caso in cui non sia la stessa persona.

Per Sapienza Università di Roma il Responsabile della conservazione coincide con il Coordinatore della gestione documentale.

CAPITOLO 3 - IL DOCUMENTO

3.1. Documento informatico e analogico: definizione e disciplina giuridica

Il documento elettronico è qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.

Il documento informatico è un documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Il documento analogico è la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Qualsiasi documento non informatico (ad esempio, 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.

Secondo quanto disposto dall'articolo 3 del Regolamento "electronic IDentification Authentication and Signature" - Regolamento UE 910/2014 (d'ora in poi "Regolamento eIDAS"), per firma elettronica si devono intendere i dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.

L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono valutabili in giudizio tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

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

Il documento informatico può essere sottoscritto con firma elettronica, avanzata, qualificata 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 (art. 2712 codice civile, art. 23-quater CAD, art. 2713 codice civile).

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 digitale, se formato nel rispetto delle regole 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 di firma digitale si presume riconducibile al titolare, salvo che questi ne dia prova contraria.
Il documento informatico sottoscritto con firma elettronica avanzata, se formato nel rispetto delle regole 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 elettronica qualificata, se formato nel rispetto delle regole 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 di firma elettronica avanzata e di firma elettronica qualificata 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.
Si precisa che tutti i contratti stipulati da Sapienza Università di Roma, anche quando quest'ultima agisce *iure privatorum*, richiedono la forma scritta *ad substantiam*.
L'Ateneo ha stabilito che i propri documenti siano predisposti secondo il modello di carta intestata descritto nel Manuale grafico di identità visiva, pubblicato alla pagina:
https://www.uniroma1.it/it/pagina/manuale-grafico

3.2. Redazione/formazione del documento informatico

Il documento informatico è formato mediante una delle seguenti modalità:

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

Il documento informatico deve essere identificato in modo univoco e persistente. L'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento.

L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti.

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

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

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza;
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS, valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento a un sistema di conservazione.

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

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

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

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

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente a esso i relativi metadati di cui all'allegato 5 alle Linee guida.

La disponibilità e la riservatezza delle informazioni contenute nel documento informatico sono garantite attraverso l'adozione di specifiche politiche e procedure predeterminate da Sapienza, in conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali.

L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'allegato 2 alle Linee guida**.**

3.2.1. Validazione temporale

Costituiscono validazione temporale:

- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata;

- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica;
- 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 a un minuto primo;
- 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.

3.2.2. Formati

Sapienza usa per la formazione e per la gestione dei documenti informatici le tipologie di formato previste dall'allegato 2 "Formati di file e riversamento" delle Linee guida.

3.3. Redazione e formazione del documento amministrativo informatico

Per documento amministrativo informatico si intende "*ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa*"[2].

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico.

Il documento amministrativo informatico è identificato e trattato nel sistema di gestione informatica dei documenti.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità descritte in precedenza per il documento informatico, anche con la sua registrazione nel registro di protocollo, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti.

Al documento amministrativo informatico vengono associati l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA, i metadati relativi alla classificazione ai sensi dell'articolo 56 del TUDA e ai tempi di conservazione, in coerenza

[2] Linee guida AgID, Allegato 1.

con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.

Le amministrazioni pubbliche formano gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici, 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 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.

3.4. Redazione e formazione del documento amministrativo analogico

Per documento analogico si intende un documento formato utilizzando una grandezza fisica (ad esempio, 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 esempio, documento scritto a

mano) o con strumenti informatici (ad esempio, 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 terzo 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 autografa, 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 esempio, 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 di Sapienza 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 registratura.

Trattandosi di un documento informatico nativo non si procederà alla stampa e apposizione tramite timbro della segnatura prima della registratura a protocollo.

3.8. Distinzione dei documenti in base allo stato di trasmissione (arrivo, partenza, scambiati tra UOR, 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, "tra uffici" (scambiati tra UOR).

I documenti scambiati tra AOO dell'Ateneo non sono considerati documenti interni ma in arrivo o 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 o "tra uffici" sono utilizzati solo nell'ambito della AOO Amministrazione centrale mentre non sono presenti per le altre AOO.

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 è ricevuto e trasmesso per posta elettronica interna e di norma le comunicazioni non sono protocollate.

Per documenti scambiati tra AOO dell'Amministrazione 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. Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.
I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 alle Linee guida.
Nel caso in cui non vi sia l'attestazione di un pubblico ufficiale, la conformità della copia per immagine a un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'articolo 20, comma 1-bis del CAD, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.
Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine.
Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.
La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'articolo 22, commi 4 e 5 del CAD.

3.10. Duplicati, copie ed estratti informatici di documenti informatici

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

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".doc" in un documento ".pdf".

L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto.

Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta.

In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo" alle Linee guida.

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

Nel caso in cui non vi sia l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico a un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto.

L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico.

Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

3.11. Copie su supporto informatico di documenti amministrativi analogici

Alle copie su supporto informatico di documenti amministrativi analogici si applicano le disposizioni previste per le copie per immagine su supporto informatico di documenti analogici.

L'attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dall'Amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine.

Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato.

3.12. Metadati

Sono definiti nell'allegato 1 alle Linee guida come "*dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura – così da permetterne la gestione nel tempo – in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017*".

La codifica dell'informazione digitale, a differenza di altre, non è mai né auto-sufficiente né auto-esplicativa, ma deve sempre e necessariamente documentare sé 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.

3.12.1. Obiettivi dei metadati archivistici

Gli obiettivi dei metadati archivistici sono:

- garantire l'identificazione permanente dei singoli oggetti informativi, ad esempio l'identificativo univoco (numero di protocollo, data, autore, etc.);

- garantire l'identificazione permanente delle relazioni tra gli oggetti informativi, ad esempio gli indici di classificazione e fascicolatura;
- conservare le informazioni che supportano l'intellegibilità degli oggetti informativi, ad esempio il procedimento amministrativo cui il documento è connesso.

3.12.2. 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.

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[3].

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

Si possono distinguere cinque tipologie di fascicolo:

1. *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 (ad esempio: l'istituzione di un gruppo di lavoro o un corso di formazione professionale);
2. *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 (ad esempio: il rilascio dei permessi per il parcheggio interno al personale);
3. *Procedimento amministrativo*: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un atto finale;
4. *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

[3] DPR n. 445/2000, art. 64 comma 4: «*Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo*».

una persona fisica determinata. La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'ente;

5. *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 dello 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: 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 digitali.

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;
- oggetto del fascicolo, cioè una stringa di testo per descrivere compiutamente un affare, una pratica, un *dossier*, 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 (« »): ad 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.

4.3. Il fascicolo informatico: formazione, implementazione e gestione

Per ogni procedimento, affare e attività, l'Ateneo ha l'obbligo di conservare in un fascicolo informatico gli atti, i documenti e i dati da chiunque formati su supporto informatico: 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.
Quando si riceva un documento in conferenza di servizi, oppure in copia conoscenza, questo non va fascicolato.
In sintesi:

• i documenti in arrivo e in partenza vengono fascicolati a cura del responsabile del procedimento;
• in caso protocollo tra uffici il mittente (responsabile della minuta) fascicolerà la minuta, il destinatario (responsabile dell'originale) l'originale.
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 da documenti esclusivamente informatici questa attività è sufficiente; se è costituito da documenti informatici e documenti cartacei bisogna rinominare anche la camicia del fascicolo cartaceo.
Il fascicolo informatico in un sistema totalmente digitale garantisce la possibilità di essere direttamente consultato e alimentato dalle UOR 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.

4.4. Il fascicolo ibrido

Il fascicolo, inteso come unità logica, può conservare documenti creati 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; 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.
Tale peculiarità rende, ovviamente, 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.

4.5. 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 obbligatori del fascicolo informatico, previsti dalle Linee guida, sono:

- identificativo rappresentato da una sequenza di caratteri alfanumerici associata in modo univoco al fascicolo in modo da consentirne l'identificazione;
- tipologia fascicolo (affare, attività, persona fisica, persona giuridica, procedimento amministrativo);
- indicazione dei soggetti coinvolti, a vario titolo, nella costituzione del fascicolo (amministrazione titolare, amministrazioni partecipanti, RUP, etc.);
- informazioni relative all'assegnazione per conoscenza o competenza;
- data apertura;
- classificazione;
- progressivo numerico;
- oggetto;
- data chiusura;
- nel caso di fascicolo di tipologia "procedimento amministrativo", il procedimento a cui afferisce, con lo stato di avanzamento e le relative fasi;
- elenco degli identificativi dei documenti contenuti nel fascicolo;
- nel caso di fascicolo cartaceo digitalizzato o ibrido, la posizione fisica del fascicolo cartaceo.

4.6. 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.

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.

Durante la fase di deposito viene trasferita la gestione dei fascicoli, ma non la responsabilità.

Nel caso di documenti cartacei, per la movimentazione dei fascicoli, viene effettuata una richiesta di accesso da parte della UOR.

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 par. 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 abbia 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.

I documenti creati nel corso dell'attività d'ufficio sono soggetti a fascicolazione obbligatoria ai sensi del TUDA, 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 UOR costituenti l'Amministrazione.

Un'attività secondaria 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, 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 esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad esempio, appunti, promemoria, copie di normativa e documenti di carattere generale).

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 titolario è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (titolo e classe) stabilite sulla base delle funzioni di Sapienza.

Ciascun documento, registrato in modalità arrivo, partenza, interno, ovvero non protocollato, è classificato in ordine alla corrispondenza tra il suo contenuto e la relativa voce attribuibile, desunta dal titolario e successivamente fascicolato.

La classificazione, necessaria e fondamentale, è prodromica all'inserzione di un documento all'interno di un determinato fascicolo.

La relazione tra i documenti (vincolo archivistico) di un'unità archivistica è garantita dalla segnatura archivistica completa (anno di istruzione, classificazione, numero del fascicolo).

Il titolario può essere corredato da un'appendice denominata voci di indice. Si tratta di un ulteriore strumento, strettamente correlato al titolario, che agevola le operazioni di classificazione e di protocollazione/registrazione.

Consiste in una serie di varianti lessicali, trattate e riportate in modo analitico, che individuano singole tipologie di documenti ricorsivi e che, in modo automatico, propone: classificazione, oggetto standardizzato e indicazione dell'RPA.

Il titolario 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 titolario siano storicizzate, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della loro registrazione.
Il titolario è sottoposto, altresì, all'approvazione della Direzione generale archivi del Ministero della Cultura e comunicato alla Soprintendenza archivistica e bibliografica del Lazio.
Il titolario unico, valido per tutte le AOO di Sapienza Università di Roma, è descritto nell'allegato 3 al presente Manuale.

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 titolario, è lo strumento di gestione e di reperimento dei fascicoli.
La struttura del repertorio rispecchia quella del titolario di classificazione e, di conseguenza, varia in concomitanza con l'aggiornamento di quest'ultimo.
Mentre il titolario rappresenta, in astratto, le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta, in concreto, le attività svolte e i documenti prodotti in relazione a tali attività. Il repertorio dei fascicoli è costantemente aggiornato.

5.3.4. Repertori

Per repertorio si intende il registro in cui sono annotati con numerazione progressiva i documenti, uguali per forma e diversi per contenuto, per i quali è prevista una registrazione particolare.
I documenti sono comunque 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.
Sono un esempio la registrazione di decreti, contratti e convenzioni, deliberazioni, etc.
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 a uno specifico registro di protocollo attivo per ogni area organizzativa omogenea dell'Ateneo.
Nell'allegato 4 al presente Manuale sono elencati tutti i repertori attivi presso la Sapienza.

5.3.5. Piano di Conservazione

Il TUDA prevede all'art. 68 l'obbligo per i soggetti pubblici di dotarsi di un "*piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni contenute in materia di tutela dei beni culturali e successive modificazioni ed integrazioni*".
Il piano di conservazione è quindi lo strumento con cui l'Amministrazione individua le disposizioni di massima e definisce i criteri e le procedure per la corretta esecuzione delle operazioni di selezione ai fini della conservazione e dello scarto documentale; infatti i documenti che non rivestono interesse storico ai fini della conservazione permanente e hanno esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della Soprintendenza archivistica e bibliografica del Lazio.
Il piano di conservazione definisce pertanto i tempi di invio in conservazione e i tempi di scarto per ciascuna tipologia documentaria.
Il Piano di conservazione viene sottoposto al nulla osta della Soprintendenza Archivistica del Lazio e deve intendersi come un documento dinamico ed è soggetto a revisione periodica, almeno ogni tre anni, come stabilisce l'art. 7, comma 2 del D.P.R. 37/2001.
Per quanto attiene lo scarto, la proposta di scarto, formulata su apposito elenco 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 e bibliografica del Lazio nelle modalità concordate, che rilascia autorizzazione ai sensi del D.Lgs. 42/2004, art. 21.
A seguito dell'autorizzazione, l'Ateneo avvia il procedimento per individuare il soggetto legittimato al ritiro del materiale e alla eliminazione fisica dei documenti; la ditta affidataria individuata effettua le operazioni di ritiro e macero della documentazione con rilascio di relativo verbale di esecuzione.
Per i fascicoli informatici la proposta di scarto segue lo stesso iter per quanto riguarda l'autorizzazione della Soprintendenza e il Coordinatore/Responsabile della gestione documentale invierà un documento informatico firmato digitalmente.

Il fascicolo inerente al procedimento di scarto è a conservazione illimitata.

Il piano di conservazione di Sapienza è consultabile alla pagina: https://www.uniroma1.it/it/pagina/settore-archivio-storico

5.3.6. 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 se trattasi di struttura decentrata o al Coordinatore della gestione documentale se trattasi dell'Amministrazione centrale, producendo un apposito elenco dei fascicoli soggetto di spostamento.

L'Ufficio Affari generali e gestione documentale 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[4].

[4] D.Lgs 42/2004, art. 21, c. 3: «*Lo spostamento degli archivi correnti dello Stato e degli enti ed istituti pubblici non è soggetto ad autorizzazione*».

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 di Sapienza.

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 o scambiati tra AOO dello stesso ente, e tutti i documenti informatici, ad eccezione di quelli espressamente esclusi dalla normativa vigente e altri documenti informatici già soggetti a registrazione particolare[5].
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 immodificabile.
La registrazione di protocollo per ogni documento è effettuata mediante la memorizzazione di elementi obbligatori immodificabili, elementi obbligatori modificabili ed elementi non obbligatori e modificabili.
La registrazione degli elementi obbligatori immodificabili del protocollo informatico non può essere modificata, integrata, cancellata ma soltanto annullata mediante un'apposita procedura in capo al Coordinatore/Responsabile della gestione documentale e a persone espressamente delegate.

---

[5] DPR n. 445/2000, art. 53 comma 5: «*Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione*».

L’inalterabilità e l’immodificabilità della registrazione di protocollo sono garantite dal sistema di gestione documentale.

6.1.1. Elementi obbligatori immodificabili (Registratura)

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

Essi sono:

- numero di protocollo progressivo e costituito da almeno sette cifre numeriche, generato automaticamente dal sistema;
- data di registrazione, assegnata automaticamente dal sistema;
- 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;
- data e protocollo del documento ricevuto, se disponibili.

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 fascicoli diversi da quello d’inserimento;
- tipologia di documento;
- durata della conservazione;

- altri tipi di annotazioni (ad esempio, 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 riguardanti il documento stesso.
Essa consente di identificare ciascun documento in modo univoco e certo.

6.3.1. Per il documento informatico

Le informazioni minime da associare al documento informatico sono:

- numero di protocollo;
- data di protocollo;
- codice identificativo dell'amministrazione;
- codice identificativo dell'AOO.

Oltre alle informazioni minime la segnatura include:

- 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 (si veda l'allegato 6 alle Linee guida), purché siano adottate idonee modalità di formazione dello stesso in formato PDF/A.

6.3.2. Per il documento analogico

Le informazioni da associare al documento analogico 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.

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

La segnatura su un documento cartaceo viene apposta tramite etichetta adesiva oppure mediante timbro meccanico che riporta gli elementi normalizzati della segnatura.

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 etc.), 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 Coordinatore/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.

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

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.

6.7. Documenti esclusi dalla registrazione di protocollo

Sono esclusi per legge dalla registrazione di protocollo[6]:

- 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;

[6] TUDA, art. 53 comma 5.

- le riviste;
- i libri;
- i materiali pubblicitari;
- gli inviti a manifestazioni.

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, immodificabile e integra.

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

Gli elementi memorizzati del registro giornaliero sono i seguenti:

- identificativo univoco e persistente, espresso in Codice IPA, AOO, anno, mese e giorno;
- 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 esempio, "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 Coordinatore della gestione documentale attiva il registro di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica, dandone immediata comunicazione mediante avviso sul sito *web* dell'Ateneo.

Il registro viene predisposto su postazioni di lavoro operanti fuori rete e, nel caso in cui il normale utilizzo del protocollo sia impedito dalla mancanza di energia elettrica, viene utilizzato un registro di emergenza in formato cartaceo.

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 Coordinatore 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 (continuando la numerazione di protocollo raggiunta al momento di interruzione del servizio), 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.
Soluzioni analoghe sono adottate dal Responsabile della gestione documentale di ciascuna AOO, previa intesa, con il Coordinatore della gestione documentale.
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.

CAPITOLO 7 – FLUSSO DI LAVORAZIONE DEI DOCUMENTI

7.1. Flusso del documento informatico in arrivo

Il Settore Protocollo registra in modo avalutativo i documenti che rivestono un valore giuridico-probatorio.

La documentazione da protocollare viene registrata, classificata e smistata alla UOR competente.

Il Responsabile della UOR, a sua volta, assegna al documento (e di conseguenza al procedimento amministrativo cui si riferisce) il RPA.

L'informativa 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 ordinaria (*e-mail*);
- tramite posta elettronica certificata (PEC);
- tramite servizio postale o corriere;
- con consegna a mano;
- altri applicativi.

7.2. Ricezione di documenti informatici nella casella di posta elettronica istituzionale

L'*e-mail* è un mezzo di trasmissione di documenti tramite allegato; tuttavia è possibile che la comunicazione sia inclusa nel corpo stesso della *mai*l, cioè come parte del messaggio stesso.

Sia che il messaggio sia costituito dal mero corpo della *e-mail*, sia che il documento principale sia contenuto in allegato, si procede alla sua registrazione nel sistema di gestione documentale soltanto se il contenuto viene ritenuto rilevante al fine giuridico-probatorio.

Si possono avere i seguenti casi:

- documento che arriva alla casella di posta elettronica istituzionale del Settore Protocollo (protocollosapienza@uniroma1.it) come allegato;

- documento costituito dal corpo della *mail*: si procede al salvataggio in formato PDF/A e lo si associa al sistema di gestione documentale procedendo alla registratura in arrivo con le consuete modalità.
- documento che arriva alla casella di posta elettronica istituzionale di una UOR diversa da protocollosapienza.uniroma1.it. La UOR ricevente inoltra l'e-mail corredata degli eventuali allegati alla casella protocollosapienza.uniroma1.it che converte il *file* in PDF/A, registra nel protocollo informatico e associa il *file* con estensione PDF/A;
- il mittente è l'autore della *e-mail* e non la UOR che ha inoltrato il *file* al Settore Protocollo. Nel caso di *e-mail* da cui non sia possibile desumere l'indicazione di nome e cognome il documento sarà trattato come Anonimo (cfr. par. 8.15);

Analogamente se un dipendente riceve nella propria casella di posta fornita dall'Amministrazione documenti concernenti affari o procedimenti amministrativi dell'Amministrazione è tenuto a inoltrare tempestivamente il messaggio *e-mail* alla casella istituzionale del Settore Protocollo che provvede alla relativa protocollazione.

7.3. 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.

La PEC utilizzata in Ateneo è di tipo "chiuso" e incorporata nel sistema di gestione documentale.

Per questa ragione, pervengono solo documenti informatici da PEC e non anche da posta elettronica semplice.

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

Si identifica il mittente (non sempre coincidente con il proprietario della PEC).

Una registrazione (sia in arrivo che in partenza via PEC), non permette di modificare i file informatici associati ad essa. I

l sistema di gestione documentale genera tutte le ricevute previste dalla normativa in materia di posta elettronica certificata.

Per altri esempi si veda il Capitolo 8 - Casistica e comportamenti.

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) viene comunque registrato al protocollo.
Spetta al responsabile del procedimento valutare se accettare il documento informatico assegnato non sottoscritto o non conforme agli standard e richiedere il documento al mittente.

7.3.1. Documenti informatici prodotti da applicativi dell'Ateneo o prodotti da applicativi di terzi

I documenti inseriti e convalidati da applicativi dell'Ateneo o prodotti da applicativi 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[7].

Ad esempio, ordini e fatture attive in formato Fattura PA destinati a pubbliche amministrazioni generati sul sistema di contabilità *U-GOV* sono trasferiti automaticamente al sistema di gestione documentale tramite un workflow automatico.
Prima di attivare una procedura automatica, il Coordinatore 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 il Settore Protocollo di scadenze massive (gare, bandi, valutazioni comparative, immatricolazioni alle scuole di specializzazione, dottorati di ricerca, etc.) scrivendo, di norma, almeno una settimana prima di tali scadenze, una *mail* alla sua casella istituzionale.

7.4. Flusso del documento analogico

La corrispondenza analogica in arrivo perviene all'Ateneo 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 al Settore Protocollo;
- posta recapita personalmente, *brevi manu*.

[7] In analogia a quanto avviene per i documenti ricevuti tramite PEC.

7.5. Apertura delle buste

Tutte le buste vanno aperte a cura del Settore Protocollo.

Fanno eccezione e pertanto non vanno aperte, le buste:

- riportanti le seguenti diciture: riservato, personale, confidenziale, etc. o dalla cui confezione si evinca il carattere di corrispondenza privata (ad esempio, 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 esempio, il CIG);
- le altre buste indirizzate nominativamente al personale vanno aperte nella convinzione che nessun dipendente utilizzi l’Amministrazione come casella postale privata. Chiunque riceva, tramite corrispondenza privata, documenti concernenti affari o procedimenti amministrativi dell’Amministrazione è tenuto a farli pervenire tempestivamente al Settore Protocollo.

7.5.1. Conservazione delle buste

Le buste pervenute tramite posta raccomandata, corriere o altra modalità, sono spillate assieme al documento e trasmesse alla UOR.

7.6. Priorità nella registrazione dei documenti in arrivo

Indipendente dalla modalità di arrivo dei documenti informatici o analogici, 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 della Rettrice;
- documenti ricevuti direttamente dalla segreteria della Direttrice Generale;
- documenti ricevuti direttamente dall’Ufficio Legale;
- documenti relativi a procedimenti ispettivi;

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.

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.

7.7. Protocollo riservato

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

- documenti di carattere politico e di indirizzo di competenza della Rettrice o della Direttrice 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 categorie particolari di dati personali;
- documenti legati a vicende di persone o a fatti privati e, in particolare, i documenti riportanti dati giudiziari.

7.7.1. Procedure del protocollo riservato

Le tipologie di documenti da registrare nel protocollo riservato sono individuate dal Coordinatore della gestione documentale, in collaborazione con gli organi monocratici e d'intesa con i responsabili delle AOO/UOR.

A protezione della riservatezza il documento analogico viene trasmesso direttamente al RPA in busta chiusa, sigillata e firmata sui lembi di chiusura.

Alla Rettrice, alla Direttrice 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 riservato saranno gli organi monocratici a definirne l'utilizzo in collaborazione con il Coordinatore della gestione documentale/Responsabile della gestione documentale.

Per le altre AOO dell'Ateneo sarà il rispettivo Responsabile della gestione documentale ad essere abilitato alla tenuta e gestione del protocollo riservato della AOO medesima.

7.8. Eccezioni - documentazione registrata in appositi gestionali

L'Ateneo utilizza *software* gestionali dedicati alla registrazione e gestione di tipologie documentali e procedimenti che, pur non rientrando nelle registrazioni riservate, non sono

integrati al sistema di protocollo e pertanto non sono acquisiti da questo ultimo (ad esempio, diritto allo studio, gestione presenze e giustificativi del personale, etc.).

7.9. Annullamento di una registrazione

È consentito l'annullamento di una registrazione di protocollo per motivate e verificate ragioni.

Solo il Coordinatore della gestione documentale, i Responsabili della gestione documentale e le persone espressamente delegate sono autorizzati 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;
- 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 dalla UOR che ha richiesto l'annullamento.

La richiesta di annullamento, inviata a mezzo *e-mail* alla casella istituzionale della AOO di competenza, sarà associata alla registrazione di protocollo del documento annullato a cura del Coordinatore della gestione documentale/dei Responsabili della gestione documentale o delle persone espressamente delegate.

In Titulus i documenti annullati devono essere inseriti nei rispettivi fascicoli o, nel caso di documento non inerente a specifico procedimento, in un fascicolo annuale.

Se il documento analogico o informatico annullato costituisce una tipologia documentale soggetta a registrazione particolare (ad esempio, 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.

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.

Si può comunque procedere all'annullamento di un documento ricevuto con PEC sebbene il mittente abbia già la ricevuta di avvenuta consegna. In questo caso il mittente riceverà una notifica di annullamento del suo documento con la relativa motivazione.

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), che viene protocollato e inviato via PEC.

7.10. 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 il Settore Protocollo 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 in Sapienza.

7.11. 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;
- Trasmissione al Settore Protocollo dei repertori analogici per la conservazione illimitata.

7.12. Casi di assegnazione dubbia

Nel caso di assegnazione da parte del Settore Protocollo di un documento in arrivo ad una UOR non corretta, il responsabile della UOR stessa deve inviare tempestivamente una *e-mail* al Settore Protocollo chiedendo la derubrica.

Il Settore Protocollo, effettuate le opportune verifiche, provvede a cambiare l'assegnazione inviando il documento alla UOR di competenza.

I documenti possono comunque essere riassegnati direttamente nel caso di UOR appartenenti alla stessa Area.

Nel caso di documento originale analogico, si può procedere alla nuova assegnazione ad altra UOR solo dopo aver ricevuto nuovamente l'originale.

In caso di conflitto di competenze tra UOR è la Direttrice Generale, con il supporto del Coordinatore della gestione documentale, a determinare l'assegnazione definitiva.

7.13. Flusso del documento informatico in partenza

Il documento informatico prodotto deve essere redatto preferibilmente nel formato PDF/A o per casi particolari secondo gli altri formati stabiliti in precedenza (cfr. par. 3.2.2) 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:
    - logo;
    - 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;
- 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*:

- logo;
- 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 documento informatico protocollato può essere trasmesso via *e-mail* e a mezzo PEC.

7.14. 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, gli stessi possono essere prodotti in PDF/A e la registrazione a protocollo costituisce firma elettronica avanzata.

7.15. Flusso del documento informatico tra AOO dell'Ateneo

A partire dal 30 ottobre 2023 il flusso dei documenti informatici tra le AOO dell'Ateneo prevede l'utilizzo della funzione di interoperabilità tra AOO interne. Tramite questa funzione in sostituzione della PEC si utilizzano i *web service* di Titulus per l'invio e la ricezione dei documenti all'interno dell'Ateneo, mantenendo lo stesso valore giuridico probatorio della PEC.

L'attivazione di un workflow automatico trasferisce la documentazione che dai Centri di spesa è indirizzata alla AOO Amministrazione centrale, indipendentemente dal destinatario indicato dal mittente Centro di spesa, di default al Settore Protocollo nella casella "Bozze" o "Da altre AOO". Il Settore Protocollo provvede poi a modificare eventualmente l'oggetto, classifica il documento e lo assegna alla UOR competente, come indicato dal Centro di spesa, che si occuperà della fascicolatura.

I documenti inviati dall'AOO Amministrazione centrale ai Centri di spesa e scambiati tra Centri di spesa, vengono ricevuti dai destinatari nelle caselle "Bozze" o "Da altre AOO".

Le indicazioni operative sono consultabili alla pagina: https://www.uniroma1.it/it/pagina/settore-protocollo-gestione-e-conservazione-documentale

7.16. 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*, etc.), 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.

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 eIDAS corrisponde alla firma digitale italiana; utilizzata per tutti i documenti per cui viene richiesto dalla normativa.

Firma digitale: particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. Ha effetti giuridici equivalenti ad una firma elettronica qualificata.

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

CAPITOLO 8 – CASISTICA E COMPORTAMENTI

8.1. Gestione delle gare d'appalto

8.1.1. 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.

Nell'oggetto si riporta la descrizione della gara/offerta così come è riportata sulla busta, Gli uffici che indicono le procedure possono dare disposizione di apporre sulla busta una dicitura, ad esempio, "Non aprire: offerta per la procedura negoziata per la realizzazione di… - CIG: … - CUP: …".

8.1.2. 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.

8.2. 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 esempio, delle pubblicazioni]".

Nei casi in cui l'istanza viene prima esaminata dalla UOR e gli allegati trattenuti, è possibile trasmettere al Settore Protocollo 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 Settore/Ufficio …".

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

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

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

8.3. Atti giudiziari

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

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

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

Ai sensi dell'art. 149-bis codice di procedura civile, la copia estratta dal documento originale deve essere firmata digitalmente dall'ufficiale giudiziario e, se non è fatto espresso divieto dalla legge, la notificazione può eseguirsi a mezzo posta elettronica certificata, anche previa estrazione di copia informatica del documento analogico.

In questo caso, l'ufficiale giudiziario trasmette copia informatica dell'atto sottoscritta con firma digitale all'indirizzo di posta elettronica certificata del destinatario risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni.

La notifica si intende perfezionata nel momento in cui il gestore rende disponibile il documento informatico nella casella di posta elettronica certificata del destinatario.
Per mittente si intende la parte istante, cioè il legale/avvocato delegato mediante procura alle liti che agisce in nome e per conto del soggetto interessato e che ha richiesto la notifica dell'atto.
Anche un sindacato o un'associazione non riconosciuta, può essere mittente, nel caso in cui agisca in nome e per conto di un lavoratore in una controversia sindacale.
Il mittente del documento non è l'organo giudiziario indicato generalmente sul frontespizio dell'atto (ad es., Tribunale, Corte di Appello), ma colui che ha richiesto la notificazione, generalmente il legale a cui il ricorrente/attore che ha conferito mediante mandato la procura alle liti (quindi il corrispondente apposto di norma sulla prima pagina dell'atto in alto a destra).
Quando l'atto è notificato presso l'Avvocatura Distrettuale o Generale dello Stato, in quanto soggetto che assicura la difesa in giudizio dell'Amministrazione, l'Avvocatura stessa generalmente procede alla trasmissione dell'atto all'Ateneo, dandone informativa, quindi il mittente da indicare nella registrazione di protocollo è l'Avvocatura.
In tal caso si tratta di una comunicazione, non di una notifica, il cui mittente da indicare nella registrazione di protocollo è appunto l'Avvocatura, come per tutte le comunicazioni dalla stessa provenienti.
Diverse sono poi le comunicazioni (quali quelle consistenti in avvisi di deposito di note o di fissazione di udienza) che provengono direttamente dalla cancelleria dell'autorità giudiziaria (Tribunale, Corte di appello, etc.) innanzi a cui pende il giudizio.
In questi casi il mittente è sicuramente l'autorità giudiziaria medesima.
Le comunicazioni che provengono dalla cancelleria dell'autorità giudiziaria arrivano tramite l'applicativo del processo civile telematico – PTC, sono conservate nella casella PEC, rilasciata dall'ordine professionale a cui è iscritto l'avvocato che ha in carico la pratica.
Si noti che, nei procedimenti giuslavoristici (cause di lavoro), contestuale al ricorso introduttivo del giudizio si trova il pedissequo decreto di fissazione di udienza, in calce al ricorso stesso.
In tal caso si è in presenza, contestualmente di un atto di parte e di un atto prodotto dall'organo giurisdizionale.

8.4. 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 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”.

8.5. 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 ss.mm.ii., 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 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.
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.
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[8].

8.6. 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, questo avrà durata pari a quanto indicato nel documento stesso; in caso di indisponibilità 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.
Questo avviso è acquisito come documento protocollato.
A questo punto è possibile consultare il sistema del DURC *on-line* e procedere come per i DURC immediatamente disponibili.

[8] DM MEF 17 giugno 2014.

8.7. Denunce di infortuni

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

Le denunce di infortunio sono inviate esclusivamente in modalità telematica dai datori di lavoro di Sapienza abilitati sul portale dell'INAIL (ovvero i Presidi, i Direttori di Dipartimento/Area/Centro di Ricerca e di Servizi e/o dai loro delegati) che accedono ai servizi online dell'Istituto unicamente tramite credenziali digitali SPID, CIE, CNS.

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 fornire la descrizione dell'infortunio e le informazioni necessarie con ogni mezzo disponibile.

Il delegato alle denunce che riceva tale informazioni in modo incompleto dovrà chiederne tempestivamente l'integrazione all'infortunato.

La procedura telematica sul portale INAIL sostituisce il protocollo in uscita del documento, quindi le denunce di infortunio sono una tipologia di documenti esclusa dalla registrazione di protocollo (vengono protocollati solo eventuali scambi con l'INAIL relativi a richieste di informazioni/integrazioni successive alla denuncia e che pervengono via PEC).

8.8. 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.

8.9. 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 descritti di seguito.

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,* stipulate da Consip, ai sensi dell'art. 26 della Legge 488/99, nell'ambito delle quali i fornitori aggiudicatari di gare 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)
- Sistema Dinamico di Acquisizione (SDAPA)

8.9.1. 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.

8.9.2. Adesioni – Convenzioni

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

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

Il punto ordinante controlla la bozza, genera attraverso la piattaforma il file pdf/a che costituisce il documento d'ordine (Ordine di Acquisto OdA), lo scarica localmente, lo firma digitalmente, lo registra nel sistema di protocollo e lo ricarica a sistema.

La piattaforma MePA chiede il numero di protocollo per procedere nella registrazione.

Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l'emissione del corrispondente documento gestionale.

8.9.3. Procedure negoziate (RdO) - MePA

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

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 e lo ricarica a sistema.

8.9.4 Sistema Dinamico di Acquisizione (SDAPA)

Strumento di negoziazione disciplinato all'art. 32 del Dlgs 36/2023, introdotto da Consip nel 2012, dopo le Convenzioni, il Mercato Elettronico e gli Accordi Quadro. Attraverso lo SDAPA le stazioni appaltanti negoziano gli appalti autonomamente e, a differenza delle

Convenzioni ed Accordi Quadro, con tale strumento Consip si limita esclusivamente a mettere a disposizione il sistema di e-procurement.
Attraverso lo SDAPA è possibile aggiudicare appalti di qualsiasi valore economico, anche superiore alla soglia comunitaria.

8.10. Documenti pervenuti via PEC

La ricezione via PEC di un documento comprova il fatto che lo stesso ha raggiunto il destinatario.
In ogni caso sono soggetti a registrazione di protocollo:

- il messaggio;
- i *file* allegati.

Per quanto riguarda la corretta identificazione del mittente, bisogna tener presente che la PEC è solo un vettore, il mittente è colui che sottoscrive il documento allegato o, nel caso di testo nel corpo del messaggio (*body message*) senza allegato, colui che lo trasmette.
Nel caso in cui con uno stesso messaggio PEC pervengano documenti di firmatari diversi, senza alcun documento con funzione di lettera di trasmissione, è prodotta una registrazione distinta per documento, corredata di annotazioni esplicative.
In alternativa è lasciato l'indirizzo così come pervenuto e nell'oggetto è scritto: "Trasmissione di documenti con firmatari diversi"; oppure, se si evince che l'indirizzo PEC è riconducibile in mondo certo a uno dei firmatari dei documenti trasmessi, si indica nell'oggetto: "Cognome Nome trasmette per sé e per …".
La regola generale da seguire, in base al principio di simmetria delle forme, è che a un documento pervenuto con PEC si risponde con un documento trasmesso con PEC, utilizzando lo stesso canale di comunicazione.
Qualora il messaggio di posta elettronica pervenga a una casella di PEC dello stesso ente, ma diversa da quella competente, si protocolla il documento in entrata, si inoltra il messaggio PEC alla casella corretta e nella causale si indica l'AOO corretta e il relativo indirizzo PEC.

8.11. Gestione di soli allegati pervenuti via PEC e di documenti costituiti dal solo corpo della PEC

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

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

8.12.1. 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 al Settore Protocollo di Ateneo.

L'art. 65 comma 1 lettera c) del CAD recita: "Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica…" "…sono valide…" "… quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'art. 64, comma 2".

L'insieme di queste disposizioni fornisce la possibilità di sostituire la firma autografa su un modulo analogico con l'invio del modulo compilato da un indirizzo di posta elettronica istituzionale fornito dall'ente.

Le richieste di informazioni su orari di apertura, sul funzionamento di procedure, lamentele, doglianze, comunicazioni di disservizi devono essere valutate caso per caso.

8.13. 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, etc.). Per i documenti sottoscritti con firma elettronica è necessario verificare anche che la data e l'ora di firma coincidano.

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

Se il secondo esemplare perviene in formato analogico, si appone su di esso la segnatura di protocollo e l'indicazione "Secondo esemplare".

Nella registrazione di protocollo si inserisce la "Annotazione" in modo immodificabile "Pervenuto secondo esemplare mediante raccomandata a/r" al fine di poter recuperare tutti gli esemplari pervenuti nel caso si debba, ad esempio, modificare la UOR indicata nella segnatura di protocollo.

Nel caso di arrivo mediante PEC o altro sistema informatico (*e-mail* semplice, etc.) si effettua una registrazione come "Documento non protocollato", riportando 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 immodificabile del tipo “Il documento non è stato protocollato in quanto trattasi di secondo esemplare del documento già pervenuto e registrato con il prot. n. 000 del gg/mm/aaaa”.
Nella registrazione di protocollo del primo esemplare andrà invece inserita l’annotazione “Pervenuto secondo esemplare via PEC (o altro mezzo) – vedi id. n. 000).

8.14. Documenti anonimi

Il comportamento di un operatore durante la fase di registrazione di un documento in arrivo deve essere improntato 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.

8.15. 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 9 – DALL'ARCHIVIO CORRENTE ALL'ARCHIVIO DI DEPOSITO

L'archivio di deposito è la fase intermedia del processo di tenuta dei documenti prodotti dall'Ateneo nel corso della propria attività e si colloca temporalmente tra l'archivio corrente e l'archivio storico.

Il suo carattere di transitorietà e l'introduzione dell'informatizzazione degli archivi hanno condotto alla sottovalutazione di un momento gestionale che ha, prima di tutto, una dimensione logica e un'importanza funzionale rilevanti.

L'archivio di deposito è il momento di decantazione dei documenti e delle informazioni relative, organizzati in fascicoli inerenti ad affari, attività e procedimenti conclusi, per i quali non risulta più necessaria la trattazione corrente o verso i quali sussista solo un interesse sporadico.

Le attività che connotano questa fase d'archivio sono definite dal TUDA, artt. 67, 68 e 69 e riguardano l'obbligo della periodicità dei trasferimenti di documenti dall'archivio corrente, la conservazione ordinata delle unità archivistiche e la disponibilità dei mezzi di corredo per assicurare le funzioni di controllo e di ricerca del materiale (registri di protocollo, piani di classificazione, repertori dei fascicoli, etc.)[9].

I documenti sono conservati rispettando l'organizzazione che essi avevano nell'archivio corrente.

La produzione e gestione informatica di dati e di documenti comporta una diversificazione delle procedure di gestione durante la fase di deposito determinata dalla peculiarità del supporto.

Ciononostante, non cambia il ruolo e la funzione concettuale svolta dall'archivio di deposito nella tenuta del sistema documentale.

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

I documenti nativi digitali sono caratterizzati dalla predeterminazione dei termini di conservazione.

Ciò significa che la durata della vita di un documento è determinata nel momento stesso in cui il documento viene creato.

[9] P. Carucci, M. Guercio, *Manuale di archivistica*, p. 217.

Si tratta di una forma di impostazione della selezione a priori dei documenti, attività che avviene anche per i documenti analogici, ma che è messa in atto solo in un secondo momento, durante la fase di deposito.

I servizi e le attività che caratterizzano l'archivio di deposito analogico sono:

- Attività preliminari finalizzate alla creazione di locali d'archivio a norma:
    - individuare, attrezzare adeguatamente e gestire i locali da destinare a deposito d'archivio (accesso limitato al solo personale qualificato, pulizia periodica, etc.);
    - individuare il responsabile del servizio.
- Attività ordinarie caratterizzanti la gestione dell'archivio di deposito:
    - trasferimenti periodici dei documenti dagli uffici e acquisizione delle unità da parte dell'archivio di deposito: predisposizione annuale del trasferimento dei fascicoli relativi ad affari conclusi con la predisposizione di appositi elenchi di consistenza;
    - concentrazione ordinata dei documenti, mantenendo le aggregazioni (serie e fascicoli) create nella fase di formazione e revisione degli elenchi di trasferimento: schedatura sommaria delle unità trasferite in archivio attribuendo una numerazione univoca, continua e progressiva che determina la posizione logica e fisica delle unità nell'elenco di consistenza e nel locale d'archivio;
    - selezione della documentazione sulla base del Piano di conservazione;
    - campionatura di determinate tipologie documentali da non destinare integralmente alla conservazione a lungo termine;
    - scarto della documentazione;
    - riordinamento e ricostituzione delle serie originarie;
    - conservazione adeguata dei documenti: sostituzione delle unità di condizionamento laddove danneggiate o non adatte alla conservazione a medio o lungo termine, mantenimento delle condizioni ambientali ottimali, etc.;
    - versamento della documentazione all'archivio storico: predisposizione degli elenchi di versamento e aggiornamento dell'elenco di consistenza;
    - servizio di ricerca documentale;

- predisposizione di statistiche sia per le attività di trasferimento e versamento che di consultazione per una adeguata programmazione degli spazi e ottimizzazione dei servizi.

- Selezione della documentazione e redazione di:
  - elenco di scarto, contenente la descrizione della documentazione per la quale chiedere l'autorizzazione per l'invio al macero;
  - elenco di versamento all'archivio storico, contenente la descrizione della documentazione da conservare senza limiti di tempo;
  - elenco di consistenza dell'archivio di deposito, contenente la descrizione della documentazione rimasta dopo lo scarto ed il versamento in archivio storico, da conservare in archivio di deposito in attesa di successivi versamenti/scarti;
  - procedura di scarto.

Pertanto l'archivio di deposito dell'Ateneo si configura come la somma di numerosi fondi (relativi all'Amministrazione Centrale e alle varie strutture periferiche) fisicamente distribuiti in diversi locali e sedi dell'Ateneo.

Per quanto riguarda i documenti digitali, si preferisce distinguere tra produzione, gestione e conservazione.

La fase di deposito tradizionalmente intesa, va a collocarsi a cavallo tra le fasi di gestione e conservazione.

Pertanto quando si parla di trasferimento delle unità archivistiche informatiche si intende la generazione e trasmissione dei pacchetti di versamento al sistema di conservazione, avvalendosi anche di processi di automazione disponibili nel sistema di gestione documentale.

Le attività e i servizi relativi all'archivio di deposito sono in fase di implementazione/riorganizzazione da parte dell'Ateneo che si riserva una più puntuale descrizione nelle successive versioni del presente Manuale.

CAPITOLO 10 – IL SISTEMA INFORMATICO

Il sistema di gestione informatica dei documenti 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[10].

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.

Affinché il processo di gestione informatica dei documenti possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento.

Il presente capitolo tratta, tra i vari argomenti, le misure di sicurezza fisica e logica e le procedure comportamentali adottate per la protezione dell'infrastruttura del sistema di gestione documentale, delle informazioni e dei dati.

In essi è data evidenza di quali ambiti siano gestiti e curati dal Consorzio Cineca, quali siano curati dal Centro InfoSapienza dell'Ateneo e quali invece rimangano in carico esclusivo a ogni specifica Area Organizzativa Omogenea.

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

10.1. 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 Centro InfoSapienza[11].

Nell'ambito della gestione documentale, l'Ateneo ha acquisito 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

[10] TUDA, art.1, lettera r.

[11] Istituito con decreto del Rettore il 1° gennaio 2011. Con delibere del Senato Accademico e del Consiglio di Amministrazione, rispettivamente nelle sedute del 30.11.2010 e del 7.12.2010, si è dato seguito a quanto previsto dall'art. 15 dello Statuto di Ateneo, trasformando la preesistente Area Infosapienza in Centro di spesa, con proprio Regolamento. Svolge attività di progettazione e sviluppo di nuove soluzioni tecnologiche finalizzate all'ammodernamento ed all'innovazione dei servizi erogati all'utenza universitaria; progettazione, sviluppo e gestione del sistema informativo della Sapienza; implementazione e gestione delle infrastrutture tecnologiche delle piattaforme architetturali sulle quali operano i sistemi informativi della Sapienza; nonché gestione degli strumenti informatici in ausilio alla produttività individuale; pianificazione, sviluppo, funzionamento e monitoraggio della rete dati e fonia della Sapienza. Cfr. https://web.uniroma1.it/infosapienza/chi-siamo.

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.

10.2. 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 ne permettono l'utilizzo tramite meccanismi di interoperabilità.

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[12], 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.

10.3. Sicurezza del sistema informatico

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

Il piano della sicurezza informatica relativo a formazione, gestione, trasmissione, interscambio, accesso, memorizzazione dei documenti informatici, ivi compresa la gestione delle copie di sicurezza è predisposto e aggiornato annualmente dal Consorzio Cineca.

10.3.1. Sicurezza fisica dei *data center*

Le misure adottate per garantire un adeguato livello di sicurezza fisica del *data center* del Consorzio Cineca sono descritte nella scheda tecnica *Servizio di Hosting Cineca*.

Sono illustrate 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

[12] GARR è la rete nazionale a banda ultralarga dedicata alla comunità dell'istruzione e della ricerca. Il suo principale obiettivo è quello di fornire connettività ad alte prestazioni e di sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti e per la collaborazione a livello internazionale. La rete GARR è ideata e gestita dal Consortium GARR, un'associazione senza fini di lucro fondata sotto l'egida del Ministero dell'Istruzione, dell'Università e della Ricerca.

misure adottate per la protezione dei dati e le caratteristiche del servizio di *Disaster Recovery*.

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

10.3.2. 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 nel Regolamento per l'utilizzo della Rete Dati di Ateneo[13].

Nello specifico, è stabilito che la rete trasmissione di Sapienza può essere utilizzata esclusivamente per l'attività didattica, scientifica e strumentale che rivesta un interesse per l'Ateneo; qualsiasi accesso alla rete deve essere associato ad una persona fisica, attraverso la registrazione di un indirizzo IP fisso, alla quale saranno riconducibili le attività svolte dall'indirizzo IP di cui è responsabile.

Ogni utente della rete sarà identificato e sarà tenuto ad adottare le necessarie misure per non interferire nel corretto funzionamento delle comunicazioni, per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti ed evitare che le attività svolte producano disturbo o danni agli altri utenti.

Le regole tecniche di gestione della rete sono affidate al Settore Rete dati e fonia del Centro InfoSapienza.

Il Centro InfoSapienza, in qualità di amministratore della rete di Ateneo, assicura in modo esclusivo e tempestivo la gestione, il monitoraggio, l'aggiornamento e l'ampliamento della rete dati di Ateneo (cablaggio e parte attiva), sia sotto l'aspetto fisico che logicistico, 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.

[13] Sul tema, cfr. Regolamento generale per l'utilizzo della rete telematica di Sapienza Università di Roma, www.sapienzanet.uniroma1.it/regolamento.asp

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.
Ciascuna AOO è responsabile dei dispositivi collegati alla rete di Ateneo e utilizzati 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.

10.3.3. Le postazioni di lavoro

Le postazioni di lavoro degli utenti dell'Amministrazione Centrale sono gestite dal Centro InfoSapienza.
Ogni AOO verifica il coerente utilizzo delle postazioni di lavoro, da tavolo o portatili, o gli strumenti comunque funzionalmente assimilabili, mentre il Centro InfoSapienza predispone la necessaria dotazione di dispositivi (*hardware*) e programmi (*software*) tali da consentire il corretto funzionamento e il mantenimento in condizioni di sicurezza ai fini del regolare svolgimento dell'attività lavorativa.
Le postazioni di lavoro soddisfano i criteri minimi di sicurezza, in particolare:

- il sistema operativo è aggiornato e aggiornabile;
- gli applicativi installati e i loro componenti software aggiuntivi (ad esempio, *plug-in*) sono aggiornati e aggiornabili;
- sono dotate di un programma antivirus con funzionalità automatica di aggiornamento periodico;
- l'accesso al sistema operativo della postazione di lavoro è protetto da password di adeguata complessità, cambiata con cadenza regolare;
- sono dotate di *firewall* locale impostato per consentire solo le connessioni instaurate dal *client* stesso e per i servizi legittimi (*client mode*);
- 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*, etc.);
- 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.

10.4. Sicurezza dei documenti informatici

L'accesso al sistema di gestione documentale di ogni utente di tutte le AOO dell'Ateneo è gestito centralmente ed è subordinato all'abilitazione a cura del Settore Protocollo.

Le identità digitali utilizzate per l'accesso al sistema di gestione documentale sono costituite da *nome utente* e *password* (sistema di Identity Management).

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

Ciascun utente ha la possibilità di cambiare la propria *password* in qualsiasi momento ed è auspicabile che ciò avvenga nel caso in cui si presume che essa abbia perso il requisito della segretezza.

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

Il sistema di gestione documentale rispetta le misure di sicurezza previste dal D.Lgs. n. 101/2018, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" e dalla Circolare n. 2/2017 AgID recante le misure minime di sicurezza ICT per le pubbliche amministrazioni.

I dati sono resi disponibili e accessibili a chiunque ne abbia diritto; i soggetti preposti al trattamento dei dati (titolare del trattamento, responsabili del trattamento, designati al trattamento, etc.) sono individuati nel Regolamento in materia di protezione dei dati personali[14]; con apposito atto il Consorzio Cineca è stato nominato Responsabile del trattamento[15].

10.4.1. Accesso ai dati e ai documenti informatici

Il sistema adottato dall'Ateneo garantisce:

- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso ai documenti, alle informazioni e ai dati esclusivamente agli utenti abilitati;

[14] Cfr. https://www.uniroma1.it/sites/default/files/field_file_allegati/regolamento_protezione_dati_prot.pdf
[15] Atto di nomina a responsabile del trattamento prot. n. 14917 del 18/02/2019.

- 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 Coordinatore della gestione documentale di concerto con i Responsabili del trattamento dei dati e i Responsabili della gestione documentale delle diverse AAO, sono in sintesi:

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

10.4.2. 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;

- 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’Ateneo 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*.

ALLEGATI

Allegato 1 - Riferimenti normativi

- Legge 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto del Presidente della Repubblica 4 aprile 2002, n. 101, Regolamento recante criteri e modalità per l'espletamento da parte delle amministrazioni pubbliche di procedure telematiche di acquisto per l'approvvigionamento di beni e servizi;
- Direttiva del Ministro per l'innovazione e le tecnologie 9 dicembre 2002, Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali;
- Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali;
- Legge 9 gennaio 2004, n. 4, Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti Informatici;
- Decreto legislativo 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
- Decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale;
- Legge 24 dicembre 2007, n. 244, Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008);
- Decreto legge 29 novembre 2008, n. 185, Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale;
- Legge 3 marzo 2009, n. 18 Ratifica ed esecuzione della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, con Protocollo opzionale, fatta a New York il 13 dicembre 2006 e istituzione dell'Osservatorio nazionale sulla condizione delle persone con disabilità;
- Legge 18 giugno 2009, n. 69, Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile;

- Decreto legislativo 27 ottobre 2009, n. 150, Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche Amministrazioni;
- Deliberazione del Garante per la protezione dei dati personali 2 marzo 2011, n. 88, Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web;
- Decreto Legge n. 9 febbraio 2012, n. 5 coordinato con la Legge di conversione 4 aprile 2012, n. 35, Disposizione urgenti in materia di semplificazione e di sviluppo;
- Legge 17 dicembre 2012, n. 221, Conversione in legge, con modificazioni, del Decreto Legge 18 ottobre 2012, n. 179 recante ulteriori misure urgenti per la crescita del Paese;
- DPCM 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Circolare dell'Agenzia per l'Italia Digitale 29 marzo 2013, n. 61, Disposizioni del Decreto legge n. 79 del 18 ottobre 2012 in tema di accessibilità dei siti web e servizi informatici. Obblighi delle pubbliche amministrazioni;
- Decreto del Ministro dell'Economia e delle Finanze 3 aprile 2013, n. 55, Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244;
- DPCM 3 dicembre 2013, Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Deliberazione del Garante per la protezione dei dati personali 15 maggio 2014, n. 243, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati;
- Decreto del Ministro dell'Economia e delle Finanze 17 giugno 2014, Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005;

- Regolamento del Parlamento e del Consiglio dell'Unione europea 23 luglio 2014, n. 910, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (eIDAS);
- Decreto legge 24 aprile 2014, n. 66, Misure urgenti per la competitività e la giustizia sociale;
- Legge 16 maggio 2014, n. 78, Conversione in legge, con modificazioni, del decreto legge 20 marzo 2014, n. 34, recante disposizioni urgenti per favorire il rilancio dell'occupazione e per la semplificazione degli adempimenti a carico delle imprese;
- Decreto del Ministero del lavoro e delle politiche sociali 30 gennaio 2015, Semplificazione in materia di documento unico di regolarità contributiva (DURC);
- Circolare interpretativa n 1/DF del 9 marzo 2015 in tema di fatturazione elettronica;
- Deliberazione del Garante per la protezione dei dati personali 19 marzo 2015, n. 161, Linee guida in materia di trattamento di dati personali per profilazione on line;
- Decreto legislativo 18 aprile 2016, n. 50 Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture;
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- Circolare 18 aprile 2017, n.2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici dell'11 settembre 2020, aggiornate a maggio 2021.

Allegato 2 - Profili di abilitazioni nel sistema di protocollo

Di seguito sono elencati i principali profili di abilitazione utilizzati dall'Ateneo all'interno del sistema di protocollo Titulus.

Per gli utenti dell'Amministrazione centrale:

- Operatore di protocollo-smistamento (registra solo documenti in arrivo)
- Operatore di protocollo decentrato abilitato alla registrazione di:
    - documenti in partenza e tra uffici, oppure
    - documenti in partenza, tra uffici, decreti e disposizioni, oppure
    - documenti in partenza, tra uffici e disposizioni
- Operatore registrazione decreti e disposizioni
- Operatore ufficio concorsi (registra documenti in partenza, tra uffici, decreti, disposizioni e domande di concorso in arrivo)
- Responsabile di UOR abilitato alla registrazione di:
    - solo documenti non protocollati, oppure
    - documenti in partenza e tra uffici, oppure
    - documenti in partenza, tra uffici, decreti e disposizioni, oppure
    - documenti in partenza, tra uffici e disposizioni
- Utente incaricato (registra solo documenti non protocollati)
- Utente operatore incaricato (registra solo documenti non protocollati e visualizza documenti riservati personali e fascicoli della propria UOR).

Per gli utenti delle strutture decentrate:

- Responsabile di AOO (utilizzato per i Responsabili amministrativi delegati; può avere abilitazione alla registrazione dei documenti oppure avere diritti di sola visualizzazione)
- Protocollista abilitato alla registrazione di:
    - documenti in arrivo, in partenza e riservati, con visibilità su tutto il protocollo, oppure
    - documenti in arrivo e in partenza, oppure
    - documenti in partenza
- Protocollista in sola visualizzazione della propria UOR
- Utente in visualizzazione (registra solo documenti non protocollati, con visibilità della propria UOR).

Allegato 3 - Titolario di classificazione

TITOLARIO DI CLASSIFICAZIONE UNICO

per l'Amministrazione centrale, le strutture didattiche, di ricerca e di servizio della Sapienza

Titolo I. Amministrazione

1. Normativa e relativa attuazione
2. Statuto
3. Regolamenti
4. Stemma, gonfalone e sigillo
5. Sistema informativo, sicurezza dell'informazione e sistema informatico
6. Protezione dei dati personali
7. Archivio
8. Trasparenza e relazioni con il pubblico
9. Strategie per il personale, organigramma e funzionigramma
10. Rapporti sindacali e contrattazione
11. Controllo di gestione e sistema di qualità
12. Statistica e auditing
13. Elezioni e designazioni
14. Associazioni e attività culturali, sportive e ricreative
15. Editoria e attività informativo-promozionale
16. Onorificenze, cerimoniale e attività di rappresentanza
17. Politiche e interventi per le pari opportunità
18. Interventi di carattere politico, economico, sociale e umanitario

Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia

1. Rettore
2. Prorettore vicario e delegati
3. Direttore generale
4. Direttore
5. Preside
6. Presidente
7. Senato accademico
8. Consiglio di amministrazione
9. Consiglio
10. Giunta
11. Assemblea di facoltà
12. Giunta di facoltà
13. Collegio didattico
14. Comitato di monitoraggio
15. Comitato direttivo del centro
16. Commissione ricerca
17. Presidio qualità
18. Commissione didattica paritetica docenti-studenti
19. Collegio dei direttori di dipartimento
20. Nucleo di valutazione di ateneo
21. Collegio dei revisori dei conti
22. Collegio di disciplina
23. Commissione etica
24. Garante degli studenti
25. Comitato unico di garanzia per le pari opportunità – CUG
26. Conferenza dei rettori delle università italiane – CRUI
27. Consiglio di area didattica

Titolo III. Didattica, ricerca programmazione e sviluppo

1. Ordinamento didattico
2. Corsi di studio
3. Corsi ad ordinamento speciale
4. Corsi di specializzazione
5. Master
6. Corsi di dottorato
7. Corsi di perfezionamento e corsi di formazione
8. Programmazione didattica, orario delle lezioni, gestione delle aule e degli spazi
9. Gestione degli esami di profitto, di laurea e di prove di idoneità
10. Programmazione e sviluppo, comprese aree, macroaree e settori scientifico-disciplinari
11. Strategie e valutazione della didattica e della ricerca
12. Premi e borse di studio finalizzati e vincolati
13. Progetti e finanziamenti
14. Accordi per la didattica e per la ricerca
15. Rapporti con enti e istituti di area socio sanitaria
16. Opere dell'ingegno, brevetti e imprenditoria della ricerca
17. Piani di sviluppo dell'università
18. Cooperazione con paesi in via di sviluppo
19. Attività per conto terzi

Titolo IV. Attività giuridico-legale

1. Contenzioso
2. Atti di liberalità
3. Violazioni amministrative e reati
4. Responsabilità civile, penale e amministrativa del personale
5. Pareri e consulenze

Titolo V. Studenti e laureati

1. Orientamento, informazioni e tutorato
2. Selezioni, immatricolazioni e ammissioni
3. Trasferimenti e passaggi
4. Cursus studiorum e provvedimenti disciplinari
5. Diritto allo studio, assicurazioni, benefici economici, tasse e contributi
6. Tirocinio, placement, formazione e attività di ricerca
7. Servizi di assistenza socio-sanitaria e a richiesta
8. Conclusione e cessazione della carriera di studio
9. Esami di stato e ordini professionali
10. Associazionismo, goliardia e manifestazioni organizzate da studenti o ex studenti

Titolo VI. Strutture didattiche, di ricerca e di servizio

1. Poli
2. Facoltà
3. Dipartimenti
4. Strutture ad ordinamento speciale
5. Scuole di specializzazione
6. Scuole di dottorato
7. Centri
8. Sistema bibliotecario
9. Musei, pinacoteche e collezioni
10. Consorzi ed enti a partecipazione universitaria
11. Fondazioni

Titolo VII. Personale

1. Concorsi e selezioni
2. Assunzioni e cessazioni
3. Comandi e distacchi
4. Mansioni ed incarichi
5. Carriera e inquadramenti
6. Retribuzione e compensi
7. Adempimenti fiscali, contributivi e assicurativi
8. Pre-ruolo, trattamento di quiescenza, buonuscita
9. Dichiarazione di infermità ed equo indennizzo
10. Servizi a domanda individuale
11. Assenze
12. Tutela della salute e sorveglianza sanitaria
13. Valutazione, giudizi di merito e provvedimenti disciplinari
14. Formazione e aggiornamento professionale
15. Deontologia professionale ed etica del lavoro
16. Personale non strutturato

Titolo VIII. Finanza, contabilità e bilancio

1. Ricavi ed entrate
2. Costi ed uscite
3. Bilancio
4. Tesoreria, cassa e istituti di credito
5. Imposte, tasse, ritenute previdenziali ed assistenziali

Titolo IX. Edilizia e territorio

1. Progettazione e costruzione di opere edilizie con relativi impianti
2. Manutenzione ordinaria, straordinaria, ristrutturazione, restauro e destinazione d'uso
3. Sicurezza e messa a norma degli ambienti di lavoro
4. Telefonia e infrastruttura informatica
5. Programmazione territoriale

Titolo X. Patrimonio, economato e provveditorato

1. Acquisizione e gestione di beni immobili e relativi servizi
2. Locazione di beni immobili, di beni mobili e relativi servizi
3. Alienazione di beni immobili e di beni mobili
4. Acquisizione e fornitura di beni mobili, di materiali e attrezzature non tecniche e di servizi
5. Manutenzione di beni mobili
6. Materiali, attrezzature, impiantistica e adempimenti tecnico-normativi
7. Partecipazioni e investimenti finanziari
8. Inventari, rendiconto patrimoniale, beni in comodato
9. Patrimonio culturale – Tutela e valorizzazione
10. Gestione dei rifiuti

Titolo XI. Oggetti diversi

(Senza ulteriori suddivisioni in classi; affari che non rientrano nei precedenti titoli di classificazione, neppure per analogia)

Allegato 4 - Elenco repertori attivi

Di seguito sono elencati i repertori attivi presso l'Ateneo:

1. Accordo individuale lavoro agile
2. Atto pubblico
3. Autorizzazioni missioni e rimborsi
4. Contratti e convenzioni
5. Contratto conto terzi
6. Contratto lavoro subordinato
7. Decreti (AOO Periferiche)
8. Decreto
9. Disposizione
10. Disposizione (AOO Periferiche)
11. Ordine di servizio
12. Raccomandata arrivo
13. Richieste di accesso
14. Verbale AG Autorità Giudiziaria
15. Verbale Collegio Revisori dei Conti
16. Verbale del Consiglio di Dipartimento
17. Verbale di Giunta di Dipartimento
18. Verbali Consiglio di Amministrazione seduta ordinaria
19. Verbali Consiglio di Amministrazione seduta ristretta
20. Verbali Senato Accademico
21. Verbali UPD (Ufficio Procedimenti disciplinari)