UNIVERSITÀ
POLITECNICA
DELLE MARCHE

MANUALE DI GESTIONE DOCUMENTALE

Versione	Data
1.0	20/11/2023

Sommario

L'Università Politecnica delle Marche ha adottato le Linee Guida per l'utilizzo del Linguaggio di Genere, in ottemperanza all'azione 1.4 prevista dal Gender Equality Plan 2022-2025.
L'Ateneo garantisce parità e pari opportunità fra tutte le persone nello studio, nella ricerca e nel lavoro.
Nel presente documento qualora venga adottato l'uso del genere maschile sovraesteso, ciò è dovuto solo ad esigenze di maggiore semplicità nella lettura del testo.

Capitolo 1 - Introduzione, strumenti di lettura e disposizioni comuni

1.1 Premessa generale

Il presente Manuale è redatto ai sensi di quanto disciplinato dalle Linee Guida dell'Agenzia per l'Italia Digitale (d'ora in avanti AgID) sulla formazione, gestione e conservazione dei documenti informatici, pubblicate nel 2020 ai sensi di quanto previsto dall'art. 71 del D. Lgs. n. 82/2005 (Codice dell'Amministrazione Digitale, d'ora in avanti CAD).

Il Manuale descrive le attività di formazione, registrazione, classificazione, fascicolazione e conservazione dei documenti dell'Università Politecnica delle Marche. In particolare, fornisce le informazioni sulla gestione dei flussi documentali informatici in relazione ai procedimenti amministrativi dell'Ateneo e le istruzioni per un corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Il Manuale è destinato alla più ampia diffusione interna ed esterna in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e conservazione dei documenti informatici e si rivolge non solo agli operatori di protocollo, ma in generale a tutto il personale dell'Ateneo che a vario titolo contribuisce alla registrazione, formazione, gestione e conservazione dei documenti dell'Amministrazione stessa, nonché ai soggetti esterni che a vario titolo si relazionano con essa.

Il presente Manuale si compone di un documento principale (parte generale) e di una serie di allegati i quali, per loro natura specialistica, sono appendici tecniche.

La parte generale si compone di 6 parti: la prima dedicata alla descrizione dell'ambito di applicazione del Manuale e dei principi generali; la seconda e la terza dedicate alla descrizione analitica delle procedure di gestione dei documenti e dei flussi documentali informatici in uso presso l'Università Politecnica delle Marche; la quarta dedicata alle politiche di conservazione; la quinta dedicata alle misure infrastrutturali in uso e alle politiche di sicurezza adottate; la sesta contiene le disposizioni finali relative ad entrata in vigore, pubblicazione, divulgazione e successive modifiche.

1.2 Quadro organizzativo istituzionale

Ai sensi dell'art. 50 del D.P.R. n. 445/2000 "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" (d'ora in avanti TUDA), l'Università Politecnica delle Marche ha individuato un'unica Area Organizzativa Omogenea (d'ora in avanti AOO) per una gestione documentale unica e coordinata.

L'AOO si articola in Unità Organizzative Responsabili (d'ora in avanti UOR), corrispondenti alle strutture organizzative previste dall'Organigramma adottato dall'Ateneo e pubblicato sul sito istituzionale (https://www.univpm.it/Entra/Ateneo/Amministrazione/Amministrazione).

L'AOO unica, il relativo codice identificativo e le altre informazioni richieste dalla normativa sono descritte nell'Indice delle Pubbliche Amministrazioni - IPA. Il referente IPA di Ateneo provvede all'accreditamento ed al periodico aggiornamento dei dati nel sito IPA.

All'interno dell'Università Politecnica delle Marche il sistema archivistico è unico così come sono uniche e condivise tutte le politiche archivistiche adottate.

1.3 Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

Ai sensi dell'art. 61 del TUDA, presso l'Ateneo è istituito il servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, individuato nell'Ufficio Segreteria Direzione Generale e Gestione documentale.

Al servizio è attribuita la competenza della tenuta del sistema di gestione analogica e informatica dei documenti, dei flussi documentali e degli archivi nonché il coordinamento del servizio di conservazione digitale.

In particolare, il servizio espleta le seguenti macro-attività:

- definisce e vigila sulla correttezza delle operazioni di registrazione, sull'iter di lavorazione dei documenti in base al procedimento amministrativo a cui si riferiscono, sulla corretta applicazione ed esecuzione dei workflow, della classificazione e dello smistamento dei documenti;
- vigila e sovrintende alla corretta assegnazione dei documenti ai fascicoli di procedimento/affare/procedura;
- gestisce le richieste di annullamento delle registrazioni di protocollo;
- predispone i modelli/formati dei provvedimenti amministrativi degli Organi di Ateneo e vigila sulla loro corretta registrazione nel sistema di gestione documentale informatico.

Il servizio svolge anche attività di help desk di primo livello sul corretto uso delle maschere applicative del sistema di gestione informatica dei documenti e si interfaccia con il servizio di help desk di secondo livello presso il fornitore esterno del sistema di gestione informatica.

La medesima competenza è esercitata sull'archivio e sui documenti analogici, coerentemente con la loro specifica natura.

1.4 Figure di responsabilità

Ai sensi del TUDA, del CAD e delle Linee Guida AgID, l'Università Politecnica delle Marche ha individuato all'interno del suo organico le seguenti figure di responsabilità, a cui sono attribuiti specifici compiti. I relativi atti di nomina sono inseriti nell'allegato D.

- ***Responsabile della gestione documentale***
  (D.P.R. n. 445/2000, art. 61, comma 2 / Linee guida AgID 2020, 3.4)

  Il Responsabile della gestione documentale è individuato tra il personale in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.

In particolare, vigila sulla corretta applicazione di tutte le norme di settore relative alla documentazione amministrativa, agli archivi e ai documenti, definisce regole e criteri uniformi per la corretta creazione, gestione, tenuta a qualsiasi titolo e conservazione dei documenti amministrativi.

Vigila altresì sulla corretta sedimentazione dell'archivio, predispone ed aggiorna tutti gli strumenti necessari alla gestione documentale, in particolare il Titolario di classificazione, il Manuale di gestione, il Manuale di conservazione, il Piano di conservazione.

Vigila sulla corretta implementazione di misure organizzative atte alla dematerializzazione dei documenti e dei flussi documentali.

Definisce, su segnalazione dei responsabili delle unità organizzative, i profili di autorizzazione nel sistema di gestione documentale degli utenti e si coordina con il referente del Servizio ICT per tutte le operazioni di configurazione del sistema di gestione informatica dei documenti in merito alla gestione delle utenze e agli adeguamenti necessari coerentemente con l'organigramma di Ateneo.

Come previsto dal CAD, è coadiuvato dal Responsabile dei sistemi informativi e dal Responsabile della protezione dei dati personali (RPD) relativamente al sistema documentale.

Vigila, di concerto con il Responsabile della conservazione, sulla corretta esecuzione del servizio di conservazione da parte del conservatore esterno.

- ***Responsabile per la transizione al digitale***
  (D.Lgs. n. 82/2005 CAD, art 17, comma 1)

  Al Responsabile per la transizione al digitale sono attribuiti compiti previsti dall'art. 17 del CAD e dalla Circolare n. 3 del 1.10.2018 del Ministro della Pubblica Amministrazione. Ad esso sono affidati i processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità. Sviluppa e supporta i progetti di dematerializzazione dei processi dell'Ateneo e presidia l'applicazione delle disposizioni e delle leggi che regolano il trattamento dei dati e la digitalizzazione della Pubblica Amministrazione (d'ora in avanti PA). Nell'assolvimento dei propri doveri, il Responsabile per la transizione al digitale risponde direttamente al Rettore con riferimento ai compiti relativi alla transizione al digitale e attua l'azione amministrativa e gestionale in accordo con il Direttore Generale.

- ***Responsabile della conservazione***
  (CAD, art. 44 comma 1 quater/ Linee guida AgID 2020, 4.5)

  Il Responsabile della conservazione vigila sulla corretta applicazione delle norme di settore nonché sulla corretta applicazione delle politiche conservative e sulla qualità del servizio offerto dal conservatore esterno.

  Il Responsabile della conservazione, di concerto con il Responsabile della gestione documentale, redige e aggiorna il Manuale di conservazione.

Il Responsabile della conservazione opera d'intesa con il Responsabile dei Sistemi informativi, il Responsabile della Protezione dei Dati (RPD) oltre che con il Responsabile della gestione documentale.

- ***Responsabile della protezione dei dati personali***

(Regolamento (UE) 2016/679 (GDPR), artt. 37 e ss.)

Il Responsabile della protezione dei dati personali è la figura di riferimento di tutte le attività relative al trattamento dei dati stessi. Svolge la sua attività in autonomia e senza ricevere alcuna istruzione per l'esecuzione dei compiti che gli sono attribuiti.

Al Responsabile della protezione dei dati personali sono attribuiti i compiti previsti dall'art. 39 del Regolamento (UE) 2016/679 (d'ora in poi GDPR). L'Università assicura che il Responsabile della protezione dei dati personali sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e lo sostiene nell'esecuzione dei compiti fornendogli le risorse necessarie per assolverli, per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

- ***Responsabile esterno del trattamento dei dati***

(Regolamento (UE) 2016/679 (GDPR), art. 28)

L'Ateneo, nell'affidare servizi o l'esecuzione di attività che richiedano il trattamento di dati personali di cui è Titolare, ricorre a responsabili del trattamento che effettuano dunque il trattamento dati per conto dell'Università e che presentano garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del GDPR, anche per la sicurezza del trattamento.

In considerazione dell'esigenza da parte dell'Ateneo di affidare ad un soggetto esterno all'Amministrazione il servizio di gestione informatica dei documenti ed il sistema di conservazione dei documenti informatici, l'Ateneo ha individuato specifici responsabili esterni al trattamento dei dati.

1.5 Piano di eliminazione dei registri del protocollo diversi dal protocollo informatico

L'Ateneo è costituito dal 1° gennaio 2023 come unica AOO e il registro di protocollo è unico. A far data dal 2017 sono cessati di fatto e di diritto tutti i registri di protocolli interni già in essere.

1.6 Principi della gestione documentale

Il sistema di gestione documentale è l'insieme delle regole, prassi, standard e strumenti anche informatici atti a governare il buon andamento dell'azione amministrativa e la creazione della sua memoria documentaria. Le attività decisionali e programmatiche di ogni Amministrazione si

affiancano a quelle di registrazione, organizzazione, classificazione, archiviazione, selezione e scarto dei documenti intesi quali rappresentazione di atti e fatti giuridicamente rilevanti.

Il processo di gestione documentale è finalizzato a favorire le esigenze di comunicazione interna della PA, a raccontare il processo decisionale e a supportare il controllo di gestione e la programmazione strategica. Infine, esso garantisce la trasparenza dell'azione amministrativa.

La gestione documentale è un processo che può essere suddiviso in tre fasi principali: formazione, gestione e conservazione. Nell'ambito di ognuna delle suddette fasi sono svolte una serie di attività che si distinguono per complessità, impatto, natura, finalità o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte.

Dal punto di vista archivistico, si distinguono tradizionalmente tre fasi di gestione in ragione delle diverse modalità di organizzazione ed utilizzo dei documenti:

- archivio corrente: è formato dai documenti necessari alle attività correnti;
- archivio di deposito: è formato dai documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- archivio storico: è formato dai documenti la cui finalità è prevalentemente di consultazione ai fini storici.

Una corretta gestione dei documenti sin dalla fase di formazione, anche attraverso un sistema di gestione informatica, rappresenta la migliore garanzia di affidabilità del sistema documentale nel tempo e nello spazio giuridico di riferimento.

Nella fase di formazione devono pertanto essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza alle regole tecniche sulla formazione dei documenti informatici. A tal fine, risulta decisivo avvalersi di un valido e completo Manuale di gestione documentale, di workflow documentali, di sistemi di Document & Content Management e di applicativi informatici che si basino su elevati livelli di automazione ed interoperabilità.

La continua trasformazione digitale della PA ed il conseguente ripensamento dei flussi documentali e dei documenti impongono un costante lavoro di valutazione, monitoraggio, riprogettazione e reingegnerizzazione dei documenti e delle attività ad essi connesse nelle diverse fasi di vita del complesso documentario. Conseguentemente alla trasformazione digitale dei documenti, è necessario accorciare le distanze temporali, tipiche dell'archivio analogico, tra la fase corrente, quella di deposito e quella storica. La sedimentazione del complesso documentario va accompagnata quindi fin dalle primissime fasi della vita dei documenti introducendo misure, pratiche e regole ben definite e largamente condivise che possano gestire efficacemente il passaggio dei documenti dalla fase di formazione e gestione a quella di conservazione a lungo termine.

La gestione dei documenti deve proseguire con il periodico riversamento al sistema di conservazione, da realizzarsi in ottemperanza a quanto disposto dal CAD e dalle Linee Guida ad esso collegate.

Capitolo 2 – Formazione del documento informatico

2.1 Documento informatico

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti ed è quindi un file, costituito da una sequenza determinata di valori binari indipendente dal supporto fisico su cui è memorizzata.

L'Università Politecnica delle Marche forma gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni del CAD e delle Linee Guida AgID.

2.2 Requisiti del documento informatico

Il documento informatico deve avere le seguenti caratteristiche:

- affidabilità: deve essere capace di rappresentare i fatti a cui si riferisce ed il suo contenuto deve essere esatto, corretto e adeguato;
- immodificabilità: deve essere 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;
- integrità: deve essere tale da non aver subito nel tempo e nello spazio alcuna alterazione non autorizzata;
- autenticità: deve essere riconducibile con certezza alla volontà del suo autore e corrispondente a ciò che era nel momento originario della sua produzione.

2.3 Formazione del documento informatico

Il documento informatico, ai sensi del CAD e delle Linee Guida AgID, è formato mediante una delle seguenti modalità:

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

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

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

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

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

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

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

2.4 Formazione del documento amministrativo informatico

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

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

Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD sono identificate e trattate come i documenti amministrativi informatici.

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 descritti al paragrafo 2.3, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti.

Al documento amministrativo informatico vengono associati i metadati previsti per la registrazione di protocollo, nonché quelli relativi alla classificazione, ai tempi di conservazione in coerenza con il piano di conservazione e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.

Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti nell'ambito del contesto a cui ogni tipologia di documento si riferisce, secondo quanto previsto dall'Allegato 5 delle Linee Guida AgID. Sarà cura dell'Amministrazione individuare ulteriori metadati da associare a particolari tipologie di documenti amministrativi informatici.

Tra i documenti amministrativi informatici sono inclusi i documenti soggetti a registrazione particolare (es. Repertori), che comunque devono contenere al proprio interno o avere associati l'insieme minimo dei metadati previsti per il documento amministrativo informatico.

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

2.5 Metadati dei documenti informatici

Il documento informatico deve essere identificato in modo univoco e persistente all'interno del sistema informatico di gestione documentale.

Il documento informatico è immodificabile nelle sue parti costitutive e una volta memorizzato nel sistema di gestione documentale non può essere alterato nel suo contenuto, accesso, gestione e conservazione. Tutte le modifiche necessarie danno origine alla redazione di un nuovo documento che integra, rettifica, sostituisce in tutto o in parte il documento precedente.

Come previsto dall'art. 53 del TUDA e dall'allegato 5 "Metadati" delle Linee Guida AgID, ai documenti informatici, ai documenti amministrativi informatici ed alle aggregazioni documentali è associato, in maniera automatica all'atto della registrazione, un set di metadati.

I metadati sono informazioni di contesto che aggiungono dati informativi, gestionali e conservativi ai dati a cui si riferiscono.

Nell'allegato I è riportata una tabella riepilogativa dei principali metadati prodotti dagli attuali sistemi di gestione documentale e di conservazione in uso presso l'Ateneo. Per una trattazione esaustiva dei metadati e della loro codifica, si rimanda alle fonti normative sopracitate.

2.6 Formati

Per la formazione e gestione dei documenti informatici, l'Università Politecnica delle Marche privilegia l'utilizzo del PDF/A.

Altri tipi di formati sono ammessi, ad esempio per gli allegati tecnici di progetti, purché essi siano tra quelli ricompresi nell'Allegato 2 delle Linee Guida AgID.

Qualora dovessero pervenire documenti in formati diversi da quelli sopracitati, sarà cura della UOR assegnataria interfacciarsi con il mittente per concordare la possibilità di una conversione dei documenti nel formato che meglio tutela l'Ateneo verso gli obblighi di conservazione a lungo termine e di leggibilità nel tempo del contenuto giuridico degli stessi. Tali casistiche sono ad oggi del tutto marginali e comunque gestibili attraverso il ricorso ai formati ricompresi nel sopracitato Allegato 2.

2.7 Duplicati, copie ed estratti dei documenti

2.7.1 Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico (ad es. una scansione) è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti.

Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta (art. 22 comma 3 del CAD). Nel caso in cui non vi sia l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis.

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

2.7.2 Duplicati, copie ed estratti informatici di documenti informatici

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

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

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

Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante il raffronto dei documenti. Il ricorso al raffronto assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71 del CAD, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico (art. 23bis comma 2 del CAD). Nel caso in cui non vi sia l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale.

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

2.7.3 Copie su supporto informatico di documenti amministrativi analogici

Alle copie su supporto informatico di documenti amministrativi analogici si applicano le disposizioni di cui al paragrafo 2.7.1.

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

2.8 Sottoscrizione dei documenti informatici

A differenza del documento analogico, che viene sottoscritto con firma autografa e può essere caratterizzato da una pluralità di forme (scrittura privata, atto pubblico, scrittura privata

autenticata) da cui dipende il suo valore giuridico-probatorio, il documento informatico è sottoscritto tramite una firma elettronica.

La firma elettronica non è una mera rappresentazione informatica grafica della firma, ma consiste in un meccanismo di associazione di dati per l'imputazione di effetti giuridici in capo a un determinato soggetto, che può essere ricondotto come il suo autore.

Il documento informatico può essere sottoscritto con firma elettronica semplice, avanzata, qualificata o digitale: dal tipo di firma utilizzata dipendono il valore giuridico e l'efficacia probatoria del documento, secondo le norme previste dal CAD.

2.8.1 Tipologia delle firme elettroniche

- Firma elettronica semplice: insieme dei dati in forma elettronica riconducibili all'autore (es: log identificativo o indirizzo mail, caratterizzati da username e password), allegati o connessi ad atti o fatti giuridicamente rilevanti contenuti in un documento informatico ed utilizzati come metodo di identificazione informatica. Può essere utilizzata per i documenti interni o per apporre i visti approvativi sui documenti amministrativi informatici.
- Firma elettronica avanzata: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico, che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
- Firma elettronica qualificata: una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato.

La Firma digitale italiana è una tipologia di firma elettronica qualificata e si basa su un sistema di chiavi crittografiche, una pubblica e una privata, legate tra loro che permettono di rendere manifesta e verificare la provenienza e l'integrità di un documento informatico.

La firma digitale può essere apposta in diversi formati. In particolare, il formato CAdES (Cryptographic Message Syntax Advanced Electronic Signature) e il formato PAdES (Pdf Advanced Electronic Signatur) hanno entrambi la stessa validità ed efficacia dal punto di vista giuridico.

Di norma i documenti digitali prodotti dall'Ateneo sono sottoscritti nel formato PAdES. Nei casi in cui sia espressamente previsto dalla procedura di acquisizione della firma oppure sia specificamente richiesto dalla controparte o in altri particolari casi, il documento può essere firmato nel formato CAdES.

Per la produzione dei documenti firmati digitalmente, l'Ateneo ha progettato appositi workflow implementati all'interno del sistema di gestione documentale con la finalità di tracciare le varie fasi di formazione del documento digitale, prevendendo specifici step approvativi dei vari responsabili dell'istruttoria (c.d. sigla digitale), fino all'apposizione della firma digitale e alla protocollazione.

La sottoscrizione digitale dei documenti avviene tramite l'utilizzo della firma digitale remota oppure tramite l'utilizzo di dispositivo usb per la firma digitale associato a specifici programmi.

Il sistema di gestione documentale consente di gestire al suo interno gli strumenti di firma digitale, grazie a specifiche funzionalità applicative di interoperabilità.

2.8.2 Efficacia giuridico probatoria dei documenti informatici

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, ai sensi di quanto previsto dall'art. 20 del CAD.

In particolare:

- Il documento informatico privo di sottoscrizione è una copia informatica e come tale forma piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime (2712 cc, 23 quater CAD, 2713 cc).
- Il documento informatico sottoscritto con firma elettronica semplice è liberamente valutabile in giudizio sia per quanto riguarda l'efficacia giuridica sia 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 o firma digitale, se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, fa piena prova della provenienza fino a querela di falso.

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.

Le firme elettroniche qualificate e digitali, con un certificato elettronico revocato, scaduto o sospeso sono considerate valide se alle stesse è associabile una validazione temporale opponibile ai terzi che collochi l'apposizione delle suddette firme in un momento precedente alla scadenza, revoca o sospensione del certificato.

La legge stabilisce le tipologie di documenti informatici che devono essere sottoscritti con firma elettronica qualificata o digitale a pena di nullità (art. 21 comma 2-bis del CAD, art. 15 comma 2-bis della L. n. 241/1990).

2.8.3 Validazione temporale

La validazione temporale consiste nell'associazione al documento di un riferimento temporale certo, che può essere:

- contenuto nella segnatura di protocollo;

- ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una PA;
- ottenuto attraverso l'utilizzo di posta elettronica certificata;
- realizzato dai certificatori accreditati mediante marche temporali.

2.9 Documenti analogici

Per documento analogico si intende la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti, genericamente su supporto analogico.

Il documento analogico rappresenta una modalità di redazione dei documenti in progressivo superamento da parte della PA, che ai sensi del richiamato art. 40 del CAD è tenuta progressivamente a produrre documenti informatici.

Presso l'Università Politecnica delle Marche i documenti analogici sono gradualmente sostituiti da documenti informatici e/o sono limitati a tipologie o casistiche particolari previste dalla normativa vigente. È fatto divieto di produrre in formato analogico tipologie documentali che la normativa dispone che devono essere formate esclusivamente in originale informatico.

Capitolo 3 – Gestione informatica dei documenti

L'Università Politecnica delle Marche si è dotata del sistema informatico di gestione documentale "Titulus", attraverso il quale realizza le funzionalità di gestione dell'archivio corrente, dell'archivio di deposito, dei flussi documentali, di automatizzazione dei procedimenti amministrativi, nonché le funzionalità relative alla registrazione di protocollo e alle altre forme di registrazione.

3.1 Registro di protocollo

Il registro di protocollo è un atto pubblico di fede privilegiata disconoscibile solo attraverso una querela di falso. Esso svolge un'azione certificatoria dei documenti inviati e ricevuti dall'Ateneo e una funzione giuridico probatoria in merito all'esistenza di un documento all'interno del sistema di gestione documentale dell'Ateneo stesso.

Il registro di protocollo viene generato automaticamente dal sistema di gestione informatica dei documenti a cadenza giornaliera e riporta le registrazioni di protocollo effettuate nella giornata lavorativa precedente, comprendendo una serie di metadati che il sistema di gestione associa al numero di protocollo in fase di registrazione. Il numero progressivo di protocollo è costituito da almeno sette cifre numeriche. La numerazione viene rinnovata ad ogni anno solare.

Il registro viene trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendo l'immodificabilità del contenuto.

Il registro giornaliero di protocollo comprende le informazioni minime di protocollo (art. 53 del TUDA) e in maniera organica anche le informazioni di annullamento delle registrazioni di protocollo con la relativa motivazione.

3.1.1 Registro di emergenza

Come previsto dalla normativa vigente, è necessario che i sistemi di protocollo informatico assicurino continuità operativa anche in caso di malfunzionamenti applicativi o incidenti infrastrutturali.
La procedura in uso presso l'Ateneo prevede l'installazione su una macchina fisica locale di un file in formato excel che da remoto gestisce temporaneamente le procedure di protocollazione dei documenti attribuendo i seguenti dati e metadati:

- AOO
- Anno
- Numero di protocollo di emergenza
- Data di protocollo
- Tipo di protocollo (Arrivo, Partenza, Interno)
- Oggetto
- Numero allegati
- Mittente/Destinatario
- Indirizzo mittente/destinatario

Al termine del periodo di emergenza l'Ateneo trasmette il file excel alla casa software fornitrice del sistema di protocollo informatico, il file con i dati contenuti saranno caricati, tramite procedura di recupero dati, all'interno del sistema. Per ciascun documento protocollato in emergenza, sarà creato un documento in stato di bozza che potrà essere completato dall'operatore inserendo eventuali dati aggiuntivi, provvedendo a caricare i file informatici ed infine protocollando il documento. Tali documenti saranno assegnati al Responsabile della gestione documentale dell'Ateneo e classificati con codice I/7 Archivio.

A ciascun documento registrato in emergenza verrà quindi attribuito un numero di protocollo ordinario ed un set di metadati utili a stabilire la correlazione con il numero utilizzato in emergenza (anno del registro di emergenza, numero e data del protocollo di emergenza).

3.2 Registrazione del documento nel sistema di gestione

I documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi sono registrati a protocollo nel sistema di gestione documentale.

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

La registrazione informatica di protocollo è l'insieme di dati in forma elettronica associati o connessi ad un documento al fine dell'identificazione univoca di tutti i documenti prodotti e acquisiti dall'ente. Il nucleo minimo dei suddetti dati forma la segnatura di protocollo, che costituisce l'identificatore univoco del documento. La segnatura si completa con l'associazione ad un riferimento temporale certo ed entrambi sono generati in automatico dal sistema informatico di gestione documentale e formati secondo lo standard definito (artt. 55 e 57 del TUDA).

Il sistema informatico di gestione documentale associa al documento, contestualmente alla fase di registrazione, un set di dati, di metadati e di informazioni di contesto:

- l'identificazione dell'amministrazione o dell'area organizzativa omogenea;
- l'oggetto del documento espresso in forma sintetica ma esaustiva;
- il numero e la descrizione sintetica degli allegati;
- il codice di classificazione;
- il mittente o il destinatario del documento;
- l'indicazione della struttura assegnataria del documento e del soggetto responsabile, compresi eventuali soggetti in copia conoscenza;
- ulteriori informazioni a corredo del documento (es: iter automatico di approvazione, smistamento, controlli, visti, approvazioni e sottoscrizioni digitali nel caso di documenti ai quali venga associato un workflow automatico di lavorazione).

Tale set di informazioni contribuisce a definire il contesto giuridico, amministrativo ed archivistico in cui il documento è formato o gestito e a cui sarà associato nel corso del suo ciclo vitale.

In base alle singole necessità gestionali, la registrazione di protocollo può contenere inoltre ulteriori elementi descrittivi. In particolare, nel campo annotazione possono essere inserite informazioni gestionali e/o amministrative di dettaglio.

3.2.1 Formato della segnatura di protocollo

La segnatura di protocollo è l'associazione o l'apposizione al documento informatico delle informazioni riguardanti il documento stesso. La segnatura di protocollo, calcolata in automatico all'atto della registrazione del documento nel sistema informatico, è associata all'intero record di protocollo (dati, metadati, documento principale o primario e suoi allegati). Essa è costituita da uno schema XML che individua la struttura del cosiddetto file di segnatura, al fine di consentire nello scambio di messaggi tra sistemi di protocollo delle pubbliche amministrazioni una soddisfacente interoperabilità.

La segnatura informatica si compone di quattro sezioni:

a. "Intestazione": contiene i dati identificativi e le informazioni fondamentali del messaggio (obbligatoria);
b. "Riferimenti": contiene le informazioni relative al contesto generale di cui il messaggio fa parte (obbligatoria);
c. "Descrizione": contiene le informazioni descrittive riguardanti il contenuto del messaggio (opzionale);
d. "PiuInfo": contiene ulteriori informazioni specifiche qualora due o più amministrazioni stabiliscano di scambiarsi informazioni non previste tra quelle definite nello schema (opzionale).

In particolare, la sezione "Intestazione" contiene gli elementi essenziali di identificazione e caratterizzazione amministrativa del messaggio protocollato nonché le informazioni relative alla trasmissione del messaggio:

a. numero progressivo di protocollo;
b. data di registrazione;
c. codice identificativo dell'amministrazione;
d. indicazione della AOO mittente;
e. indicazione del registro nell'ambito del quale è stata effettuata la registrazione.

Nel caso di un documento protocollato in uscita, il file di segnatura comprende anche le informazioni relative all'oggetto e al mittente/destinatario.

3.2.2 Annullamento delle informazioni registrate in forma immodificabile

I documenti registrati nel sistema di gestione documentale a cui è stato attribuito un numero di protocollo non possono essere cambiati negli elementi immodificabili della registrazione. Si rende dunque necessario l'annullamento della stessa, con conseguente perdita di validità del numero seriale di protocollo. Tutte le informazioni relative all'annullamento vengono memorizzate direttamente dal sistema di gestione documentale, in modo trasparente ed immodificabile.

L'annullamento può essere richiesto nel caso di errore nell'indicazione degli elementi non modificabili della registrazione o nel caso in cui, successivamente alla registrazione di protocollo, sopravvengano circostanze e/o ragioni che ne giustifichino l'annullamento (es: duplicazione per

errore di una protocollazione o documento non ancora inviato che contiene errori materiali o refusi oppure una modifica sostanziale nel testo del documento).

La procedura di annullamento è di competenza del Responsabile della gestione documentale o dei suoi delegati, ai quali è riconosciuto apposito diritto applicativo nel sistema. L'annullamento viene compiuto attraverso una funzionalità dedicata del software che, in piena trasparenza, memorizza i metadati relativi all'annullamento, comprensivi della motivazione. Il documento annullato resta ricercabile e consultabile nel sistema e mantiene tutte le informazioni originarie, ma riporta la dicitura "annullato".

La procedura vale sia per l'annullamento di un protocollo sia per l'annullamento di un repertorio e viene compiuta con le stesse modalità applicative e procedurali.

Per poter procedere all'annullamento di una registrazione, è necessario che la UOR assegnataria del documento invii la richiesta all'indirizzo di posta elettronica istituzionale della UOR Responsabile della gestione documentale, indicando;

- gli estremi del documento (num. protocollo/repertorio, data, oggetto del documento, eventuale codice identificativo – id documento);
- la descrizione della motivazione dell'annullamento, che va inserita come metadato giustificativo nel sistema.

3.3 Repertori

Oltre alla registrazione di protocollo, il D.P.R. n. 445/2000 prevede la possibilità che alcune tipologie di documenti siano soggette ad una registrazione particolare, in quanto aggregazioni uniformi di documenti omogenei per tipologia o contenuto e riconducibili alla medesima natura formale, e dunque aggregabili in una serie archivistica giuridicamente rilevante.

Tali documenti sono registrati in appositi Repertori o Registri particolari, in ordine cronologico e identificati con un numero seriale che ha cadenza annuale (es: repertorio dei Decreti del Rettore) o continua (es: repertorio dei contratti in forma pubblica amministrativa). In entrambi i casi, la numerazione è crescente e non ammette numeri duplicati o mancanti.

Il nome del repertorio viene sempre esplicitato nella segnatura, insieme al numero seriale e alla data di registrazione. I documenti registrati nei repertori hanno comunque associato anche un numero di protocollo.

L'elenco completo dei repertori integrati all'interno del sistema di gestione documentale ed attivati dall'Università Politecnica delle Marche è contenuto nell'allegato E.

Ogni tipologia di repertorio è unica per tutto l'Ateneo. Ciascuna UOR registra nei relativi repertori i documenti di propria competenza e può consultare solo quelli di cui ha visibilità (in quanto RPA o inserita in copia conoscenza). Solo gli utenti amministratori del sistema di gestione documentale possono visualizzare i repertori nella loro interezza.

I documenti di natura negoziale (es: contratti, convenzioni, accordi, ecc) sono registrati nel relativo repertorio solamente quando il documento è stato perfezionato e firmato da tutte le parti

contraenti; la registrazione va effettuata tempestivamente, una volta acquisita l'ultima firma sul documento.

Tutti i documenti registrati nei repertori vanno sempre inseriti nei fascicoli di pertinenza (es: una determina a contrarre va inserita nel fascicolo del procedimento di acquisto alla quale essa si riferisce).

3.4 Regole di organizzazione delle serie archivistiche

3.4.1 Classificazione

La formazione dell'archivio corrente non è conseguenza di una circostanza casuale che si dilata nel tempo, ma va intesa come risultato di una sedimentazione periodica ed attentamente presidiata con regole e strumenti.

Le componenti documentarie di un complesso archivistico sono unità legate tra loro da un vincolo indissolubile e vengono organizzate attraverso un sistema di classificazione, ovvero uno schema logico costruito sulla base delle funzioni dell'Ateneo rappresentate in una stringa ragionata di codici numerici. Tale organizzazione permette che l'accesso al patrimonio informativo dell'Ateneo risponda alla duplice funzione di certezza giuridica e manifestazione pubblica della volontà amministrativa.

Classificare i documenti significa quindi identificarli ed ordinarli sulla base del nesso esistente tra essi e le attività a cui si riferiscono, attribuendo loro una collocazione logica.

L'operazione di classificazione è obbligatoria per tutti i documenti prodotti o ricevuti dall'Università ed è in carico all'operatore che registra il documento all'interno del sistema di gestione documentale. È possibile modificare la classificazione di un documento. I documenti che non ricevono una corretta classificazione all'atto della protocollazione devono essere adeguatamente classificati e fascicolati dalle UOR responsabili del procedimento.

Il codice di classificazione è contenuto anche nella denominazione di ogni fascicolo e i documenti in esso contenuti seguono la stessa classificazione; fanno eccezione i documenti inseriti in copia, che mantengono invece la classificazione del fascicolo principale a cui appartengono.

Lo schema sistematico su cui poggia tutta l'attività di organizzazione dell'archivio e la conseguente formazione organica delle serie archivistiche, cioè dei raggruppamenti di documenti con caratteristiche omogenee, è il Titolario (o Piano) di classificazione.

3.4.2 Titolario o Piano di classificazione

Le Università italiane si sono da tempo dotate di strumenti archivistici concordati e condivisi, tra cui un titolario di classificazione standard, disegnato sulle specifiche competenze degli Atenei ed integrabile nel sistema di gestione informatica dei documenti. Il Titolario di classificazione dell'Università Politecnica delle Marche è stato redatto con i dovuti adattamenti secondo tale modello.

Il Titolario ha una struttura ad albero ed è articolato su due livelli, i titoli e le classi.

I titoli identificano le funzioni principali dell'Ateneo o le aree di competenza entro cui si muove l'azione amministrativa universitaria e sono attualmente dodici.

Ogni titolo si articola in sottolivelli chiamati classi, che descrivono le macroattività per ciascuna funzione dell'Ateneo. Attualmente ciascun titolo si compone di un numero variabile di classi.

Per il dettaglio del Titolario di classificazione si rimanda all'allegato F.

3.5 Regole di assegnazione dei documenti

I documenti registrati nel sistema di gestione documentale sono assegnati al responsabile della UOR competente per materia alla gestione del relativo procedimento/attività/affare, sulla base delle competenze individuate nel modello organizzativo dell'Ateneo.

La UOR assegnataria del documento ha l'onere di provvedere alla corretta gestione del documento all'interno del sistema informatico di gestione documentale (es: inserimento del documento nel fascicolo di competenza, eventuali correzioni della classificazione, collegamenti a protocolli precedenti e/o successivi, ecc.).

Nel caso in cui sia stata effettuata una errata assegnazione, il responsabile della UOR che ha ricevuto il documento deve tempestivamente provvedere, tramite apposite funzionalità previste nel sistema di gestione documentale, a restituirlo alla UOR che ha assegnato erroneamente il documento (funzionalità di "reso") o a trasferire il documento alla corretta UOR competente (funzionalità di "cambio RPA"). Una volta reso/riassegnato il documento, questo non sarà più disponibile né consultabile dalla UOR a cui era stato erroneamente assegnato.

Il responsabile della UOR a cui è stato assegnato il documento, può indicare il soggetto interno alla propria struttura incaricato alla gestione diretta del documento e della sua istruttoria (c.d. operatore).

Nel caso in cui un documento sia inerente a più procedimenti o sia di interesse/competenza anche di altre UOR, queste sono contestualmente aggiunte in copia conoscenza al momento della registrazione del documento e/o successivamente dal responsabile della UOR competente, previa opportuna valutazione.

Tutti i passaggi di competenza anche temporanea del documento, vengono tracciati e memorizzati dal sistema, che li rende visibili in una apposita sezione (storia del documento).

Nel caso in cui il documento, per il suo contenuto, debba essere trattato come documento riservato, questo viene assegnato al responsabile della UOR tramite un'apposita funzionalità dell'applicativo, che limita la visibilità del documento alle sole persone specificamente indicate all'atto dell'assegnazione. Per tutti gli altri utenti appartenenti alla UOR indicata come assegnataria, il documento risulterà non disponibile.

Per agevolare la presa in carico del documento, ogni assegnazione effettuata all'interno del sistema di gestione documentale (RPA, cc, operatore, richiesta di sigla/firma digitale), viene notificata anche tramite una e-mail.

3.6 Tipologie di registrazione dei documenti informatici nel sistema di gestione

3.6.1 Documenti in entrata

I documenti in entrata sono tutti i documenti acquisiti dall'Amministrazione nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato.

La protocollazione ed assegnazione della corrispondenza in arrivo è centralizzata presso l'ufficio Segreteria Direzione Generale e Gestione documentale. È prevista una gestione decentrata dei documenti in arrivo per singole UOR appositamente individuate (Centri di Ateneo, Area Sanità, Uffici amministrativi delle Strutture Didattico Scientifiche).

3.6.2 Documenti in uscita

I documenti in uscita sono tutti i documenti prodotti dall'Ente nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato.

La protocollazione e trasmissione della corrispondenza in uscita è decentrata presso le singole UOR.

3.6.3 Documenti interni

I documenti interni o tra uffici sono tutti i documenti scambiati tra le diverse UOR dell'Ateneo.

Essi possono essere o meno oggetto di registrazione di protocollo tramite la funzione del protocollo "tra uffici" e sono da considerarsi documenti endo-procedimentali.

Essi sono prodotti in pdf/a e di norma non necessitano di firma digitale, salvo i casi specifici previsti dalla normativa vigente.

Sono soggetti a registrazione di protocollo quei documenti interni redatti per documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative che assumono carattere giuridico-probatorio, o se riguardano documenti dal quale possano nascere diritti, doveri o legittime aspettative di terzi.

L'identificazione del mittente, all'interno del sistema di gestione informatica, è assicurata dai metadati di sistema.

Non devono essere registrate a protocollo le e-mail informali tra uffici, intese come scambio di informazioni, con o senza documenti allegati, o contenenti dati o informazioni prodromiche alla formazione di un provvedimento amministrativo. Sono altresì esclusi dalla registrazione a protocollo gli atti preparatori (es: bozze di atti, proposte non ufficiali, ecc. trasmesse tramite posta elettronica interna).

3.6.4 Documenti non protocollati

Il sistema di gestione documentale consente di registrare anche documenti non protocollati, che non hanno quindi associato un numero univoco di protocollo. Essi costituiscono una parte residuale del processo documentario e sono costituiti da documenti che si ritiene utile archiviare nel relativo fascicolo informatico ai fini amministrativi correnti. Tale documentazione potrà poi essere selezionata o scartata in base alla valutazione del responsabile del procedimento amministrativo.

3.7 Trasmissione di documenti informatici

Il documento informatico deve essere redatto secondo le modalità descritte nel capitolo 2 e sottoscritto digitalmente, se necessario. Per la produzione dei documenti sottoscritti digitalmente, sono previsti appositi flussi approvativi (workflow di firma digitale) implementati all'interno del sistema di gestione documentale, finalizzati a tracciare il flusso del documento dalla sua formazione fino al momento dell'apposizione della firma digitale e della protocollazione (cfr. par. 2.8).

In conformità a quanto previsto dall'art. 47 del CAD, le modalità di trasmissione del documento informatico sono le seguenti:

- posta elettronica certificata;
- cooperazione applicativa;
- posta elettronica (e-mail istituzionale).

È in ogni caso esclusa la trasmissione di documenti a mezzo fax.

La trasmissione di documenti in modalità analogica è residuale e riservata a casi straordinari (es: domicilio digitale non rilevabile) o previsti da specifiche disposizioni.

3.7.1 PEC – Posta Elettronica Certificata

La PEC (posta elettronica certificata) è il canale informatico privilegiato per la gestione della corrispondenza in entrata e in uscita dell'Ateneo.

L'Università Politecnica delle Marche ha eletto un indirizzo PEC associato all'unica AOO, quale domicilio digitale attraverso cui ricevere e spedire i documenti e le comunicazioni da e verso le PA, le persone giuridiche e le persone fisiche. Sono inoltre istituiti ulteriori indirizzi PEC associati a specifiche UOR (Strutture didattico scientifiche e Centri di Ateneo).

Gli indirizzi PEC sono consultabili sul sito web dell'Ateneo alla sezione Amministrazione Trasparente https://www.univpm.it/Entra/PEC_Posta_Elettronica_Certificata e sull'indice IPA. Tra gli indirizzi PEC è compresa anche la casella dedicata alla gestione della fatturazione elettronica. L'aggiornamento degli indirizzi di posta elettronica certificata, nonché la gestione e manutenzione tecnica delle caselle sono di competenza del Servizio ICT.

Le caselle PEC sono integrate nel sistema di gestione documentale di Ateneo. L'indirizzo PEC associato all'unica AOO è accessibile e gestito dalla UOR del Responsabile della gestione documentale. Le ulteriori caselle PEC istituite per le Strutture didattico scientifiche e i Centri di Ateneo, sono gestite dalle UOR alle quali sono state associate.

I messaggi PEC ricevuti dall'Ateneo e presenti nella casella di posta elettronica certificata sono intercettati e trasferiti periodicamente nel sistema di gestione documentale che li identifica, attraverso un'attribuzione automatica dei relativi metadati gestionali, come "bozze in arrivo" di competenza della specifica UOR a cui la PEC è associata.

L'UOR preposta alla gestione della PEC associata all'AOO unica di Ateneo, registra le bozze come documenti protocollati in entrata, di norma entro la giornata lavorativa successiva alla loro ricezione, attribuendo il codice di classificazione in base al titolario, normalizzandone l'oggetto se necessario e assegnandole all'ufficio competente per la lavorazione della pratica amministrativa conseguente.

Le UOR preposte alla gestione delle PEC associate alle singole strutture didattico scientifiche, registrano le bozze come documenti protocollati in entrata di propria competenza, di norma entro la giornata lavorativa successiva alla loro ricezione, attribuendo il codice di classificazione in base al titolario e normalizzandone l'oggetto, se necessario. Se la PEC ricevuta non è di competenza della struttura didattico scientifica, la "bozza in arrivo" va assegnata all'UOR Responsabile della gestione documentale, che la protocollerà individuando l'ufficio competente per la lavorazione della pratica amministrava conseguente.

Nel caso in cui l'Ateneo riceva per errore una PEC non di competenza, sarà cura della UOR ricevente annullare la PEC in entrata con apposita funzionalità applicativa, specificando il motivo dell'annullamento. Contestualmente, sarà inviata al mittente una comunicazione di mancata presa in carico della PEC per errato destinatario, tramite notifica automatica dell'annullamento da parte del sistema o tramite invio di PEC predisposta dalla UOR.

La trasmissione dei documenti in uscita tramite PEC è effettuata a cura delle singole UOR responsabili del procedimento amministrativo di riferimento, che hanno l'onere di verificare anche la corretta trasmissione e consegna della PEC tramite le relative ricevute associate al sistema di gestione documentale.

Le ricevute, una volta recepite nel sistema, sono automaticamente inserite nella registrazione del documento inviato e il sistema valorizza i metadati che descrivono lo stato dell'invio (inviato – accettato – consegnato – rifiutato ecc.). Le ricevute (in formato .xml e/o .eml) sono visibili, verificabili e scaricabili dagli utenti.

Il documento informatico ricevuto/spedito tramite 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.

Il documento ricevuto/spedito con PEC ha lo stesso valore legale della raccomandata con avviso di ricevimento.

3.7.2 Cooperazione Applicativa

Per la ricezione e trasmissione di documentazione di particolari e specifici procedimenti, l'Ateneo si avvale dello strumento della cooperazione applicativa mediante piattaforme on line integrate con il sistema di gestione documentale (es: istanze, concorsi per il reclutamento del personale, gare di appalto, procedure d'acquisto su MEPA).

3.7.3 Posta Elettronica Ordinaria istituzionale (e-mail)

L'Ateneo è dotato di indirizzi di posta elettronica istituzionale (e-mail) sia personali sia riferiti alle singole UOR.

I documenti in entrata pervenuti tramite posta elettronica ordinaria (e-mail) sono soggetti alla registrazione di protocollo solo se il contenuto è rilevante al fine giuridico-probatorio. In questo caso, l'e-mail viene inoltrata dalla UOR competente all'indirizzo di Ateneo dedicato per procedere alla loro protocollazione in ingresso (es: ricezione di comunicazione/istanza costituita dal mero corpo della e-mail).

L'invio di documenti protocollati in uscita tramite e-mail istituzionale è residuale ed è consentito per raggiungere destinatari sprovvisti di indirizzo PEC (es: nei rapporti internazionali), previa registrazione del documento nel sistema di gestione documentale e fermo restando la comunicazione al destinatario, in maniera diretta o mediata, della segnatura di protocollo (trasmissione del file .xml comprensivo di stampigliatura o comunicazione della segnatura nel corpo dell'e-mail).

Lo scambio in entrata ed in uscita di e-mail personali o di struttura inerenti comunicazioni, informazioni, documenti informatici non ancora perfezionati, informali o prodromici non è soggetto a protocollazione. Il responsabile della UOR può valutare l'opportunità di inserire autonomamente tali e-mail nel sistema di gestione documentale come "documenti non protocollati" (si vedano i par. 3.6.3 e 3.6.4).

3.8 Formazione e gestione delle aggregazioni documentali

3.8.1 Fascicolo: definizione e funzione

Tutti i documenti prodotti e ricevuti dall'Ateneo, analogici o digitali, protocollati o non soggetti a protocollazione, devono necessariamente confluire nei fascicoli di competenza (cfr. art. 64 comma 4 del TUDA).

Il fascicolo è l'unità di base dell'archivio e comprende i documenti riconducibili ad un unico affare di natura giudiziaria, amministrativa, economico patrimoniale ecc. Di norma esso viene predisposto dall'ufficio competente che ne cura la tenuta in tutte le sue fasi di vita, dalla gestione dell'attività corrente sino alla conservazione, salvo diverse istruzioni.

I documenti che formano il fascicolo vengono classificati in maniera omogenea secondo il grado attribuito dal titolario di classificazione.

Il fascicolo può essere articolato in livelli interni di raggruppamenti omogenei di documenti (c.d. sotto fascicoli), che facilitano la consultazione e la gestione dell'intera pratica amministrativa e possono agevolare le operazioni di sfoltimento degli atti a conclusione della stessa.

Il fascicolo deve essere chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare stesso. I fascicoli chiusi devono essere predisposti per la conservazione in ragione degli originali che li compongono.

Il fascicolo contribuisce sia alla corretta sedimentazione dell'archivio sia all'esercizio del diritto di accesso alla documentazione amministrativa.

3.8.2 Fascicolo informatico e tipologie in uso

Come disposto dagli artt. 41 commi 2, 2-bis e 2-quater del CAD e dalle Linee Guida AgID, l'Università Politecnica delle Marche raccoglie in fascicoli informatici gli atti, i documenti e i dati relativi ai procedimenti da chiunque formati, secondo i principi della gestione documentale e la disciplina della formazione, gestione, conservazione e trasmissione del documento informatico.

Il fascicolo informatico è formato in modo da garantire la corretta collocazione, la facile reperibilità e il collegamento dei singoli documenti in esso inseriti, in relazione al contenuto ed alle finalità.

Condividendo quanto definito dal gruppo di lavoro degli Atenei italiani, l'Università Politecnica delle Marche adotta principalmente cinque note tipologie di fascicolo:

Fascicolo di Affare: contiene documenti relativi a una competenza non legata ad una procedura definita né ad un procedimento amministrativo. I documenti in esso contenuti dunque non sono riferibili ad affari con tempistiche definite a priori o iter procedimentali fissi. L'affare si articola e conclude secondo la sua particolare natura, senza una definizione normativa e senza l'adozione di un provvedimento amministrativo conclusivo (es: fascicolo di istituzione di gruppi di lavoro, fascicolo di corso di formazione per il personale, o in generale fascicoli che non si aprono con istanza di parte, o conservano documenti con una pluralità di argomenti e non si caratterizzano per il "botta e risposta").

Fascicolo di Attività: contiene documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di avanzamento della procedura anche se non è comunque prevista l'adozione di un provvedimento finale. Si tratta di un fascicolo che contiene documenti riferibili ad una stessa procedura, aggregati per arco temporale o per soggetto richiedente (es: istanza di parte) e riuniti ad altri documenti che rappresentano la stessa azione amministrativa (es: fascicolo di memorie e pareri legali, fascicolo di conferme titolo di studio, richieste di patrocini o logo di ateneo, e in generale fascicoli che si aprono con istanze di parte e si caratterizzano per il "botta e risposta").

Fascicolo di Procedimento amministrativo: contiene una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento finale (es: fascicolo relativo a una procedura concorsuale o ad un affidamento di beni e servizi).

Fascicolo di Persona fisica: contiene 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 della persona con l'ente (es: fascicoli del personale dipendente, fascicoli delle carriere degli studenti).

Fascicoli di Persona giuridica: contiene i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica (es: fascicoli delle aziende controllate o partecipate, consorzi, fondazioni, spin off ecc).

I fascicoli informatici sono creati in coerenza con il piano di fascicolazione di Ateneo che si basa sulla definizione delle competenze attribuite alle singole UOR e identificate con il Titolario di classificazione adottato. La composizione del fascicolo deve seguire i criteri di trasparenza, coerenza e buon andamento dell'azione amministrativa.

Il fascicolo è creato, implementato, gestito e mantenuto dal responsabile dell'ufficio e dai suoi collaboratori in base alle abilitazioni assegnate all'interno del sistema di gestione documentale.

È buona prassi creare delle articolazioni del fascicolo principale (sotto fascicoli) nei casi in cui il fascicolo risulti molto corposo, a causa della natura complessa della competenza a cui si riferisce (es.: gestione della carriera di una persona fisica), oppure quando si riscontri la necessità di raggruppare i documenti in sezioni coerenti più piccole. Un'eccessiva frammentazione del fascicolo

dovuta alla proliferazione non coerente dei sotto fascicoli è sconsigliata, come pure vanno evitati fascicoli privi di arco temporale.

Il fascicolo deve essere chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare stesso.

Per ragioni di reperibilità dei documenti, laddove la pratica sia formata da originali analogici ed originali informatici, l'Ateneo dispone la creazione del "fascicolo ibrido", da gestirsi esclusivamente nella fase corrente. Ai fini conservativi, i documenti analogici avranno una gestione dedicata nella sezione fisica e separata dell'archivio cartaceo.

Nel caso di fascicolo ibrido, nel sistema informatico di gestione documentale è presente il fascicolo completo, che contiene gli originali dei documenti informatici e le copie, per scansione, dei documenti originali analogici.

3.9 Definizione dei tempi di conservazione

Il patrimonio documentario delle pubbliche amministrazioni è un bene culturale fin dall'origine, soggetto al regime del demanio pubblico ed è inalienabile. Gli archivi devono essere pertanto tutelati, ordinati e valorizzati (art. 10, comma 2b del D.Lgs. 22 gennaio 2004 n. 42, Codice dei beni culturali e del paesaggio).

Lo scopo della conservazione dei documenti è quello di tutelare i diritti dell'Ateneo, del personale, degli studenti e dei cittadini titolari di interessi legittimi, nonché di conservarne la memoria storica.

3.9.1 Piano di conservazione o Massimario di selezione e scarto

L'art. 68 del TUDA prevede che ogni amministrazione pubblica debba dotarsi di un "piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti".

Il Piano di conservazione (o Massimario di selezione e scarto) è quindi lo strumento che individua i tempi di conservazione della documentazione amministrativa per ciascuna tipologia di documento o serie archivistica, siano esse di tipo nativo digitale che analogico. A seconda della rilevanza storica o giuridico-amministrativa, la conservazione può essere permanente o limitata ad un periodo di tempo variabile, al termine del quale può essere attivata la procedura di scarto della documentazione amministrativa.

Il Piano di conservazione dell'Università Politecnica delle Marche è descritto nell'allegato G ed è integrato con il Piano di classificazione (Titolario) in uso presso l'Ateneo.

Il Piano di conservazione è redatto tenendo conto della normativa nazionale in tema di conservazione – D.Lgs. 42/2004 "Codice dei beni culturali e del paesaggio" – e nel rispetto dei principi del GDPR in tema di protezione dei dati personali.

3.9.2 Procedura di selezione e scarto

Lo scarto dei documenti d'archivio di un Ente è subordinato alla preventiva autorizzazione della Soprintendenza Archivistica (art. 21, comma 1d D. Lgs. n. 42/2004).

La procedura di selezione e scarto dei documenti non soggetti a conservazione illimitata, che hanno esaurito la loro utilità giuridico-amministrativa e non hanno un rilevante interesse come fonte storica, può essere attivata trascorso il periodo minimo indicato nel Piano di conservazione (allegato G).

Le istruzioni relative alla procedura di selezione e scarto dei documenti amministrativi analogici sono descritte nel Piano di conservazione. Per i documenti informatici, la procedura specifica di scarto è in corso di definizione anche in accordo con i conservatori a cui l'Ateneo ha affidato il servizio di conservazione digitale.

3.10 Flussi di trasferimento in archivio di deposito e versamento in archivio storico dei documenti digitali

Una corretta gestione documentale fin dalla fase di formazione dei documenti rappresenta la migliore garanzia per la creazione di un sistema documentale pienamente rispondente ai principi archivistici, giuridici e amministrativi.

L'Università Politecnica delle Marche è un Ateneo relativamente giovane essendo stato istituito nel 1969 (nell'assetto di Libera Università di Ancona). Il nucleo documentale è costituito principalmente da atti e documenti analogici che, per scelta metodologica, trovano una trattazione residuale in questo Manuale.

Da un archivio prevalentemente analogico, l'Ateneo negli ultimi anni si è dotato progressivamente di un corpus di documenti informatici sempre più rilevante.

A partire dal 2017 il processo di digitalizzazione di Ateneo ha infatti avuto un forte impulso grazie all'implementazione del sistema informatico di gestione documentale "Titulus", dapprima utilizzato unicamente come registro informatico di protocollo. In particolare, con l'associazione delle caselle di posta elettronica certificata e posta elettronica semplice al sistema di gestione documentale, è possibile gestire i documenti informatici nativi digitali dematerializzando tutti i metadati.

Inoltre, l'introduzione nel 2020 dei flussi approvativi a supporto degli iter decisionali e delle firme digitali sui documenti amministrativi informatici ha permesso di accelerare il processo di digitalizzazione dell'archivio di Ateneo, di cui il presente Manuale costituisce regolamentazione primaria.

Al momento della redazione del presente Manuale, la produzione di documenti cartacei è residuale ed essi sono archiviati nel sistema di gestione documentale come copie informatiche di documenti analogici, associando ai metadati di registrazione la scansione del documento.

Il software "Titulus", grazie alle potenzialità infrastrutturali e applicative già insite nel programma, è oggi lo strumento principale per la gestione, archiviazione e conservazione dei documenti informatici, sostituendo di fatto l'archivio corrente e gran parte di quello di deposito, dal momento che gestisce la maggior parte delle funzioni archivistiche necessarie al transito dei documenti dal primo al secondo stadio della loro vita archivistica.

In particolare, si evidenziano alcune fasi che caratterizzano l'iter documentale nella fase corrente dell'archivio digitale.

- *Fase della registrazione nel sistema*

  Il documento informatico viene salvato come bozza nel sistema di gestione documentale recando con sé un set di metadati amministrativi per la compilazione della maschera di registrazione. Contestualmente alla registrazione, l'operatore si occupa di assegnare il documento alla UOR di competenza individuando il responsabile del documento (RPA), eventuali persone in copia conoscenza (CC) e se del caso ulteriori utenti con diritto specifico sul documento (operatore incaricato, conferenza di servizi, ecc ecc).

- *Fase della gestione amministrativa*

  Il documento in gestione all'ufficio competente viene valutato e se erroneamente assegnato, può essere rifiutato tornando automaticamente in assegnazione all'operatore che lo ha registrato, oppure può essere direttamente assegnato ad altro ufficio senza il tramite dell'operatore iniziale. In alcuni casi si può ricorrere in questa fase all'annullamento della registrazione nel sistema, come descritto nel capitolo 3.

  L'ufficio competente a cui il documento viene assegnato, prima di avviare l'istruttoria conseguente, deve verificare la validità dell'eventuale firma digitale e la corrispondenza del formato dei file, come descritto nel paragrafo 2.6.

- *Fase della fascicolazione*

  Una volta determinata l'assegnazione di responsabilità, il documento deve essere associato alla pratica a cui si riferisce, come previsto dalla normativa vigente. La creazione del fascicolo informatico e la sua relativa implementazione con l'inserimento dei documenti ad esso associati sono onere del responsabile dell'UOR; tali operazioni vanno condotte secondo le regole condivise in questo Manuale in base alla tipologia del fascicolo stesso (cfr. par. 3.8).

Al fine di accompagnare ulteriormente la progressiva transizione al digitale dell'Archivio, si ritiene utile mantenere logicamente unite le due entità del fascicolo ibrido in capo al responsabile dell'ufficio competente, definendo politiche di monitoraggio e presidio. La chiusura del fascicolo informatico in seguito all'esaurimento amministrativo della pratica non coincide quindi con il suo trasferimento all'archivio di deposito ed esso resta di competenza UOR fino a diversa disposizione.

Tale regola si è resa necessaria perché allo stato di redazione del presente Manuale i fascicoli ibridi impongono una fase di gestione mista, facilmente attuabile presso l'UOR responsabile. Si ritiene di mantenere tale regola fin quando le percentuali dei documenti digitali nativi saranno tali da sostituire almeno all'85% la natura ibrida della pratica mista.

Il documento digitale, per le sue caratteristiche impone anche di anticipare le politiche conservative: così come si contrae lo spazio tra la sezione corrente e quella di deposito, allo stesso modo va anticipata la fase di conservazione e dunque la sezione storica dell'archivio digitale. Il versamento dei documenti informatici alla sezione storica avviene tramite un servizio dedicato integrato nel sistema di gestione informatica dei documenti, che invia periodicamente e in maniera automatica al sistema di conservazione i documenti individuati come idonei per effetto di una configurazione di sistema predefinita. Le specifiche del sistema di conservazione adottato dall'Ateneo sono descritte nel capitolo 4.

Capitolo 4 - Conservazione del documento e delle serie archivistiche informatiche

La conservazione dei documenti digitali è un obbligo previsto dalla normativa di settore. In particolare, l'art. 44 del CAD e le Linee Guida AgID disciplinano il sistema di conservazione: esso è logicamente distinto dal sistema di gestione informatica dei documenti ed assicura, tramite l'adozione di regole, procedure e tecnologie, la conservazione degli oggetti digitali in esso contenuti, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità nel tempo.

Secondo quanto disposto dalle Linee Guida AgID, l'Ateneo si è dotato di un Manuale di conservazione, che descrive il processo di conservazione dei documenti digitali dell'Università Politecnica delle Marche illustrandone l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, le procedure, la descrizione dei processi, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento nel tempo del sistema di conservazione.

Il Manuale di conservazione è consultabile nella sezione Amministrazione Trasparente del portale di Ateneo, come previsto dalle Linee Guida AgID.

L'Università Politecnica delle Marche, in ragione della complessità dei mezzi tecnologici connessi alla conservazione digitale, ha affidato il servizio di conservazione tramite appositi accordi a conservatori esterni, come espressamente previsto dall'art. 34, comma 1-bis del CAD.

La scelta del conservatore esterno è stata operata in base a due principi cardine: da un lato la rispondenza del servizio offerto in merito ai requisiti di qualità, sicurezza e organizzazione individuati dall'AgID; dall'altro lato, il grado di integrabilità del Sistema di gestione documentale con il Sistema di conservazione per poter garantire la loro piena interoperabilità.

Le tipologie di documenti e le serie archivistiche di riferimento per le quali è prevista la conservazione digitale, i conservatori esterni a cui l'Ateneo ha affidato il Servizio di conservazione ed i relativi processi di conservazione sono descritti nel Manuale di Conservazione dell'Ateneo e nei relativi Manuali di conservazione dei conservatori esterni ad esso allegati.

In particolare, i Manuali di conservazione dei conservatori esterni descrivono le politiche conservative che il servizio di conservazione si impegna ad offrire all'Ateneo per effetto dei relativi accordi sottoscritti, nonché la descrizione delle infrastrutture che sottendono al servizio, le politiche e le procedure di sicurezza anche in caso di disastro, le figure di responsabilità e la descrizione del modello conservativo posto in essere.

Il Sistema di conservazione è realizzato nel rispetto del principio di integrità e riservatezza, nonché dei principi di protezione fin dalla progettazione e per impostazione predefinita, e dei conseguenti adempimenti previsti dal GDPR.

Capitolo 5 – Misure di sicurezza e protezione dei dati personali

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, definisce le misure di 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, anche in funzione delle tipologie di dati trattati (art. 32 del GDPR).

In conformità all'art. 28 del GDPR, i soggetti esterni a cui è eventualmente delegata la tenuta del sistema di gestione informatica dei documenti sono individuati come responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

5.1. Misure di sicurezza

5.1.1 Sistema informatico di gestione documentale

Il sistema informatico di gestione documentale 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 (art. 1, lett. r del TUDA). La gestione informatica dei flussi documentali è caratterizzata da un insieme di regole e funzionalità che consentono di trattare e di organizzare la documentazione prodotta e ricevuta dalle amministrazioni.

5.1.2 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'Università Politecnica delle Marche sono curati dal Servizio ICT.

Per l'ambito di competenza qui descritto, il Servizio ICT cura tutte le postazioni di lavoro (PDL) ed i pacchetti di programmi installati che permettono l'utilizzo del sistema informatico di Ateneo. È di sua specifica competenza, inoltre, l'infrastruttura di rete utilizzata per la connessione verso il Consorzio Cineca per mezzo della rete GARR compresa la tenuta e gestione del sistema di autenticazione (LDAP) per la gestione delle utenze di servizio.

La gestione informatica dei documenti viene coordinata attraverso l'applicativo software dedicato "Titulus". Il titolare dell'applicativo, gestito secondo il modello in house providing, è il Consorzio Interuniversitario Cineca.

Titulus è una soluzione di tipo Software as a Service (SaaS) le cui funzionalità sono rese disponibili attraverso un sito web, il cui accesso è subordinato a un processo di autenticazione informatica

effettuato mediante il sistema centralizzato dell'Ateneo che presuppone l'utilizzo di uno username ed una password memorizzata in modo crittografato nell'Active Directory di Ateneo.

La gestione operativa del sistema è curata direttamente dal Consorzio Cineca a cui, in virtù di un apposito contratto di servizio, 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.

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.

5.1.3 Sicurezza fisica dei data center

Il Data center Cineca ospita in hosting il software di gestione documentale "Titulus". La sicurezza fisica e logica è pertanto interamente demandata a Cineca. Il Data center Cineca è conforme allo standard ANSI/TIA 942-B-2017.
Tale standard riguarda tutti gli aspetti di un data center mission-critical, quali:

- l'infrastruttura delle telecomunicazioni;
- la struttura dell'edificio;
- l'infrastruttura elettrica e meccanica;
- la posizione del sito;
- i sistemi antincendio;
- la sicurezza fisica.

La certificazione assegna un rating che rappresenta il livello di affidabilità nell'erogazione dei servizi. Cineca ha ottenuto la certificazione a Rating 3: Concurrently Maintainable data center infrastruttura del sito mantenibile contemporaneamente, ossia un data center con componenti di capacità ridondanti e percorsi di distribuzione indipendenti multipli al servizio delle apparecchiature informatiche.

5.1.4 Rete dati di Ateneo

La rete di Ateneo è connessa direttamente alla rete Garr (Gruppo di armonizzazione delle reti della ricerca) tramite il nodo del PoP Garr presente a Montedago a cui l'Ateneo è connesso alla velocità di 2Gb/s. Le altre Facoltà di Medicina ed Economia sono connesse tramite l'aggiudicatario del Sistema Pubblico di Connettività a 200Mb/s. Tutte le restanti sedi periferiche sul territorio regionale sono connesse tramite l'aggiudicatario del Sistema Pubblico di Connettività a velocità comprese tra gli 8Mb/s e i 100Mb/s. La sicurezza perimetrale è assicurata da una coppia di firewall Fortinet.

5.1.5 Sistema di autenticazione

L'Ateneo si è dotato di un repository di utenti centralizzato in grado di garantire un sistema a "credenziali uniche" per tutte le applicazioni di Ateneo.

L'infrastruttura è basata su standard diffusi e comprende:

- Repository LDAP/MS Active Directory distribuito geograficamente;

- DBMS Oracle;
- Tecnologie di virtualizzazione per la realizzazione di tutti i server;
- Software per l'implementazione di cluster simmetrici per l'alta affidabilità/disponibilità;
- WebServices in standard SOAP/REST;
- Shibboleth-IDP per l'adesione alla federazione GARR-IDEM.

5.1.6 Politiche di autenticazione, controllo degli accessi e tracciamento nel sistema di gestione documentale

Le politiche di autenticazione, controllo degli accessi e tracciamento degli eventi all'interno del sistema di gestione documentale adottate dall'Ateneo garantiscono:

- 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.

5.1.7 Accesso al sistema di gestione documentale e profili di abilitazione

L'accesso al sistema di gestione documentale è soggetto ad autenticazione, previa opportuna profilazione dell'utente nell'apposita sezione di Access Control List.

Le identità digitali utilizzate per l'accesso al sistema di gestione documentale tramite autenticazione sono costituite da username e password. L'identificazione informatica dell'utente, cioè la validazione dell'identità digitale, è operata attraverso una infrastruttura e autenticazione centralizzata (IDP). Ogni utente è tenuto a preservare con cura e responsabilità la segretezza delle credenziali di accesso secondo le specifiche raccomandazioni fornite dall'Ateneo per il tramite del Servizio ICT.

L'abilitazione dell'utente al sistema di gestione documentale è effettuata dal Servizio ICT nell'apposita sezione di Access Control List (ACL), tramite associazione:

- alla UOR di appartenenza, sulla base dell'inquadramento contrattuale e dell'unità organizzativa di assegnazione;
- ad un eventuale specifico ruolo di Responsabilità, che rispecchia la posizione organizzativa ricoperta all'interno dell'Ateneo sulla base dell'organigramma;
- ad uno specifico profilo, che definisce le azioni possibili che l'utente può compiere sui documenti e sull'archivio digitale.

Le tipologie di profili presenti nell'ACL sono impostate dal Servizio ICT in accordo con il Responsabile della gestione documentale e prevedono differenziati livelli di autorizzazione, sia relativamente alle azioni di inserimento e modifica dei dati e dei documenti all'interno del sistema di gestione documentale, sia relativamente alla loro visibilità, compreso il diritto di visibilità dei documenti gestiti come riservati.

I profili, che possono quindi configurarsi di tipo standard o avanzato, sono attribuiti all'utente in ragione della UOR di appartenenza e delle mansioni svolte all'interno della stessa, nonché in ragione della posizione organizzativa e/o del ruolo ricoperti secondo l'organigramma di Ateneo.

Per esigenze organizzative possono essere associate specifiche profilazioni a singoli utenti appartenenti ad una UOR, su apposita e motivata richiesta del responsabile della stessa e in accordo con il Responsabile della gestione documentale.

La gestione degli accessi e della profilazione delle utenze, nonché ogni relativo futuro aggiornamento e disattivazione è di competenza del Servizio ICT, di concerto con il Responsabile della gestione documentale.

Gli utenti abilitati nel sistema di gestione documentale, nella gestione dei dati e delle informazioni desumibili dai documenti trattati in virtù della propria attività all'interno della UOR di appartenenza, sono tenuti, come tutti i dipendenti dell'Ateneo nell'esercizio delle proprie funzioni, all'osservanza del segreto d'ufficio, degli obblighi previsti dalla normativa di riferimento e di quanto disciplinato dal Codice di comportamento.

5.1.8 Accesso ai dati ed ai documenti informatici

L'accesso ai dati e ai documenti inseriti nel sistema di gestione documentale è limitato dal profilo associato a ciascun utente e vincolato alla struttura di appartenenza (UOR); pertanto, gli utenti possono visualizzare esclusivamente i documenti che sono stati associati all'ufficio a cui lo stesso utente appartiene o di cui ha la visibilità.

Il sistema consente un tracciamento puntuale di tutte le azioni effettuate dall'utente.

Tutti i dati e documenti sono immodificabili una volta salvati nel sistema e comunque, qualora il profilo lo consenta, le eventuali modifiche e/o rettifiche alle registrazioni sono tracciate.

Le azioni disponibili che possono essere associate ai singoli profili (individuati come sopra descritto dal Servizio ICT in accordo con il Responsabile della gestione documentale) sono:

- visualizzazione e consultazione dei documenti;
- inserimento e modifica dei dati per effettuare una registrazione, limitatamente agli elementi modificabili dall'utente non amministratore di sistema e non obbligatori ed immodificabili;
- creazione e rimozione di fascicoli, inserimento dei documenti nei fascicoli;
- attivazione di workflow di firma;
- ricerca di informazioni registrate ai fini della visualizzazione o consultazione;
- operazioni di assegnazione dei documenti;
- download dei file associati alla registrazione;
- stampa dei metadati associati alle registrazioni.

Tutte le azioni devono intendersi limitate ai documenti assegnati alla struttura di appartenenza dell'utente o agli specifici diritti di visibilità degli stessi (ad esempio su singoli repertori o su documenti riservati).

Le azioni disponibili agli utenti a cui è associato il profilo di amministratore di sistema sono comprensive anche dell'annullamento delle registrazioni e dei workflow.

L'accesso ad utenti esterni è inibito; spetta agli utenti abilitati effettuare le operazioni di estrazione dei dati e documenti qualora sussistano le esigenze legate alle procedure di accesso generalizzato alla documentazione amministrativa ai sensi L. n. 241/1990.

5.2. Protezione dei dati personali

5.2.1 Sistema informatico di gestione documentale e Data protection

Il sistema informatico di gestione documentale, affinché possa essere efficace e sicuro, deve essere presidiato da specifiche procedure e strumenti informatici in grado di governare ogni singolo accadimento che coinvolge la vita del documento. Inoltre, vanno messi in atto tutti quei principi generali applicabili in materia di trattamento e protezione dei dati personali, in primis dei principi della "Privacy by Design" e "Privacy by Default".

La "Privacy by Design" (principio di «protezione dei dati personali fin dalla progettazione») è il principio che prevede che ogni titolare o responsabile del trattamento debba tenere in considerazione, sin dalla ideazione e progettazione delle attività di trattamento che intende realizzare, la protezione dei dati personali degli interessati cui il trattamento si riferisce, minimizzando i rischi e rispettando la tutela degli interessati.

La "Privacy by Default" (principio di «protezione dei dati personali per impostazione predefinita») è il principio che prevede che ogni titolare o responsabile effettui il trattamento dei soli dati personali degli interessati nella misura e per il tempo necessari a raggiungere le specifiche finalità del trattamento.

L'Università ha predisposto un organigramma di data protection, quale misura di accountability, con cui il Titolare del trattamento ha descritto dettagliatamente la propria organizzazione nell'ambito di cui trattasi e tra cui sono previsti: i designati (con un focus sulle designazioni in ambito di ricerca), gli autorizzati, il data manager, i referenti IT per la protezione dei dati personali ed il Referente protezione dei dati. Nello stesso documento, sono attribuiti ad ognuno dei soggetti individuati specifici compiti ed istruzioni che risultano essere trasversali rispetto alla struttura organizzativa a cui afferiscono.

L'organigramma di data protection e la normativa interna di Ateneo in materia di protezione dati è descritta nell'Allegato H.

In coerenza con il modello organizzativo adottato dall'Ateneo, al titolare del software di gestione documentale (Consorzio Cineca) è conferito il ruolo di responsabile esterno del trattamento.

Il sistema di gestione documentale rispetta quanto previsto dall'art. 32 del GDPR in materia di sicurezza del trattamento e da ogni altra disposizione in materia di protezione dei dati personali.

I dati sono resi disponibili e accessibili a chiunque ne abbia diritto nel rispetto delle disposizioni del GDPR e della normativa interna di Ateneo in materia di Data Protection.

Nelle relative sezioni del presente Manuale sono descritte specifiche misure adottate dall'Ateneo, in conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali, per

garantire la riservatezza delle informazioni contenute nei documenti informatici, nonché le specifiche misure di sicurezza in materia di autenticazione, profilazione e accesso.

5.2.2 Principio di minimizzazione dei dati e archivi

I dati personali sono raccolti e trattati solamente se è davvero necessario in relazione alle finalità per le quali vengono trattati e sono "conservati in una forma che consenta l'identificazione degli interessati" (ovvero le persone fisiche a cui si riferiscono) solamente per il tempo necessario a raggiungere la finalità per la quale sono stati raccolti (art. 5.1. lett. b e lett. e del GDPR). I dati personali "possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica", e purché si assumano specifiche misure "a tutela dei diritti e delle libertà dell'interessato" (art. 5.1 lett. e GDPR).

Fermo restando il principio di esaustività ed accuratezza dei dati inseriti nel sistema quali futuri parametri di ricerca di documenti e fascicoli, è necessario contemperare tali principi con quello di minimizzazione, evitando quindi i riferimenti ai dati sensibili e/o personali al momento della registrazione del documento e in particolare nella redazione dell'oggetto dei documenti e nella denominazione dei fascicoli, che devono essere descritti in forma sintetica ed esaustiva ponendo particolare attenzione al trattamento dei dati personali.

Capitolo 6 – Disposizioni finali

6.1. Modalità di approvazione e pubblicazione

Il presente Manuale è adottato con Decreto del Direttore Generale ed è pubblicato nella sezione Amministrazione Trasparente del portale di Ateneo, come previsto dalle Linee Guida AgID.

6.2. Revisione del Manuale

Il presente Manuale è sottoposto a costante aggiornamento, in ragione dell'evoluzione normativa, dei cambiamenti tecnologici e dell'obsolescenza degli oggetti e degli strumenti digitali utilizzati.

Le modifiche apportate alla parte generale sono da considerarsi una revisione del Manuale stesso e sono adottate con Decreto del Direttore Generale.

La modifica o l'aggiornamento di uno o più allegati al Manuale non comporta la revisione del Manuale stesso. Gli allegati sono costantemente aggiornati a cura del Responsabile della gestione documentale e le modifiche sono rese evidenti nella cronologia delle versioni di ciascun allegato.

ALLEGATI

A. Cronologia delle versioni e delle revisioni del Manuale

B. Glossario

C. Normativa di riferimento

D. Figure di responsabilità

E. Elenco repertori

F. Titolario di Classificazione

G. Piano di conservazione (o Massimario di scarto)

H. Disposizioni in materia di Data Protection

I. Metadati dei documenti informatici