UNIVERSITÀ
DEGLI STUDI
FIRENZE

MANUALE DI GESTIONE DOCUMENTALE

Versione 1.0 - 31/12/21

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Sommario

UNIVERSITÀ DEGLI STUDI FIRENZE

CAPITOLO 1. IL MANUALE DI GESTIONE DOCUMENTALE

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

Il manuale di gestione è uno strumento operativo che descrive il sistema di produzione e di gestione documenti (analogici e digitali) previsto dalle norme vigenti.

Serve a indicare le procedure e a fornire le istruzioni per la corretta formazione, gestione, tenuta e conservazione della documentazione analogica e digitale. Esso descrive, altresì, le modalità di gestione dei flussi documentali e degli archivi, in modo tale da organizzare e governare la documentazione ricevuta, inviata o comunque prodotta dall'amministrazione secondo parametri di corretta registrazione di protocollo, smistamento, assegnazione, classificazione, fascicolatura, reperimento e conservazione dei documenti.

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

1.2. Modalità di redazione

La redazione del manuale di gestione deve contemperare l'assolvimento dell'obbligo normativo (vedi ALLEGATO 1) e le esigenze concrete dell'Amministrazione.
Per la redazione di questo manuale è stato utilizzato il modello proposto dal Gruppo di lavoro nell'ambito del progetto Procedamus per gli atenei aderenti (www.procedamus.it).

1.3. Forme di pubblicità e di divulgazione

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

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

CAPITOLO 2. QUADRO ORGANIZZATIVO ISTITUZIONALE

2.1. Area organizzativa omogenea e unità organizzativa responsabile

L'Ateneo è organizzato in Area organizzativa omogenea unica (AOO) (vedi ALLEGATO 2).

L'area organizzativa omogenea (AOO) è l'insieme di funzioni e di strutture individuate dall'amministrazione cui sono assegnate funzioni omogenee. Essa, pertanto, presenta esigenze di gestione documentale in modo unitario e coordinato, ai sensi della normativa vigente. L'unità organizzativa responsabile (UOR) è, all'interno della AOO, un complesso organizzato di risorse umane e strumentali cui è stata affidata una competenza omogenea nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari, attività e procedimenti amministrativi (ALLEGATO 3).

L'Ateneo è organizzato come previsto dalla legge 7 agosto 1990, n. 241 (artt. 4-6) e dal DPR 28 dicembre 2000, n. 445 (ALLEGATO 4).

La 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. La gestione dei flussi documentali e degli archivi: servizi

Nell'Università degli Studi di Firenze opera Sistema Archivistico di Ateneo (ALLEGATO 5) con funzioni di tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, oltre a ulteriori specifici compiti attribuiti dalla legge o dall'ordinamento interno dell'Ateneo.
Al Sistema Archivistico di Ateneo è attribuita la competenza di tenuta del sistema di gestione analogica e informatica dei documenti, dei flussi documentali e dell'archivio corrente, nonché il coordinamento degli adempimenti previsti dalla normativa vigente, come previsto dal DPR 445/2000, art. 61 relativo al "Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi". In particolare il servizio cura:

- la correttezza delle operazioni di registrazione, segnatura, gestione dei documenti e dei flussi documentali;
- le richieste di annullamento delle registrazioni di protocollo delle UOR di loro competenza.

Al Sistema Archivistico di Ateneo sovraintende anche alla corretta gestione, tenuta e tutela dei documenti nell'Archivio di Deposito e Storico, vigilando sull'osservanza della normativa in materia di gestione documentale nel ciclo di vita dei documenti riversati.

Nell'Università degli Studi di Firenze opera Sistema Informatico dell'Ateneo Fiorentino - SIAF che soprintende, secondo le sue competenze, anche al sistema di gestione documentale in applicazione del DPR 445/2000, art. 61 "Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi", curando:

- Abilitazione e disabilitazione delle utenze in base alle richieste dei Dirigenti, RAD e Responsabili UOR.
  Le abilitazioni sono gestite con un sistema di profili disegnati in base alle necessità funzionali tipiche della struttura.
  In generale ogni utente sarà attribuito ad un profilo ed eventuali eccezioni saranno valutate da SIAF insieme alla struttura richiedente;
- la notifica ai Responsabili delle UOR di Ateneo l'eventuale indisponibilità del sistema e l'attivazione del registro di emergenza secondo quanto disposto al § 6.9;
- l'adeguamento del sistema di gestione documentale alle eventuali modifiche dell'organigramma e funzionigramma dell'Ateneo a seguito di idonea comunicazione al Sistema Informatici dell'Ateneo Fiorentino - SIAF;
- L'assistenza tecnica per tutti i problemi di funzionamento del gestionale in uso presso l'ateneo;
- L'attivazione o disattivazione delle funzionalità applicative offerte dal protocollo informatico a corredo delle attività tipiche del protocollo considerando le esigenze emerse in Ateneo e concordandole con il fornitore del servizio;

- La gestione degli aggiornamenti del protocollo informatico concordandoli con il fornitore del servizio.

2.3. La gestione dei flussi documentali e degli archivi: figure operative

L'Ateneo è responsabile della gestione dei documenti dalla formazione alla conservazione. Nell'ambito di questa responsabilità l'Ateneo ha individuato le seguenti figure operative sul protocollo e sul sistema di conservazione:

- il Responsabile della gestione documentale
- il Responsabile della conservazione
- il Responsabile alla transizione digitale

2.3.1. Il Responsabile della gestione documentale

Il Direttore generale nomina il Responsabile della gestione documentale (vedi ALLEGATO 6) in ottemperanza alle norme vigenti. Il Responsabile della gestione documentale è coadiuvato dal Sistema Archivistico di Ateneo, dal referente dei sistemi informatici documentali e della sicurezza informatica e dal referente della protezione dei dati personali relativamente alla gestione del sistema documentale.

È compito del Responsabile della gestione documentale:

- definire e assicurare criteri uniformi di trattamento dei documenti e di classificazione e archiviazione;
- predisporre e mantenere aggiornato il manuale di gestione;

- predisporre, di concerto con il Responsabile della conservazione, il responsabile dei sistemi informativi e con il responsabile del trattamento dei dati personali, il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici secondo quanto dettagliato al Capitolo 12;
- produrre, insieme al Responsabile della conservazione (vedi § 2.3.2.), il pacchetto di versamento e assicurare il trasferimento del suo contenuto al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione predisposto dal Responsabile della conservazione.

2.3.2. Responsabile della conservazione

Il sistema di conservazione opera secondo modelli organizzativi espliciti, definiti e distinti dal sistema di gestione documentale. Qualora la conservazione sia svolta all'esterno dell'Ateneo, all'interno della struttura organizzativa è nominato un Responsabile della conservazione che fornisce le indicazioni utili alla definizione delle politiche del sistema di conservazione e alla predisposizione del manuale di conservazione.
Il Responsabile della conservazione è nominato dal Direttore Generale ed opera d'intesa con il Responsabile del trattamento dei dati personali e con il Responsabile della sicurezza, oltre che con il Responsabile della gestione documentale (vedi ALLEGATO 7).

2.3.3. Responsabile alla transizione digitale

L'Ateneo ha provveduto a nominare il Responsabile per la Transizione Digitale (RTD) (ALLEGATO 8), che opera in accordo con le altre figure coinvolte nel processo di digitalizzazione della pubblica amministrazione: Responsabile per la gestione documentale, Responsabile per la conservazione documentale, Responsabile per la protezione dei dati personali, Responsabile per la sicurezza informatica, Responsabile per la prevenzione della corruzione e della trasparenza. Il RTD, tra i suoi compiti, è tenuto a pianificare e coordinare il processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità, nonché il processo di integrazione e interoperabilità tra sistemi.

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

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

Il Responsabile della gestione documentale riceve dai responsabili delle UOR dell'Amministrazione e dai responsabili delle strutture

didattiche, scientifiche e di servizio richiesta scritta di abilitazione per ciascun utente, concordando, con i referenti del Coordinamento tecnico applicativi, le tipologie di abilitazione.
Il profilo di ogni utente è generato mediante la personalizzazione di modelli predefiniti.

2.5. Posta elettronica istituzionale

Ciascuna UOR è dotata della casella istituzionale di posta elettronica.
La casella viene denominata in modo da rendere facilmente individuabile la UOR di riferimento. Tutti i dipendenti sono dotati di una casella di posta elettronica istituzionale.
L'utilizzo della casella istituzionale di posta elettronica è regolamentato da linee guida descritte nell'ALLEGATO 9.

2.6. Posta Elettronica Certificata (PEC) istituzionale

L'Università degli Studi di Firenze si è dotata di caselle di Posta Elettronica Certificata (PEC).
L'utilizzo delle PEC dell'Ateneo sono regolate da linee guida pubblicate nell'ALLEGATO 10, insieme all'elenco di quelle attivate.

2.7. Il software per la gestione documentale e il protocollo informatico

Per la gestione documentale e il protocollo informatico l'Università degli Studi Firenze ha adottato la piattaforma "Titulus" di CINECA le cui funzioni permettono l'acquisizione, la registrazione, la

ricerca e la consultazione delle diverse tipologie di documenti trattati nell'ambito dei processi amministrativi interni e dei processi di scambio con l'esterno, nonché l'organizzazione dei documenti secondo un piano di classificazione ed archiviazione in fascicoli.

Si accede a Titulus attraverso le credenziali di ateneo dopo la richiesta di autorizzazione al referente del servizio protocollo e con il Sistema Pubblico di Identità Digitale (SPID) o con la Carta d'Identità Elettronica (CIE).

CAPITOLO 3. IL DOCUMENTO

3.1. Documento analogico e informatico: definizione e disciplina giuridica

Il documento analogico è la rappresentazione non informatica, di atti, fatti o dati giuridicamente rilevanti. Qualsiasi documento non informatico (ad es., un documento cartaceo) è, dunque, un documento analogico.
Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Il documento informatico è, quindi, un file, cioè una sequenza determinata di valori binari indifferente al supporto fisico su cui è memorizzata.

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

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

L'idoneità del documento informatico a soddisfare il requisito della

forma scritta e il suo valore probatorio sono valutabili in giudizio tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e 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 modificato, 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 avanzata, se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità, al pari di una scrittura privata, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta, se colui

contro il quale è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta.

Il documento informatico sottoscritto con firma qualificata, se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta.

L'utilizzo del dispositivo si presume riconducibile al titolare, salvo che questi ne dia prova contraria.

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

3.2. Redazione / formazione del documento informatico

Il documento informatico è formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software: in

tal caso il documento informatico assume le caratteristiche di immodificabilità e di integrità con la sottoscrizione con firma digitale/firma elettronica qualificata o con l'apposizione di una validazione temporale o con il trasferimento a soggetti terzi con PEC con ricevuta completa o con la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza o con il versamento ad un sistema di conservazione;

- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione

statica dei dati e il trasferimento della stessa nel sistema di conservazione;

- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

3.2.1. Validazione temporale

Costituiscono validazione temporale:

- i riferimenti temporali realizzati dai certificatori accreditati mediante marche temporali;
- i riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato secondo la scala di tempo UTC (IT) (INRIM) con una differenza non superiore ad un minuto primo;
- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di

conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;

- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata;
- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica.

3.2.2. Formati

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

Si adottano preferibilmente i formati PDF/A, XML e TIFF.

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

3.3. Redazione / formazione del documento amministrativo informatico

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

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

Le amministrazioni pubbliche formano gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici, di cui al § 3.1 ovvero acquisendo le istanze, le dichiarazioni e le comunicazioni previste dalla legge.

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

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

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità oltre che nei modi di cui al § 3.2

anche con la registrazione nel registro di protocollo unico dell'Area organizzativa omogena (AOO), nei repertori, negli albi, contenuti nel sistema di gestione documentale.

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

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

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

3.4. Redazione / formazione del documento amministrativo analogico

Per documento analogico si intende un documento formato utilizzando una grandezza fisica (ad es., le tracce su carta, le immagini contenute nei film e le magnetizzazioni su nastro).

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

L'originale analogico è il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali (sigillo, carta intestata, formulario amministrativo) e sostanziali, comprendente tutti gli elementi di garanzia e di informazione, del mittente e del destinatario e dotato di firma autografa.

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

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

Come regola generale di Ateneo, è da evitare la produzione di molteplici originali analogici (es. Decreti del Rettore, Determine etc.).

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

- 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.

L'Ateneo ha stabilito che i propri documenti siano predisposti secondo il Manuale di identità visiva disponibile sul sito web di Ateneo.

3.5. Documenti redatti in originale su supporto analogico

Ai sensi del DPCM 21 marzo 2013, per particolari tipologie di documenti analogici originali unici, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato. Per documenti originali unici si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta (ad es., i verbali di una riunione o di un'assemblea). Pertanto, tutti i documenti su cui vengono apposti manualmente dati di registrazione a protocollo, sigle e firma autografa (che non sono sottoscritti con firma elettronica, semplice, avanzata o digitale), sono documenti amministrativi analogici.

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

La posta elettronica certificata costituisce un mezzo di trasmissione che consente lo scambio di comunicazioni e documenti la cui trasmissione e ricezione sono giuridicamente rilevanti.

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, se il contenuto è rilevante al fine giuridico-probatorio, è da considerarsi documento amministrativo informatico il corpo del messaggio pervenuto via PEC.

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

L'e-mail costituisce un mezzo di trasmissione che consente lo scambio di comunicazioni e documenti. Dal momento che per comporre il messaggio occorre autenticarsi tramite credenziali (username e password), il testo della mail è imputabile ad una persona fisica la cui identità è associata alle credenziali di casella mail e pertanto è assimilabile a un documento sottoscritto con firma elettronica semplice

Se il contenuto della mail ricevuta è rilevante al fine giuridico-probatorio, il corpo del messaggio è da considerarsi documento amministrativo informatico.

3.8. Distinzione dei documenti in base allo stato di trasmissione (arrivo, partenza, interni)

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).

Per documenti in arrivo ("Protocollo / Entrata") 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, pervenuti all'indirizzo PEC di Ateneo o consegnati brevi manu. Anche il documento inviato o consegnato all'Ateneo da un proprio dipendente è considerato documento in arrivo se non inviato o consegnato nell'esercizio delle proprie funzioni.

Di seguito, a mero titolo esemplificativo, si riportano alcuni esempi:

- documenti provenienti da privati inerenti procedimenti di concorso, gara, accesso agli atti, etc.;
- documenti provenienti da altri enti sia pubblici che privati come ad esempio ministeri, comuni, fondazioni, etc., quali circolari, accordi di collaborazione, richieste/conferme requisiti autodichiarati, etc.

Per documenti in partenza ("Protocollo / Uscita") 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.

Di seguito, a mero titolo esemplificativo, si riportano alcuni esempi:

- documenti indirizzati a privati in risposta a procedimenti amministrativi, risposte ad accesso agli atti, etc.
- documenti indirizzati ad altri enti sia pubblici che privati come ad esempio Ministeri, Comuni, Fondazioni, etc. quali accordi di collaborazione, richieste/conferme requisiti autodichiarati, etc.

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

Di seguito, a mero titolo esemplificativo, si riportano l'esempio:

- documenti a firma del responsabile di una UOR alla Direzione Risorse Umane per la presa servizio di personale nuovo assunto, scheda di rischio/scheda individuale di destinazione lavorativa, autorizzazioni al pagamento di fatture, etc.

Per comunicazioni informali tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è

facoltativa la conservazione. Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e di norma non sono protocollate.

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

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

3.9. Duplicato del documento informatico e analogico

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

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

documento originario.

Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

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

3.10. Copia del documento informatico e analogico: nozione

La copia di documento informatico è un documento informatico che, mediante processi e strumenti idonei, assicura la corrispondenza della copia alle informazioni del documento informatico di origine attraverso l'utilizzo di uno dei formati idonei ai sensi della normativa vigente. La copia di documento informatico è, dunque, un documento informatico che muta il formato del documento originario o che muta il supporto del documento originario informatico.

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

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

3.11. Copia informatica del documento amministrativo analogico

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

In entrambi i casi l'attestazione deve essere sottoscritta con firma

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

Per copia informatica di un documento analogico si intende:

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

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

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

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

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

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

3.12. Estratto informatico di documento amministrativo informatico

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

3.2.2.

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

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

3.13. Copia analogica di documento amministrativo informatico

La copia analogica di documento amministrativo informatico è, di norma, la stampa cartacea.
La copia su supporto analogico di documento informatico, sottoscritto con firma elettronica avanzata, qualificata o digitale, per avere la stessa efficacia probatoria dell’originale da cui è tratta, deve essere certificata come conforme all’originale in tutte le sue componenti da un pubblico ufficiale autorizzato a eseguire

tale attestazione nell'esercizio delle sue funzioni (copia "autentica") salvo che la conformità allo stesso non sia espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

3.14. Metadati

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

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

3.14.1. Obiettivi dei metadati archivistici

Gli obiettivi dei metadati archivistici sono:

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

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

3.14.2. Metadati essenziali per la registrazione nel protocollo informatico

Al documento informatico è associato l'insieme minimo dei metadati, con riferimento alle regole tecniche del Codice dell'Amministrazione Digitale - CAD.

L'insieme minimo dei metadati è il seguente:

- identificativo univoco e persistente;
- data di chiusura;
- oggetto;
- soggetto produttore;
- destinatario.

Al documento amministrativo informatico sono inoltre associati altri metadati indicati nell'art. 53 del DPR 445/2000 e quelli previsti dall'art. 9 del DPCM 3 dicembre 2013 Regole tecniche per il protocollo informatico.

CAPITOLO 4. IL FASCICOLO

4.1. Il fascicolo: definizione e funzione

Il fascicolo è l'unità di base dell'archivio corrente. Ogni fascicolo contiene documenti che ineriscono a uno stesso affare, attività o procedimento e sono classificati in maniera omogenea, in base al contenuto e secondo il grado divisionale attribuito dal titolario (o piano di classificazione), salvo alcune eccezioni, come il fascicolo di persona (e le rispettive tipologie, di personale, di studente, etc.) e il fascicolo di fabbricato.
All'interno di ciascun fascicolo i documenti sono inseriti secondo l'ordine cronologico di registrazione e la loro sedimentazione avviene in modo tale che si individui subito il documento più recente. L'ordine cronologico di sedimentazione è rispettato anche all'interno dei sottofascicoli, se istruiti. L'obbligo di fascicolatura dei documenti riguarda sia i documenti contraddistinti dalla segnatura di protocollo sia i documenti procedurali non registrati. La corretta tenuta del fascicolo garantisce sia la sedimentazione che l'esercizio del diritto di accesso.

Si possono distinguere cinque tipologie di fascicolo:

- Affare: conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata. Per gli affari non esiste un termine per la conclusione previsto da norme;
- Attività: conserva i documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o

attività di aggiornamento procedurale e per la quale non è comunque previsto l'adozione di un provvedimento finale;

- Procedimento amministrativo: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un atto finale;
- Persona fisica: conserva i documenti relativi a diversi procedimenti amministrativi, distinti per affari o per attività, ma legati da un vincolo archivistico interno, relativo a una persona fisica determinata. La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'ente;
- Persona giuridica: conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica.

Il fascicolo può essere ulteriormente suddiviso in sottofascicoli e inserti. Queste suddivisioni sono identificate grazie a un'ulteriore sequenza numerica progressiva.

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. A tal proposito l'Ateneo si sta dotando di un piano di fascicolazione (vedi ALLEGATO 11a) che indichi per ciascun procedimento/affare/attività le seguenti:

- Tipologia di fascicolo (procedimento, attività, affare, etc.)
- Indice di classificazione

- Esempi di stesura dell'oggetto
- Regole di apertura e chiusura
- UOR e eventuali altre unità organizzative coinvolte (visibilità)
- Elenco delle tipologie dei documenti contenuti
- Struttura in eventuali sottofascicoli
- Tempi di conservazione (di fascicolo e sottofascicoli)

La chiusura dei fascicoli compete al Responsabile della UOR. I fascicoli annuali ripetitivi (annuali) sono chiusi e riaperti sul nuovo anno a cura dei Responsabili delle UOR competenti a seconda delle abilitazioni degli utenti.

A titolo informativo, un fascicolo per procedimento o per affare viene chiuso una volta inseriti tutti relativi documenti. Un fascicolo per attività viene chiuso solo al termine dell'annualità di riferimento (il fascicolo per attività infatti ha durata annuale e va aperto in caso di attività ripetitive). Un fascicolo per persona fisica (studente o del personale) o giuridica viene chiuso alla cessazione del rapporto di lavoro o della carriera.

4.2. Il fascicolo analogico: formazione, implementazione e gestione

Per ogni procedimento, affare e attività, l'Ateneo ha l'obbligo di conservare in un fascicolo cartaceo gli atti, i documenti e i dati da chiunque formati su supporto analogico; cioè un documento nativo su supporto cartaceo deve essere conservato in originale su tale

supporto all'interno dell'apposito fascicolo. Ovviamente un fascicolo analogico può contenere anche copie analogiche di documenti nativi digitalmente.

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

- anno di apertura (o di istruzione);
- numero di fascicolo, cioè un numero sequenziale all'interno dell'ultimo grado divisionale, da 1 a n con cadenza annuale;
- l'oggetto del fascicolo, cioè una stringa di testo per descrivere compiutamente un affare, una pratica, un dossier, una carpetta, un procedimento amministrativo o più di questi insieme.

Per convenzione, il riferimento al titolario va scritto in numeri romani, mentre gli altri gradi divisionali vanno scritti in cifre arabe (esempio: 2016 - IX/1.6 «Costruzione della nuova sede degli uffici»).

Il fascicolo raccoglie i documenti, creati e ricevuti, fino al termine della pratica. La chiusura della pratica comporta la chiusura del fascicolo. I fascicoli chiusi sono conservati presso l'Ufficio produttore per un limite minimo di un anno al fine di consentire l'eventuale reperimento dei documenti necessari allo svolgimento delle attività giornaliere.

Non si forniscono limiti massimi di giacenza dei fascicoli chiusi presso l'archivio corrente poiché i tempi possono risultare diversi a

seconda della natura della pratica e dell'attività d'ufficio.

In ogni caso, i responsabili di UOR non devono mantenere i fascicoli di attività cessate non più consultati e che non hanno più alcuna utilità diretta presso gli uffici per evitare un eccessivo ingombro e una conseguente difficoltà nella gestione dei fascicoli aperti e attivi. Il trasferimento dei fascicoli chiusi dall'archivio corrente all'archivio di deposito avviene secondo le modalità presentare al § 11.2.

4.3. Il fascicolo informatico: formazione, implementazione e gestione

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

Il fascicolo informatico reca le seguenti indicazioni:

- amministrazione titolare del procedimento;
- altre amministrazioni partecipanti;
- nominativo del responsabile del procedimento;
- oggetto del procedimento;
- elenco dei documenti contenuti;
- indice di classificazione (titolo, classe, etc.);

- numero del fascicolo, identificativo di una catena numerica relativamente alla classe e al titolo di riferimento dell'anno di creazione;
- data di apertura e di chiusura del fascicolo.

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

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

Il fascicolo informatico in un sistema totalmente digitale garantisce la possibilità di essere direttamente consultato e alimentato dalle 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. I fascicoli annuali ripetitivi

È possibile prevedere la possibilità di aprire automaticamente fascicoli annuali ripetitivi. L'indicazione della UOR e del RPA concorrono all'identificazione del fascicolo e alla individuazione del responsabile. La UOR e il RPA devono essere gli stessi di ciascun documento, del fascicolo e degli eventuali sottofascicoli. Ogni qualvolta cambia il RPA il fascicolo informatico deve essere immediatamente trasferito per competenza al nuovo responsabile del procedimento.

I fascicoli informatici saranno trasferiti in conservazione, mediante pacchetto di versamento, a cura del Responsabile della conservazione d'intesa con il Responsabile della gestione documentale o dal suo vicario, dopo la loro chiusura.

4.5. Il fascicolo ibrido

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

L'unitarietà del fascicolo è comunque garantita dal sistema di

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

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

4.6. Metadati del fascicolo informatico

I metadati sono un insieme di dati associati a un fascicolo informatico per identificarlo e descriverne il contesto, il contenuto

e la struttura, nonché per permettere la gestione nel tempo nel sistema di conservazione.

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

I metadati minimi del fascicolo informatico sono:

- identificativo univoco e persistente rappresentato da una sequenza di caratteri alfanumerici associata in modo univoco e permanente al fascicolo in modo da consentirne l'identificazione;
- UOR responsabile del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- responsabile del procedimento (RPA): cognome e nome;
- eventuali amministrazioni partecipanti al procedimento;
- oggetto: metadato funzionale a riassumere brevemente il contenuto del fascicolo comunque a chiarirne la natura;
- elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità;
- data di apertura del fascicolo;
- data di chiusura del fascicolo.

4.7. Il repertorio dei fascicoli informatici

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

riportante:

- anno e numero progressivo del fascicolo;
- classificazione nell'ambito del titolario adottato;
- oggetto dell'affare/procedimento/attività;
- UOR responsabile dell'affare/procedimento/attività;
- nominativo del responsabile dell'affare/procedimento/attività;
- date di apertura e chiusura del fascicolo;
- numero dei documenti contenuti nel fascicolo;
- dati relativi alla movimentazione del fascicolo;
- stato: chiuso/aperto.

Il repertorio dei fascicoli informatici è unico per tutto l'Ateneo, ha cadenza annuale ed è generato e gestito in forma automatica dal sistema di gestione del protocollo informatico dei documenti.

4.8. Raccoglitore

Il raccoglitore non è un fascicolo, ma un contenitore che raggruppa documenti relativi a uno stesso argomento e afferenti a procedimenti diversi e quindi a fascicoli diversi, privi di una classificazione e una numerazione propria.
In buona sostanza, si tratta di un dossier a uso e consumo del Responsabile del procedimento amministrativo (RPA) per propria memoria e autodocumentazione, di norma, non destinato alla conservazione.

CAPITOLO 5. LA GESTIONE DELL'ARCHIVIO CORRENTE

5.1. Definizione

Per archivio corrente si intende il complesso dei documenti relativi ad affari, ad attività e a procedimenti amministrativi in corso di istruttoria e di trattazione o, comunque, verso i quali sussista un interesse non ancora esaurito.
L'organizzazione dell'archivio deve rispondere a criteri di efficienza ed efficacia al fine di garantire la certezza dell'attività giuridico amministrativa dell'Ente e la conservazione stabile della memoria nel tempo. L'archivio corrente è, quindi, il primo elemento gestionale per il corretto funzionamento del sistema documentale.
Il Responsabile del procedimento amministrativo (RPA) 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.

In caso di versamento all'Archivio di deposito gestito dal Sistema Archivistico di Ateneo passa solo la gestione logistica dei fascicoli, ma non la responsabilità e titolarità degli stessi che resta alla UOR di provenienza.

5.2. Buone prassi per la gestione dell'archivio corrente

Il Responsabile del procedimento amministrativo (RPA), come si è detto sopra, è incaricato della corretta gestione dell'archivio corrente di sua pertinenza e ciò comporta in primo luogo la corretta creazione dei fascicoli e inserimento dei relativi documenti; in secondo luogo il responsabile del procedimento è tenuto alla corretta gestione dei fascicoli stessi e tale incombenza varia a seconda del supporto con cui vengono creati.

I fascicoli analogici devono essere creati secondo le indicazioni fornite nel § 4.2 e successivamente conservati all'interno di appositi faldoni o cartelle nell'archivio corrente situato presso gli uffici di ciascuna UOR. Il faldone, per consentire l'agevole e immediato reperimento dei fascicoli deve riportare sul dorso le seguenti informazioni:

- l'ufficio produttore;
- l'oggetto;
- gli estremi cronologici;
- gli estremi identificativi dei fascicoli contenuti (indice di

classificazione e numero progressivo di repertorio).

Laddove una pratica avesse dimensioni tali da occupare singolarmente più di un faldone, questi andranno contrassegnati con le medesime indicazioni esterne e con una numerazione progressiva, a partire da 1, così da risultare immediata la comprensione del legame tra le unità di conservazione.

I fascicoli restano collocati presso ogni singola struttura per la parte di propria responsabilità e competenza nel trattamento dell'affare, fino al momento del loro trasferimento nell'archivio di deposito.

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

Un'attività secondaria, ma molto utile da un punto di vista di gestione corrente delle unità di archivio, è lo sfoltimento dei fascicoli. Lo sfoltimento è l'operazione preliminare e propedeutica a una corretta conservazione documentale: al momento della

chiusura del fascicolo, oppure prima del trasferimento dello stesso all'archivio di deposito, il carteggio di carattere transitorio e strumentale deve essere selezionato ed estratto dal fascicolo da parte dell'operatore incaricato del trattamento della pratica. Si tratta, cioè, di estrarre dal fascicolo le copie e i documenti che hanno appunto carattere strumentale e transitorio, utilizzati dall'operatore incaricato o dal responsabile del procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad es., appunti, promemoria, copie di normativa e documenti di carattere generale).
Questa operazione riguarda principalmente i fascicoli cartacei.

5.3. Gli strumenti dell'archivio corrente

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

5.3.1. Registro di protocollo

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

di un determinato documento all'interno del sistema di gestione documentale e garantendone l'autenticità. Il registro di protocollo è un atto pubblico di fede privilegiata.

5.3.2. Titolario (piano di classificazione)

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

La classificazione, necessaria e fondamentale, è un'azione preventiva 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. In esso sono presenti le possibili varianti lessicali, trattate e riportate in modo analitico, che possono essere incontrate nel contenuto del documento. 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 descritto nell'ALLEGATO 11b.

5.3.3. Repertori

I repertori si riferiscono a serie omogenee di documenti uguali per forma e diversi per contenuto. Essi sono soggetti a registrazione particolare, cioè con l'assegnazione di una numerazione continua e progressiva per anno. Sono un esempio la registrazione di decreti, contratti e convenzioni, deliberazioni, etc. (vedi ALLEGATO 12).

5.3.4. Repertori 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

5.3.5. Piano di conservazione (Massimario di selezione e scarto)

Il Piano di conservazione o Massimario di selezione e scarto (vedi ALLEGATO 13), integrato con il Titolario di classificazione, è uno strumento da utilizzare durante la fase di deposito dell'Archivio, come previsto dall'art. 68 "Disposizioni per la conservazione degli archivi", del DPR 28 dicembre 2000, n. 445.

Il massimario di selezione è lo strumento che indica le disposizioni di massima dei criteri e delle procedure attraverso i quali i documenti, non rivestendo interesse storico ai fini della conservazione permanente, avendo esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della Soprintendenza archivistica e bibliografica, ai sensi del D.Lgs. 22 gennaio 2004, n. 42, art. 21.

Il massimario individua le tipologie documentali in rapporto ai procedimenti che le costituiscono e, a partire da tali tipologie, si applicano i criteri e le disposizioni atti ad individuare i termini di conservazione o la possibilità di procedere alla loro distruzione.

La proposta di scarto formulata, cioè l'elenco di scarto, con le tipologie documentarie, gli estremi cronologici, il volume (espresso in numero di contenitori o in metri lineari, per i documenti

analogici), insieme alle motivazioni dell'eliminazione è inviata per l'autorizzazione alla Soprintendenza archivistica e bibliografica competente, 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.

Per i fascicoli informatici la proposta di scarto segue lo stesso iter per quanto riguarda l'autorizzazione della Soprintendenza.

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

5.4. Spostamento di un archivio corrente analogico

Qualora una UOR dovesse spostare la documentazione corrente, a seguito di mutamento della sede operativa o per altra ragione, dovrà darne informazione tempestiva al Responsabile della gestione documentale, producendo un apposito elenco dei fascicoli soggetto di spostamento.

Inoltre, il personale del Sistema Archivistico di Ateneo provvederà a effettuare un sopralluogo per verificare l'idoneità degli spazi e la correttezza della collocazione del nuovo archivio, rimanendo in ogni caso a disposizione per eventuali chiarimenti o consigli sulle modalità di spostamento della documentazione (§ CAPITOLO 11).
Lo spostamento dell'archivio corrente non necessita di alcuna autorizzazione preventiva da parte della Soprintendenza archivistica e bibliografica competente per territorio, alla quale

deve essere fatta obbligatoriamente debita comunicazione della nuova collocazione della documentazione (in base al D.Lgs. 42/2004 art. 21 c.3).

CAPITOLO 6. IL PROTOCOLLO INFORMATICO

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

Il registro di protocollo ha cadenza annuale: inizia il 1° gennaio e termina il 31 dicembre di ogni anno ed è unico per tutto l'Ateneo, in quanto è stata individuata un'unica AOO per l'intera l'Università degli Studi di Firenze.

6.1. Registratura: registrazione a protocollo o a repertorio

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

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'Ateneo, ossia i cui destinatari sono esterni all'ente, e quelli scambiati tra le UOR 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 (DPR 445/2000, art. 53, comma 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 Responsabile della gestione documentale e a persone espressamente delegate. L'inalterabilità e l'immodificabilità della registrazione di protocollo devono essere garantite dal sistema di gestione documentale.

6.1.1. Dati obbligatori non modificabili

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

probatorio (DPR 445/2000, art. 53; DPCM 3/12/2013, Regole tecniche per il protocollo informatico, artt. 9, 19 e 21).

Essi sono:

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

L'insieme di tali elementi è denominato registratura.

6.1.2. Altri dati 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. Dati non obbligatori non modificabili

Gli elementi non obbligatori immodificabili sono:

- data del documento ricevuto

- protocollo del documento ricevuto
- annotazioni

6.1.4. Dati non obbligatori modificabili

Gli elementi non obbligatori modificabili sono:

- mezzo di trasmissione del documento
- durata conservazione
- note
- collegamento ad altri documenti o fascicoli

6.2. Data e ora regolate sul tempo universale coordinato

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 di protocollo

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 o nei registri particolari, i cosiddetti repertori.

Essa consente di individuare ciascun documento in modo univoco.

La segnatura di protocollo è effettuata contestualmente alla registrazione di protocollo.

6.3.1. Per il documento informatico

Le informazioni minime da associare al documento informatico secondo la Circolare AGID 23/1/2013, n. 60 e il DPCM 3/12/2013, artt. 9, 20 e 21, sono:

a) Informazioni minime obbligatorie:

- codice identificativo dell'Amministrazione, dell'AOO e del registro;
- data e numero di protocollo;
- oggetto del documento;
- mittente/destinatario o destinatari.

b) Informazioni facoltative:

- indicazione della persona o dell'ufficio assegnatario;
- indice di classificazione;
- identificazione degli allegati;
- informazioni sul procedimento e sul trattamento da applicare;
- informazioni che due o più amministrazioni concordano di scambiarsi per lo svolgimento di determinati procedimenti.

Per i documenti informatici trasmessi ad altre pubbliche amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD).

6.3.2. Per il documento analogico

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

- l'identificazione in forma sintetica o estesa dell'amministrazione individuata ai fini della registrazione e della gestione del documento;
- il numero progressivo di protocollo;
- la data di protocollo nel formato gg/mm/aaaa;
- la classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento;
- la sigla della UOR/RPA o delle UOR/RPA a cui il documento è assegnato per competenza e responsabilità;
- le eventuali sigle della UOR/RPA o delle UOR/RPA in copia conoscenza.

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

6.3.3. Ragioni della scelta di un timbro meccanico

La segnatura su un documento cartaceo si appone mediante un timbro meccanico che riporta gli elementi normalizzati della registratura, trascritti dall'operatore di protocollo a penna

all’interno degli spazi predisposti.

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

6.4. Modalità di produzione e di conservazione delle registrazioni

Ogni registrazione di protocollo informatico produce un record nel sistema di gestione documentale che viene accodato in una base dati accessibile esclusivamente all’amministratore del sistema. Ogni operazione di inserimento e modifica viene registrata inoltre su un file di log corredato da codici di controllo in grado di evidenziare eventuali tentativi di manipolazione. Da esso l’amministratore del sistema è in grado di ottenere l’elenco delle modifiche effettuate su una data registrazione, permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione (smistamento, invio per conoscenza, restituzione, fascicolatura ecc.), ottenendo in dettaglio:

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

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

6.5. La registrazione differita (o "protocollo differito")

È possibile effettuare la registrazione differita di protocollo nel caso di temporaneo, eccezionale e imprevisto carico di lavoro e qualora dalla mancata registrazione di un documento nell'ambito del sistema nel medesimo giorno lavorativo di ricezione, possa venire meno un diritto di terzi. La registrazione differita di protocollo informatico è possibile esclusivamente per i documenti in arrivo.

Operando in un sistema di protocollo diffuso spetta all'operatore incaricato della registrazione annotare la motivazione del ritardo.

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

6.6. La ricevuta di avvenuta registrazione

6.6.1. Per il documento analogico

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è

cura di chi effettua la protocollazione rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal sistema di gestione documentale.

La ricevuta della consegna di un documento analogico, su richiesta, è solitamente costituita dalla stampa della prodotta dal gestionale, o dalla fotocopia del documento stesso con apposto timbro di avvenuta consegna riportante la data.

Le buste delle assicurate, corrieri, espressi, raccomandate etc. si inoltrano insieme ai documenti da protocollare.

6.6.2. Per il documento informatico

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

Se il documento informatico è pervenuto tramite e-mail, la ricevuta, se richiesta, sarà generata in formato PDF e inviata via e-mail al mittente.

6.7. Documenti esclusi dalla registrazione di protocollo

Ai sensi dell'articolo 53, DPR 445/2000, sono esclusi dalla registrazione di protocollo:

- le gazzette ufficiali, i bollettini ufficiali P.A., i notiziari P.A.;
- le note di ricezione delle circolari;

- le note di ricezione di altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali;
- le riviste;
- i libri;
- i materiali pubblicitari;
- gli inviti a manifestazioni;
- bolle accompagnatorie.

Sono inoltre escluse dalla protocollazione alcune tipologie documentali:

- tutti i documenti già soggetti a registrazione particolare dell'amministrazione;
- in generale, tutte le notifiche automatiche.

Inoltre, non devono essere protocollati i documenti informali di carattere meramente eventuale (appunti, brevi comunicazioni di rilevanza meramente informativa ecc.) scambiati tra UOR.

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, a mente del DPCM 3 dicembre 2013.

Gli elementi memorizzati del registro giornaliero sono i seguenti:

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

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

6.9. Il registro di emergenza

Il Responsabile della gestione documentale, ai sensi dell'art. 63 del DPR 445/2000, attiva il registro di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica, dandone immediata comunicazione.
Sul registro di emergenza sono riportate la causa, la data e l'ora di

inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.
Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le 24 ore, per cause di eccezionale gravità, il Responsabile della gestione documentale autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.
Sul registro di emergenza devono essere riportati gli estremi del provvedimento di autorizzazione. La sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea.
Durante la fase di ripristino, a ciascun documento protocollato nel registro di emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.
I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo ordinario.
La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo. In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.
Il registro di emergenza si rinnova ogni anno solare: inizia il 1°

gennaio e termina il 31 dicembre di ogni anno.
Al termine dell'emergenza, il Responsabile della gestione documentale, chiude il registro e dà contestuale comunicazione della revoca dell'emergenza.

CAPITOLO 7. REGISTRI E REPERTORI INFORMATICI

7.1. Repertorio - Nozione

Per repertorio si intende il registro in cui sono annotati con numerazione progressiva tutti i documenti per i quali è prevista la registrazione particolare.

Il complesso dei documenti registrati a repertorio per forma omogenea costituisce una serie.

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

I documenti messi a repertorio sono comunque associati al fascicolo archivistico di loro pertinenza. In caso di documento originale cartaceo, l'originale sarà inserito nella serie a repertorio, mentre nel fascicolo di pertinenza ne verrà, eventualmente, messa una copia analogica.

7.2. Repertori attivi

L'elenco dei repertori attivi presso L'Ateneo è descritto nell'ALLEGATO 12.

Pertanto anche per i documenti sottoposti a registrazione particolare ci sono delle informazioni minime obbligatorie:

- dati identificativi sul contenuto dell'atto (autore, oggetto);

- indice di classificazione;
- data di registrazione e numero di repertorio progressivo e annuale (identificativo univoco), generato in modo automatico e non modificabile.

7.3. Repertorio dei fascicoli

I fascicoli, 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.

CAPITOLO 8. FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Il flusso di lavorazione dei documenti amministrativi riguarda quelli in entrata, quelli in uscita e quelli interni.

La gestione del flusso documentario riguarda l'insieme delle operazioni connesse all'acquisizione o produzione, gestione e conservazione dei documenti di Ateneo.

Esistono diversi canali di ricezione e trasmissione di documenti amministrativi informatici, sia internamente all'Ateneo sia nei confronti di utenti esterni (cittadini, imprese, PA).

8.1. Canali di comunicazione

8.1.1. PEC (Posta Elettronica Certificata)

La Posta Elettronica Certificata (PEC) 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, pertanto, nei casi in cui è necessario avere certezza legale dell'invio e della consegna del messaggio di posta.

Una casella PEC può essere intestata tanto a una persona giuridica (es. Ateneo) quanto a una persona fisica (es. cittadino, studente etc.) ed è rilasciata da un prestatore di servizi fiduciari accreditato

presso l'Agenzia per l'Italia Digitale (AgID), sul cui sito è disponibile l'elenco completo.

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, od ordinaria, ha le seguenti peculiarità:

- 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.

La PEC è un mezzo di trasmissione tramite allegato del documento principale e dei suoi eventuali allegati. Tuttavia è possibile che la comunicazione sia inclusa nel corpo stesso della mail, cioè come parte del messaggio stesso.

L'Ateneo ha adottato un'apposita circolare per regolare l'uso della PEC istituzionale (progressivo 36990/18): la circolare ribadisce che la PEC è unicamente un mezzo di trasmissione di documenti. Di conseguenza, prima di inviare una qualsiasi PEC, viene prescritta la creazione, il perfezionamento e, quindi, la registrazione a norma di legge (DPR 445/00, articolo 53, comma 5) del documento da inviare.

Le caratteristiche delle caselle PEC adottate in Ateneo sono

descritte al paragrafo 2.6 del presente Manuale.

L'elenco delle PEC dell'Ateneo è disponibile all'ALLEGATO 10, con le Linee guida operative sull'uso della PEC e della Posta Elettronica Ordinaria.

8.1.2. La posta elettronica ordinaria

La posta elettronica ordinaria istituzionale / e-mail costituisce un mezzo di trasmissione di uso comune e diffuso. Essa non è rilasciata da prestatori di servizi fiduciari accreditati presso AgID (come invece accade per la PEC), quindi a monte del rilascio non è prevista una fase di identificazione dell'intestatario della casella e non costituisce uno strumento valido per garantire l'opponibilità dell'invio e della consegna del messaggio di posta. Pertanto ne è sconsigliato l'uso per la trasmissione di documentazione amministrativa che possa impegnare l'Ateneo verso terzi.
Tuttavia, i messaggi provenienti da caselle di posta elettronica istituzionale personale di altre PA vengono considerati sottoscritti con firma elettronica semplice, in quanto per il rilascio delle credenziali di accesso si è proceduto all'identificazione certa del titolare.

La posta elettronica ordinaria istituzionale / e-mail è un mezzo di trasmissione di documenti tramite allegato, tuttavia è possibile che la comunicazione sia inclusa nel corpo stesso della mail, 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 dal Responsabile del Procedimento Amministrativo.

In Ateneo ogni dipendente (personale tecnico, amministrativo, docente e ricercatore) dispone di una casella mail nominativa.

La posta elettronica ordinaria istituzionale / e-mail viene utilizzata per l'invio e ricezione di comunicazioni, informazioni e documenti sia all'interno dell'Ateneo, sia nei rapporti con i cittadini e altri soggetti privati, sia con altre Pubbliche Amministrazioni.

8.1.3. Altri canali

Posta ordinaria: Per posta ordinaria si intende il servizio di spedizione e ricezione della corrispondenza cartacea (sia a mezzo di posta ordinaria, assicurata o raccomandata, o simile).

Corriere: Per corriere si intende il servizio di spedizione e ricezione di corrispondenza e pacchi a mezzo di corriere.

Posta interna: Per posta interna si intende il servizio di spedizione e ricezione della corrispondenza cartacea tra le varie UOR e strutture dell'Ateneo.

8.2. Protocollo in entrata

8.2.1. Canali di comunicazione

Al Sistema Archivistico di Ateneo è tenuto ad accettare tutti i plichi (corrispondenza cartacea) indirizzati correttamente alla sede legale all'Ateneo ed è delegato all'apertura. Questo tipo di

comunicazione prevede l'apertura dei plichi, comprese le notifiche da parte dell'amministrazione giudiziaria o multe, salvo nei casi riportanti le seguenti diciture:

- riservato, personale, confidenziale, spm/sgm (sue proprie mani/sue gentilissime mani), etc. o dalla cui confezione si evinca il carattere di corrispondenza privata (ad es. busta particolare);
- «offerta», «gara d'appalto», «non aprire» o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara (ad es. in presenza del CIG);

Qualora il plico riportante la dicitura «personale» o «riservata personale» venga aperta per errore, l'operatore dell'Ufficio Protocollo e Servizio Postale provvederà a sigillarla, ad apporre la dicitura «aperta per errore» e la propria firma, quindi a trasmetterla al destinatario.

Chiunque riceva, tramite corrispondenza privata, documenti concernenti affari o procedimenti amministrativi dell'Amministrazione deve provvedere a registrarlo a protocollo.

In tutti i casi la documentazione da protocollare viene registrata, classificata e smistata alla UOR competente e, contestualmente, viene assegnata all'RPA ovvero al Responsabile del Procedimento Amministrativo, cui si il documento si riferisce.

Documento informatico - possibili canali di ricezione di documenti

amministrativi informatici:

- Tramite la casella PEC istituzionale - Le PEC in uso in Ateneo possono ricevere documenti informatici provenienti tanto da altre PEC. La trasmissione via PEC attribuisce data certa alla ricezione dell'atto, grazie alle notifiche di accettazione e consegna.
- Tramite la casella posta elettronica ordinaria - Le e-mail ricevute nelle caselle di posta istituzionale degli uffici o nominative (sempre d'ufficio) possono venir protocollate dall'ufficio stesso se ritenute rilevanti dall'RPA, ai fini del procedimento amministrativo cui si riferiscono. Se un dipendente riceve nella propria casella di posta fornita dall'Ateneo documenti concernenti affari o procedimenti amministrativi è tenuto a farli pervenire/inoltrare tempestivamente ai referenti della protocollazione definiti per la propria UOR.
- Tramite banche dati o sistemi (in house o presso terzi) - I documenti prodotti da applicativi gestionali integrati con il sistema di protocollo, arrivano nel sistema di gestione documentale e sono automaticamente protocollati con classificazione e assegnazione alla UOR competente e al RPA. A tal fine, nel sistema di gestione documentale, viene predisposto un flusso che consentirà il transito dei documenti inseriti e convalidati dalla banca dati al sistema di protocollo.

Indipendentemente dal canale di comunicazione, si procede alla registrazione a protocollo solo se il contenuto della comunicazione/messaggio è rilevante al fine giuridico-probatorio.

Non si procede alla registrazione a protocollo, sia nei casi dei documenti esclusi dal protocollo (vedi paragrafo 6.7), sia nel caso in cui il contenuto della comunicazione/messaggio non sia rilevante al fine giuridico-probatorio.

Documento analogico - possibili canali di ricezione di documenti amministrativi analogici:

- Ricezione dei documenti analogici tramite fax, consegna a mano, posta ordinaria o corriere pervenuti al Sistema Archivistico di Ateneo - Di norma tutta la corrispondenza su supporto analogico pervenuta all'Ateneo (tanto per l'amministrazione centrale, quanto per l'amministrazione periferica) è aperta, protocollata (se necessario) e poi smistata alle UOR di competenza;
- Ricezione dei documenti analogici tramite consegna a mano, posta ordinaria o corriere pervenuti alle altre UOR di Ateneo - Quando le buste e i relativi documenti contenuti pervengono direttamente alla UOR, è compito di quest'ultima inoltrarla e recapitarla all'Archivio e trattamento degli atti – Gestione documentale per la registrazione a protocollo.

L'apertura di peculiari tipologie documentali, anche oggetto di

registrazione particolare, è delegata ai Responsabili di Procedimento.

I documenti analogici ricevuti, protocollati e assegnati, e la posta che non necessita di protocollazione, sono resi disponibili ai destinatari tramite il servizio interno di distribuzione della posta cartacea.

Le buste pervenute tramite posta raccomandata, corriere o altra modalità per la quale si renda rilevante evidenziare il mezzo di trasmissione e il timbro postale, sono spillate assieme al documento e trasmesse alla UOR.

8.2.2. Validità delle istanze o dichiarazioni pervenute

Le istanze e le dichiarazioni trasmesse per via telematica (si intenda quindi pervenute e/o ricevute da PEC, posta elettronica ordinaria o piattaforme telematiche) devono ritenersi valide a tutti gli effetti di legge, qualora (cfr. DPR 445/2000, art. 38; D. Lgs. 82/2005, art. 65):

- siano regolarmente sottoscritte dall'istante con firma digitale, altro tipo di firma elettronica qualificata, o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'art. 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e

inequivoca, la sua riconducibilità all'autore. Tale firma deve essere, quindi, dotata di certificato valido rilasciato da un certificatore accreditato;

- il sottoscrittore è identificato dal sistema informatico con l'uso della carta d'identità elettronica (CIE), della Carta Nazionale dei Servizi (CNS) o del Sistema pubblico di identità digitale (SPID);
- si tratti di rappresentazioni digitali di documenti originali cartacei sottoscritti e presentati unitamente alla copia del documento d'identità;
- se trasmesse dall'istante o dal dichiarante dal proprio domicilio digitale purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con Linee guida, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce elezione di domicilio speciale.

L'Ateneo accetta formati che possiedono requisiti di leggibilità, interscambiabilità e staticità al fine di garantire la loro inalterabilità nel tempo. Pertanto l'Ateneo ha stabilito di accettare (e quindi registrare) comunicazioni e documenti informatici nei seguenti formati: PDF, PDF/A, XML, TIFF, JPG, con o senza firma digitale, anche presentati in cartelle/file compressi (in formato ZIP); se trasmessi a mezzo PEC sono accettati anche i formati TXT, DOCX e XLSX, come consente il DPCM 13/11/2014, art. 3, c. 4, lett. c).

Le istanze e le dichiarazioni trasmesse per via tradizionale (cartacea) o consegnate a mano devono ritenersi valide a tutti gli effetti di legge, qualora (cfr. DPR 445/2000, art. 38, c. 3) devono essere sottoscritte dall'interessato in presenza del dipendente addetto ovvero sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore.

Le comunicazioni e i documenti ricevuti/trasmessi tra Pubbliche Amministrazioni, attraverso l'utilizzo della posta elettronica, sono valide ai fini del procedimento una volta che ne sia verificata la provenienza, ovvero quando:

- sono sottoscritti con firma elettronica qualificata o digitale;
- sono dotati di segnatura di protocollo;
- sono trasmessi attraverso sistemi di posta elettronica certificata.

Al di fuori delle predette ipotesi, i documenti ricevuti da altre Pubbliche Amministrazioni sono valutati in ragione della loro rispondenza a ragionevoli criteri di attendibilità e riconducibilità al mittente dichiarato e successivamente soggette, se del caso, a protocollazione.

8.2.3. Controlli

I controlli e le verifiche sono svolti dall'operatore di protocollo e dall'operatore che gestisce il procedimento.

L'operatore di protocollo controlla e verifica che:

- non si tratti di messaggi malevoli.
- della presenza del documento principale.

il formato documento principale informatico sia tra quelli accettati dal sistema di registrazione. In caso contrario il documento viene comunque sottoposto a registrazione registrando l'intero messaggio.

Inoltre individua la UOR competente: nel caso in cui la UOR individuata dal Sistema Archivistico di Ateneo non sia corretta, la UOR destinataria è tenuta a sua volta a smistare il documento ricevuto, nell'ottica della collaborazione tra le strutture dello stesso ente, e comunicare al Sistema Archivistico di Ateneo quale sia la UOR ritenuta corretta.

L'operatore che gestisce il procedimento controlla e verifica che:

- la documentazione inerente al procedimento amministrativo sia completa per richiedere eventuali integrazioni. Spetta al RPA, ove ne rilevi la necessità, richiedere al mittente la regolarizzazione dell'istanza o della dichiarazione, acquisendo ogni utile documentazione integrativa, compresa la firma autografa del documento, se prevista;
- l'identità del mittente dell'istanza (provenienza dell'istanza) sia confermata nel caso la documentazione pervenga da caselle e-mail ordinarie. Quando il messaggio perviene da una casella mail ordinaria e il documento in esso contenuto non è firmato, l'operatore deve inserire una nota nel campo 'Annotazioni' (non modificabile); queste verranno comunque

protocollate, ma sarà in capo al RPA l'eventuale richiesta di integrazione e/o la effettiva accettazione o rigetto dell'istanza. Se il documento è invece sottoscritto con firma digitale, non è necessario annotare nulla. Nel caso in cui il RPA chieda documentazione integrativa o la ritrasmissione di documentazione precedentemente inoltrata in modo errato, ciò che perverrà alla PEC di Ateneo sarà da considerare come un nuovo protocollo e non un secondo esemplare.

- i formati dei documenti siano conformi rispetto alla richiesta/istanza. Nel caso in cui il documento pervenuto all'Ateneo abbia un formato non conforme a quanto richiesto dall'Ateneo stesso o previsto dalla tipologia di istanza o dalla normativa vigente, spetta al RPA segnalarlo al mittente e chiedere l'integrazione dell'istanza.
- la presenza della firma autografa (per i documenti cartacei). L'eventuale assenza andrà segnalata nel campo Annotazioni e sarà richiesta da parte del RPA l'integrazione della documentazione presentata.
- i certificati di firma siano validi. Il controllo dei certificati di firma è effettuato dai Responsabili dei procedimenti, all'interno o all'esterno del sistema di gestione documentale.

8.2.4. Priorità di registrazione

In fase di protocollazione deve essere data priorità alla registrazione dei documenti che implicano scadenze a breve e comunque alle seguenti tipologie documentali:

- domande di partecipazione a selezioni pubbliche;
- offerte di gare;
- documenti provenienti dal MIUR;
- documenti di rilevanza finanziario-contabile (ad esempio documenti provenienti da Corte dei conti, Ministero dell'Economia e delle Finanze, ecc.);
- documenti ricevuti direttamente dall'Ufficio Legale;
- documenti ricevuti direttamente dalla Segreteria della Direzione Generale;
- documenti ricevuti direttamente dalla Segreteria del Rettorato.

8.2.5. Assegnazioni

Operando in un sistema di protocollo diffuso gli operatori abilitati alla protocollazione in ingresso provvedono ad assegnare i documenti acquisiti tramite il sistema di protocollo informatico al personale competente per materia/funzione.

I documenti informatici e le copie immagine di documenti analogici sono resi disponibili ai responsabili di procedimento, esclusivamente tramite il sistema di gestione informatica dei documenti.

L'assegnatario può a sua volta smistare i documenti agli uffici afferenti o condividendolo con essi nel gestionale documentale, tenendo conto che:

- la UOR che riceve un documento (qualunque sia il mezzo

trasmissivo) in fase di protocollazione deve individuare anche le eventuali altre UOR o altri RPA assegnatari, considerandoli come "corresponsabili" (vedi par. 8.7), in base al livello di partecipazione del relativo procedimento ammnistrativo;

- la UOR che riceve un documento (qualunque sia il mezzo trasmissivo), se individua che deve essere trasmesso ad un'altra o più UOR mediante lettera di trasmissione, eventualmente aggiungendo altri documenti, utilizza il "Protocollo tra uffici" (vedi par. 8.4), considerandole come "corresponsabili" del procedimento (vedi par. 8.7).

Nel caso di un'assegnazione errata, la struttura che riceve il documento provvederà, di regola e nel più breve tempo possibile, ad assegnare lo stesso alla struttura ritenuta effettivamente competente oppure potrà restituirla all'unità di protocollazione, corredata di segnalazione, da inserire nel campo Annotazioni motivando il rigetto e indicando la UOR competente. Il documento informatico ritorna così in carico all'Archivio e trattamento degli atti – Gestione documentale che potrà immediatamente inoltrarlo alla UOR competente.

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 il Responsabile della Gestione documentale che determina lo smistamento definitivo.

Nessun documento, analogico e/o informatico, deve rimanere in

carico all'Archivio e trattamento degli atti – Gestione documentale, al di fuori di quelli afferenti a procedimenti o attività/affari di sua responsabilità.

Il sistema di gestione informatica dei documenti tiene traccia dei passaggi di cui sopra, memorizzando per ciascuno di essi l'identificativo dell'operatore agente, della data e ora di esecuzione.

8.2.6. Casi di rigetto delle istanze

È in capo alla UOR a cui viene assegnato il documento stabilire la casistica di rigetto delle istanze, sulla base della manifesta irricevibilità, inammissibilità, improcedibilità o infondatezza della domanda (Legge 241/1990, art. 2, comma 1).

8.2.8. Casi particolari

Per la registrazione e gestione di particolari casistiche di documenti, vedi il capitolo 9 del presente Manuale.

I casi presentati riguardano:

- gestione delle gare d'appalto, indagini di mercato, offerte ed aste pubbliche;
- gestione concorsi e procedure di selezione;
- DURC on-line;
- denunce di infortunio;
- certificati di malattia.

8.3. Protocollo in uscita

Al pari di quello in entrata, anche il documento in partenza può essere redatto sia su supporto digitale che analogico e può essere inviato con diversi mezzi di trasmissione.

Se analogico, sarà trasmesso con i mezzi tradizionali dei servizi postali (posta ordinaria o corriere), o via fax, del quale è consentito, benché sconsigliato, l'utilizzo solo per comunicazioni verso privati e imprese (la trasmissione di documenti a mezzo fax tra pubbliche amministrazioni è vietata ai sensi dell'art. 47, c. 2, lett. c) del D.Lgs 82/2005).

Se digitale, il documento sarà trasmesso di preferenza con la PEC oppure via mail semplice, o mediante altre piattaforme informatiche qualificate.

L'Ateneo privilegia, laddove possibile, la produzione di documenti informatici, in armonia con quanto previsto dal legislatore.

A prescindere dal supporto, il documento inviato deve contenere requisiti minimi di forma e contenuto:

- logo/sigillo e intestazione;
- indicazione dell'Ufficio produttore e del suo Responsabile (e del RPA);
- segnatura di protocollo (nota bene: se il documento originale è analogico, è presente su di esso un'etichetta o comunque l'indicazione del numero e data di registrazione; se il documento originale è digitale, la segnatura è, invece,

associata al documento in formato XML);
- numero degli allegati;
- testo;
- data completa (luogo, giorno, mese, anno) scritta per esteso;
- firma di sottoscrizione;
- indicazione dell'indirizzo PEC o e-mail del destinatario (opzionale);
- classificazione;
- identificativo/numero di fascicolo;
- eventuali indicazioni necessarie a individuare il procedimento amministrativo a cui il documento si riferisce.

8.3.1. Canali di comunicazione

Documento informatico - I documenti vengono trasmessi, dopo essere stati classificati, fascicolati e protocollati, secondo le procedure previste, per questi canali:

- via PEC
- in caso di spedizione di un documento al cittadino/utente, all'indirizzo PEC comunicato in qualità di domicilio digitale e inserito all'interno dell'ANPR;
- in caso di PA all'indirizzo pubblicato sul sito web Indice PA (https://www.indicepa.gov.it/);
- in caso di imprese e professionisti all'indirizzo pubblicato sull'Indice nazionale degli indirizzi PEC delle imprese e dei professionisti INI PEC (https://www.inipec.gov.it/);

- via posta elettronica ordinaria, alla casella dichiarata dal destinatario;
- via posta ordinaria.

Si tratta di una casistica specifica: in assenza di un recapito telematico, infatti, l'Ateneo può predisporre le comunicazioni ai cittadini come documenti informatici originali digitali ed inviare ai cittadini stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia analogica di tali documenti, all'interno della quale deve essere riportata la dicitura che l'esemplare originale del documento è conservato dall'Ateneo. L'Ateneo conserva l'originale digitale nel proprio archivio.

In caso di trasmissione via PEC è possibile verificare l'avvenuto recapito dei documenti e il collegamento delle ricevute elettroniche alle registrazioni di protocollo.

La spedizione di documenti informatici, attraverso posta elettronica, al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni senza che a queste l'Ateneo riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dal Codice dell'Amministrazione Digitale - CAD, all'art. 49 "Segretezza della corrispondenza trasmessa per via telematica", a quanto previsto nel capitolo 12 del presente Manuale e dal Piano di sicurezza informatica dei documenti dell'Ateneo.

Documento cartaceo - Qualora sia necessario spedire documenti originali analogici, questi devono essere completi, oltre che dei requisiti minimi sopra riportati, anche della firma autografa del responsabile del procedimento.

Il documento originale analogico in uscita, una volta protocollato (classificato e fascicolato) a cura della struttura che lo ha prodotto, viene recapitato all'Ufficio posta, che provvede alla sua spedizione al destinatario.

8.3.2. Requisiti minimi del documento in uscita

Il documento informatico prodotto deve essere redatto preferibilmente nel formato PDF/A o per casi particolari (cfr. capitolo 9) secondo gli altri formati stabiliti in precedenza (cfr. paragrafo 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:

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 di protocollo;

- numero degli allegati;
- sottoscrizione autografa (nei casi previsti dalla normativa deve essere corredato da dichiarazione di conformità sottoscritta con firma digitale).
- 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;
- sottoscrizione con firma digitale.

8.4. Protocollo interno tra uffici

Il "Protocollo interno tra uffici" è rappresentato dalla registrazione e trasmissione formale di documenti tra le UOR della medesima AOO inerenti specifici procedimenti, affari o attività dell'Ateneo. Effettua la registrazione la UOR che invia.

Le semplici comunicazioni informali ricevute o trasmesse per posta elettronica, che consistano in semplice scambio di informazioni che non impegnino l'Ateneo verso terzi, non devono essere protocollate.

A titolo esemplificativo non sono soggette a registrazione di protocollo (interno tra uffici):

- richieste di servizio di pulizie;

- richieste di attività di facchinaggio;
- richieste di fornitura di cancelleria;
- richieste di piccole manutenzioni;
- richieste di sopralluoghi ai servizi tecnici;
- richieste di sopralluoghi archivistici.

Buona prassi è evitare la trasmissione di documenti cartacei tra UOR della AOO. Se ciò avviene la UOR mittente li fa pervenire alla UOR destinataria attraverso il servizio di posta interna.

8.5. Protocollo riservato/altamente confidenziale

È previsto l'utilizzo del "Protocollo riservato" (sia in entrata, sia in uscita) per la trasmissione e/o ricezione di documenti riguardanti particolari procedimenti. Sono previste particolari forme di riservatezza e di accesso controllato al protocollo unico per:

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

Il complesso dei documenti registrati col protocollo riservato costituisce un archivio "particolare" con modalità di consultazione abilitate diverse a seconda se riservato o altamente confidenziale.

8.6. Annullamento di una registrazione

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

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

- documento già registrato;
- documento registrato non perfezionato;
- errore nell'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;
- la motivazione per cui il documento è stato prodotto è venuta meno purché il documento non sia già stato diffuso;
- assenza del documento principale.

L'operazione di annullamento è eseguita con le modalità di cui all'art. 54 del DPR 445/2000, Informazioni annullate o modificate.

L'annullamento della registrazione di protocollo viene effettuata da incaricati dotati di utenza con specifiche configurazioni (per i profili utente del sistema di gestione documentale) tramite specifica funzione del sistema di protocollo informatico. Sono autorizzate ad annullare la registrazione:

- per l'Amministrazione centrale il Responsabile della gestione documentale e le persone espressamente delegate del Sistema Archivistico di Ateneo;
- per le altre UOR i responsabili abilitati. Per annullare la registrazione dei protocolli interni tra UOR sono abilitati solo i responsabili destinatari o il personale del Sistema Archivistico di Ateneo.

La richiesta di annullamento di una registrazione deve essere inviata per e-mail dalla UOR, indicando:

- i dati identificativi della registrazione da annullare;
- la motivazione dettagliata della richiesta di annullamento, con eventuale indicazione dell'ulteriore registrazione documentale presente in archivio per lo stesso documento.

La motivazione della richiesta di annullamento viene riportata nell'annotazione sul documento registrato dall'operatore che annulla la scheda stessa.

Nel caso in cui il documento da annullare sia sostituito da una nuova registrazione nelle annotazioni si deve indicare che il documento è stato correttamente registrato, riportando il nuovo numero di protocollo e la data in formato gg/mm/aaaa.

La registrazione annullata resta visibile all'interno del sistema di gestione documentale.

I documenti annullati sono inseriti nei rispettivi fascicoli.

Non può, invece, essere annullato un documento in uscita già

trasmesso. In particolare, con l'invio a mezzo PEC, in quanto il destinatario è già in possesso del documento stesso. In questo caso, si procede a redigere, protocollare ed inviare, con lo stesso mezzo di trasmissione precedentemente usato, un nuovo documento che rettifica e sostituisce il precedente.

8.7. Corresponsabilità di un documento e di un fascicolo

Tenendo conto che l'Università degli Studi di Firenze opera come una AOO unica, la corresponsabilità di un documento e/o di un fascicolo è data dalla partecipazione al procedimento amministrativo di più UOR.

Nella corresponsabilità, 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 oppure che è stata inserita per prima 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.

CAPITOLO 9. CASISTICA E COMPORTAMENTI

9.1. Gestione delle gare d'appalto

Le gare d'appalto vengono gestite in modalità telematica, attraverso l'utilizzo delle piattaforme Mepa (Mercato elettronico della PA) e START (Sistema Telematico Acquisti della Regione Toscana). Eventuali affidamenti diretti non gestiti tramite queste piattaforme vengono formalizzati mediante PEC, quindi tramite protocollo informatico dalla Centrale Acquisti

I documenti inerenti le gare svolte mediante portale telematico non sono oggetto di protocollazione mentre i documenti pervenuti in modalità elettronica (PEC o e-mail) protocollati dalla Centrale Acquisti

9.2. Gestione di concorsi e selezioni

Le istanze di partecipazione a concorsi e selezioni, pervenute in formato analogico, vengono automaticamente acquisite a protocollo con i soli allegati obbligatori (carta di identità e attestazione versamento dei diritti).

Eventuali altri allegati non sono acquisiti a protocollo, ma restano su apposita piattaforma.

Se le istanze di partecipazione a concorsi e procedure di selezione sono inviate in modalità telematica, a mezzo PEC, gli allegati

saranno automaticamente associati alla registrazione.

9.3. Atti e comunicazioni giudiziarie

La notifica, quando non è disposto diversamente, avviene con la consegna dell'atto eseguita dall'ufficiale giudiziario, nelle mani proprie del destinatario o a soggetto rappresentante dell'amministrazione autorizzato a ricevere l'atto, tramite servizio postale, a mezzo PEC o nelle altre modalità stabilite dalla legge. La notifica tramite il servizio postale o a mezzo PEC può essere eseguita anche da avvocati e procuratori legali autorizzati (ai sensi della L.53/94 e dell'art. 55 L.69/2009).

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

Se l'atto è notificato a mezzo PEC, ai sensi dell'art. 149-bis cpc, la copia estratta dal documento originale deve essere firmata digitalmente dall'ufficiale giudiziario o dall'avvocato/procuratore autorizzato e, se non è fatto espresso divieto dalla legge, la notificazione può eseguirsi anche previa estrazione di copia informatica del documento analogico. L'ufficiale giudiziario o l'avvocato/procuratore autorizzato trasmette copia informatica dell'atto sottoscritta con firma digitale all'indirizzo di posta elettronica certificata del destinatario risultante da pubblici elenchi

o comunque accessibili alle pubbliche amministrazioni. La relata di notifica deve essere redatta su documento informatico separato, sottoscritto con firma digitale. La notifica si intende perfezionata nel momento in cui il gestore rende disponibile il documento informatico nella casella di posta elettronica certificata del destinatario.

In tutti i casi su esposti, per mittente si intende l'avvocato/procuratore istante, munito di apposita procura alle liti, che agisce in nome e per conto del soggetto interessato e che ha richiesto la notifica dell'atto. Anche un sindacato o un'associazione non riconosciuta, può essere mittente, nel caso in cui agisca in nome e per conto di un lavoratore in una controversia sindacale.

Il mittente del documento non è l'organo giudiziario indicato generalmente sul frontespizio dell'atto (ad es., Tribunale, Corte di Appello), ma il soggetto che ha richiesto la notificazione, generalmente il legale a cui il ricorrente/attore che ha conferito mediante mandato la procura alle liti.

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

le comunicazioni dalla stessa provenienti.

Diverse sono poi le comunicazioni (quali quelle consistenti in avvisi di deposito di note o di fissazione di udienza) che provengono direttamente dalla cancelleria dell'autorità giudiziaria (Tribunale, Corte di appello, ecc.) innanzi a cui pende il giudizio. In questi casi il mittente è sicuramente l'autorità giudiziaria medesima.

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

9.4. Documenti informatici con oggetto multiplo

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

Compatibilmente con la funzionalità del sistema di gestione documentale, ciascuna UOR corresponsabile potrà (dovrà) creare la propria copia informatica al fine di proseguire con la gestione e la fascicolatura. Nel caso di documento in partenza è compito della UOR responsabile verificare che il documento prodotto tratti un solo argomento, chiaramente espresso nel campo "oggetto".

9.5. Fatture elettroniche (Fattura PA)

La fattura elettronica rispetta i requisiti di formato e contenuto prescritti dal Decreto Ministeriale 3 aprile 2013, n. 55 (e successive modifiche), per la compatibilità con l'apposito Sistema di Interscambio (SdI).

È obbligatorio emettere fatture elettroniche nei confronti di tutte le amministrazioni pubbliche, sia per il ciclo attivo che per quello 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). In tal caso la fattura andrà gestita come qualsiasi documento analogico: protocollata, assegnata, registrata nel registro delle fatture e fascicolata.

Le fatture cartacee che avrebbero dovuto essere emesse in formato elettronico vanno restituite al mittente attraverso il medesimo canale con cui sono pervenute.

La fattura elettronica perviene in formato XML via PEC, agli indirizzi dichiarati dall'ente e registrati sull'indice IPA nel corrispondente Ufficio di fatturazione oppure tramite File Transfer Protocol - FTP.

Le fatture elettroniche trasmesse dai fornitori alle PA sono obbligatoriamente conservate in modalità elettronica, secondo

quanto espressamente disposto dalla legge.

9.6. DURC on-line

Ai sensi dell'art. 4 della Legge 78/2014 la verifica della regolarità contributiva avviene con modalità esclusivamente telematiche. La risultanza dell'interrogazione avrà validità di 120 giorni dalla data di acquisizione e sostituirà ad ogni effetto il Documento unico di regolarità contributiva (DURC), ovunque previsto, fatta eccezione per le ipotesi di esclusione individuate dalla legge.

La verifica della regolarità contributiva è l'attestazione dell'assolvimento, da parte dell'impresa, degli obblighi legislativi e contrattuali nei confronti di INPS, INAIL e Cassa Edile.

Trattandosi di documento necessario alla corretta documentazione in caso di acquisizione di beni/servizi, il DURC è registrato nell'apposito repertorio e inserito nel fascicolo corrispondente a cura della UOR.

Il documento della verifica della regolarità contributiva generate attualmente dal sistema di INPS/INAIL/CASSA EDILE viene scaricato telematicamente e repertoriato su Titulus (repertorio "verifiche fornitori – in arrivo")

9.7. Denunce di infortuni

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

l'indennizzabilità.

Pertanto, per non incorrere nelle sanzioni previste dall'art. 2 della L. n. 561/1993, come modificato dall'art. 1, comma 1177, della Legge Finanziaria per il 2007, è necessario provvedere tempestivamente, e comunque entro i termini previsti dalla normativa vigente, alla registrazione della documentazione di infortunio pervenuta all'Ateneo. La documentazione è protocollata in modalità "riservato".

Le denunce di infortunio sono inviate esclusivamente in modalità telematica accedendo al portale dell'INAIL con apposite credenziali rilasciate ai dipendenti incaricati. L'invio delle denunce tramite PEC è consentito solo in caso di malfunzionamento del sistema. Considerato che il sistema per l'invio telematico della denuncia prevede l'inserimento obbligatorio di dati ulteriori rispetto a quelli presenti sul certificato del pronto soccorso, è onere del lavoratore consegnare la dichiarazione di infortunio sul lavoro compilata in ogni sua parte. Il delegato alle denunce che ricevesse tale modulo compilato in modo incompleto dovrà chiederne tempestivamente l'integrazione all'infortunato.

9.8. Certificati di malattia

I certificati di malattia vengono trasmessi da INPS, a predisposto indirizzo PEC.

La comunicazione è assunta a protocollo, e successivamente inserita nel fascicolo personale del dipendente.

Nell'eventualità non avvenga la trasmissione dell'attestazione di malattia telematica, è possibile, con apposite credenziali rilasciate a dipendenti incaricati, scaricare i medesimi direttamente dal sito INPS.

9.9. Documenti del portale degli acquisti della pubblica amministrazione

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

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

Gli Accordi quadro, aggiudicati da Consip a più fornitori a seguito della pubblicazione di specifici Bandi, definiscono le clausole generali che, in un determinato periodo temporale, regolano i

contratti da stipulare. Nell'ambito dell'Accordo quadro, le Amministrazioni che hanno effettuato l'abilitazione al sistema Acquisti in Rete, attraverso la contrattazione di "Appalti Specifici", provvedono poi a negoziare i singoli contratti, personalizzati sulla base delle proprie esigenze.

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

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

9.9.1. Affidamenti diretti sulla piattaforma MePA (OdA)

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

Il processo può essere così brevemente schematizzato: il punto istruttore effettua una bozza dell'ordine attraverso la piattaforma e la invia al punto ordinante. Il punto ordinante, cioè la persona che dispone di potere di spesa e del dispositivo di firma digitale, controlla la bozza, genera attraverso la piattaforma il file PDF/A che costituisce il documento d'ordine, lo scarica localmente, lo

firma digitalmente, lo registra nel sistema di protocollo e lo ricarica a sistema.

La piattaforma MePA chiede il numero di protocollo come campo obbligatorio per procedere nella registrazione. Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l'emissione del corrispondente documento gestionale. Nel caso sia un documento di tipo "ordine", questo può essere trasmesso al sistema di gestione documentale dove si genera una bozza per la registratura a protocollo e la fascicolatura. Nel caso invece sia un documento di tipo "contratto" dal sistema contabile può essere richiamato il numero di protocollo assegnato all'ordine emesso sulla piattaforma MePA.

Il numero di protocollo richiesto da Mepa relativo al contratto viene completato una volta scaricato il documento di stipula e firmato digitalmente, poiché viene repertoriato (registro scritture private) e successivamente reinserito sul portale con il relativo numero di repertorio.

9.9.2. Adesioni – Convenzioni (OdA)

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

Il processo può essere così brevemente schematizzato: il punto istruttore seleziona la convenzione, effettua una bozza dell'ordine

attraverso la piattaforma e la invia al punto ordinante.

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

La piattaforma MePA (Acquisti in rete PA) chiede il numero di protocollo per procedere nella registrazione.

Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l'emissione del corrispondente documento gestionale. Nel caso sia un documento di tipo "ordine", questo può essere trasmesso al sistema di gestione documentale dove è generata una bozza per la registratura a protocollo e la fascicolatura.

Nel caso invece sia un documento di tipo "contratto" dal sistema contabile può essere richiamato il numero di protocollo assegnato all'ordine emesso sulla piattaforma MePA.

Il numero di protocollo richiesto da Mepa relativo al contratto viene completato una volta scaricato il documento di stipula e firmato digitalmente, poiché viene repertoriato (registro scritture private) e successivamente reinserito sul portale con il relativo numero di repertorio

9.9.3. Procedure negoziate (RdO) - MePA

Nei casi previsti dalla normativa e dai regolamenti vigenti, si fa

ricorso ad una richiesta di offerta (RdO), che consiste nell'espletamento di una gara telematica con gli strumenti offerti dalla piattaforma MePA. Nell'esecuzione dell'iter che conduce alla creazione della RdO, è possibile allegare dei documenti prodotti dall'amministrazione, sia di carattere amministrativo che tecnico-economico, al fine di supportare i fornitori nella predisposizione dell'offerta. Esempi di tali documenti sono il disciplinare di gara, il capitolato tecnico, ecc.

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

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

9.10. Gestione del secondo esemplare

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

anche che la data e l'ora di firma coincidano.

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

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

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

9.11. Documenti anonimi

La ratio che deve governare il comportamento di un operatore

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

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

CAPITOLO 10. ALBO ON-LINE

Ogni amministrazione pubblica istituisce un unico Albo on-line, raggiungibile dalla pagina iniziale del sito web istituzionale.

Il repertorio dell'Albo on line è gestito esclusivamente e conservato permanentemente in ambiente digitale.

La pubblicazione all'Albo on line sostituisce ogni altra forma di pubblicità legale in altri siti informatici, salvo i casi espressamente previsti dall'ordinamento o dall'autorità giudiziaria. La pubblicazione integrale di documenti con le procedure descritte nell'articolo 32, comma 7, della legge 18 giugno 2009, n. 69, soddisfa, nei casi previsti, il requisito di efficacia; in questo caso all'albo on line, può essere pubblicato l'atto integrale oppure un avviso di avvenuta pubblicazione.

Per le pubblicazioni all'Albo on line si rimanda alle apposite linee guida e al Regolamento per la pubblicazione dei documenti all'Albo on-line di Ateneo (vedi ALLEGATO 14).

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

11.1 Archivio corrente

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

Il responsabile si attiene alle indicazioni che vengono fornite a livello generale dal Responsabile della gestione documentale e da quanto espressamente indicato nel presente Manuale di gestione.

Per la documentazione/fascicoli analogici qualora una UOR dovesse spostare la documentazione corrente, a seguito di mutamento della sede operativa o per altra ragione, dovrà darne informazione tempestiva al Responsabile della gestione documentale.

11.2 Archivio di deposito analogico

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

nell’archivio corrente.

11.3 Trasferimento dei fascicoli cartacei all’archivio di deposito

Il Responsabile del procedimento amministrativo (RPA), sentito il Responsabile della gestione documentale, trasferisce periodicamente, per la conservazione nell’archivio di deposito, i fascicoli relativi ad affari, attività e a procedimenti amministrativi conclusi e non più necessari ad una trattazione corrente. Per il trasferimento viene predisposto a cura del RPA l’elenco dei fascicoli trasferiti.

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

La non corrispondenza, anche parziale, tra l’elenco di consistenza

e il materiale documentale effettivamente versato sarà oggetto di dichiarazione a cura del Responsabile della gestione documentale e sarà informata la struttura versante con invito a provvedere entro 10 giorni alla regolarizzazione.

11.4 Trasferimento dei fascicoli informatici

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

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

Se il soggetto conservatore è diverso dal soggetto produttore (cioè l'Ateneo) il trasferimento della documentazione, configurandosi come una particolare forma di outsourcing, deve

essere preventivamente autorizzato dalla competente Soprintendenza archivistica e bibliografica; la fattispecie può essere autorizzata una tantum nella forma di generale nulla osta all'affidamento della documentazione digitale al conservatore accreditato prescelto.

11.5. Trasferimento delle serie archivistiche

Le serie archivistiche (contratti, decreti, verbali, ecc.) sono trasferite all'archivio di deposito nella loro unitarietà, secondo un termine che può variare da serie a serie.
Le modalità di trasferimento sono le medesime previste per i fascicoli cartacei e informatici.

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

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

uno a repertorio e il secondo nel fascicolo della pratica relativa o, in alternativa, copia conforme.

11.6 Ordinamento archivistico

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

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

classificazione.

Fascicoli e documenti analogici, prodotti senza l'applicazione di un titolario o piano di classificazione, sono ordinati dopo un'adeguata analisi degli stessi, al fine di un ordinamento secondo criteri condivisi e orientati a essere perduranti nel tempo.

Gli interventi su questa documentazione vanno comunque valutati insieme alla Soprintendenza Archivistica e bibliografica competente.

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

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

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

Il Sistema Archivistico di Ateneo è titolare e responsabile del servizio di ricerca documentale, effettuato su richiesta degli uffici dell'Ateneo o di altri soggetti autorizzati.

Il servizio, ove necessario, viene effettuato con la collaborazione degli uffici produttori o interessati. Il servizio è di norma erogato

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

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

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

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

Il Responsabile della gestione documentale (o suo delegato) tiene traccia delle richieste di prelievo dei fascicoli dall'archivio di deposito in un apposito registro di carico e scarico costituito da un documento informatico in formato xlsx. Il registro riporta, oltre ai dati identificativi del fascicolo, l'unità organizzativa richiedente, il nominativo del richiedente, la motivazione, la data della richiesta,

la data di evasione della richiesta, la data della effettiva restituzione ed eventuali note sulla documentazione consegnata.

11.9. Conservazione

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

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

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

CAPITOLO 12. MISURE DI SICUREZZA DEL SISTEMA INFORMATICO

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

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

Le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017.

In tale ottica, il responsabile della gestione documentale in accordo con il responsabile della conservazione, con il responsabile per la transizione al digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)39, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie

particolari di cui agli artt. 9-10 del Regolamento stesso.

L'Ateneo pertanto in questa logica ha previsto la redazione del Piano della Sicurezza riportato nel seguente articolato di cui gli allegati riferiti fanno parte integrante.

Tale piano deve considerare gli aspetti rilevanti per la sicurezza dei documenti considerando le diverse componenti della sicurezza quali ad esempio il livello organizzativo, fisico e logico.

12.1. Il modello organizzativo

I servizi di information and communication technology per il supporto all'attività amministrativa e per le esigenze della didattica e della ricerca dell'Ateneo sono curati da SIAF.
Nell'ambito della gestione documentale, l'Ateneo ha acquisito - secondo il modello in house providing - dal Consorzio CINECA l'applicativo Titulus con una soluzione di tipo Software as a Service (SaaS): le funzionalità del programma sono rese disponibili attraverso un sito web, il cui accesso è subordinato a un processo di autenticazione informatica effettuato mediante ricorso al 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 (ALLEGATO 15)

12.1.1 Il sistema di gestione documentale

II sistema di gestione documentale è conforme alle specifiche previste dalla normativa vigente e deve consentire:

- l'accesso controllato al protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle

informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili e giudiziari;

- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

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

In particolare, sono parte integrante dell'infrastruttura i cablaggi e gli apparati di rete presenti presso le sedi dell'Ateneo e necessari per la connettività verso il Consorzio CINECA per mezzo della rete GARR, i sistemi informatici e le componenti software sottese al sistema di autenticazione dell'Ateneo e tutte le postazioni di lavoro utilizzate dagli utenti del sistema di gestione documentale. Le misure di sicurezza fisica e logica specifiche e le procedure comportamentali adottate per la protezione dell'infrastruttura del sistema di gestione documentale, delle informazioni e dei dati sono riportate nei paragrafi seguenti e nelle "Istruzioni operative per l'utilizzo dei dispositivi elettronici" ALLEGATO 16. Per gli ambiti curati dal Consorzio CINECA si veda l'ALLEGATO 15 in cui sono descritte le misure adottate per garantire un adeguato livello di sicurezza fisica del data center del Consorzio CINECA. Esso illustra le misure per la protezione fisica dei locali tecnici finalizzate a

garantire l'integrità e la disponibilità degli apparati di rete, dei server e delle applicazioni, nonché le misure adottate per la protezione dei dati e le caratteristiche del servizio di Disaster Recovery per il quale è dichiarato un punto di ripristino RPO (Restore Point Objective) pari ad 8H o 24H con un RTO (Recovery Time Objective) di 72 ore in caso di Disaster & Recovery; non è previsto un piano di business continuity essendoci un RTO diverso da 0.

Per quanto riguarda invece di competenza dell'Ateneo si rimanda ai paragrafi seguenti.

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

12.2. PIANO DI SICUREZZA

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

Il piano della sicurezza informatica relativo a formazione, gestione, trasmissione, interscambio, accesso, memorizzazione dei documenti informatici, ivi compresa la gestione delle copie di sicurezza nel rispetto delle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017 è predisposto e aggiornato annualmente dal Consorzio CINECA in quanto in-house provider dell'applicazione di gestione del

protocollo Titulus, anche in relazione alle norme sulla protezione dei dati personali.

Dal momento che alcune delle componenti del sistema (quali ad esempio gli elementi relativi all'autenticazione) sono gestiti dall'Ateneo nel Datacenter interno di Via delle Gore presso SIAF, si ritiene opportuno integrare quanto predisposto dal Consorzio CINECA con le misure presenti all'interno dell'Ateneo e che sono dettagliate nel seguito.

12.2.1. Obiettivi del piano di sicurezza

II piano di sicurezza garantisce che:

- esista e sia aggiornata l'analisi dei rischi che incombono sui dati (personali e non) e/o sui documenti trattati anche utilizzando specifiche Analisi di Impatto;
- i documenti e le informazioni trattate dall'Ateneo siano disponibili, integre e riservate;
- i dati personali comuni, sensibili e/o giudiziari vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento;
- pianificazione degli interventi da attuare in esito ai risultati ottenuti dalle attività precedenti;

- predisposizione, all’occorrenza, di piani specifici di formazione degli addetti.

12.2.2. Generalità

Considerato che la fruizione del sistema di gestione documentale è gestita da un erogatore esterno gran parte delle funzioni/responsabilità di sicurezza sono demandate a detto all'erogatore. All’Ateneo, in quanto fruitore del servizio, è demandata la componente "locale" della sicurezza, affinché attraverso la propria organizzazione, nonché le sue misure e le politiche di sicurezza, contribuisca a stabilire adeguati livelli di sicurezza proporzionati al "valore" dei dati/documenti trattati.

Il piano di sicurezza si articola, di conseguenza, in due componenti: una di competenza del soggetto erogatore, una di competenza dell’Ateneo, e si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e i documenti trattati (anche nel rispetto del modello di shared responsibility applicato in generale ai servizi di tipo SaaS), rispettivamente, nei locali dove risiedono le apparecchiature utilizzate dall’erogatore e nei locali dell’Ateneo;

Esso definisce pertanto le politiche generali e particolari di sicurezza da adottare all'interno dell’Ateneo, le modalità di accesso al sistema di gestione documentale e gli aspetti operativi della sicurezza, nonché i piani specifici di formazione degli addetti e le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano della sicurezza specifica quindi che si debba procedere a:

- assegnare ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione; tale credenziale potrà essere anche sostituita da un accesso tramite SPID/CIE/CNS;
- prevedere il cambio delle password con frequenza almeno semestrale durante la fase di esercizio stabilito tramite azioni automatiche tecnica o tramite procedura manuale demandata all'utente;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I contenuti del piano sono soggetti a revisione formale con cadenza almeno biennale, anche se esso può essere modificato in ogni momento a seguito di eventi gravi.

12.2.3. Sicurezza dei documenti informatici e della loro formazione

L'accesso al sistema di gestione documentale di ogni utente dell'Ateneo è gestito centralmente ed è subordinato all'abilitazione

a cura del Responsabile della gestione documentale. Le identità digitali utilizzate per l'accesso al sistema di gestione documentale sono costituite da nome utente e password o accesso SPID/CIE (CNS come documentato nel paragrafo 12.2.2. L'identificazione informatica dell'utente, cioè la validazione dell'identità digitale, è operata attraverso una infrastruttura di autenticazione centralizzata (IDP) o tramite ricorso ai servizi dei gestori SPID/CIE.

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

Il sistema di gestione documentale rispetta misure di sicurezza idonee a garantire i diritti degli interessati come previsto dalla normativa in materia di protezione dei dati personali (art. 32 del Regolamento Generale sulla Protezione dei Dati Reg. UE 679/2016).

I dati sono resi disponibili e accessibili a chiunque ne abbia diritto.

L'Ateneo nel rispetto delle previsioni di cui all'art. 4 par. 1 10) e all'art. 2 -quaterdecies del D.lgs. 196/2003, si è dotato di una propria organizzazione per la protezione dei dati approvata dal Consiglio di Amministrazione del 23 dicembre 2020. Tale organizzazione oltre al titolare del trattamento, individuato nell'Università degli Studi di Firenze nel suo complesso quale soggetto che determina le finalità e i mezzi del trattamento di dati personali prevede altre figure quali:

i Delegati:

- Dirigenti delle Aree dell'amministrazione centrale
- i Direttori dei Centri di Servizio
- i Responsabili amministrativi dei Dipartimenti relativamente ai dati personali trattati nella gestione amministrativa delle rispettive strutture
- i Direttori dei Dipartimenti nella funzione di sorveglianza generale sul regolare andamento delle attività didattiche e di ricerca - Art. 16 lett. g) Regolamento di Ateneo dei Dipartimenti
- i Presidenti delle Scuole;

i Referenti per la protezione dati:

- i titolari di posizioni organizzative relative alle unità organizzative afferenti alle varie Aree o Centri di servizio (Unità di processo, Unità Funzionali, Biblioteche, sezioni museali) o di altre strutture comunque subordinate ad una delle figure designate Delegato
- i Responsabili di progetti di ricerca.

gli incaricati del trattamento individuati secondo il principio di preposta funzione:

- il personale strutturato (personale tecnico amministrativo, personale docente e ricercatore) documentalmente assegnato ad un'unità organizzativa / struttura / dipartimento deputata a compiere operazioni di trattamento sui dati personali in possesso dell'Ateneo
- qualunque persona fisica che, a seguito di atto di

assegnazione anche temporaneo (collaborazioni coordinate e continuative, contratti a progetto, 150 ore per studenti, stage, volontari del servizio civile, dottorandi, borsisti, tutor, assegnisti di ricerca, ecc.) si trovi ad afferire ad un'unità organizzativa / struttura / dipartimento deputata a compiere operazioni di trattamento sui dati personali trattati dall'Ateneo per i trattamenti e le finalità di pertinenza di ciascuna unità organizzativa / struttura / dipartimento, individuate nel Registro delle attività di trattamento.

Per particolari attività di trattamento l'Università degli studi di Firenze può ricorrere a Responsabili del trattamento ai sensi dell'art. 28 del Reg. UE 676/2019. In tale contesto per la conduzione del Sistema di gestione documentale, al Consorzio CINECA è conferito il ruolo di Responsabile del trattamento; in virtù di tale ruolo è il Consorzio che, per le attività di conduzione del sistema, gestione applicativa e assistenza, provvede alla nomina dell'amministratore di sistema, ne assolve i compiti e conseguenti adempimenti.

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

Le risorse strumentali e le procedure utilizzate per la formazione

dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e la struttura di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche riportate nell'ALLEGATO 17;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'accessibilità dei documenti ai sensi delle vigenti norme tecniche riportate nell'ALLEGATO 18.

I documenti sono prodotti con l'ausilio di applicativi di videoscrittura o editor di testi anche se per la forma finale del documento si adottano preferibilmente i formati PDF/A e XML.

I documenti informatici redatti con strumenti che generino formati diversi sono convertiti, prima della loro sottoscrizione con firma digitale, nei suddetti formati standard.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto, si applicano le regole per la validazione temporale e per

la protezione dei documenti informatici previste dalle normative vigenti, implementate comunque all'interno del sistema di gestione documentale.

12.2.4. Sicurezza fisica del data center

II controllo degli accessi fisici alle risorse dei locali a cui afferisce il Data Center di Ateneo è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;
- i meccanismi di controllo dell'accesso sono più selettivi all'aumentare del livello di protezione del locale; in particolare per l'accesso ai locali del datacenter è previsto un secondo badge fisico distinto da quello del controllo accessi di edificio che porta anche agli uffici;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti non possono entrare e trattenersi nelle aree protette se non accompagnati da personale dell'Ateneo del servizio autorizzato a quel livello di protezione;
- il personale della sede ha l'obbligo di utilizzare il badge in ingresso alla sede.

12.2.5. Sicurezza infrastrutturale del data center

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

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

- locali dedicati esclusivamente a ospitare gli apparati server e i dispositivi di rete;
- sistema di controllo degli accessi;
- sistema automatico di estinzione degli incendi;
- alimentazione elettrica protetta da dispositivi di stabilizzazione e continuità della tensione (UPS);
- gruppo elettrogeno che interviene automaticamente in caso di mancanza dell'alimentazione principale di rete;
- impianto di climatizzazione automatico ridondato e opportunamente dimensionato in grado di mantenere una temperatura ambientale non superiore ai 24°.

Eventuali interventi di qualsiasi natura (anche non informatica) nei locali ospitanti gli apparati server e apparati di rete avvengono sempre in maniera coordinata tra Servizio ICT ed i servizi Tecnici delle Aree di Ateneo.

12.2.6. Sicurezza logica del data center

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Nell'ambito dell'Ateneo e più in particolare in relazione ai sistemi correlati al sistema di gestione documentale quali la gestione dell'autenticazione, tale componente è stata realizzata attraverso:

- l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema

informatico:

- riservatezza dei dati;
- integrità dei dati;
- integrità del flusso dei messaggi;
- la ridondanza dei sistemi di esercizio.

· l'infrastruttura di sicurezza realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione degli addetti dell'Ateneo con le seguenti caratteristiche:

- unico sistema di repository delle credenziali di accesso degli utenti;
- unico database delle anagrafiche contenente tutti i profili di utenza.

12.2.7. Rete dati

L'utilizzo del sistema di gestione documentale è garantito dalla rete dati di Ateneo e dalla rete GARR. L'accesso alla rete dati di Ateneo è effettuato in conformità alle regole definite nella Acceptable Use Policy – AUP stabilite dal Consortium GARR (vedi ALLEGATO 19) e nelle Istruzioni Operative per l'utilizzo dei Dispositivi Elettronici (vedi ALLEGATO 16).

SIAF, in qualità di amministratore della rete di Ateneo, assicura la gestione, il monitoraggio, l'aggiornamento e l'ampliamento della rete dati di Ateneo (cablaggio e parte attiva), sia sotto l'aspetto fisico che logico, fino alla presa utente compresa.

12.2.8. Accesso ai dati e ai documenti informatici

Il sistema adottato dall'Ateneo garantisce:

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

Il controllo degli accessi è assicurato dall'utilizzo di credenziali di autenticazione con differenti profili di autorizzazione in relazione ai diversi ruoli di ciascun utente. I trattamenti associabili a ciascun profilo, preventivamente individuati dal Responsabile della gestione documentale di concerto con i Responsabili delle strutture in base al ruolo loro assegnato nell'organizzazione per la protezione dei dati, sono in sintesi:

- inserimento dei dati per effettuare una registrazione;
- modifica dei dati di una registrazione;
- annullamento di una registrazione;
- ricerca di informazioni registrate ai fini della visualizzazione o consultazione;

- visualizzazione e consultazione;
- download dei documenti associati alla registrazione.

Periodicamente, e comunque almeno annualmente, è verificata a cura del Responsabile della gestione documentale di concerto con i Responsabili delle strutture, la sussistenza delle condizioni per il mantenimento dei profili di autorizzazione. Per quanto riguarda la garanzia di immodificabilità dei contenuti si rimanda a quanto illustrato al § 6.8.

Quando l'accesso ai dati e agli strumenti informatici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, in caso di prolungata assenza o impedimento dell'incaricato l'accesso ai dati è assicurato mediante l'organizzazione interna alla UOR che necessariamente prevede la ridondanza di operatori incaricati sulle medesime procedure. Le stesse credenziali non possono essere assegnate a persone diverse, neppure in tempi diversi, quindi le credenziali sono strettamente personali.

Ciascun utente ha la possibilità di cambiare la propria password in qualsiasi momento.

CAPITOLO 13 - APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI

13.1. Modalità di approvazione e aggiornamento del manuale

Il Manuale di Gestione documentale è adottato con decreto del Direttore Generale, su proposta del Responsabile della Gestione Documentale, previa comunicazione del contenuto al Consiglio di Amministrazione dell'Ateneo.

Il presente Manuale potrà essere aggiornato a seguito di:

normativa sopravvenuta;

introduzione di nuove pratiche tendenti a migliorare l'azione amministrativi in termini di efficacia, efficienza e trasparenza;

inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.

Le eventuali modifiche che dovessero intervenire sugli allegati al presente Manuale senza modifiche all'articolato vengono emanate con circolare del Direttore Generale.

13.2. Operatività del presente manuale

II presente Manuale è operativo il primo giorno del mese

successivo a quello della sua approvazione.

13.3. Norme di rinvio

Per quanto non espressamente previsto dal presente manuale, si farà riferimento alla normativa vigente in materia, adottando comportamenti ispirati ai principi del buon andamento dell'attività amministrativa.

UNIVERSITÀ
DEGLI STUDI
FIRENZE

ALLEGATI

UNIVERSITÀ DEGLI STUDI FIRENZE

1 - RIFERIMENTI NORMATIVI

Elenco delle normative di riferimento aggiornate al dicembre 2021

1. Legge 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
2. Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
3. Direttiva del Ministro per l'innovazione e le tecnologie 9 dicembre 2002, Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali
4. Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati Personali
5. Legge 9 gennaio 2004, n. 4, Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici
6. 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
7. Decreto legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale - CAD e ss.mm.ii
8. Legge 24 dicembre 2007, n. 244, Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008)
9. Decreto legge 29 novembre 2008, n. 185 convertito dalla Legge 28 gennaio 2009, n. 2, Misure urgenti per il sostegno a

famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale

10. 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
11. Legge 18 giugno 2009, n. 69, Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile
12. 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
13. Provvedimento 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
14. Decreto Legge n. 9 febbraio 2012, n. 5 convertito dalla Legge 4 aprile 2012, n. 35, Disposizione urgenti in materia di semplificazione e di sviluppo
15. Decreto Legge 18 ottobre 2012, n. 179 convertito dalla Legge 17 dicembre 2012, n. 221, Ulteriori misure urgenti per la crescita del Paese
16. 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

17. Circolare interpretativa del Ministero dell'Economia e Finanze numero 1/DF del 9 marzo 2015 in tema di fatturazione elettronica
18. 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
19. 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
20. DPCM 3 dicembre 2013, Regole tecniche in materia di sistema di conservazione degli archivi Digitali, art. 2 comma 1, Oggetto e ambito di applicazione; art. 6, Funzionalità; art. 9, Formato della segnatura di protocollo; art. 18 commi 1 e 5, Modalità di registrazione dei documenti informatici; art. 20, Segnatura di protocollo dei documenti trasmessi; art. 21, Informazioni da includere nella segnatura (a partire dalla data di applicazione delle Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici, maggio 2021, sono abrogate tutte le altre disposizioni fatte salve le

precedenti).

21. Provvedimento 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
22. 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
23. 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)
24. Decreto Legge 24 aprile 2014, n. 66, convertito dalla Legge 23 giugno 2014, n. 89, Misure urgenti per la competitività e la giustizia sociale
25. Decreto Legge 20 marzo 2014, n. 34 convertito dalla Legge 16 maggio 2014, n. 78, Disposizioni urgenti per favorire il rilancio dell'occupazione e per la semplificazione degli adempimenti a carico delle imprese
26. Decreto del Ministero del lavoro e delle politiche sociali 30 gennaio 2015, Semplificazione in materia di documento unico

di regolarità contributiva (DURC)
27. Provvedimento del Garante per la protezione dei dati personali 19 marzo 2015, n. 161, Linee guida in materia di trattamento di dati personali per profilazione online
28. 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
29. 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)
30. Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici maggio 2021
31. DPCM 12 agosto 2021, n. 148 Regolamento recante modalità di digitalizzazione delle procedure dei contratti pubblici, da adottare ai sensi dell'articolo 44 del decreto legislativo 18 aprile 2016, n. 50.

2 - ATTUAZIONE AREA ORGANIZZATIVA OMOGENEA UNICA DI ATENEO

Circolare su Introduzione del protocollo unico di Ateneo. Indicazioni operative e vademecum (Repertorio n. 32, Prot. n. 103035 del 22/12/2014)

3 – MAPPATURA DEI PROCEDIMENTI AMMINISTRATIVI DELL'ATENEO

(in corso di elaborazione)

4 – DISEGNO ORGANIZZATIVO DELLE AREE DELL'AMMINISTRAZIONE CENTRALE E DEI DIPARTIMENTI

Funzionigramma di Ateneo e sottoarticolazione della struttura organizzativa

- Funzionigramma di Ateneo - Febbraio 2015
  http://www.unifi.it/upload/sub/ateneo/organigramma/2018/funzionigramma_di_ateneo.pdf
-

Sottoarticolazione della struttura organizzativa

- Amministrazione Centrale - Settembre 2021
  https://www.unifi.it/upload/sub/ateneo/organigramma/2021/funzionigramma_amministrazione_centrale_0921.pdf
- Dipartimenti e Scuole - Luglio 2021
  https://www.unifi.it/upload/sub/ateneo/organigramma/2021/funzionigramma_scuole_dipartimenti_0721.pdf

5 - REGOLAMENTO DEL SISTEMA ARCHIVISTICO DI ATENEO

Emanazione del nuovo *Regolamento del Sistema Archivistico di Ateneo dell'Università degli Studi di Firenze*, Decreti del Rettore, Repertorio n. 123, Prot n. 21705 del 16/02/2016

6 - NOMINA DEL RESPONSABILE DELLA GESTIONE DOCUMENTALE

Nomina del dott. Fabio Silari a "*Responsabile della gestione documentale dell'Ateneo*", Decreti Dirigenziali, Repertorio n. 1054, Prot n. 219901 del 30/08/2021

7 - NOMINA DEL RESPONSABILE DELLA CONSERVAZIONE

Nomina della dott.ssa Vincenza Lombardo a "*Responsabile della conservazione dell'Archivio digitale*", Decreti Dirigenziali, Repertorio n. 1259, Prot n. 113568 del 31/07/2017

8 – NOMINA, COMPETENZE E RISORSE DEL RESPONSABILE PER LA TRANSIZIONE DIGITALE

- Conferimento dell'incarico all'ing. Marius Bogdan Spinu di "Responsabile della transizione digitale 2021-2024" (Decreto Rettorale n. 1423, prot. num. 261615 del 7 ottobre 2021) https://www.unifi.it/upload/sub/intranet/transizione-digitale/decreti/20211007-DR1423_2021_prot0261615.pdf | precedente incarico Decreto Rettorale n. 1328/2017 https://www.unifi.it/upload/sub/intranet/transizione-digitale/decreti/20171212-ddg_1328_2017_responsabile%20digitale.pdf
- Istituzione ufficio del Responsabile per la Transizione Digitale (RTD), e nuova funzione di responsabilità denominata 'Supporto gestione all'utenza' Decreto del Direttore Generale n. 968/2019 (prot. num. 108007 del 12 giugno 2019) https://www.unifi.it/upload/sub/intranet/transizione-digitale/decreti/20190612-UfficioRTD_Supporto_FTO.pdf
- Personale tecnico-amministrativo assegnato all'Ufficio del Responsabile per la transizione digitale" Decreto del Direttore Generale n. 1523, prot. Num. 0231045 del 18 dicembre 2020 https://www.unifi.it/upload/sub/intranet/transizione-digitale/decreti/20201218-afferenza_Ufficio_RTD_FTO.pdf

9 - LINEE GUIDA PER L'UTILIZZO DEL SERVIZIO DI POSTA ELETTRONICA ISTITUZIONALE

Regolamento di utilizzo dei servizi di comunicazione dell'ateneo, Decreto Rettorale, Repertorio n. 22, Prot n. 4643 del 15/01/2015 https://www.unifi.it/upload/sub/normativa/dr_22_15_reg_servizi_comunicazione.pdf

10 - LINEE GUIDA PER L'UTILIZZO DELLA POSTA ELETTRONICA CERTIFICATA E ELENCO CASELLE PEC

- Linee guida (in corso di elaborazione)
- Elenco delle caselle di Posta Elettronica Certificata (in corso di elaborazione)

UNIVERSITÀ DEGLI STUDI FIRENZE

11a - PIANO DI FASCICOLAZIONE

(in corso di elaborazione)

11b - TITOLARIO (PIANO DI CLASSIFICAZIONE)

Titolario unico di classificazione (in vigore dal 1 gennaio 2019, D.D. 2130 del 21 dicembre 2018)
https://www.unifi.it/upload/sub/amm_centrale/archivio/titolario_unico_2019.pdf

12 – REPERTORI

(al novembre 2021)

Accessori stipendiali PTA
Albo ufficiale di Ateneo
Assenze PD
Assenze PTA
Atti di cantiere
Certificazioni previdenziali e fiscali
Comunicazione
Contratti - Convenzioni
Contratti Europei
Contratti co.co.co.
Contratti e convenzioni di didattica e di ricerca
Contratti ed incarichi dirigenziali
Contratti personale PTA
Contratti t.d. di lavoro subordinato per attività di ricerca
Convenzioni per attività in conto terzi
Corrispondenza visite fiscali ASL
// Decreti del Direttore (DD)
Decreti del Rettore (DR)
Infortuni
Permessi Sindacali
Proposta
Registro scritture private
Richieste Accesso e Certificazioni
Richieste visite fiscali
Rilascio certificati
Servizio civile
Ufficiale Rogante
Variazione orari
Verbali
Verifiche dati e certificazioni
Decreti Dirigenziali
Decreti del Presidente/Direttore
Circolari
Delibere Organi
DURC
Rapporto di versamento
Registro informatico giornaliero di protocollo
Documenti Valutazione dei Rischi
Verifiche Fornitori - arrivo
Verifiche Fornitori - partenza

13 - MASSIMARIO DI CONSERVAZIONE E SCARTO

Massimario di conservazione e scarto dei documenti amministrativi dell'Università degli Studi di Firenze: Approvato dal Senato Accademico, il 20 dicembre 2018 (Repertorio n. 45, Prot n. 1784 del 07/01/2019), e dal Consiglio di Amministrazione, il 21 dicembre 2018 (Repertorio n. 45, Prot n. 1784 del 07/01/2019) https://www.unifi.it/upload/sub/saa/massimario_unifi.pdf

14 - PUBBLICAZIONE DEI DOCUMENTI ALL'ALBO ONLINE DI ATENEO

A. Regolamento e altre disposizioni
B. Pubblicazione atti con firma digitale sul sito web di Ateneo

A. REGOLAMENTO DELL'ALBO UFFICIALE DI ATENEO
https://www.unifi.it/upload/sub/normativa/reg_albo_testo_coordinato.pdf

B. Pubblicazione atti con firma digitale sul sito web di Ateneo - Prot. n. 146182 del 18/05/2021

Considerati i progressi che l'Ateneo ha fatto nell'utilizzo della firma digitale e considerate le impostazioni della normativa in vigore, fermo restando quanto previsto dal Regolamento dell'Albo Ufficiale di Ateneo, si raccomanda con la presente la pubblicazione in tutte le sezioni dei siti web di Ateneo (Albo ufficiale incluso) dei documenti originali firmati digitalmente evitando la produzione e la pubblicazione di copie (tipo quelle con la dicitura "firmato da nome cognome").
Sono ammesse eccezioni per motivi di accessibilità, protezione dei dati personali o situazioni in cui vanno unificati in un unico PDF file molteplici. Le procedure per la gestione delle eccezioni saranno rese disponibili dall'ufficio competente come individuato dal Regolamento sopracitato.
L'Ufficio del Responsabile per la Transizione al Digitale è a disposizione per eventuali necessità di supporto.
Responsabile per la Transizione al Digitale

15 – SERVIZIO SOFTWARE-AS-A-SERVICE (SAAS)

Il servizio Software-as-a-Service (SaaS) è gestito dal consorzio CINECA. Vedi: https://www.cineca.it/sistemi-informativi-universita/servizi-di-infrastruttura-digitale-le-universita

16 - ISTRUZIONI OPERATIVE PER L'UTILIZZO DEI DISPOSITIVI ELETTRONICI

(in fase di elaborazione)

17 – LINEE GUIDA PER L'UTILIZZO DELLA FIRMA DIGITALE

A cura dell'Ufficio Funzionale di supporto al Responsabile per la Transizione Digitale

Linee guida per la Firma digitale (vers. 2 del 17/05/2021): informazioni di base relative alla firma digitale, giuridiche e tecniche, modalità di utilizzo e di richiesta del certificato di firma digitale remota. Destinatari: personale tecnico-amministrativo e docenti.

https://www.unifi.it/upload/sub/intranet/transizione-digitale/2021/0517_LineeGuidaFirmaDigitaleUNIFI_v3.pdf

Linee guida per la Firma digitale con Smart Card (vers. 2 del 17/05/2021): informazioni sul rilascio ed utilizzo del certificato di firma digitale su Smart Card. Destinatari: Rettore, Direttore Generale e Direttori di Dipartimento.

https://www.unifi.it/upload/sub/intranet/transizione-digitale/2021/0517_LineeGuidaFirmaSmartCardUNIFI_v2.pdf

18 – LINEE GUIDA PER I DOCUMENTI ACCESSIBILI

Disponibile sull'intranet dell'Ateneo

https://www.unifi.it/upload/sub/intranet/transizione-digitale/accessibilita/LineeGuidaDocumentiAccessibili_Ed1.pdf?v=2021

19 - REGOLE DI UTILIZZO DELLA RETE - ACCEPTABLE USE POLICY (A.U.P.)

Sono applicate le regole approvata dal CDA GARR del 25 giugno 2020

https://www.garr.it/it/regole-di-utilizzo-della-rete-aup