



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

MANUALE DI GESTIONE DOCUMENTALE DELL'UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

A cura del Servizio di Coordinamento della Gestione documentale

Versione: 1.0

Data ultima revisione: 24.06.2026

Stato: Definitivo



INDICE

INDICE	2
INDICE DELLE FIGURE.....	5
INDICE DELLE TABELLE.....	5
INTRODUZIONE	6
1. GENERALITÀ	7
1.1. Tabella delle versioni.....	7
1.2. Tabella degli allegati.....	7
1.3. Tabelle degli acronimi e delle definizioni	7
2. MANUALE DI GESTIONE DOCUMENTALE	13
2.1. Introduzione.....	13
2.2. Scopo e ambito di applicazione del Manuale	15
2.3. Redazione, adozione, aggiornamento e pubblicità del Manuale	16
2.4. Normativa di riferimento	17
3. MODELLO ORGANIZZATIVO DEL SISTEMA DI GESTIONE DOCUMENTALE	18
3.1. Il Sistema di Gestione Documentale.....	18
3.2. La struttura organizzativa dell'Università.....	18
3.3. Area Organizzativa Omogenea.....	19
3.4. Servizio per il coordinamento della gestione documentale	22
3.5. Ruoli e responsabilità	24
3.5.1. Il Responsabile della Gestione Documentale presso ciascuna UOR (RGD)	24
3.5.2. Il Responsabile della Transizione al Digitale (RTD).....	25
3.5.3. Il Responsabile della Protezione dei Dati (RPD)	25
3.5.4. Il Referente per l'Indice della Pubblica Amministrazione (IPA)	25
3.5.5. Responsabile della Conservazione (RC)	26
3.6. Il sito WEB per l'eGovernment.....	27
4. IL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI.....	29



4.1.	Caratteristiche generali di un Sistema di gestione informatica dei documenti e dei flussi documentali.....	29
4.2.	Il sistema di gestione informatica dei documenti dell'Ateneo.....	30
4.3.	Il modello organizzativo del sistema di gestione documentale UniNA	31
5.	FORMAZIONE DEI DOCUMENTI	34
5.1.	Modalità di formazione e contenuti minimi dei documenti amministrativi.....	34
5.2.	Copie di documento amministrativo informatico o analogico	35
5.3.	Conservazione degli originali analogici da cui sono tratte le copie informatiche.....	37
5.4.	Copie analogiche di documenti informatici: il contrassegno elettronico	38
5.5.	Formato dei documenti.....	39
5.6.	Sottoscrizione dei documenti	39
5.7.	Verifica delle firme	40
6.	PROTOCOLLO INFORMATICO	42
6.1.	Unicità del protocollo informatico.....	42
6.2.	Registro informatico di protocollo	43
6.3.	Registrazione di protocollo	43
6.4.	Segnatura di protocollo	45
6.5.	Registrazione e segnatura XML dei documenti informatici.....	45
6.6.	Registrazione e segnatura dei documenti analogici.....	47
6.7.	Documenti esclusi dalla registrazione di protocollo.....	47
6.8.	Registrazioni nel registro di protocollo particolare	49
6.9.	Altre tipologie di registri gestiti nel Protocollo Informatico	50
6.9.1.	Registro giornaliero di protocollo e dei repertori gestiti dal Protocollo	51
6.9.2.	Registro di emergenza	51
6.10.	Annullamento parziale o totale di protocollo	53
6.11.	Differimento delle registrazioni	54
7.	ALTRE ATTIVITÀ DI GESTIONE DOCUMENTALE	56
7.1.	Classificazione.....	56



7.2.	Titolario di classificazione	57
7.3.	Fascicolazione	58
7.3.1.	Aggregazioni documentali informatiche.....	59
7.3.2.	Il Fascicolo informatico	59
7.3.3.	Piano di fascicolazione	63
7.3.4.	Altre aggregazioni documentali informatiche.....	63
7.3.5.	Modalità operative per la fascicolazione dei documenti	64
8.	MODELLO ORGANIZZATIVO PER LA GESTIONE DEI FLUSSI DOCUMENTALI .	67
8.1.	Mezzi di spedizione.....	67
8.2.	Flussi documentali in entrata	68
8.2.1.	Descrizione generale	68
8.2.2.	Ricezione di documenti informatici su supporti rimovibili	71
8.2.3.	Ricezione di documenti sulla casella istituzionale	72
8.2.4.	Modifica delle assegnazioni	72
8.2.5.	Errata ricezione di documenti	73
8.2.6.	Rilascio di ricevute attestanti la ricezione di documenti	74
8.3.	Flussi documentali in uscita	75
8.4.	Flussi documentali interni	77
9.	CONSERVAZIONE.....	80
9.1.	Archivio dell'Ateneo	80
9.1.1.	Archivio corrente	81
9.1.2.	Archivio di deposito	82
9.1.3.	Archivio storico	84
9.2.	Piano di conservazione	86
10.	MISURE DI SICUREZZA	87
10.1.	Finalità e contesto normativo.....	87
10.2.	Protezione dei dati personali e gestione degli incidenti	87
10.3.	Piano della sicurezza del sistema di gestione informatica dei documenti.....	88
10.3.1.	Criteri di identificazione e autenticazione per l'accesso al sistema	90
10.3.2.	Policy di visibilità dei dati e dei documenti e di abilitazione alle funzionalità	90
10.3.3.	Accesso alla documentazione riservata e contenente dati particolari	91
10.3.4.	Funzioni di logging e monitoraggio.....	92
10.3.5.	Continuità operativa, backup e disaster recovery.....	92
10.3.6.	Sistemi che evidenziano eventi anomali	93
10.3.7.	Rilevazione e ripristino affidabilità software.....	93
10.3.8.	Manutenzione del software applicativo	94
10.3.9.	Qualità dei dati.....	94
10.3.10.	Controllo interscambio dati	95



INDICE DELLE FIGURE

Figura 1 – I componenti architeturali del Sistema di Gestione Documentale (SGD)	18
Figura 2 – La struttura organizzativa UNINA	19
Figura 3 – Il sito per l’eGovernment UniNA	28
Figura 4 – Il modello per la gestione documentale UniNA.....	32
Figura 5 – Il processo di versamento in conservazione.....	85

INDICE DELLE TABELLE

Tabella 1 - Tabella delle versioni.....	7
Tabella 2 - Tabella degli allegati	7
Tabella 3 - Tabella degli acronimi.....	9



INTRODUZIONE

Il presente Manuale di gestione documentale dell'Università degli Studi di Napoli Federico II, redatto nella sua prima edizione "integrale" nel corso del 2013 con il titolo "Manuale di gestione del protocollo informatico, dei documenti e dell'archivio dell'Università degli Studi di Napoli Federico II", tiene conto dell'insieme dei decreti, degli atti, delle comunicazioni, dei documenti tecnici ed amministrativi, dei manuali e delle guide operative che negli anni hanno costituito l'insieme delle politiche e delle prassi operative adottate dall'Ateneo in materia di gestione e di tenuta dei flussi documentali informatici. Tale patrimonio informativo, pubblicato e reso disponibile all'indirizzo www.praxis.unina.it, è stato quindi unificato, integrato ed aggiornato, anche in funzione dei recenti e strutturali cambiamenti organizzativi dell'Ateneo, oltre che dell'attuale quadro normativo di riferimento.

L'obiettivo è l'emanazione e la messa a disposizione di tutto il personale e dei cittadini, nel formato standard proposto dall'Agenzia per l'Italia Digitale, di un documento di riferimento che illustri - in modo integrato e coerente - le scelte tecnico-organizzative operate negli anni dall'Università per la gestione ed il trattamento dei flussi dei documenti amministrativi informatici, con particolare riguardo al loro processo di formazione, classificazione, fascicolazione, registrazione di protocollo, assegnazione, gestione dell'iter, trasmissione e archiviazione informatica. Il documento non ha pretesa di completezza. Al contrario, rappresenta una prima base di sistematizzazione della materia e si raccorderà e completerà con gli altri documenti programmatici che saranno redatti nei mesi a seguire dai rispettivi responsabili: dai Manuali di conservazione dei documenti informatici e dei documenti analogici, al Massimario di scarto dei documenti amministrativi, al Catalogo dei procedimenti amministrativi.

Pertanto, negli anni a venire, il presente Manuale sarà sottoposto a un processo di revisione, arricchimento ed aggiornamento continuo, in modo tale da risultare sempre più adeguato a descrivere un sistema, quello documentale, in continuo cambiamento sia per gli aspetti organizzativi che normativi che tecnologici.

1. GENERALITÀ

1.1. Tabella delle versioni

Versione	Cambiamenti rispetto alla versione precedente	Autore	Data redazione
1.0-draft	Rilascio della versione bozza per revisione	Clelia Baldo	03.06.2026
1.0	Rilascio versione definitiva	Clelia Baldo	24.06.2026

Tabella 1 - Tabella delle versioni

1.2. Tabella degli allegati

Allegato	Descrizione
Allegato 1	Riferimenti normativi
Allegato 2	UOR, UO afferenti e domicili digitali
Allegato 3	Modello dei processi di gestione documentale
Allegato 4	Atto di nomina del Responsabile del Servizio di coordinamento della gestione documentale
Allegato 5	Titolario di classificazione
Allegato 6	Il processo di autorizzazione, elenco dei ruoli e dei permessi applicativi
Allegato 7	Caratteristiche generali del sistema di gestione informatica dei documenti UniNA
Allegato 8	Organizzazione logica dell'archivio digitale ed elenco dei repertori attivi

Tabella 2 - Tabella degli allegati

1.3. Tabelle degli acronimi e delle definizioni

Nella seguente tabella vengono riportati, in ordine alfabetico, gli acronimi ricorrenti all'interno del Manuale:



Sigla	Descrizione
ACN	Agenzia per la Cybersicurezza Nazionale
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale (D.lgs. n. 82/2005 e ss.mm.ii.)
CSI	Centro Servizi Informativi di Ateneo
CSIRT	Computer Security Incident Response Team
CU	Capo Ufficio
DG	Decreto del Direttore Generale
D.lgs.	Decreto legislativo
DPR	Decreto del Presidente della Repubblica
DPCM	Decreto del Presidente del Consiglio dei Ministri
eIDAS	Regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio del 23.07.2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
eIDAS2	Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio dell'11.04.2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale
FE	Firma Elettronica
FEA	Firma Elettronica Avanzata
FEQ	Firma Elettronica Qualificata
GDPR	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
HSM	Hardware Security Module
IAM	Identity Access Management
IPA	Indice dei domicili digitali delle Pubbliche Amministrazioni e dei Gestori di pubblici servizi
LLGG AgID	Linee Guida in materia di formazione, gestione e conservazione dei documenti informatici" emanate dall'AgID con Determinazione n. 420/2020, aggiornate con Determinazione n. 371/ 2021
MdG	Manuale di Gestione documentale
NIS2	Direttiva UE 2022/2555, Network and Information Security. È la normativa europea sulla cybersicurezza che impone standard di sicurezza e obblighi di notifica più severi a enti pubblici e privati operanti in 18 settori critici. In Italia è in vigore tramite il D.Lgs. 138/2024, sotto la supervisione dell'Agenzia per la Cybersicurezza Nazionale (ACN)



Sigla	Descrizione
OCC	Organi Collegiali
PdV	Pacchetto di Versamento
PEC	Posta Elettronica Certificata
PEO	Posta Elettronica Ordinaria
DPCM-Protocollo	DPCM 3 dicembre 2013 recante le “Regole tecniche per il protocollo informatico”, parzialmente abrogato dalle LLGG AgID
RGD	Responsabile Gestione Documentale della UOR
RPA	Responsabile del Procedimento Amministrativo
RPD/DPO	Responsabile della Protezione dei Dati
RPV	Responsabile del Versamento in conservazione
RCGD	Responsabile Coordinamento Gestione Documentale
RSI	Responsabile del Servizio Informatico per la gestione del sistema di gestione documentale. Nel caso dell’Università, coincide con il Centro Servizi Informativi di Ateneo (C.S.I.)
RTD	Responsabile per la Transizione al Digitale
RUP	Responsabile Unico di Progetto
SCGD	Servizio Coordinamento Gestione Documentale
SGD	Sistema di Gestione Documentale
SD	Sistema Documentale che fa parte del Sistema di gestione informatica dei documenti e dei flussi. Nel caso dell’Università è l’applicazione eDocumento
SD-C	Modulo di SD dedicato alla Conservazione
SIEM	Security Information and Event Management
SPI	Sistema Protocollo Informatico – l’applicazione sviluppata o acquisita dall’Amministrazione per implementare il servizio di protocollo informatico. Nel caso dell’Università è l’applicazione eGrammata
DPR 445/2000 TUDA	Testo Unico in materia di Documentazione Amministrativa DPR 28 dicembre 2000 n. 445 e ss.mm.ii.
UniNA/ Ateneo/ Amministrazione	Università degli Studi di Napoli Federico II
UO	Unità Organizzativa
UOP	Unità Organizzativa di registrazione di Protocollo
UOR	Unità Organizzativa Responsabile

Tabella 3 - Tabella degli acronimi

Nella seguente tabella sono riportate, in ordine alfabetico, le definizioni di maggior rilievo che ricorrono nel presente Manuale, tenendo presente che, ai fini del presente Manuale, valgono le definizioni di cui all'articolo 3 del Regolamento eIDAS, all'art. 1 del CAD e all'Allegato 1 alle LLGG AgID:



Definizione	Descrizione
Pubblica Amministrazione	L'insieme degli enti di cui all'art. 1, comma 2 del d.lgs. 165/2001
AOO- Area Organizzativa Omogenea	Raggruppamenti organizzativi caratterizzati da un unico domicilio digitale, la cui gestione del Protocollo è demandata a particolari Unità Organizzative Responsabili (UOR), così come stabilito dall'articolo 50, comma 4, del DPR 28 dicembre 2000, n. 445
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività (LLGG AgID, All. 1)
Archivio corrente	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale
Archivio di deposito	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento del procedimento amministrativo o comunque verso i quali sussista un interesse sporadico
Archivio informatico	Archivio costituito da documenti informatici organizzati in aggregazioni documentali informatiche (LLGG AgID, All. 1)
Archivio storico	Costituito da complessi di documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto, alla conservazione perenne
Assegnazione	L'operazione d'individuazione dell'Unità Organizzativa (UO) competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore (LLGG AgID, All. 1)
Coordinatore della Gestione documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50, comma 4, del DPR 28 dicembre 2000, n. 445 nei casi di Amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del



Definizione	Descrizione
	contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa (LLGG AgID, All. 1)
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (LLGG AgID, All. 1)
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (LLGG AgID, All. 1)
Domicilio digitale	Un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento eIDAS
Evidenza informatica	Una sequenza finita di bit che può essere elaborata da una procedura informatica (LLGG AgID, All. 1)
Fascicolazione	L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o attività o procedimenti amministrativi
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica Amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del CAD - Codice dell'Amministrazione Digitale
Firma digitale	Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1, comma 1, lett. s) del D.lgs.7 marzo 2005, n. 82)
Funzione di hash crittografica	Funzione matematica che genera, a partire da un'evidenza informatica, una impronta crittografica o digest in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti (LLGG AgID, All. 1)



Definizione	Descrizione
Gestione documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti (LLGG AgID, All. 1)
Hash	Termine inglese usato, impropriamente, come sinonimo di “impronta crittografica” o “digest” (LLGG AgID, All. 1)
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica (LLGG AgID, All. 1)
Marca temporale	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (art. 1, comma 1, lett. i) del DPCM 22 febbraio 2013)
Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art 1, comma 1, lett. v) del D.lgs. 7 marzo 2005, n. 82)
Responsabile del procedimento amministrativo (RPA)	È la persona, alla quale è stata affidata la trattazione di un affare amministrativo ivi compresa la gestione/creazione del relativo fascicolo dell'archivio corrente
SIEM	
Sistema di gestione informatica dei documenti	L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'art. 52 del DPR 445/2000
Sistema di gestione documentale	È l'insieme coordinato di regole, processi, ruoli e strumenti finalizzati alla formazione, gestione, organizzazione e conservazione dei documenti informatici e delle aggregazioni documentali, garantendone autenticità, integrità, affidabilità, leggibilità e reperibilità nel tempo. È dunque un ecosistema complesso che riguarda: organizzazione, processi e strumenti. Dal punto di vista tecnologico, comprende i sistemi di gestione informatica dei documenti e dei flussi documentali, definiti negli articoli 52 e 65 del DPR 445/2000

Tabella 4- Tabella delle definizioni



2. MANUALE DI GESTIONE DOCUMENTALE

2.1. Introduzione

Le “Linee Guida AgID sulla formazione, gestione e conservazione dei Documenti informatici” (di seguito Linee Guida AgID oppure LLGG AgID), in combinato disposto con il DPCM del 3 dicembre 2013 avente come oggetto “Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005” (di seguito DPCM-Protocollo), dispongono l'obbligo di predisposizione e pubblicazione del “Manuale di Gestione documentale” (di seguito Manuale) da parte di ciascuna Pubblica Amministrazione di cui all'art. 2 del decreto legislativo 30 marzo 2001, n. 165 e delle proprie AOO – Aree Organizzative Omogenee.

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, archiviazione dei documenti e gestione dei flussi documentali, con particolare riguardo ai seguenti aspetti:

- a) Organizzativi,
- b) Formati dei documenti,
- c) Protocollo informatico e registrazioni particolari,
- d) Classificazione e selezione,
- e) Formazione delle aggregazioni documentali,
- f) Flussi di lavorazione dei documenti in uso,
- g) Organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche,
- h) Misure di sicurezza e protezione dei dati personali,
- i) Conservazione.

Più in particolare, ai sensi delle LLGG AgID (par. 3.5), il presente Manuale descrive:

relativamente agli aspetti organizzativi

- le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno e all'esterno delle AOO, applicando le modalità di trasmissione indicate nell'Allegato 6 alle LLGG AgID (Comunicazione tra AOO di Documenti Amministrativi Protocollati);
- l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo e di archiviazione dei documenti all'interno dell'Amministrazione e delle AOO;



- l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso altre amministrazioni;
- i criteri e le modalità per il rilascio delle abilitazioni di accesso al sistema di gestione informatica dei documenti;

relativamente ai formati dei documenti

- l'individuazione dei formati utilizzati per la formazione del documento informatico, conformemente a quelli indicati nell'Allegato 2 alle LLGG AgID (Formati di file e riversamento);
- le procedure per la valutazione periodica di interoperabilità dei formati previste ai sensi delle disposizioni dell'Allegato 2 alle LLGG AgID;

relativamente al protocollo informatico e alle registrazioni particolari

- le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;
- la descrizione completa e puntuale delle modalità di utilizzo della componente "sistema di protocollo informatico" del sistema di gestione informatica dei documenti;
- le modalità di utilizzo del Registro di emergenza ai sensi dell'art. 63 del DPR 445/2000, inclusa la funzione di recupero dei dati;
- l'elenco dei documenti esclusi dalla registrazione di protocollo, per cui è prevista una registrazione particolare ai sensi dell'art. 53, comma 5, del DPR 445/2000;
- i metadati associati ai documenti soggetti a registrazione particolare, assicurando le obbligatorioità previste dall'Allegato 5 alle LLGG AgID (Metadati);
- i registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche;

relativamente alle azioni di classificazione e selezione

- il Titolario di classificazione adottato dall'Amministrazione e integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione della documentazione;
- le modalità di aggiornamento del Titolario di classificazione;

relativamente alla formazione delle aggregazioni documentali

- le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni documentali informatiche, con l'insieme minimo dei metadati ad essi associati;
- il Piano di fascicolazione, che è stato integrato con il Titolario di classificazione e con il Piano di conservazione;



relativamente ai flussi di lavorazione dei documenti in uso

- la descrizione dei flussi di lavorazione dei documenti ricevuti, inviati o ad uso interno dell'Amministrazione;

relativamente all'organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche

- la definizione della struttura dell'archivio all'interno del sistema di gestione informatica dei documenti, formato ai sensi del DPR 445/2000, in modo da assicurare certezza e trasparenza all'attività giuridico-amministrativa;

relativamente alle misure di sicurezza e protezione dei dati personali adottate

- le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, anche in materia di protezione dei dati personali;

relativamente alla conservazione

- il Piano di conservazione, integrato con il Titolario di classificazione, contenente l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate;
- le procedure di selezione periodica, di scarto e di invio in conservazione.

2.2. Scopo e ambito di applicazione del Manuale

Scopo del presente Manuale è descrivere il ciclo di vita dei documenti informatici all'interno della AOO dell'Amministrazione, partendo dalla loro formazione e/o acquisizione, passando per la gestione all'interno del sistema documentale e fino alla loro conservazione e/o scarto.

Esso **sostituisce** il Manuale di Gestione del protocollo Informatico, dei documenti e dell'archivio dell'Università degli Studi di Napoli Federico II, aggiornandolo ed ampliandone il contesto dal Protocollo Informatico a quello più completo della gestione documentale e dei flussi.

Il presente Manuale descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'**Università degli Studi di Napoli Federico II** che, a partire dal **1° gennaio 2007**, ha costituito la propria Area Organizzativa Omogenea e avviato il sistema di Protocollo Generale di Ateneo e, a partire dal **2 gennaio 2014**, il sistema eDocumento, per una completa gestione informatica dei documenti e dei flussi documentali.



Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi e con i sistemi istituzionali più rilevanti dell'Ateneo, tale sistema realizza infatti le condizioni operative per una più efficiente gestione dell'archivio digitale dell'Ateneo e del flusso informativo e documentale interno dell'amministrazione, anche ai fini dello snellimento delle procedure, della trasparenza dell'azione amministrativa, della corretta organizzazione e tenuta di dati e documenti, per un loro più rapido reperimento e preservazione nel tempo.

Il presente documento, pertanto, si rivolge non solo agli operatori del sistema documentale di Ateneo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

2.3. Redazione, adozione, aggiornamento e pubblicità del Manuale

L'Amministrazione adotta con decreto del Direttore Generale il presente "Manuale di gestione documentale dell'Università degli Studi di Napoli Federico II", redatto dal Responsabile del Servizio di Coordinamento della gestione documentale (RCGD), d'intesa con il Responsabile della transizione digitale (RTD) e il Responsabile della Conservazione, acquisito il parere del Responsabile della protezione dei dati personali (RPD).

Il presente Manuale è redatto sulla base dei modelli di riferimento predisposti dal MUR (Ministero dell'Università e della Ricerca) e dal MIM (Ministero dell'Istruzione e del Merito) e, a norma dell'art. 22 della legge 7 agosto 1990, n. 241, è reso disponibile alla consultazione del pubblico e di tutto il personale dell'Amministrazione che ne può prendere visione in qualsiasi momento. A tal fine, viene pubblicato sul sito istituzionale nella sezione "Amministrazione trasparente" del sito istituzionale dell'Ateneo:

<https://www.unina.it/it/ateneo/amministrazione-trasparente>

Il presente manuale potrà essere aggiornato a seguito di:

- modifiche normative o regolamentari sopravvenute;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- sostanziali modifiche apportate nell'ambito dell'architettura di servizio.

Non ha invece impatto sulla riedizione del presente Manuale il successivo aggiornamento e pubblicazione sul sito istituzionale dell'Ateneo, a cura del RCGD, degli allegati contenenti informazioni di carattere "dinamico" (quali, ad esempio, il Titolario, l'Organigramma, l'elenco dei Repertori, etc.) e, quindi, soggetti a modifiche. Analogamente, non determinano l'aggiornamento del presente Manuale gli adeguamenti tecnologici e informatici che non modificano le politiche generali di gestione e di sicurezza del sistema.



La tenuta del presente manuale è affidata al RCGD che sottoporrà le nuove versioni del Manuale all'approvazione ed autorizzazione da parte del Direttore Generale, previo parere favorevole di RTD, RC e RPD.

2.4. Normativa di riferimento

I riferimenti normativi presi in considerazione per la stesura del presente Manuale sono riportati in **Allegato 1**.

3. MODELLO ORGANIZZATIVO DEL SISTEMA DI GESTIONE DOCUMENTALE

3.1. Il Sistema di Gestione Documentale

Di seguito lo schema che rappresenta i componenti architetturali in cui si articola il Sistema di Gestione Documentale (SGD) dell'Università:

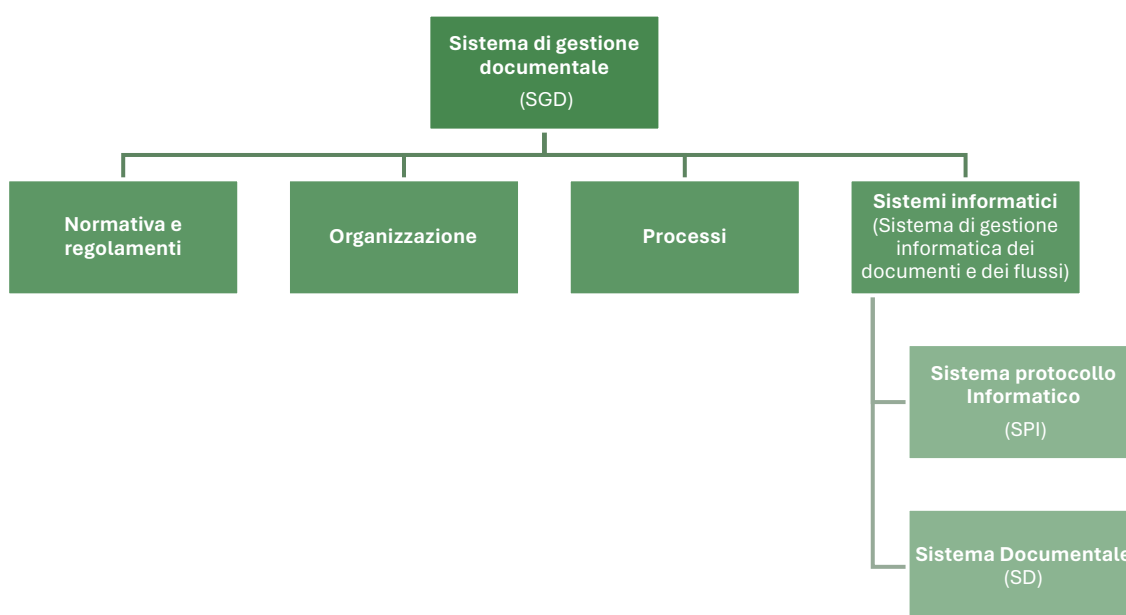


Figura 1 – I componenti architetturali del Sistema di Gestione Documentale (SGD)

3.2. La struttura organizzativa dell'Università

L'Università degli Studi di Napoli Federico II, ai sensi del proprio Statuto, è articolata in Scuole, Dipartimenti, Centri di Ateneo, Centri di Eccellenza, Centri Interdipartimentali di Ricerca e di Servizio, Centri Interuniversitari di Ricerca, Scuole di Specializzazione, Centri Museali, Biblioteche, Aree dell'Amministrazione Centrale e Uffici amministrativi; il tutto in più sedi dislocate sul territorio.

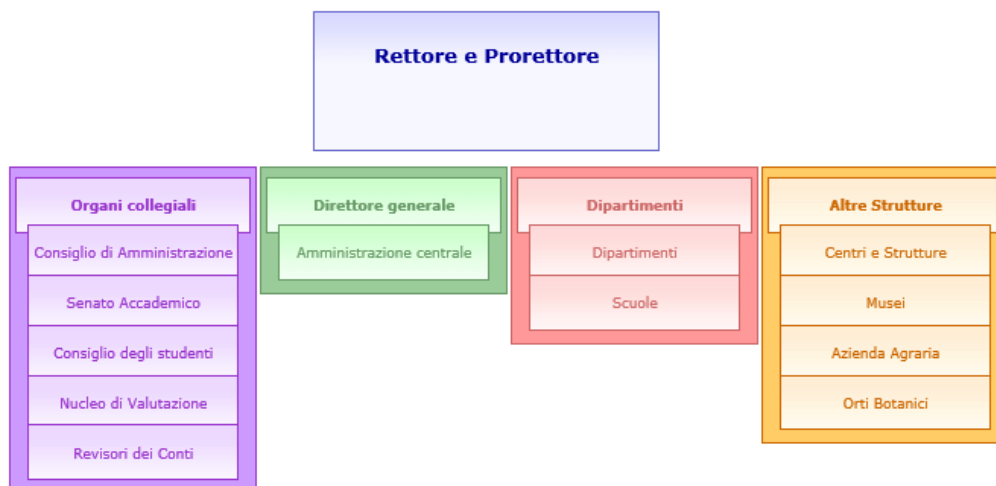


Figura 2 – La struttura organizzativa UNINA

L'organigramma generale è consultabile al seguente indirizzo:

<https://www.unina.it/ateneo/organigramma/organigramma-generale>

3.3. Area Organizzativa Omogenea

Ai sensi dell'art. 50, comma 4, del DPR 445/2000 e delle LLGG AgID, l'Ateneo ha individuato e istituito la propria area organizzativa omogenea (AOO) e i relativi uffici di riferimento (UOR o UO), al fine di garantire una gestione unica e coordinata dei documenti, assicurando criteri uniformi di classificazione e di archiviazione, nonché di comunicazione ad altre AOO.

Coerentemente con quanto riportato nell'Indice PA (indicepa.gov.it) e nell'Organigramma, la scelta operata dall'Ateneo è stata di configurarsi, ai fini della gestione documentale, come **unica Area Organizzativa Omogenea** denominata "Università degli Studi di Napoli Federico II", di seguito AOO, composta dall'insieme di tutte le sue strutture UOR/UO, e di definire, quindi, un registro di protocollo generale, unico per tutte le proprie strutture.

In caso di variazione del modello organizzativo per la gestione documentale, viene data dall'Amministrazione tempestiva comunicazione al Referente IPA e a tutti gli utenti interessati, nonché al Centro Servizi Informativi dell'Ateneo per le modifiche alla configurazione degli applicativi impattati, in termini di cambio della struttura organizzativa e delle abilitazioni degli utenti.

Di seguito, si riporta una tabella in cui si evidenziano i vantaggi derivanti da tale scelta organizzativa.

Caratteristica	Vantaggi
Unicità del Registro di protocollo	▪ Riduzione della frammentazione ▪ Riduzione del numero di registrazioni di protocollo ▪ Maggiore flessibilità del servizio ▪ Indipendenza dalle dinamiche di riorganizzazione dell'Ateneo ▪ Standardizzazione (es. titolario di classificazione) ▪ Maggiore coesione tra le strutture
Unicità dell'archivio elettronico contenente i documenti protocollati	▪ Riduzione della ridondanza della documentazione da gestire ▪ Semplificazione delle operazioni di reperimento dei documenti
Unicità del Manuale di Gestione	▪ Omogeneità di organizzazione del servizio ▪ Riduzione dei costi di gestione del servizio
Flussi interni di tipo "intra-AOO"	▪ Semplificazione dell'iter documentale ▪ Snellimento dei procedimenti amministrativi

A livello istituzionale, la AOO è costituita dalle UOR di I livello, strutture organizzative di vertice costituite da uffici (UO) oppure, nel caso più complesso dell'Amministrazione Centrale, da UOR di secondo livello (le Aree) articolate in Uffici (UO) afferenti. Le UOR, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.

Per ciascuna UOR, il responsabile pro tempore della struttura è anche Responsabile della gestione documentale (RGD) della UOR. L'Ateneo ha inoltre istituito il Servizio di Coordinamento della Gestione Documentale, ai sensi dell'art. 61, comma 2, del DPR 445/2000 e delle LLGG AgID.

Di seguito, i dati riportati in IPA relativamente all'Ente e alla AOO:

Dati identificativi dell'Amministrazione

Denominazione dell'Amministrazione	Università degli Studi di Napoli Federico II
Acronimo	UNINA
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	Corso Umberto I, n. 40 – 80138 NAPOLI
Natura giuridica	Università pubblica
Indirizzo PEC primario	ateneo@pec.unina.it
Altra email	urp@pec.unina.it



Caratterizzazione dell'Area Organizzativa Omogenea

Denominazione dell'Area Organizzativa Omogenea	Università degli Studi di Napoli Federico II	
Codice univoco AOO	A44A282	
Codice Identificativo assegnato alla AOO	Unina-Federicoll	
Domicilio digitale	ateneo@pec.unina.it	
Indirizzo email Responsabile	rettore@pec.unina.it	
Indirizzo completo della sede principale della AOO a cui indirizzare l'eventuale corrispondenza convenzionale	Corso Umberto I, n. 40 – 80138 NAPOLI	
Data di istituzione della AOO	1.1.2007	
Articolazione della AOO in UOR	▪ Amministrazione Centrale, articolata in Aree e relativi Uffici afferenti ▪ Dipartimenti ▪ Centri Interdipartimentali di Ricerca e di Servizio ▪ Centri d'Ateneo ▪ Centri museali ▪ Centri d'Eccellenza ▪ Centri Interuniversitari ▪ Biblioteche di Area ▪ Altre strutture (Azienda Torre Lama, Orto botanico, Scuola specializzazione professioni legali)	
Articolazione della AOO in Unità Organizzative di registrazione di Protocollo - UOP	Il Responsabile dell'UOR definisce autonomamente le proprie UOP	Ciascuna UOP protocolla sia in ingresso che in uscita

L'elenco completo dei domicili digitali delle UOR (riportati in IPA) assieme agli indirizzi PEC istituzionali delle UO afferenti alle UOR dell'Amministrazione Centrale, è consultabile all'indirizzo:

<https://www.unina.it/UNINAPEC>

Nell'**Allegato 2** è anche riportato l'elenco delle UOR UniNA e delle UO afferenti che costituiscono la struttura organizzativa ai fini della gestione documentale e dei flussi dell'Ateneo.

All'interno dell'Amministrazione il sistema di protocollazione è unico e totalmente distribuito per la corrispondenza in entrata e in uscita; pertanto, ogni UOR, struttura complessa a cui sono demandate le responsabilità nella gestione di particolari competenze, attività e procedimenti amministrativi, svolge anche i compiti di UOP,



fermo restando che tale abilitazione viene assegnata in alcuni casi (in funzione di particolari esigenze organizzative) anche a UO sottostanti. Tale “decentramento”, da un punto di vista operativo, segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del RCGD. Tutte le UO di Ateneo sono comunque abilitate alla consultazione del SPI, per quanto di propria competenza, e alla gestione del proprio archivio nel sistema SD.

In tutte le UOR è utilizzato il medesimo sistema di numerazione di protocollo e l'operatore incaricato dell'attività di protocollazione è abilitato dal RSI sulla base della richiesta comunicata (mediante utilizzo del modello SICURDAT/B, come sarà dettagliatamente descritto nell'**Allegato 6** al Manuale) dal Responsabile UOR/UO all'Ufficio Privacy e da quest'ultimo autorizzata e inviata a RSI.

3.4. Servizio per il coordinamento della gestione documentale

Con decreto del Direttore Generale dell'Ateneo, il DG n. 870 del 02.10.2019, nell'AOO precedentemente individuata è stato istituito a decorrere dal 02.10.2019, ai sensi all'art. 61 del succitato DPR 445/2000, il “Servizio di Coordinamento della Gestione Documentale di Ateneo” (SCGD) con le seguenti specifiche competenze:

- Definire e assicurare, sentiti i responsabili della gestione documentale delle UOR dell'Ateneo, criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione e archiviazione, nonché di comunicazione interna tra dette strutture, nel rispetto della autonomia operativa di ciascuna di esse, con funzione di coordinamento, monitoraggio e controllo in merito agli adempimenti connessi con la procedura del protocollo informatico e di gestione dei documenti e dei flussi documentali, ai sensi dell'art. 4, comma 2, del DPCM-Protocollo e dell'art. 50, comma 4, del DPR 445/2000;
- Garantire che il sistema informatico consenta lo svolgimento delle operazioni di registrazione e di segnatura di protocollo in ottemperanza con quanto stabilito dalla legislazione vigente in materia;
- Gestire e configurare il sistema documentale di Ateneo in ottemperanza con quanto disposto dall'art. 44, comma 1-bis, del CAD;
- Versare nel sistema documentale i repertori gestiti nell'ambito del sistema di protocollo e individuati nel Manuale di Conservazione, ai fini della loro conservazione;
- Assicurare la corretta trasmissione del contenuto dei pacchetti versati a partire dal sistema di Protocollo o di Gestione Documentale al Sistema di Conservazione, eventualmente coordinandosi, ove nominate con specifico provvedimento, con le figure dei “Responsabili del Versamento” e con il “Responsabile della Conservazione dei documenti informatici dell'Ateneo”;
- Attivare le competenti strutture del CSI affinché le funzionalità dei sistemi di protocollo e di gestione documentale, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile, coerentemente con livelli di servizio preventivamente concordati e, comunque entro le ventiquattro ore dal blocco delle attività;

- Stabilire con le competenti strutture del CSI le procedure per la corretta produzione e conservazione del registro giornaliero di protocollo e per la conservazione delle copie di salvataggio delle informazioni del sistema e vigila sull'osservanza di quanto concordato;
- Definire i profili di abilitazione (ruoli) per l'accesso alle funzioni ed ai dati del sistema di Protocollo Informatico e del sistema Documentale che i responsabili di UOR attribuiscono ai propri incaricati;
- Proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, e, più in generale, dei protocolli diversi dal protocollo informatico;
- Fornire consulenza alle strutture di Ateneo per quanto attiene alla attuazione delle politiche di gestione informatica dei documenti, dei fascicoli e dei flussi documentali;
- Predisporre e aggiornare, d'intesa con il Responsabile della Conservazione, con il Presidente del CSI, con il Responsabile per la Transizione al Digitale (RTD) e con il Responsabile della protezione dei dati personali di Ateneo (RPD):
 - il Manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali e in coerenza con quanto previsto nel Manuale di conservazione;
 - il Piano per la sicurezza informatica relativo alla protezione della integrità, della riservatezza e della disponibilità dei documenti e delle informazioni trattate nell'ambito del sistema di Protocollo Informatico e del sistema Documentale;
- Collaborare alla redazione e all'aggiornamento del Manuale della Conservazione;
- Garantire l'adeguatezza degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e di gestione informatica degli archivi elettronici;
- Aggiornare il Titolario di classificazione e il catalogo dei procedimenti, sulla base delle indicazioni fornite dalle UOR, sentito il Direttore Generale.

Il Servizio SCGD è istituito nell'ambito dell'Area Tecnica "e-Government" del CSI e il Responsabile del Servizio (RCGD) è il Direttore dell'Area Tecnica "e-Government" del CSI, che risponde direttamente al Direttore Generale.

Come riportato più avanti, RCGD, in qualità di Referente IPA, apporterà le modifiche intervenute nell'organigramma dell'Ateneo anche nel registro IPA.

L'atto che istituisce il servizio è riportato nell'**Allegato 4**.



3.5. Ruoli e responsabilità

L'Ateneo, essendo un'Amministrazione complessa e diramata sul territorio, al fine di assicurare una gestione documentale il più uniforme ed omogenea, ai sensi della normativa vigente, oltre al ruolo di RCGD precedentemente illustrato, ha previsto la nomina delle seguenti figure:

- Il Responsabile della Gestione Documentale presso ciascuna UOR (RGD)
- Il Responsabile della Transizione al Digitale (RTD)
- Il Responsabile della Protezione dei Dati (RPD)
- il Referente per l'Indice della Pubblica Amministrazione;
- il Responsabile della Conservazione (RC).

3.5.1. Il Responsabile della Gestione Documentale presso ciascuna UOR (RGD)

Come già anticipato nel paragrafo 3.2, per ciascuna UOR, il Responsabile pro-tempore della struttura svolge anche il ruolo di Responsabile della gestione documentale (RGD), figura che, in materia di gestione documentale, garantisce il rispetto della normativa vigente in materia di gestione documentale e di trattamento dei dati personali e recepisce le policy di Ateneo e le linee di indirizzo fornite dal Servizio di coordinamento della gestione documentale (SCGD).

Ciascun RGD svolge, per quanto di propria competenza, le funzioni di formazione e tenuta del sistema di gestione dei documenti, dei flussi documentali e degli archivi, con il compito di:

- garantire che le operazioni di registrazione, di segnatura di protocollo e di gestione dei flussi documentali siano svolte nel rispetto della normativa vigente;
- vigilare sull'osservanza, da parte del personale autorizzato e degli incaricati, del corretto utilizzo del sistema di protocollo e di gestione documentale, in conformità alle disposizioni normative vigenti e alle indicazioni del presente Manuale;
- vigilare sulla corretta funzionalità del sistema di protocollo e di gestione documentale e, in caso di guasti o indisponibilità, sollecitare il ripristino dello stesso nel più breve tempo possibile;
- autorizzare le operazioni di annullamento delle registrazioni di protocollo effettuate dalla UOR;
- supportare RCGD nella verifica e nell'aggiornamento del Titolare di classificazione integrato con il Piano di conservazione e con il Piano di fascicolazione.

Nell'ambito di ciascuna struttura (UOR), RGD può essere coadiuvato dalle seguenti figure, ciascuno dotato di idoneo profilo operativo:

- l'Ufficio/Servizio di Protocollo (**UOP**);
- I Capi Ufficio delle UO afferenti alla UOR (**CU**);



- il Responsabile del Servizio di Protocollo (**RSP**);
- il Gestore Documentale (**GD**), incaricato da RGD della visualizzazione e della gestione (informatica) di tutti i documenti pervenuti alla UOR e relativi uffici afferenti (UO) oppure prodotti dalla UOR e relative UO;
- l'incaricato delle registrazioni di Protocollo Generale (**PR**);
- il Responsabile del Procedimento Amministrativo, tipicamente il Capo Ufficio, che prende in carico esplicitamente un documento che gli è stato assegnato come destinatario, oppure smistato, dalla propria UOR/UO afferente (**RPA**).

L'elenco dei profili operativi degli incaricati della gestione del sistema documentale presso le UOR e i relativi uffici afferenti è riportato in **Allegato 6**.

3.5.2. Il Responsabile della Transizione al Digitale (RTD)

L'Ateneo ha nominato quale Responsabile della Transizione Digitale, di cui all'art. 17 del CAD, il Presidente del CSI e ne ha registrato il nominativo su IPA.

3.5.3. Il Responsabile della Protezione dei Dati (RPD)

Un ruolo particolare all'interno della gestione documentale dell'Amministrazione è assunto dal Responsabile della protezione dei dati personali (RPD), nominato ai sensi degli artt. 37, 38 e 39 del Regolamento (UE) 2016/679. Tale Responsabile è chiamato ad esprimere pareri sulle modalità e sulle misure di sicurezza adottate dal Titolare del trattamento dei dati personali gestiti attraverso il sistema documentale (protocollo, documentale, conservazione).

Maggiori dettagli su Regolamenti, Riferimenti, Informative, Documentazione e Modulistica attinenti alla tutela dei dati personali sono reperibili all'indirizzo:

<https://www.unina.it/ateneo/statuto-e-normativa/privacy>.

3.5.4. Il Referente per l'Indice della Pubblica Amministrazione (IPA)

L'indice dei domicili digitali delle Pubbliche Amministrazioni (IPA) rappresenta il pubblico elenco di fiducia nel quale sono indicati i domicili digitali da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge tra le pubbliche amministrazioni e i privati, ai sensi dell'art. 6-ter del CAD e delle "Linee guida dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi" emanate da AgID.

In tale indice sono riportate le informazioni relative all'Ente: AOO e relative UOR con i rispettivi domicili digitali.



Il Referente IPA dell'Amministrazione ha il compito, sia organizzativo sia operativo, di interagire con AgID per l'inserimento e la modifica tempestiva, e comunque con cadenza almeno semestrale, dei dati dell'Ente, nonché per ogni altra questione riguardante la presenza dell'Ente nell'IPA. La mancata comunicazione degli elementi necessari al completamento dell'Indice e al loro aggiornamento è valutata ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato dei dirigenti responsabili.

Le modifiche all'organigramma utilizzato dal sistema di gestione documentale sono formalmente comunicate dall'Amministrazione al RCGD in funzione di variazioni derivanti da istituzioni o cessazioni di strutture, ratificate da decreti rettorali o direttoriali e da questi comunicate **al Referente IPA** per consentire l'aggiornamento dei dati ivi pubblicati.

Il Referente IPA è nominato dalla Direzione Generale, d'intesa con il Presidente del CSI, nell'ambito del SCGD e, alla data, tale ruolo è ricoperto da RCGD.

3.5.5. Responsabile della Conservazione (RC)

Il RC, Responsabile della conservazione, nominato ai sensi dell'art. 44, comma 1-quater, del CAD, opera in conformità a quanto previsto dalle LLGG AgID. Per tale posizione l'Ateneo ha individuato e nominato, con decreto del Direttore Generale n. 1071 del 24.07.2013, un funzionario dipendente dell'Ateneo, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica.

Ai sensi dell'art. 44, c. 1-quater, del CAD, per la gestione del processo di conservazione, tale soggetto opera d'intesa con il RPD, con il Responsabile della sicurezza, con il Responsabile dei sistemi informativi, nonché con il Responsabile del Coordinamento della Gestione Documentale (RCGD).

Visto che, in conformità alle disposizioni di cui all'art. 34, comma 1-bis, del CAD, attualmente l'Ateneo provvede in autonomia alla conservazione dei propri documenti informatici, svolgendo così anche il ruolo di conservatore, RC:

- definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che l'Ateneo svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità;
- predispone il Manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;
- genera e sottoscrive il rapporto di versamento degli oggetti digitali inviati in conservazione, secondo le modalità previste nel Manuale di conservazione;



- genera e sottoscrive il pacchetto di distribuzione, nei casi previsti dal Manuale di conservazione, e assicura la presenza di un pubblico ufficiale nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione e predispone le misure necessarie per la sicurezza fisica e logica dello stesso;
- effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentali;
- adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, al fine di garantire la conservazione e l'accesso ai documenti informatici; adotta analoghe misure con riguardo all'obsolescenza dei formati provvedendo, inoltre, alla duplicazione o alla copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale di conservazione;
- assicura agli organismi competenti previsti dalla norma l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvede al versamento dei documenti informatici e delle aggregazioni informatiche, nonché degli strumenti che ne garantiscono la consultazione, nell'Archivio storico, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali.
- predispone, assieme a RCGD, il Manuale di Conservazione e ne cura gli aggiornamenti periodici.

Per ulteriori dettagli si rimanda al Manuale di Conservazione di cui al punto 9.2.

3.6. Il sito WEB per l'eGovernment

Maggiori dettagli ed informazioni sugli argomenti sopra descritti sono disponibili sul sito istituzionale gestito da SCGD:

<https://www.praxis.unina.it>

in cui vengono messi a disposizione dell'utente normative, regolamenti interni, manuali, guide operative e strumenti software di utilità.

Realizzato con l'obiettivo di dare ordine alle informazioni creando specifiche sezioni tematiche riguardanti l'eGovernment, il protocollo informatico, il sistema documentale, la firma digitale, la posta elettronica certificata, nonché una sezione con i collegamenti rapidi alle procedure informatiche, il sito è stato sviluppato in ottemperanza con la normativa vigente in materia di accessibilità.

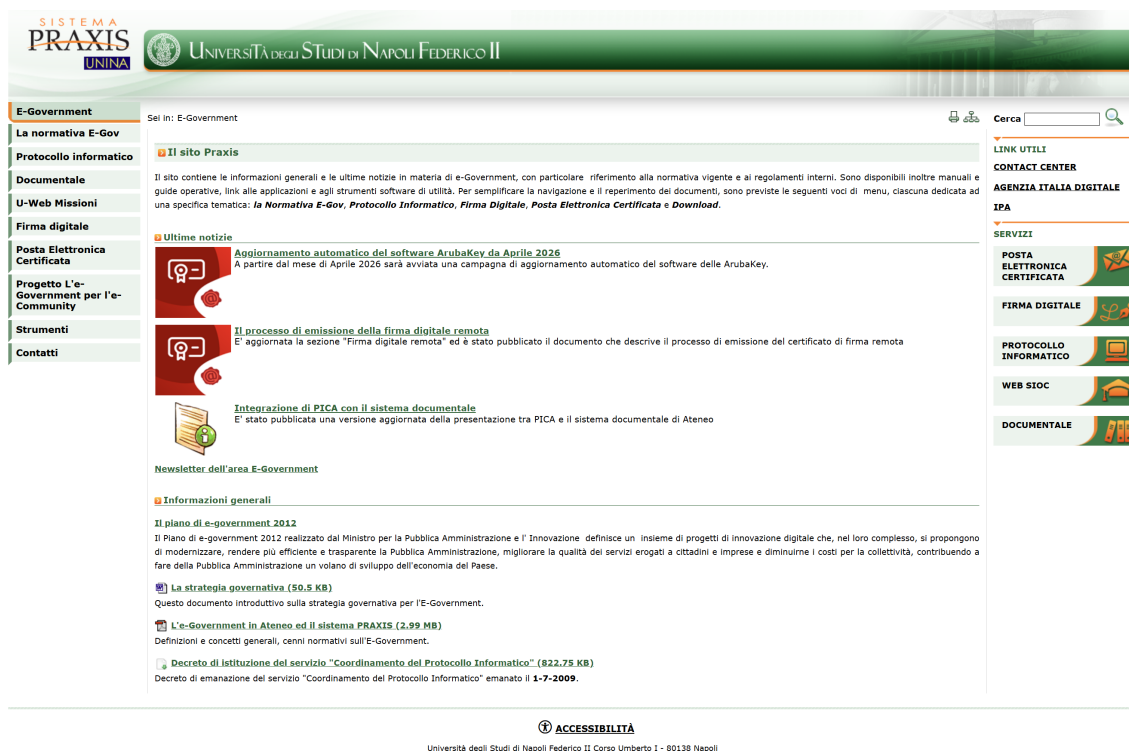


Figura 3 – Il sito per l'eGovernment UniNA

Le news inserite per data di pubblicazione e per canale tematico, il motore di ricerca interno dotato di funzionalità avanzate per la limitazione delle ricerche a singoli argomenti o sezioni, la mappa del sito aggiornata in tempo reale ad ogni inserimento di nuove voci nel menu di navigazione, la generazione dei percorsi a "briciole di pane" (sequenza di link) che informano costantemente il navigatore in quale punto del sito si trova, sono solo alcune delle funzionalità offerte dal sito.

4. IL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

4.1. Caratteristiche generali di un Sistema di gestione informatica dei documenti e dei flussi documentali

Il sistema di gestione informatica dei documenti, ai sensi dell'art. 52 del DPR 445/2000, deve:

- a) garantire la sicurezza e l'integrità del sistema;
- b) garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
- c) fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
- d) consentire il reperimento delle informazioni riguardanti i documenti registrati;
- e) consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
- f) garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Inoltre, ai fini della gestione dei flussi documentali, oltre a rispettare i requisiti sopra elencati, ai sensi dell'art. 65 del DPR 445/2000, deve:

- a) fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;
- b) consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;
- c) fornire informazioni statistiche sull'attività dell'ufficio;
- d) consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi.

La finalità generale di un sistema di gestione informatica dei documenti e dei flussi è quindi quella di fornire a ogni struttura il necessario supporto documentario per lo svolgimento efficiente e a fini di testimonianza giuridicamente valida delle proprie attività, garantendone la conservazione e la fruizione sia a fini interni che di trasparenza amministrativa, perseguendo i seguenti obiettivi:

- la produzione/acquisizione di documenti attendibili a fini giuridici e a fini strumentali;

- l'assegnazione e il trattamento dei documenti;
- l'organizzazione e la tenuta della produzione documentaria in modo ordinato e coerente alle funzioni esercitate, dalla formazione al versamento in conservazione;
- la trasmissione e conservazione di documenti autentici, cioè integri e di provenienza certa e identificata;
- la rapidità e l'efficienza del reperimento nell'ambito dell'attività amministrativa svolta.

Il sistema di gestione informatica dei documenti, in accordo con quanto riportato più avanti, è configurato e utilizzato nel rispetto dei principi di protezione dei dati personali di cui all'art. 5 del Regolamento (UE) 2016/679 applicabili alla gestione documentale, con particolare riferimento alla minimizzazione dei dati, alla limitazione degli accessi, alla conservazione dell'integrità dei dati, alla riservatezza e alla tracciabilità delle operazioni rilevanti.

Le funzionalità del sistema sono utilizzate secondo criteri coerenti con le competenze organizzative degli utenti e con le esigenze dei procedimenti amministrativi trattati.

Nel prosieguo del presente documento, il sistema di **“gestione informatica dei documenti e dei flussi documentali”** sarà anche per brevità denominato **“sistema di gestione informatica dei documenti”**.

4.2. Il sistema di gestione informatica dei documenti dell'Ateneo

I requisiti precedentemente riportati per il sistema di gestione informatica dei documenti sono assolti **dall'esercizio coordinato e interoperabile del Sistema del Protocollo Informatico (SPI) basato sull'applicazione eGrammata e del Sistema Documentale (SD) basato sull'applicazione eDocumento**, ciascuno per le proprie finalità e ambito e con le proprie caratteristiche tecnico-funzionali.

Tali sistemi costituiscono quindi l'asset principale della parte informatica del sistema di gestione documentale dell'Ateneo.

Al sistema del Protocollo Informatico (SPI) basato sull'applicazione eGrammata, avviato dal 1° gennaio 2007, si è successivamente affiancato in modo incrementale, a partire dal 1° gennaio 2014, il Sistema Documentale (SD) basato sull'applicazione eDocumento per la gestione della documentazione amministrativa dell'Ateneo e i flussi di lavoro tra i soggetti che partecipano, a vario titolo, nel trattamento di un dato procedimento.

L'applicazione eDocumento, cuore dell'architettura per la gestione documentale UniNA, è stata realizzata secondo un approccio olistico di tipo archivistico, fortemente orientato ai procedimenti amministrativi, alla classificazione dei documenti e alla loro organizzazione strutturata in aggregazioni documentali informatiche. È una piattaforma



che offre le funzionalità di creazione, salvataggio, ricerca, gestione del ciclo di vita dei documenti e dei fascicoli, fino alla conservazione, con un orientamento particolare all'integrazione con i restanti sistemi istituzionali dell'Ateneo, in particolare: il Protocollo Informatico, la Firma Digitale centralizzata, la PEC, la posta elettronica, la gestione delle carriere degli studenti, la gestione delle carriere del personale, la contabilità, la gestione delle procedure concorsuali, le missioni, le convocazioni degli Organi Collegiali, gli Ordinativi di Pagamento e Incasso, nonché il sistema di Identity Access Management (IAM). Nell'ambito del processo di creazione, classificazione e organizzazione dei fascicoli e dei documenti, un ruolo molto importante è svolto dall'utilizzo coordinato nell'ambito di SD del Titolare di classificazione, del Catalogo dei procedimenti (procedimenti amministrativi, affari e attività) e del Catalogo delle tipologie documentali, documenti in aggiornamento continuo e revisione da parte dell'Amministrazione.

Nell'**Allegato 7** al presente Manuale è riportato un quadro di sintesi delle caratteristiche tecnico-funzionali dei sistemi SPI e SD.

4.3. Il modello organizzativo del sistema di gestione documentale UniNA

L'organizzazione complessiva dell'archivio informatico dei documenti amministrativi dell'Ateneo si conforma a un modello "federativo", in cui vari sistemi informatici concorrono ad alimentare l'archivio complessivo dell'Ente, condividendo regole, formati, organigramma, piano di classificazione della documentazione, catalogo dei procedimenti e delle tipologie documentali, in modo da garantire l'integrità e la coerenza del patrimonio informativo.

Il sistema SPI è preposto alla registrazione e classificazione dei documenti amministrativi in entrata nella AOO o da questa in uscita, nonché alla tenuta di alcune serie archivistiche rilevanti; ma è nel sistema SD che viene consentito il collegamento tra la documentazione e i procedimenti, nonché l'organizzazione e la tenuta dell'archivio digitale, l'associazione a documenti e fascicoli di un insieme ampio di metadati descrittivi, gli strumenti per la gestione di tutto il ciclo di vita dei documenti, dalla formazione, alla classificazione, alla registrazione di protocollo o particolare, fino alla loro conservazione a lungo termine e alla selezione e scarto.

L'obiettivo fondamentale per l'Amministrazione è garantire la corretta organizzazione e sedimentazione del proprio patrimonio documentale, anche ai fini storici oltre che amministrativi e giuridici. Pertanto, in considerazione della profonda differenza di ambito di applicazione dei due sistemi SPI e SD e della loro complementarità, gli utenti devono utilizzare in modo consapevole gli strumenti che consentono di utilizzarli e farli interoperare.

Più in dettaglio, a meno di casi specifici, un documento potrà:

- essere registrato nel sistema SPI (nel registro di protocollo generale o in uno dei repertori tenuto da SPI) e quindi essere successivamente importato in SD e

archiviato nella relativa aggregazione documentale (fascicolo procedimentale o serie tipologica),
oppure,

- collocato nel fascicolo procedimentale creato dall'utente in SD e quindi, a seguire e nei casi previsti dalla legge e dal presente Manuale, essere registrato nel protocollo, utilizzando direttamente le chiamate di SD alle API di SPI.

Altre applicazioni (ad esempio, quelle per: la gestione della didattica e degli studenti, la gestione del personale, la gestione e la consultazione delle convocazioni degli OOCC, la gestione delle istanze di concorso, delle missioni, delle fatture e degli ordinativi di pagamento e incasso) potranno altresì gestire e archiviare unità documentali di specifici procedimenti secondo un approccio di interoperabilità a servizi, mediante l'invocazione di opportuni componenti messi a disposizione da SD per la creazione di nuovi repertori e fascicoli informatici, di super fascicoli (di carriera dello studente o dei dipendenti) e per l'inserimento, la modifica e la cancellazione di documenti amministrativi.

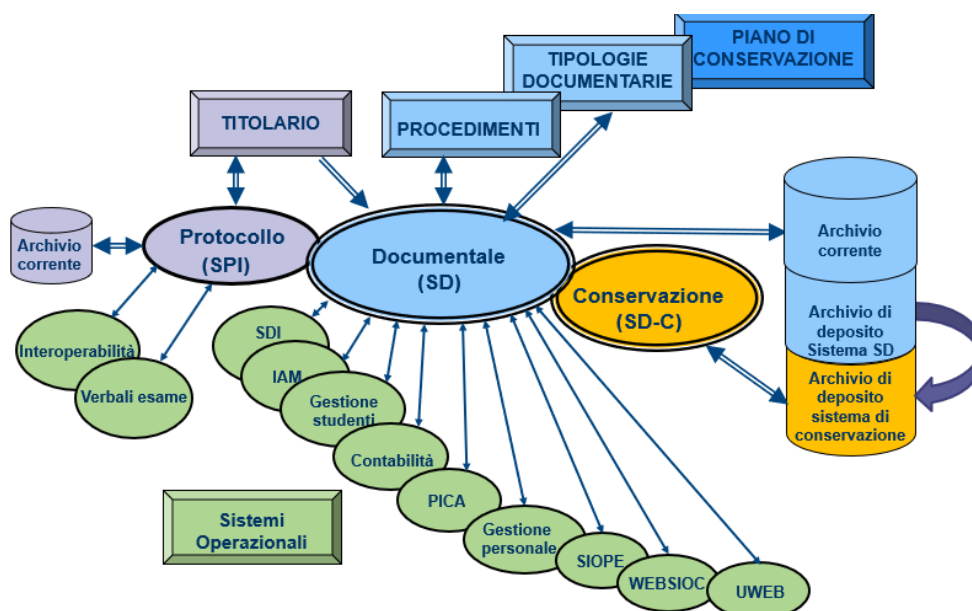


Figura 4 – Il modello per la gestione documentale UniNA

Per quanto riguarda le serie tipologiche gestite da SPI (es.: i decreti, i verbali digitali di esame, le gare, le convenzioni, etc.), i documenti amministrativi digitali in esse contenuti, con i relativi allegati e metadati, sono versati annualmente in SD mediante un processo eseguito dal Servizio di Coordinamento della Gestione Documentale (SCGD) che effettua l'estrazione da SPI, la produzione di pacchetti contenenti le unità documentali estratte, la trasmissione e, quindi, l'importazione delle unità documentali in SD e da questo, il versamento e la conservazione in SD-C. Le serie tipologiche gestite in SD sono versate con cadenza annuale nel sistema di conservazione, a cura di RCGD, e quindi conservate in SD-C, a cura di RC. Tutti gli oggetti (fascicoli e/o documenti amministrativi) presenti in SD saranno comunque versabili nel modulo SD-C dedicato alla conservazione, secondo quanto riportato più avanti.



I documenti registrati esclusivamente nel registro di protocollo generale non sono destinati a essere tra di loro collegabili né riferibili a un dato procedimento amministrativo o una specifica tipologia documentale e, quindi, non sono versabili in conservazione, a differenza dei documenti collocati in un'aggregazione documentale di SPI, come precedentemente detto. La mancata conservazione del Registro Generale di Protocollo come aggregazione documentale non pregiudica la conservazione dei documenti amministrativi, i quali vengono versati al sistema di conservazione nell'ambito dei fascicoli e dei repertori cui appartengono, secondo le modalità descritte nel presente Manuale e nel Manuale di Conservazione.

5. FORMAZIONE DEI DOCUMENTI

5.1. Modalità di formazione e contenuti minimi dei documenti amministrativi

I documenti amministrativi aventi rilevanza esterna, prodotti dall'Amministrazione sia in formato analogico che digitale, contengono un insieme minimo di informazioni, quali:

- la denominazione e il logo dell'Amministrazione;
- la denominazione dell'AOO e dell'UOR;
- l'indicazione del Responsabile del procedimento;
- l'oggetto del documento.

Nella redazione dei documenti possono essere inserite ulteriori informazioni in base alle specifiche necessità e a discrezione degli RPA o dei responsabili delle UOR.

In generale, nella formazione dei documenti amministrativi contenenti dati personali deve essere rispettato il principio di minimizzazione, evitando l'inserimento di informazioni non necessarie rispetto alla finalità del documento e al procedimento di riferimento.

Per quanto riguarda le modalità di formazione dei documenti informatici, come previsto nelle LLGG AgID, è possibile distinguere quattro tipologie di formazione:

1. redazione tramite l'utilizzo di appositi strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'Allegato 2 delle LLGG AgID;
2. acquisizione per via telematica o su supporto informatico del documento, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
3. 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;
4. generazione o il 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.

In particolare, nel primo caso rientrano i documenti prodotti dall'Amministrazione con i principali strumenti software di collaboration e di produttività. Nel secondo caso rientrano, invece, le copie digitali di documenti analogici che sono prodotte come copie per immagine o come documenti nativi digitali formati mediante la trascrizione del contenuto del documento originale analogico, come descritto nel dettaglio nel successivo paragrafo del presente Manuale.



Nel presente Manuale sono altresì descritte le modalità adottate dall'Ateneo nel sistema di gestione informatica dei documenti per trattare a norma il documento amministrativo informatico: identificarlo in modo univoco e persistente, secondo le regole specificate nell'**Allegato 8**, assicurarne immodificabilità, integrità, completezza e correttezza dei metadati, tutelarne la riservatezza e garantirne la disponibilità.

5.2. Copie di documento amministrativo informatico o analogico

Ai fini di una corretta gestione dei documenti amministrativi informatici trattati, è opportuno ricordare il quadro normativo e le disposizioni vigenti atte ad assicurare valore ed efficacia probatoria a copie, duplicati, estratti di documenti analogici e informatici.

Per copia di un documento si intende la riproduzione di un documento originale attraverso processi e strumenti idonei ad assicurare la corrispondenza della copia rispetto al documento originale da cui è tratto. Pertanto, la copia di un documento conserva la medesima efficacia probatoria del documento originario da cui è tratto nel caso in cui la sua conformità sia attestata da un pubblico ufficiale o un funzionario pubblico a ciò preposto (in tal caso si parla di copia conforme), oppure nel caso in cui la sua conformità non sia espressamente disconosciuta. Ai sensi di quanto disposto dal CAD e dalle LLGG AgID, si distinguono le seguenti fattispecie di copie.

Duplicato, copia o estratto di un documento amministrativo informatico

- ***Duplicato informatico***: si intende la memorizzazione, sullo stesso dispositivo o su altri dispositivi, della medesima evidenza informatica nello stesso formato o estensione del documento originale. Tale duplicato mantiene lo stesso valore giuridico del documento da cui è tratto se è ottenuto mediante la memorizzazione, nel medesimo formato o estensione, della sequenza binaria originaria.
- ***Copia di un documento informatico***: si intende un documento il cui contenuto è il medesimo dell'originale ma è rappresentato con una diversa evidenza informatica e/o con un diverso formato o estensione.
- ***Estratto di un documento informatico***: è una parte del documento originale con una diversa evidenza informatica.

Le copie e gli estratti hanno lo stesso valore probatorio dell'originale da cui hanno tratto origine se la loro conformità non viene espressamente disconosciuta. Al fine di assicurare la stessa efficacia probatoria dell'originale (quindi una copia conforme), è necessario che la conformità della copia o dell'estratto sia attestata da un pubblico ufficiale autorizzato, mantenendo valido, ove previsto, l'obbligo di conservazione dell'originale informatico.

La conformità delle copie o degli estratti di documenti informatici può essere attestata mediante uno dei seguenti metodi:



- raffronto dei documenti;
- certificazione di processo.

Il ricorso ad uno dei suddetti metodi assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico originale.

Per ulteriori dettagli sui requisiti tecnici per la certificazione di processo si rimanda all'Allegato 3 delle LLGG AgID (Certificazione di processo).

Fatto salvo quanto previsto dall'art. 23-bis, 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 è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto dei documenti.

Copia per immagine del documento amministrativo analogico

Per copia per immagine su supporto informatico di un documento amministrativo analogico si intende la copia prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo. Un esempio di tali tipologie di copie sono i documenti in formato JPEG o PDF prodotti mediante scansione di documenti originali analogici.

La conformità della copia al documento amministrativo originale è garantita:

- mediante attestazione di un pubblico ufficiale o di un funzionario pubblico a ciò incaricato;
- mediante la sottoscrizione con firma digitale o firma elettronica qualificata o firma elettronica avanzata da parte del personale che effettua il raffronto;
- mediante certificazione di processo, come descritto nell'Allegato 3 alle LLGG AgID.

L'attestazione di conformità può essere inserita nel documento informatico contenente la copia informatica, oppure può essere prodotta come un documento separato (caratterizzato in maniera mandatoria da un riferimento temporale e dall'impronta informatica della copia per immagine). In entrambi i casi, è necessario che l'attestazione di conformità sia sottoscritta con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

Nell'eventualità in cui vi sia un numero elevato di copie conformi da generare, dovuto a esigenze di dematerializzazione massiva di documenti analogici, è possibile assicurare in un'unica soluzione che i documenti informatici abbiano contenuto e forma identici a quelli dei documenti analogici da cui sono tratti adottando la certificazione di processo

in luogo del raffronto per ogni singolo documento. In tal caso, si deve fare riferimento alle disposizioni dell'Allegato 3 alle LLGG AgID per la corretta esecuzione del processo.

Copia informatica del documento analogico

Per copia informatica del documento analogico si intende la copia avente contenuto identico a quello del documento analogico da cui è tratta, ma forma diversa. Un esempio di tale tipologia di copia è un documento prodotto tramite un text editor (ad esempio Word), contenente la trascrizione del contenuto del documento originale analogico. Per garantire la conformità di tali tipologie di copie rispetto agli originali si applicano le medesime disposizioni previste per le copie per immagine di documenti amministrativi analogici.

5.3. Conservazione degli originali analogici da cui sono tratte le copie informatiche

Le copie informatiche di documento analogico, ai sensi dell'art. 22, commi 1, 1 bis, 2 e 3 del CAD sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge.

Per le copie informatiche tratte da documenti originali analogici **unici** – siano esse copie per immagine o documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, formati in origine su supporto analogico – **permane l'obbligo di conservazione degli originali analogici nel caso in cui si tratti di documenti rientranti nelle categorie indicate nell'Allegato A al D.P.C.M. 21 marzo 2013** (che individua come non eliminabili documenti quali, ad esempio, gli atti giudiziari e processuali per i venti anni successivi alla loro formazione, documenti aventi valore storico-artistico, documenti storico-demaniali conservati negli archivi), nonché per le copie digitali per le quali non è certificata la conformità.

Salvo i casi previsti dalla legge che prescrivono l'obbligo di conservazione dell'originale analogico unico, la conservazione sostitutiva (con distruzione dell'originale analogico) può essere effettuata se l'attestazione di conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico conservato. Un caso di documenti analogici unici è quello delle ricevute di pagamento di spese sostenute in missione in Stati appartenenti all'elenco dell'Unione Europea delle giurisdizioni non cooperative ai fini fiscali (c.d. paesi black list), registrate nel repertorio "RRM" gestito dal Sistema Documentale SD. Con decreto del Direttore Generale n. 1060 del 12.09.2023 sono state impartite le istruzioni per la corretta gestione di tali documenti anche ai fini della conservazione sostitutiva, con possibilità di distruzione degli originali cartacei.



5.4. Copie analogiche di documenti informatici: il contrassegno elettronico

Ai sensi dell'art. 23, comma 1 e comma 2-bis, del CAD, le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con le regole tecniche di cui all'articolo 71 del CAD, tramite il quale è possibile accedere al documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico.

Sulla copia analogica in formato stampabile del documento informatico viene apposto un timbro crittografico (il formato utilizzato dall'Ateneo è il PDF417) che riporta almeno gli elementi indispensabili all'individuazione del documento amministrativo informatico originale registrato nell'archivio dell'Amministrazione e le informazioni per consentire la verifica dell'integrità della copia prodotta rispetto all'originale archiviato nel sistema di gestione documentale dell'Università.

Più in dettaglio, il timbro crittografico apposto è in formato PDF417 e contiene gli stessi dati riportati in chiaro con l'aggiunta dell'impronta elettronica del documento (impronta calcolata ed associata, in maniera immodificabile, al documento all'atto della sua registrazione nel sistema di gestione documentale dell'Università). Il documento digitale viene quindi rappresentato, in modo sicuro e controllato, in un nuovo documento "pdf", esportabile ed eventualmente stampabile in modo molto semplice dagli interessati.

Il pdf generato a seguito del processo sopra delineato è dunque una rappresentazione del documento originale firmato digitalmente che è registrato e custodito dal sistema di gestione documentale dell'Ateneo. Il destinatario della copia potrà verificarne l'autenticità mediante l'utilizzo di un software open source per la lettura e la decodifica dei codici a barre messo gratuitamente a disposizione dall'Università (sul sito dell'eGovernment di Ateneo: <http://www.praxis.unina.it>).

La soluzione UniNA sopra descritta è referenziata nella Circolare AgID n. 62 del 30 aprile 2013 recante "Linee guida per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5, del CAD".

5.5. Formato dei documenti

I sistemi SPI e SD gestiscono le principali tipologie di formati, sia per i documenti primari che per gli allegati. Per contrastare i rischi legati all'obsolescenza tecnologica e per garantire la disponibilità, la consultabilità e la leggibilità dei documenti nel tempo, l'Amministrazione adotta solo formati di file conformi alle disposizioni dell'Allegato 2 alle LLGG AgID e con un elevato livello di interoperabilità. L'Amministrazione provvede, inoltre, ad effettuare dei controlli periodici per verificare l'idoneità dei formati di memorizzazione dei file in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, prevedendo, se necessario, il loro riversamento, conformemente a quanto disposto nell'Allegato 2 alle LLGG AgID.

Pertanto, indipendentemente dal formato con il quale sono prodotti i documenti, prima della sottoscrizione mediante firma digitale e della loro acquisizione nel sistema di gestione documentale, questi devono essere convertiti in formato PDF (preferibilmente, PDF/A) o XML, al fine di garantire l'immodificabilità del loro contenuto, la loro accessibilità e conservazione nel tempo, nonché l'usabilità e la reperibilità degli stessi da parte di utenti con disabilità.

5.6. Sottoscrizione dei documenti

I documenti prodotti dall'Amministrazione aventi rilevanza esterna, prima di essere protocollati o trasmessi all'esterno, sono sottoscritti dal dirigente e/o dal responsabile dell'ufficio o del procedimento con una delle seguenti modalità:

- Firma olografa o a mezzo stampa (art. 3, comma 2, del DPR 39/93);
- Firma elettronica, firma elettronica avanzata o firma digitale (anche remota), come rilasciata dall'Amministrazione.

I formati di firma digitale ammessi sono:

- PAdES, limitatamente ai file con estensione .pdf;
- XAdES per i file XML;
- CAdES per tutti i formati di file.

I documenti possono essere altresì sottoscritti/acquisiti nel SD con la modalità Cades-T/Pades-T/Xades-T, cioè, firmati con certificati qualificati di durata ristretta, con contestuale apposizione del time-stamp (la cosiddetta "firma one shot").

Nei casi in cui sia previsto l'utilizzo del sigillo elettronico, per gli utenti abilitati al suo utilizzo (alla data, solo il Direttore Generale) sono, inoltre, disponibili delle specifiche funzioni sul sistema SPI, in accordo con quanto previsto nell'Allegato 6 delle LLGG AgID per la gestione della trasmissione dei documenti protocollati tra AOO, con l'apposizione automatica del sigillo qualificato.



Come previsto dalla normativa vigente, l'utilizzo della firma digitale per la sottoscrizione dei documenti soddisfa i requisiti di cui all'art. 20, comma 1-bis, del CAD e all'art. 2702 del Codice civile. Quindi, è idoneo a garantire la validità giuridica dei documenti, il mantenimento della loro integrità e riservatezza, l'immodificabilità del loro contenuto, il non ripudio degli stessi in fase di giudizio.

Il formato di firma previsto in modo preferenziale per i documenti amministrativi dell'Università è il Cades. In tal caso, l'estensione del file prodotto è ".p7m".

I documenti possono essere sottoscritti da più soggetti: in tal caso, sono apposte firme multiple, di tipo parallelo o di tipo controfirma. La firma dell'intera busta crittografica è prevista solo in casi particolari, espressamente previsti e regolamentati dallo specifico procedimento.

Nel caso di apposizione di firme multiple, i sottoscrittori successivi al primo devono effettuare preventivamente la verifica di validità ed integrità del documento che devono firmare.

Per la sottoscrizione dei documenti informatici,

- l'Ateneo utilizza servizi fiduciari qualificati;
- firme elettroniche qualificate;
- sigilli elettronici qualificati ove previsti;
- strumenti conformi al Regolamento eIDAS e successive modifiche.

Gli strumenti per apporre la firma digitale su un documento amministrativo sono l'applicazione rilasciata dalla Certification Authority fornitrice dei certificati di firma UniNA, eseguibile sulla postazione di lavoro del sottoscrittore, oppure l'utilizzo del sistema di firma digitale centralizzato invocato a servizi direttamente dalle applicazioni di gestione documentale.

L'Ateneo sta migrando in questi mesi dal servizio di firma digitale su dispositivo sicuro (SIM con token USB) al servizio di firma remota, basato sull'utilizzo di certificati qualificati di firma digitale e di un servizio fiduciario qualificato offerto dalla CA per l'apposizione della firma mediante dispositivo HSM conforme ai requisiti dettati dalla normativa europea eIDAS2.

Maggiori dettagli sul servizio di firma digitale sono reperibili al seguente indirizzo:

<https://www.praxis.unina.it/firma-digitale>

5.7. Verifica delle firme

I documenti sottoscritti con firma digitale sono sottoposti a verifica di validità e di integrità grazie all'utilizzo dei servizi di verifica disponibili in tutti i prodotti di mercato di

firma digitale. Tale processo deve essere realizzato in modo conforme a quanto prescritto dalla normativa vigente (si vedano le norme pubblicate sul sito AgID).

L'operazione di verifica deve essere svolta sia dal sottoscrittore che deve apporre una firma parallela (come detto nel paragrafo precedente) mediante applicazioni locali, sia dal sistema di gestione informatica dei documenti (SPI e SD) in fase di registrazione/importazione del documento. Anche in tali sistemi sono infatti previste funzioni automatiche di verifica di integrità del documento e di autenticità della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare. L'esito della verifica viene persistito e associato in modo imm modificabile e permanente al documento stesso.

Più in dettaglio, la sequenza delle operazioni previste dai sistemi per la gestione informatica dei documenti è la seguente.

- apertura della busta "virtuale" contenente il documento firmato, in formato p7m ("cades"), pdf ("pades") o xml ("xades"), anche di tipo "one shot";
- verifica della validità dei certificati di firma (sono più di uno nel caso di documento contenente firme digitali multiple);
- verifica della integrità del documento;
- verifica che la firma del certificato di firma dell'utente sia apposta da una Certification Authority (CA) presente nell'elenco pubblico dei certificatori accreditati e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle CA accreditate con periodicità giornaliera;
- inserimento nel sistema documentale dell'Amministrazione sia del documento originale firmato sia del documento in chiaro;
- registrazione nei metadati di registrazione delle informazioni, imm modificabili, relative all'esito delle verifiche di autenticità e integrità.

Nel caso di verifica fallita di validità e integrità il sistema SD ne impedisce il caricamento. Pertanto, si raccomanda di sottoscrivere i documenti con certificati non prossimi alla scadenza o, comunque, di essere tempestivi nella registrazione nel sistema SPI, oppure nella acquisizione nel sistema SD del documento sottoscritto. In caso di certificato scaduto, il sistema SPI notifica l'esito della verifica fallita all'operatore di protocollo e chiede la conferma a procedere. In tal caso, l'esito di fallita verifica di validità (e/o di integrità) del certificato è riportato in modo imm modificabile tra i metadati della registrazione. La richiesta di protocollazione di documenti sottoscritti con firma digitale eseguita da applicazioni esterne mediante l'apposito servizio di SPI, nel caso di verifica fallita, può essere rifiutata o eseguita, a seconda della modalità di invocazione del servizio di registrazione di protocollo.



6. PROTOCOLLO INFORMATICO

Le operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti, ai sensi dell'art. 56 del DPR 445/2000, sono la registrazione, la segnatura di protocollo e la classificazione dei documenti.

In Ateneo, come già illustrato in precedenza, tali operazioni sono garantite dal sistema di protocollo informatico (SPI) che partecipa alla formazione del sistema di gestione informatica dei documenti, sistema conforme alle disposizioni del DPR 445/2000 e alle LLGG AgID.

Il sistema di protocollo informatico consente, quindi, in particolare, lo svolgimento delle seguenti operazioni:

- la corretta e puntuale registrazione di protocollo di ogni documento ricevuto o spedito dall'amministrazione, di cui all'art. 53 del DPR 445/2000, effettuata dal sistema in un'unica soluzione, con l'esclusione di interventi intermedi, garantendo l'unicità e la completezza dell'intera operazione; fatti salvi casi di cui al comma 5 del predetto articolo;
- le operazioni di segnatura di protocollo, come specificato dall'art. 55 del DPR 445/2000;
- il reperimento delle informazioni riguardanti i documenti registrati;
- l'assegnazione e la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato;
- la produzione del Registro giornaliero di protocollo e l'invio dello stesso al sistema di conservazione, in un formato idoneo a garantire l'immodificabilità del suo contenuto.

Per ulteriori dettagli sulle funzionalità e sulle misure di sicurezza del sistema informatico di protocollo si rimanda ai successivi paragrafi del Manuale e all'**Allegato 7**.

6.1. Unicità del protocollo informatico

Nell'ambito dell'Amministrazione, il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo, centralizzato o distribuito delle UOP, adottato dall'Amministrazione medesima. Nel caso dell'Università degli Studi di Napoli Federico II, come si è detto già nel capitolo 3, il modello organizzativo adottato dall'Ateneo è distribuito.

La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.



Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo, costituito da almeno sette cifre numeriche.

La documentazione che non è stata registrata presso una UOP viene considerata giuridicamente inesistente presso l'Amministrazione.

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

6.2. Registro informatico di protocollo

Il Registro di protocollo è informatico ai sensi dell'art. 50, comma 2, del DPR 445/2000. Rappresenta lo strumento archivistico attraverso il quale sono registrati tutti i documenti ricevuti, trasmessi e scambiati internamente all'Amministrazione, ad eccezione di quelli non oggetto di protocollazione o per i quali è prevista una registrazione particolare. Rappresenta, inoltre, un atto pubblico di fede privilegiata, che attesta e certifica la presenza dei documenti, garantendone l'autenticità e l'identificazione univoca. Quindi, restituisce agli stessi valore giuridico-probatorio. In conformità alle disposizioni del DPR 445/2000 e del CAD, presso la AOO dell'Ateneo è istituito un Registro ufficiale di protocollo, al quale è associato un domicilio digitale censito nell'IPA e integrato nel sistema di gestione documentale.

6.3. Registrazione di protocollo

La registrazione di protocollo consiste nell'associazione o nell'apposizione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. È un'attività funzionale all'identificazione univoca e certa dei documenti ricevuti, trasmessi o, ove necessario, scambiati internamente all'Amministrazione, restituendo agli stessi un valore giuridico-probatorio, nonché una validazione temporale. Il riferimento temporale ottenuto dalla segnatura di protocollo di cui all'art. 53, comma 1, lettera b) del DPR 445/2000 costituisce validazione temporale, così come riportato all'art. 41, comma 4, lettera a) del DPCM 22.2.2013.

Secondo quanto riportato al par. 3.1.4 delle LLGG. la registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione e per tutti i documenti informatici che non rientrano tra le tipologie specificate dall'art. 53, comma 5, del DPR



445/2000 e che non sono oggetto di registrazione particolare da parte dell'amministrazione, al fine di garantirne l'identificazione univoca e certa.

Le informazioni contenute nella registrazione di protocollo, conformemente alla normativa (l'articolo 53, comma 1, del TUDA), sono:

- il numero di protocollo, generato automaticamente dal sistema;
- la data e l'ora di registrazione, assegnata automaticamente dal sistema;
- il corrispondente (mittente per i documenti ricevuti, uno o più destinatari per i documenti in uscita);
- l'oggetto del documento;
- l'impronta del documento informatico e degli eventuali allegati, generata automaticamente dal sistema;

a cui si aggiungono ulteriori informazioni, ad esempio quelle inerenti all'assegnazione interna all'amministrazione e la eventuale classificazione:

- il numero e la descrizione degli allegati, se presenti;
- i dati identificativi dell'operatore di protocollo e dell'ufficio che ha effettuato la registrazione;
- l'eventuale indicazione se si tratta di un documento riservato o contenente dati particolari;
- la classificazione d'archivio;
- la tipologia di documento nel caso di documenti registrati in serie archivistiche tipologiche.

Nella compilazione dell'oggetto e degli altri metadati inerenti alla registrazione di protocollo devono essere inserite esclusivamente le informazioni strettamente necessarie, evitando l'indicazione di dati personali o di qualsiasi altro elemento non pertinente o eccedente rispetto alla finalità della registrazione stessa.

L'attività di registrazione dei documenti prevede la memorizzazione di un insieme di informazioni obbligatorie, in un'unica soluzione e senza interventi intermedi. Viene effettuata entro la giornata di ricezione o di trasmissione dei documenti. Diversamente, si deve ricorrere alla registrazione differita, che consiste nella protocollazione dei documenti in un momento differente rispetto alla loro acquisizione, come descritto più avanti.

Alcune delle informazioni generate automaticamente dal sistema sono imm modificabili.

Nell'eventuale presenza di errori, è previsto il ricorso ad una procedura di annullamento parziale o totale della registrazione di protocollo, come descritto più avanti nel presente Manuale.

Ai sensi dell'art. 57 del DPR 445/2000, la sequenza numerica di protocollo è unica e progressiva, ed è rinnovata ogni anno solare. Il numero di protocollo, come detto in precedenza, è costituito da almeno sette cifre numeriche. È generato automaticamente



dal sistema e associato al documento. Pertanto, ogni numero di protocollo è immutabile ed individua un solo documento, comprensivo degli eventuali allegati.

6.4. Segnatura di protocollo

La segnatura di protocollo consiste nell'associazione al documento protocollato (o nell'apposizione, in caso di documento cartaceo), in forma permanente e non modificabile, delle informazioni riguardanti il protocollo stesso. Tali informazioni sono memorizzate nel Registro ufficiale di protocollo e consentono di individuare ciascun documento in modo univoco.

Conformemente a quanto previsto dagli artt. 53 e 55 del DPR 445/2000, dagli artt. 9, 20 e 21 del D.P.C.M. 3 dicembre 2013 e dalle LLGG AgID, le informazioni riportate nella segnatura di protocollo sono le seguenti:

- Identificazione anche in forma sintetica dell'Amministrazione o dell'AOO;
- Registro di protocollo;
- Progressivo di protocollo;
- Data di registrazione;
- Oggetto del protocollo.

L'associazione della segnatura di protocollo ai documenti viene effettuata contestualmente alla loro registrazione. In particolare, al termine dell'operazione di registrazione il sistema genera e associa in modo automatico la segnatura ai documenti.

6.5. Registrazione e segnatura XML dei documenti informatici

Ai sensi del Regolamento di Ateneo in materia di Firma Digitale (D.R. 4064 del 31/10/2006), tutti i documenti che rappresentano atti amministrativi dell'Università devono essere informatici e firmati digitalmente e acquisiti nel sistema di gestione informatica dei documenti che consente l'associazione al documento di un insieme di attributi di registrazione univoci ed immutabili e garantisce – tra l'altro – la data certa di formazione dell'atto e la memorizzazione dell'esito delle verifiche sulla autenticità ed integrità del documento digitale all'atto della sua acquisizione.

Se il documento è inviato ad altra AOO o ricevuto da altra AOO, deve essere obbligatoriamente anche registrato nel sistema di Protocollo Informatico (SPI).

I documenti informatici in ingresso oppure in uscita sono di norma rispettivamente ricevuti e trasmessi in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'Amministrazione, oppure delle UOR/UE dell'Amministrazione, oppure, nei casi previsti da specifiche norme, acquisiti mediante strumenti di interoperabilità applicativa (come, ad esempio, le fatture elettroniche o i flussi degli ordinativi di pagamento e incasso), quindi protocollati nel sistema SPI e, dunque, importati nel relativo fascicolo procedimentale gestito in SD.



La registrazione di protocollo di un documento informatico sottoscritto con firma digitale, nel caso di documenti informatici in uscita, viene effettuata direttamente dall'RPA se abilitato, eventualmente per il tramite di personale autorizzato, oppure dall'UOP. In tal caso, il documento, a valle della sua formazione e sottoscrizione, è inviato dall'RPA all'UOP mediante posta elettronica interna. Nel testo della mail sono specificati anche i metadati di registrazione: mittente, destinatario/i, oggetto e voce di classificazione. A seguire, il documento protocollato potrà essere importato in SD nel relativo fascicolo procedimentale da RPA.

In alternativa, il documento è caricato nel fascicolo procedimentale nel sistema SD, eventualmente è perfezionato e firmato digitalmente dai soggetti previsti (oppure può essere firmato esternamente al sistema SD ed essere successivamente caricato nel fascicolo), e quindi è protocollato a partire da tale sistema, direttamente dall'RPA o dall'UOP di competenza.

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati.

Ai fini del procedimento amministrativo, il documento originale è quello sottoscritto digitalmente custodito nell'Archivio digitale dell'Università, gestito quindi dal sistema di gestione informatica dei documenti UniNA.

Per quanto riguarda la segnatrice, nel caso di messaggi ricevuti tramite PEC, SPI acquisisce e inserisce automaticamente come allegato della registrazione di protocollo il file "Segnatrice XML" allegato al messaggio PEC. Per i documenti protocollati in uscita da inviare tramite PEC ad un'altra PA tale file viene generato a partire dai metadati di registrazione di protocollo, sottoscritto con sigillo elettronico qualificato e quindi allegato al messaggio PEC interoperabile trasmesso alla AOO esterna.

La "Segnatrice XML" è un file in formato XML che contiene i dati della segnatrice di protocollo ed altre eventuali informazioni. È lo strumento applicativo riportato nelle LLGG AgID (Allegato 6, Comunicazione tra AOO di Documenti Amministrativi Protocollati) per garantire l'interoperabilità di protocollo via PEC tra i sistemi della PA. Può eventualmente essere utilizzato per implementare meccanismi automatici di registrazione.

Il sistema SD allega il file Segnatrice XML a ciascun documento protocollato in SPI sia quando la registrazione di protocollo è effettuata a partire da SD mediante invocazione delle API di SPI, sia nel caso di importazione del documento importato tramite invocazione delle API di SPI da parte di SD. Tale file non è invece presente in SD se l'utente, con una operazione sconsigliata, scarica da SPI un documento precedentemente registrato e procede quindi a caricarlo nel sistema SD, in un fascicolo procedimentale.



6.6. Registrazione e segnatura dei documenti analogici

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza (il servizio postale pubblico e/o privato o con consegna diretta alla UOP).

La registrazione di protocollo di un documento analogico cartaceo ricevuto da un mittente esterno o inviato a un destinatario esterno viene sempre eseguita in quanto l'Amministrazione ha l'obbligo di registrare l'avvenuta ricezione o spedizione, rispettivamente verso la AOO o a partire dalla AOO. In caso di ricezione di documenti analogici l'UOP deve provvedere ad associare alla registrazione di Protocollo la copia per immagine (scansione) del documento analogico registrato.

La semplice scansione del documento non costituisce una copia conforme, e non solleva quindi l'Amministrazione dall'obbligo di conservazione dell'originale cartaceo.

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un "segno" grafico apposto su un'etichetta autoadesiva apposto sul documento sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- denominazione dell'Amministrazione;
- denominazione della UOR che ha eseguito la registrazione;
- data (facoltativamente, ora) e numero di protocollo del documento.

Nel caso dell'Amministrazione Centrale, la segnatura dei documenti protocollati dall'UOP avviene contestualmente alla acquisizione della copia per immagine del documento, di norma mediante scansione massiva. Per i documenti in partenza, tale segnatura è orizzontale in alto; per quelli in arrivo è verticale a destra.

Nel caso delle restanti UOR, il "segno" grafico è realizzato con una etichetta autoadesiva corredata di codice a barre. L'operazione di acquisizione dell'immagine dei documenti cartacei è in tal caso eseguibile solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.

Il "segno" della segnatura di protocollo deve essere apposto sulla prima pagina dell'originale.

6.7. Documenti esclusi dalla registrazione di protocollo

Come già ricordato, ai sensi di quanto previsto dall'art. 53, comma 5, del DPR 445/2000, sono esclusi dalla registrazione di protocollo:

- le gazzette ufficiali;
- i bollettini ufficiali della PA;
- i notiziari della PA;



- le note di ricezione delle circolari e di altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni (per esempio le bozze di circolari);
- i giornali e le riviste;
- i libri;
- i materiali pubblicitari;
- gli inviti alle manifestazioni;
- tutti i documenti già soggetti a registrazione particolare dell'Amministrazione.

I “documenti già soggetti a registrazione particolare” sono i documenti registrati in repertori dedicati, tenuti nell'ambito del sistema di Ateneo di gestione informatica dei documenti mediante i sistemi SPI e SD quali, ad esempio: Decreti del Rettore, Decreti del Direttore Generale, Decreti dei Dirigenti, Ordini di Servizio, Contratti, Convenzioni con altri Atenei, Contratti del Personale Contrattualizzato, Certificati di Servizio, Fatture attive e passive, Ordinativi di pagamento e incasso, etc. La registrazione in apposito repertorio o registro per una specifica tipologia documentaria è sancita da apposito regolamento di Ateneo o provvedimento diramato a tutte le Unità Organizzative interessate.

L'**Allegato 8** contiene l'elenco e le caratteristiche dei repertori gestiti nell'ambito del sistema documentale (SPI e SD) dell'Ateneo.

Per quanto riguarda i documenti interni, anche formali, scambiati tra le unità organizzative dell'Ateneo, vista l'attuale diffusione del sistema documentale, in accordo con la normativa e le prassi di riferimento in ambito documentale, **ne viene raccomandata la sola acquisizione nel sistema SD e la trasmissione agli interessati esclusivamente mediante il sistema SD**, in modo tale da permettere di tenere traccia dei documenti, classificarli e organizzarli in fascicoli coerenti con la struttura dell'archivio digitale di Ateneo come diffusamente illustrato più avanti nel presente Manuale, facilitando la loro consultazione, la condivisione e la conservazione nel tempo, e di dimostrarne l'esistenza e il contenuto in caso di necessità giuridica o probatoria. Pertanto, la previsione contenuta nell'ODS n. 372 del 13.10.2008 che stabiliva l'obbligo di protocollare tutti i documenti scambiati tra uffici dell'Amministrazione Centrale, in forza dell'adozione del presente Manuale, viene declinata ed estesa a tutte le UOR nel modo seguente: **“le diverse unità organizzative dell'Ateneo registrano i documenti prodotti nell'ambito delle proprie attività istituzionali e li scambiano all'interno della AOO mediante il sistema di gestione documentale e dei flussi e procedono alla loro registrazione di protocollo solo nei casi in cui ciò sia necessario, in base alle caratteristiche giuridiche del procedimento e/o a valutazioni di opportunità tecnico-organizzativa”**.



6.8. Registrazioni nel registro di protocollo particolare

Nell'ambito della gestione del Protocollo Informatico, al fine di garantire particolari forme di riservatezza e di accesso controllato al sistema, è istituito il Protocollo particolare, repertorio del Protocollo generale utilizzato, a discrezione del Rettore e/o del Direttore Generale, per la registrazione:

1. di documenti legati a vicende di persone o a fatti privati o particolari;
2. di documenti di carattere politico e di indirizzo di competenza del Rettore e del Direttore Generale che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
3. di documenti di carattere politico o gestionale dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
4. delle tipologie di documenti individuate dalla normativa vigente (in particolare dall'art. 24 della legge 7 agosto 1990, n. 241, dall'art. 8 del DPR 27 giugno 1992, n. 352, dalla serie di norme collegate al D.lgs. 30 giugno 2003, n. 196, e dal DR 2386 del 17.6.1998 recante le regole di attuazione della citata legge 241/90).

Tali documenti, pur appartenendo al Registro di Protocollo Generale, sono trattati in forma particolare, sia in fase di registrazione, che di scansione e di consultazione, con garanzia di livelli di accesso riservato.

I documenti soggetti a registrazione particolare divengono consultabili alla scadenza dei termini indicati dalla normativa vigente, ovvero, in mancanza dei termini, alla data fissata dal Rettore e/o dal Direttore Generale. Motivate richieste di consultazione potranno essere accolte prima della scadenza dei termini secondo quanto previsto dalla normativa in materia di accesso ai documenti amministrativi.

I documenti particolari sono dotati di un numero di protocollo progressivo nell'ambito del Protocollo generale (secondo quanto sancito dall'art. 57 del DPR 445/2000) e unico (secondo quanto enunciato dall'art. 53, comma 5, del DPR 445/2000). Contestualmente, ad ogni nuova registrazione particolare è assegnato dal SPI un codice univoco e progressivo anche nel repertorio "PP".

Le registrazioni di protocollo particolare, complete delle copie per immagine dei documenti acquisiti, sono eseguite su una postazione di lavoro presso la Segreteria della Direzione Generale da utenti autorizzati all'utilizzo di tale funzionalità del SPI.

La visualizzazione delle registrazioni particolari, al pari della registrazione, è consentita solo agli utenti all'uopo autorizzati.

L'annullamento di registrazioni effettuate nell'ambito del Protocollo particolare deve essere eseguito, previa richiesta scritta a firma del Direttore Generale, dall'Ufficio di Segreteria di Direzione. La richiesta deve contenere le indicazioni sul numero di protocollo da annullare e la motivazione del provvedimento. Le operazioni di



annullamento da eseguire nel SPI sono le stesse utilizzate per l'annullamento di registrazioni di protocollo generale.

La stampa del registro particolare è eseguita da SPI, in automatico, nell'ambito della procedura di stampa del registro giornaliero. Nella stampa del registro, per le registrazioni appartenenti al repertorio PP così come per quelle di protocollo generale, compaiono la data, il numero di protocollo, l'oggetto ed il mittente/destinatario di ciascun documento particolare protocollato.

Il processo di gestione del registro PP è parte integrante di quello del registro di Protocollo Generale.

Infine, l'utilizzo delle funzionalità per la gestione del protocollo particolare e l'accesso alle informazioni collegate ai documenti particolari sono consentiti esclusivamente al Rettore, al Direttore Generale e ai loro incaricati, mediante l'assegnazione di appositi profili di abilitazione.

6.9. Altre tipologie di registri gestiti nel Protocollo Informatico

Per i documenti oggetto di registrazione particolare ai sensi dell'art. 53, comma 5, del DPR 445/2000, nel sistema SPI l'Amministrazione prevede l'istituzione di ulteriori tipologie di registri rispetto al Registro ufficiale di protocollo, quali i Repertori. Tali registri sono implementati e mantenuti nel sistema SPI, e possono avere una visibilità circoscritta e limitata ai soli utenti abilitati da specifici permessi applicativi, in relazione alle caratteristiche di riservatezza della documentazione in essi annotata. In generale, nel paragrafo 7.3.4 sarà trattato il tema della gestione delle aggregazioni documentali per tipologia documentale nell'ambito del complesso sistema di gestione informatica dei documenti.

I Repertori gestiti da SPI sono registri utilizzati per l'annotazione di particolari tipologie di documenti aventi valenza interna e riservata per l'Amministrazione. Dal punto di vista giuridico-formale e applicativo, si tratta di strumenti del tutto simili al Registro ufficiale di protocollo: la numerazione è unica e sequenziale, si rinnova ogni anno solare e restituisce ai documenti il medesimo valore giuridico-probatorio della registrazione di protocollo generale. L'unica differenza che contraddistingue i Repertori dal Registro di protocollo generale riguarda la gestione dei corrispondenti esterni, poiché sono oggetto di repertoriazione particolare tipologie documentarie di valenza interna per l'Amministrazione, per le quali non è prevista la trasmissione verso l'esterno. L'elenco dei repertori attivi attualmente gestiti nei sistemi SPI è riportato in **Allegato 8**, con l'indicazione di quali repertori vengano versati nel sistema di conservazione a norma SD-C.

6.9.1. Registro giornaliero di protocollo e dei repertori gestiti dal Protocollo

Conformemente a quanto previsto dall'art. 53, comma 2, del DPR 445/2000, il SPI garantisce la produzione, la gestione ai fini dell'invio in conservazione del Registro giornaliero di protocollo e del Registro giornaliero di Repertorio, che sono costituiti dall'elenco delle registrazioni effettuate nell'arco di uno stesso giorno rispettivamente sul Registro ufficiale di protocollo e sui Repertori di AOO (come riportato nell'**Allegato 8**).

Come previsto dalle LLGG AgID, il Registro giornaliero è generato in un formato idoneo a garantire la non modificabilità del suo contenuto (formato PDF) e deve esserne garantita l'immodificabilità.

La soluzione realizzata dall'Ateneo è descritta di seguito.

Ogni giorno, ciascun documento recante i metadati relativi alle registrazioni di protocollo e dei repertori gestiti dal Protocollo estratti dal sistema SPI, viene registrato in un repertorio ("RGP") tenuto dallo stesso sistema di protocollo informatico o di gestione documentale. L'oggetto riporterà i codici dei repertori, la data di riferimento e gli intervalli dei numeri di ciascun repertorio contenuti nel report.

Il sistema SPI per ogni documento archiviato calcola e associa alla registrazione in modo immodificabile l'impronta e il riferimento temporale opponibile ai terzi.

La registrazione nel repertorio "RGP" del documento "Registro giornaliero di protocollo" consente di identificare univocamente il documento mediante la sua segnatura archivistica nel repertorio e, ai sensi di quanto riportato nel par. 2.1.1. delle LLG AgID, questa operazione ne garantisce immodificabilità e integrità. Pertanto, decade l'obbligo di trasmissione al sistema di conservazione entro la giornata lavorativa successiva a quella della sua produzione per garantirne l'immodificabilità del contenuto: il processo di conservazione può quindi essere pianificato con una minore frequenza. L'interpretazione dell'Ateneo, sottoposta all'AgID, ha ricevuto il parere favorevole dell'Agenzia (riferimento: Agid.AOO-AgID. Registro Ufficiale (U).0020022.22-12-2015 del 13.10.2015), registrato nel sistema SPI con PG/2015/127082.

RCGD esegue con cadenza annuale il processo di estrazione e trasferimento al sistema SD dei documenti (con i relativi metadati) registrati nel repertorio "RGP". Concluso il trasferimento, tale repertorio viene versato in conservazione, a partire dal sistema SD.

I repertori di cui attualmente viene prodotto il registro giornaliero di protocollo sono riportati nell'**Allegato 8**.

6.9.2. Registro di emergenza

Nel caso in cui la procedura informatica per la registrazione di protocollo sia indisponibile per cause tecniche o per cause di eccezionale gravità, è previsto il ricorso al Registro di emergenza, che è messo a disposizione tramite un modulo stand-alone nel



sistema di protocollo SPI. Tale modulo consente di poter operare in fase di emergenza da una o più postazioni di lavoro, attraverso una procedura di registrazione semplificata, che prevede l'assegnazione automatica della data e del numero progressivo di protocollo e la compilazione manuale degli altri dati minimi di protocollazione.

Il registro di emergenza si configura come un repertorio del protocollo generale. Ciascuna UOR è dotata di un proprio codice di registro assegnato in modo univoco alla struttura, riportato nell'**Allegato 2** e inoltre pubblicato sul sito www.praxis.unina.it.

Il ricorso al Registro di emergenza è autorizzato, sentito RCGD, dal Responsabile della UOR. Tale modalità di registrazione può essere autorizzata per un periodo di tempo non superiore alle 24 ore dall'inizio dell'interruzione del servizio o, in caso di eccezionale gravità, non superiore ad una settimana, conformemente a quanto previsto dall'art. 63 del DPR 445/2000. Il protocollista, a valle dell'autorizzazione ricevuta, dovrà registrare nel registro di emergenza l'atto stesso, prima di procedere con nuove registrazioni sul registro di emergenza.

Il registro di emergenza è lo strumento attraverso il quale, in caso di impossibilità di registrazione informatica, è possibile l'esecuzione delle operazioni di registrazione di protocollo in forma manuale (vedi anche art. 63 DPR 445/2000). Solo in caso di blocco del sistema si può ricorrere al registro cartaceo di emergenza, nel quale si continuerà la registrazione dei documenti assegnando come primo numero quello immediatamente successivo all'ultimo attribuito.

Una volta ripristinata la piena funzionalità del sistema SPI, il Responsabile della UOR provvede quindi (con apposito atto da lui sottoscritto), alla chiusura del registro di emergenza, annotando sullo stesso il numero delle registrazioni effettuate, la data e l'ora di chiusura del registro. Gli operatori UOP precederanno quindi alla registrazione nel sistema SPI dei documenti registrati in emergenza. Alle nuove registrazioni verrà attribuito come primo numero quello immediatamente successivo all'ultimo registrato prima del blocco del sistema e verranno associati gli estremi del registro di emergenza:

- identificativo registro cartaceo
- anno di protocollazione registrato sul registro cartaceo
- numero di protocollazione assegnato sul registro cartaceo.

Le nuove registrazioni potranno così essere ricercate sia con gli estremi del protocollo generale sia con gli estremi del registro di emergenza.

Solo per l'Amministrazione Centrale (il cui codice del registro di emergenza è "RE001"), nel caso di fermo programmato, è disponibile un'applicazione eseguita su postazioni preventivamente installate e configurate presso l'Ufficio di Protocollo. Tale applicazione consente di registrare nel registro di emergenza nuovi documenti e di procedere con l'automatico e sicuro caricamento nel sistema SPI delle registrazioni di emergenza effettuate non appena sono ristabilite le condizioni per il corretto funzionamento del sistema mediante l'apposita funzione informatica di recupero dei dati. Le modalità



operative sono riportate nell'apposita guida consultabile sul sito Praxis, nella sezione Protocollo Informatico/Manuali e Guide.

In generale, documenti annotati nel registro di emergenza e successivamente registrati nel protocollo generale recheranno, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo generale.

6.10. Annullamento parziale o totale di protocollo

Nell'eventuale presenza di errori sostanziali, o per motivate e comprovate ragioni, è possibile ricorrere all'operazione di annullamento totale o parziale delle registrazioni di protocollo, che può essere effettuata da utenti opportunamente abilitati, utilizzando apposite funzionalità del sistema finalizzate ad assicurare che:

- le informazioni relative ad alcuni metadati di registrazione (ad esempio, l'oggetto, il mittente/destinatario, il file primario e/o i file allegati) di una registrazione di protocollo non possano essere modificate, ma solo annullate con una specifica procedura conforme alle disposizioni di cui all'art. 54 del DPR 445/2000 che prevede la storicizzazione delle informazioni annullate e modificate, rendendole visibili e comparabili agli utenti autorizzati;
- sia possibile modificare le ulteriori informazioni di una registrazione di protocollo quali, ad esempio: l'assegnazione interna all'Amministrazione, la classificazione, il mezzo di trasmissione, etc.

L'annullamento totale consiste nell'annullamento dell'intera registrazione di protocollo. Tale operazione può essere effettuata dai soli utenti abilitati e previa autorizzazione del RGD di UOR, indicandone la motivazione e gli estremi del provvedimento autorizzativo, come richiesto dalla normativa vigente. Il protocollista, a valle del processo di autorizzazione, provvederà a protocollare l'atto, immettendo in fase di registrazione, le seguenti informazioni:

1. nel campo mittente e destinatario, la propria UOR/UO;
2. nel campo oggetto, l'oggetto della nota di annullamento, con il numero di protocollo (PG) da annullare;
3. nel campo note (facoltativamente) la motivazione dell'annullamento.

Tale operazione è da svolgersi preliminarmente all'avvio della procedura di annullamento che è costituita dalle tre fasi di seguito riportate:

- A. inserimento dell'atto precedentemente protocollato nell'elenco degli atti di autorizzazione all'annullamento,
- B. associazione dell'atto di autorizzazione alla registrazione di protocollo da annullare: quest'ultima assume lo stato di "annullabile",
- C. annullamento vero e proprio della registrazione di protocollo.

In tale ipotesi l'applicazione riporta la data, l'ora e l'autore dell'operazione di annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata



dal Responsabile UOR/UOP, nonché la dicitura “annullato” in posizione visibile e tale da consentire la lettura di tutte le informazioni originarie.

Le operazioni precedentemente elencate sono dettagliatamente illustrate nel “Manuale Operativo del Protocollo” disponibile sul sito dell’eGovernment Praxis.

L’annullamento parziale consiste, invece, nella modifica di alcuni dati obbligatori della registrazione, quali quelli relativi a:

- i corrispondenti e i rispettivi indirizzi di spedizione, che possono essere annullati o integrati con l’inserimento di nuovi mittenti/destinatari (in base alle modalità di registrazione);
- l’oggetto del protocollo;
- il file del documento principale protocollato.

Conformemente a quanto disposto dall’art. 54 del DPR 445/2000 e dalle LLGG AgID, tali operazioni di modifica sono tracciate nel sistema sotto la voce “Dati annullati” ed è inoltre garantita l’accessibilità ai dati originari eventualmente annullati, integrati o rettificati.

6.11. Differimento delle registrazioni

Nel caso di un temporaneo ed eccezionale carico di lavoro che non permetta di evadere la corrispondenza ricevuta nella medesima giornata lavorativa o comunque entro 24 ore dal ricevimento e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi (ad esempio per la registrazione di un consistente numero di offerte ad un bando di gara in scadenza), il Responsabile UOR può autorizzare l’uso del protocollo differito.

Il protocollo differito consiste nel differimento della decorrenza giuridica dei termini di arrivo del documento rispetto alla data di registrazione, dichiarandone espressamente la data effettiva di arrivo, le motivazioni del ritardo e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.

Il ricorso al protocollo differito si applica solo ai documenti in arrivo ed è autorizzato dal responsabile UOR, anche su motivata richiesta dell’RPA, mediante la sottoscrizione di un provvedimento di autorizzazione in cui si riportano le motivazioni del differimento, la data e ora di effettivo arrivo dei documenti, il numero e la descrizione dei documenti e la data entro la quale la registrazione di protocollo sarà eseguita.

Agli interessati, se necessario, viene dunque resa nell’immediato una ricevuta di consegna priva del codice di protocollo.

In pratica, nel caso di documenti analogici, il responsabile UOR (oppure dell’UOP), a valle della registrazione di protocollo del provvedimento di differimento delle operazioni di registrazione, provvede a chiudere in un plico o in un armadio chiuso a chiave o in una



stanza chiusa a chiave i documenti da protocollare. Nel caso di documenti informatici pervenuti via PEC o interoperabilità, questi resteranno memorizzati nella cartella PEC di consegna, oppure nell'area temporanea di appoggio disponibile nel SPI, per poi essere successivamente registrati.

All'atto della registrazione dei documenti di cui è stato autorizzato il differimento della protocollazione, l'operatore di protocollo valorizza quindi il campo "data e ora arrivo", nella maschera di protocollazione differita, e collegherà inoltre ciascuna registrazione differita al codice di protocollo del provvedimento di differimento sottoscritto dal responsabile UOR.

A conclusione delle operazioni di registrazione, il documento protocollato è collegato in modo indissolubile al provvedimento di autorizzazione. Nei dettagli sarà anche mostrata l'ora di effettivo arrivo del documento, attestata anche dal provvedimento di autorizzazione.



7. ALTRE ATTIVITÀ DI GESTIONE DOCUMENTALE

Oltre alla registrazione di protocollo, le altre operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti e dei flussi documentali, ai sensi degli artt. 56 e 65 del DPR 445/2000, sono la classificazione e la fascicolazione dei documenti. Tali attività sono effettuate nei sistemi SPI e SD, nella fase corrente dell'archivio utilizzando apposite funzionalità del sistema di gestione informatica dei documenti.

7.1. Classificazione

L'attività di classificazione consiste nell'associazione al documento di un indice o codice di classificazione desunto dal Titolario dell'Ente, al fine di collegare logicamente i flussi documentali gestiti nella fase corrente dell'archivio a specifiche funzioni, competenze o materie in carico all'Amministrazione.

In particolare, la classificazione consente di organizzare, in modo stabile e ordinato, la sedimentazione dei documenti che costituisce l'archivio dell'Amministrazione, secondo uno schema logico denominato Titolario o Piano di classificazione, descritto nel successivo paragrafo del presente Manuale.

Ai sensi dell'art. 52, art. 1, comma f) del DPR 445/2000 e delle LLGG AgID, sono oggetto di classificazione tutti i documenti che entrano a far parte del sistema di gestione informatica dei documenti, indipendentemente dal loro formato o dal fatto che siano protocollati o meno.

La classificazione, quindi, è considerata un'attività obbligatoria per legge ed è funzionale alla ricerca dei documenti, poiché ne facilita il reperimento. Inoltre, grazie all'integrazione del Titolario di classificazione con il Piano di conservazione, prevista ai sensi dell'art. 68 del DPR 445/2000, si assicura una gestione efficiente del processo di selezione e di conservazione della documentazione nella fase di deposito dell'archivio.

Nel disciplinare le attività di gestione documentale, presso l'Amministrazione si prevede lo svolgimento dell'attività di classificazione secondo due modalità:

- contestualmente alla acquisizione/registrazione del documento;
- dopo l'assegnazione del documento.

In quest'ultimo caso, nel sistema SPI la classificazione è demandata agli utenti delle UOR/UO competenti in materia, che ricevono per competenza il documento, mentre nel sistema SD il documento ricevuto potrà essere spostato/copiato in nuovo fascicolo, collegato a una differente voce di classificazione.



7.2. Titolare di classificazione

Il Titolare di classificazione è un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base della organizzazione funzionale dell'Amministrazione, permettendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.

Il DPR 445/2000 sancisce – tra l'altro – che per la tenuta del sistema informativo automatizzato finalizzato alla gestione del protocollo informatico e dei procedimenti amministrativi, oltre alle operazioni di registrazione e di segnatura di protocollo, è necessaria anche quella di classificazione dei documenti, effettuata sulla base di un adeguato piano di classificazione d'archivio (o titolare) definito da ciascuna amministrazione. In questo modo, il sistema di gestione informatica dei documenti può fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato e consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento.

Il piano di classificazione è quindi uno schema logico per organizzare i documenti d'archivio, è uno strumento di ordinamento ed organizzazione funzionale dei documenti che ne consente il facile reperimento, la soggettazione e l'indicizzazione. Mediante il piano di classificazione, è inoltre possibile recuperare e consultare l'archivio secondo le modalità stesse in cui i documenti sono stati ordinati nel corso del quotidiano lavoro amministrativo. Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente; le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella funzione descritta dal titolo, secondo un'articolazione gerarchica.

Il Titolare è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali e/o regionali. L'aggiornamento del Titolare compete esclusivamente al vertice dell'Amministrazione. La revisione anche parziale del Titolare viene proposta da RCGD quando è necessario ed opportuno. Dopo ogni modifica del Titolare, RCGD provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Il Titolare non è retroattivo: non si applica, cioè, ai documenti registrati prima della sua introduzione. Viene garantita la storicizzazione delle variazioni di Titolare e la possibilità di ricostruire le diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del Titolare vigente al momento della produzione degli stessi. Inoltre, per ogni modifica di una voce viene riportata la data di introduzione e la data di variazione. Di norma le variazioni vengono introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo Titolare e valgono almeno per l'intero anno.



Il Titolario è elaborato da RCGD e, a valle della revisione effettuata da un gruppo di lavoro individuato dal Direttore Generale, viene emanato con apposito decreto del Direttore Generale.

L'Amministrazione, in accordo con le prescrizioni normative sopra richiamate, il 1° gennaio 2007 ha istituito il Protocollo Generale di Ateneo e contestualmente ha avviato l'esercizio del sistema di Protocollo Informatico utilizzando, **in via transitoria**, il Titolario adottato nel 2000 dalla sola Amministrazione Centrale. A seguire, ha quindi operato la revisione del Titolario stesso, per adeguarlo al quadro normativo vigente e alla struttura organizzativa dell'Ateneo e per renderlo idoneo a soddisfare le esigenze di classificazione dei documenti di tutte le strutture dell'Ateneo.

Il Titolario è gestito tramite funzionalità del sistema SPI ed è importato nel sistema SD che ne recepisce tutte le modifiche e vi accede in sola lettura.

Al fine di facilitare l'individuazione e l'assegnazione a ciascun documento del codice di titolazione corretto, RCGD ha provveduto alla predisposizione ed alla pubblicazione del "thesaurus" contenente la descrizione di ciascun titolo/classe con un sintetico riepilogo dei contenuti di ciascuna voce di titolazione ed esempi di classificazione di alcuni tra i più rilevanti procedimenti amministrativi al seguente indirizzo:

<https://www.praxis.unina.it/protocollo-sistema-ateneo>

L'attuale versione del Titolario, approvata con decreto del Direttore Generale n. 614 del 30 luglio 2021, è riportata in **Allegato 5**.

7.3. Fascicolazione

La fascicolazione è l'attività che consente di organizzare la sedimentazione dei documenti in modo stabile e ordinato, facilitandone la ricerca e il reperimento, contribuendo, quindi, all'assolvimento dei diritti sull'accesso previsti dalla normativa attualmente in vigore (d.lgs. 33/2013, l. 241/1990, d.lgs. 97/2016, art. 124 del Codice dei beni culturali e del paesaggio).

La fascicolazione elettronica è stata disciplinata dalle LLGG AgID e consiste nella riconduzione logica dei documenti all'interno delle unità di aggregazione documentale (i fascicoli, le serie tipologiche) che ne raccolgono i precedenti, al fine di mantenere vivo il vincolo archivistico che lega ogni singolo documento alla rispettiva pratica.

Ai sensi dell'art. 64, comma 4, del DPR 445/2000, sono oggetto di fascicolazione sia i documenti protocollati nel SPI, sia i documenti non protocollati ma registrati nel SD, che concorrono tuttavia allo svolgimento delle attività amministrative.



I procedimenti, gli affari, le pratiche e le attività svolte dall'Ateneo sono gli elementi vitali dell'Ente, in quanto rispecchiano le sue funzioni pratiche, amministrative e giuridiche. Pertanto, è necessario avere cura dell'adeguata produzione dei fascicoli procedurali al fine di gestire correttamente l'Archivio digitale dell'Ateneo, dalla sua formazione fino alla conservazione.

7.3.1. Aggregazioni documentali informatiche

L'aggregazione documentale informatica è l'unità di base nella formazione dell'archivio dell'Ente che, in accordo con quanto riportato nell'all. 1 delle LLGG AgID, si caratterizza come l'insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'Ente.

7.3.2. Il Fascicolo informatico

Il fascicolo informatico, coerentemente con quanto riportato nell'all. 1 delle LLGG AgID, è un'aggregazione strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di un'attività o allo svolgimento di uno specifico procedimento.

Il fascicolo informatico assicura la gestione e la consultabilità dei documenti informatici in esso contenuti, con piena efficacia giuridica e amministrativa.

In base alla complessità del suo contenuto documentale, può essere strutturato in una serie di sotto-fascicoli. In relazione al formato dei documenti in esso contenuti, si distinguono tre tipologie di fascicoli:

- elettronico,
- cartaceo,
- ibrido.

Quest'ultimo raccoglie sia documenti in formato analogico, sia documenti informatici, tutti afferenti alla medesima pratica. Per tale tipologia di fascicolo sono previste specifiche modalità di gestione finalizzate al mantenimento del collegamento logico tra documenti distribuiti in spazi informativi distinti.

Nel fascicolo viene mantenuto il c.d. vincolo archivistico, ovvero quel collegamento logico che lega i documenti tra loro, e che ne regola la sedimentazione nel tempo. Pertanto, le cartelle del pc o di rete, file system (anche in cloud) o gestiti con sistemi di collaboration, non sono fascicoli informatici poiché non hanno le caratteristiche e i requisiti previsti dalla normativa in materia di gestione dei documenti informatici e dell'archivio di un ente.

Le LLGG AgID hanno normato la fascicolazione elettronica, prevedendo cinque tipologie standard di fascicolo e l'insieme dei metadati che corredano ciascuna di esse. Tali tipologie sono configurate nel sistema SD e sono messe a disposizione degli Utenti per lo svolgimento delle attività di fascicolazione.



A seguire, si riportano le descrizioni di ciascuna tipologia di fascicolo, in base a quanto indicato nell'Allegato 5 alle LLGG AgID.

1 Fascicolo per procedimento amministrativo: *«conserva una pluralità di documenti individuati da norme, tra loro collegati e tutti diretti alla produzione (all'interno di una procedura) di un unico atto conclusivo con rilevanza esterna, denominato provvedimento amministrativo, con il quale un'autorità amministrativa manifesta la propria volontà, nell'esercizio dei suoi poteri».*

2 Fascicolo per affare: *«conserva i documenti amministrativi relativi a una competenza non proceduralizzata né procedimentalizzata, per la quale, dunque, non è prevista l'adozione di un provvedimento finale, inteso come atto dotato di capacità di incidere nella sfera giuridica di terzi. Il fascicolo per affare ha una data di apertura e una durata circoscritta».*

3 Fascicolo per attività: *«comprende i documenti amministrativi prodotti nello svolgimento di un'attività amministrativa semplice, che implica risposte obbligate o meri adempimenti proceduralizzati, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale».*

4 Fascicolo per persona fisica: *«comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte».*

5 Fascicolo per persona giuridica: *«comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte».*

In generale,

- La classificazione dei singoli documenti corrisponde a quella del fascicolo a cui appartengono;
- La gestione del fascicolo spetta alla struttura produttrice, per il tramite dei propri incaricati, in quanto competente a trattare la documentazione relativa allo specifico procedimento. Tale struttura è responsabile della corretta tenuta del fascicolo;
- Il fascicolo informatico può contenere documenti nativi digitali, duplicati, copie immagini (scansioni) e copie informatiche di documenti analogici;
- I documenti all'interno del fascicolo si stratificano nell'ordine cronologico di registrazione e possono essere ordinati e visualizzati dal più recente al più vecchio o viceversa.



Il sistema SD eDocumento implementa tutte le tipologie di fascicolo precedentemente elencate.

Gli incaricati preposti alla gestione documentale della propria UOR/UE e gli RPA devono evitare di:

- creare un fascicolo per ogni singolo documento;
- creare fascicoli come macro-aggregazioni generiche, non corrispondenti a specifici procedimenti;
- duplicare fascicoli precedentemente inseriti oppure crearne di vuoti (da annullare se non utilizzati o creati per errore).

Nei fascicoli gestiti da SD trovano collocazione i documenti nella versione definitiva o nello stato di elaborazione che deve essere condiviso con altri nel sistema per arrivare alla loro definizione, anche attraverso alcuni passaggi formali (ad esempio: approvazione, firma).

Tutto ciò che costituisce la fase preliminare di formazione del documento (bozze, proposte, primi elaborati, report di controllo, appunti etc.) solo eccezionalmente troverà collocazione all'interno del fascicolo nel sistema documentale: a differenza di quello che può avvenire per i fascicoli cartacei e le cartelle su pc o server, di regola nel sistema documentale si collocano solo i documenti nella loro versione definitiva. Tutto quello che attiene i materiali preparatori e di lavoro per arrivare alla formazione del documento trova posto negli ambiti preposti alla gestione endo-procedimentale e viene gestito con gli strumenti informatici ritenuti più idonei in base al procedimento.

Ogni fascicolo può essere ripartito in più sotto-fascicoli in funzione della quantità, dell'articolazione del suo contenuto e/o delle varie fasi/attività del procedimento. Il sotto-fascicolo mantiene il codice di classificazione del fascicolo padre e la sua segnatura archivistica è ottenuta da quella del fascicolo padre, con l'aggiunta di un numero progressivo preceduto da un punto fermo.

Un documento potrà risiedere anche in più fascicoli, a seconda dei procedimenti in cui è inserito. In tal caso, il file che rappresenta il documento sarà unico e le varie copie saranno tra di loro distinte solo per la componente dei metadati. Sotto il profilo della conservazione, questo implica che quel documento sarà presente nel sistema fino a quando ci sarà almeno un fascicolo che lo conserva.

Ciascuna UOR/UE deve adottare regole pratiche per strutturare e valorizzare l'oggetto e la descrizione di ciascun fascicolo, in modo tale che:

- la sequenza e informazioni seguano regole standard e omogenee per una data procedura;



- le informazioni riportate seguano una gerarchia dal generale al particolare;
- siano evitate parole generiche;
- siano utilizzate sintetiche frasi di senso compiuto con indicazioni precise su “di cosa tratta” il fascicolo;
- se possibile, inserire nella descrizione almeno una parola chiave per facilitare le successive ricerche;
- evitare di attribuire a fascicoli diversi stesso oggetto e/o descrizione.

Ai sensi dell’art. 41 del CAD, l’Ateneo gestisce i procedimenti amministrativi utilizzando le funzionalità del sistema di gestione documentale e le tecnologie dell’informazione e della comunicazione. Per ciascun procedimento amministrativo di sua competenza fornisce gli opportuni servizi di interoperabilità e di integrazione. Raccoglie nei fascicoli informatici gli atti, i documenti e i dati del procedimento medesimo da chiunque formati.

Il fascicolo informatico gestito dal sistema SD, al pari delle restanti aggregazioni documentali, è realizzato garantendo la conformità ai principi di una corretta gestione documentale e alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico. Esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e il collegamento logico tra i documenti in esso contenuti. Inoltre, il fascicolo informatico è costituito in modo da garantire l’esercizio del diritto di accesso ai sensi della l. 241/1990 e del d.lgs. 33/2013, nonché l’immediata conoscibilità dello stato di avanzamento del procedimento, del nominativo e del recapito elettronico del responsabile del procedimento. A tal fine, il fascicolo informatico reca, tra l’altro, l’indicazione:

- dell’amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- del responsabile del procedimento;
- dell’oggetto del procedimento;
- dell’elenco dei documenti contenuti nel fascicolo;
- presenza o meno di dati riservati e/o personali particolari;
- dell’identificativo del fascicolo medesimo, apposto con modalità idonee a consentirne l’indicizzazione e la ricerca attraverso il sistema.

Inoltre, il fascicolo informatico “procedimentale”, nel sistema SD, reca tutti i metadati previsti nell’Allegato 5 delle LLGG AgID, esportabili in formato xml all’occorrenza.

A tali tipologie di fascicolo possono, eventualmente, avere accesso solo gli utenti abilitati e individuati dall’Amministrazione.

7.3.3. Piano di fascicolazione

Il Piano di fascicolazione è lo strumento archivistico attraverso il quale sono individuate le tipologie di fascicolo più idonee per l'organizzazione dei documenti e dei flussi documentali afferenti a determinate voci del Titolare di classificazione, ovvero a determinate funzioni e attività dell'Amministrazione.

Il Piano è stato definito dall'Ateneo conformemente a quanto disposto all'art. 64, comma 4, del DPR 445/2000, ed è stato integrato con il Titolare di classificazione e con il Piano di conservazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti, ai sensi dell'art. 68, comma 1, del DPR 445/2000, e nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali.

Per i fascicoli di tipo 1, 2 e 3 (denominati "procedimentali"), ai sensi delle LLGG AgID, nel sistema SD è stato integrato il **Catalogo dei procedimenti dell'Amministrazione**, consentendo agli utenti di selezionare i procedimenti (procedimenti amministrativi, affari o attività) a cui afferiscono i fascicoli e di valorizzare automaticamente i campi descrittivi relativi ai dati di classificazione collegati a ciascun procedimento. Tale catalogo può essere oggetto di revisione e di aggiornamento, in caso di variazione del Titolare di classificazione a cui è integrato, o in relazione alle specifiche necessità dell'Ente.

La gestione del predetto catalogo è effettuata da parte degli Amministratori di Sistema grazie a una funzionalità disponibile nel sistema SG che consente l'inserimento di un nuovo procedimento (associandolo alla relativa voce di titolare), la modifica di un procedimento esistente, oppure la cessazione, oppure l'eliminazione (consentita solo nel caso di procedimento non associato ad alcun fascicolo).

Il fascicolo procedimentale viene chiuso da RPA al termine del procedimento amministrativo o all'esaurimento dell'affare o dell'attività.

I fascicoli procedimentali possono essere associati logicamente a "super-fascicoli", relativi a persone fisiche o giuridiche, secondo l'organizzazione.

Per quanto riguarda il sistema SPI, attualmente, l'apertura di un fascicolo informatico è eseguita in automatico, in base alla voce di classificazione prescelta del documento, qualora per l'anno di riferimento non esista già un fascicolo relativo lo stesso titolo.classe per la data UOR protocollante.

Maggiori dettagli sono riportati nell'**Allegato 8**.

7.3.4. Altre aggregazioni documentali informatiche

Le serie documentarie (o repertori) sono le aggregazioni che raggruppano documenti aventi tipologia omogenea, ma difforni per contenuto, ed ordinati in sequenza cronologica. Un esempio di tale tipologia di aggregazione documentale sono i repertori

dei decreti o dei verbali. In **Allegato 8** è riportato l'elenco dei repertori attualmente gestiti nel sistema SPI e nel sistema SD.

Le serie di fascicoli sono costituite da fascicoli accorpate per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli: il sistema SD offre funzionalità applicative per la visualizzazione di tali serie.

7.3.5. Modalità operative per la fascicolazione dei documenti

In aggiunta a quanto già riportato in modo generale per un corretto trattamento dei fascicoli informatici, di seguito si riportano ulteriori raccomandazioni specifiche per la gestione dell'archivio digitale dell'Università.

Ciascuna UOR/VO afferente dell'Ateneo è tenuta a garantire la gestione delle pratiche di propria competenza.

È demandato al Responsabile UOR o al Capo Ufficio della VO o al Responsabile del procedimento amministrativo (RPA o RUP) o dell'affare di propria competenza, e agli utenti da loro incaricati, il compito di garantire la corretta creazione e tenuta dei fascicoli, in conformità alle disposizioni di cui all'art. 64, comma 4, del DPR 445/2000.

Ai fascicoli si applicano i criteri di visibilità stabiliti dal Responsabile, al fine di circoscriverne l'accesso ai soli utenti abilitati. Tali criteri sono rappresentati dalle Liste di competenza (Access Control List – ACL), che definiscono l'insieme degli utenti e/o degli uffici abilitati al loro accesso, profilandone i rispettivi permessi, e sono configurate nel sistema di gestione documentale per essere associate ai fascicoli fin dalla fase della loro creazione.

La creazione dei fascicoli informatici procedurali in SD avviene utilizzando specifiche funzionalità messe a disposizione dal sistema, accessibili agli utenti che dispongono di adeguata abilitazione (per ulteriori dettagli sui permessi applicativi associati a tale ruolo si rimanda all'**Allegato 6**).

Nel caso in cui un documento dia luogo all'avvio di una nuova pratica o di un nuovo procedimento amministrativo, è prevista l'apertura ex novo del fascicolo. Con l'apertura di un fascicolo viene eseguita la registrazione di un insieme minimo di informazioni, tra le quali:

- il procedimento di riferimento;
- il codice di classificazione associato al procedimento selezionato;
- il Responsabile del fascicolo;
- l'oggetto del fascicolo;
- la descrizione del fascicolo;
- l'identificativo univoco del fascicolo, generato e associato automaticamente dal sistema;
- la data di apertura, valorizzata automaticamente dal sistema;



- la presenza di documenti ad accesso limitato (riservati e/o contenenti dati particolari).

Per il fascicolo di tipo procedimentale (relativo a procedimento amministrativo, affare o attività) sono previsti ulteriori dati riguardanti il procedimento stesso, come descritto nel par. 7.3.2 del presente Manuale.

In presenza di un documento da inserire in un fascicolo, il soggetto deputato alla fascicolazione (UOR, oppure l'Ufficio di prima assegnazione), stabilisce se il documento si colloca nell'ambito di un procedimento in corso, oppure se dà avvio ad una nuova pratica. In funzione della scelta, si potranno prevedere le seguenti casistiche.

- a. Nel caso in cui il documento afferisca ad una pratica o a un procedimento in corso, per il quale esiste un fascicolo già memorizzato nel sistema, si dovrà:
 - ricercare e selezionare il fascicolo di interesse;
 - inserire il documento protocollato nel fascicolo selezionato, avendo cura di valorizzarne la tipologia documentale.

Nel caso in cui si trattasse di un documento su supporto cartaceo, si dovrà acquisire tramite scanner la copia digitale del documento analogico, inserendola nel fascicolo elettronico, secondo quanto riportato nel paragrafo 5.2, e assicurare la riconduzione fisica del documento originale analogico nel relativo carteggio detenuto dall'Ufficio responsabile.

- b. Nel caso in cui il documento avvii una nuova pratica o un nuovo procedimento, si dovrà:
 - creare un nuovo fascicolo, valorizzandone i metadati, tra cui il procedimento;
 - inserire il documento protocollato nel fascicolo, avendo cura di valorizzarne la tipologia documentale;
 - eventualmente assegnare il fascicolo mediante condivisione oppure workflow ad altre unità organizzative coinvolte nel procedimento.

È prevista la possibilità che uno stesso documento possa essere inserito in diversi fascicoli (mediante l'operazione di copia) e, quindi, che possa afferire a diverse pratiche. A tal fine, il sistema documentale SD mette a disposizione specifiche funzionalità di ricerca, che restituiscono l'elenco dei fascicoli nei quali è contenuto il documento.

Un documento collocato in un fascicolo procedimentale gestito dal sistema documentale SD può essere anche repertoriato (in tal caso acquisisce in automatico la tipologia documentale relativa al repertorio prescelto) e, se necessario, può essere anche protocollato nel sistema SPI, diventando in tal caso non più modificabile nel sistema SD.

Il fascicolo, in base alla complessità del suo contenuto documentale, può essere strutturato in sotto-fascicoli e in ulteriori sotto-unità, gli inserti, ciascuno collegato allo stesso procedimento del fascicolo padre, oppure differente.



La visibilità del fascicolo governata dalla Lista di competenza ad esso associata può essere temporaneamente estesa ad altri utenti o uffici non censiti nella stessa, attraverso il flusso di assegnazione dello stesso. Le modalità di assegnazione del fascicolo previste dalle LLGG AgID sono per Conoscenza e per Competenza. Attraverso quest'ultima modalità, viene estesa all'ufficio/utente assegnatario anche parte dell'operatività sul fascicolo. In caso di errore nell'assegnazione del fascicolo, l'UOR è tenuta a correggere le informazioni inserite nel sistema e a riavviare la procedura di assegnazione del fascicolo all'ufficio competente. Nel sistema documentale viene tenuta traccia di tutti gli eventi di assegnazione, memorizzando per ciascuno di essi l'identificativo dell'utente, la data e l'ora dell'operazione. Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento della pratica e viene così collocato nell'archivio di deposito gestito da SD. Tale stato è comunque ancora reversibile e, all'occorrenza, il fascicolo può essere riaperto e portato in archivio corrente, al fine di consentire la ripresa e la prosecuzione delle attività procedimentali, ove necessario.

Non sono comunque previsti dei limiti massimi di giacenza dei fascicoli nel sistema corrente, poiché le tempistiche dipendono dalla natura della pratica e dell'attività a cui essi afferiscono.

I fascicoli di pratiche concluse e non più utili ai fini dello svolgimento delle attività amministrative correnti, per le quali vige l'obbligo di conservazione, potranno essere versati in conservazione a cura del responsabile al Versamento e trasferiti così all'archivio di deposito gestito dal componente SD-C, così come descritto al successivo paragrafo 9.1.2, anche se, alla data, come già precedentemente detto, sono versati in conservazione da RCGD solo i repertori del sistema di gestione informatica dei documenti dell'Università.

8. MODELLO ORGANIZZATIVO PER LA GESTIONE DEI FLUSSI DOCUMENTALI

I flussi documentali si distinguono in flussi in *entrata*, in *uscita* e *interni*.

Nel modello organizzativo per la gestione dei flussi documentali adottato dall'Ateneo è prevista una **gestione decentrata** per i flussi in entrata, in uscita e interni, al fine di consentire alle singole UOR di operare in **piena autonomia**.

8.1. Mezzi di spedizione

In base alla tipologia di formato dei documenti, variano i mezzi di spedizione utilizzati per la loro ricezione e trasmissione. In particolare, per i documenti informatici sono da prediligere i canali telematici di comunicazione quali la PEC, la PEO, lo stesso sistema di gestione informatica dei documenti (per le comunicazioni "intra AOO") e i Web Services; per la documentazione in formato cartaceo, invece, si ricorre ai servizi postali, al corriere o alla consegna *brevi manu*.

In conformità all'art. 47, comma 3, del CAD, alla AOO dell'Ateneo è associato un domicilio PEC pubblicato sull'IPA e associato al Registro generale di protocollo, attraverso il quale vengono ricevute e trasmesse le comunicazioni oggetto di protocollazione.

L'Amministrazione ricorre prioritariamente alla PEC o alla cooperazione applicativa per lo scambio di documenti con altre pubbliche amministrazioni, in conformità alle disposizioni di cui all'art. 47, comma 1, del CAD e delle LLGG AgID. Ai sensi dell'art. 45 del CAD, i documenti trasmessi tramite PEC sono idonei ad accertarne la provenienza e soddisfano il requisito della forma scritta. Di conseguenza, la loro trasmissione non deve essere seguita da quella del documento originale, eventualmente in formato analogico.

A tal fine, nel sistema di protocollo sono integrati i domicili digitali di ciascuna UOR istituita presso l'Amministrazione. Il sistema mette a disposizione specifiche funzionalità per la gestione della corrispondenza e delle ricevute PEC, le quali sono considerate strumenti di certezza giuridica da mantenere all'interno del nucleo di protocollo, poiché equivalgono alla notificazione per mezzo della posta. In particolare, il sistema consente di inserire in modo automatico le ricevute PEC tra gli allegati del protocollo, garantendone il mantenimento nel tempo.

Il sistema SPI dialoga con il sistema di posta elettronica certificata (PEC) secondo le specifiche tecniche dell'interoperabilità sancite nell'Allegato 6 alle LLGG AgID mediante il componente Mail Connect (MC) che si occupa della interconnessione, del collegamento e integrazione del protocollo informatico con la posta elettronica



certificata al fine di semplificare le operazioni di registrazione di protocollo, in ingresso e in uscita. Alla data, sono abilitate all'utilizzo di tale funzionalità tutte le UOR di primo livello dell'Ateneo (le Aree dell'Amministrazione Centrale, i Dipartimenti, le Scuole e i Centri), oltre ad alcune UO che, per la tipologia dei procedimenti gestiti, ne hanno fatto esplicita richiesta.

Per la corrispondenza ricevuta tramite PEC, il sistema MC provvede automaticamente a collegare alla registrazione di protocollo il messaggio originale dell'e-mail (in formato .eml), il file della Segnatura XML e gli altri eventuali documenti allegati all'e-mail, come illustrato con maggiore dettaglio nel manuale "Interoperabilità e integrazione con il sistema PEC" disponibile all'indirizzo: <https://www.praxis.unina.it/protocollo-guide-manuali>.

Nel caso di UOR/UO non attiva sul sistema di interoperabilità MC, i dati e metadati con le istruzioni per la registrazione di protocollo del messaggio PEC ricevuto vengono inviati via PEO all'UOP competente. Più in dettaglio, il messaggio PEO inviato conterrà l'oggetto della registrazione, il mittente, il/i destinatario/i, la voce di Titolare da utilizzare, l'identificazione del documento primario nel caso in cui il messaggio reca più di un documento allegato, i singoli documenti allegati al messaggio PEC originario, nonché il messaggio PEC originario in formato .eml. Qualora debba essere allegato anche il testo della mail originaria, verrà allegato al messaggio PEO anche il file prodotto dallo scarico del testo del messaggio originario (in formato pdf/a). L'Ufficio protocollo registrerà quindi il documento primario e tutti gli eventuali allegati, utilizzando i metadati e le istruzioni forniti dall'Ufficio primo assegnatario.

Per quanto riguarda le comunicazioni "intra AOO" di documenti amministrativi, il mezzo di trasmissione preferenziale da utilizzare è il sistema SD, con le funzionalità di condivisione oppure di invio mediante workflow.

I flussi generalizzati riportati di seguito possono essere adottati dalle singole UOR afferenti all'Amministrazione Centrale **in forma semplificata**, dandone preventiva comunicazione alla Direzione Generale. Per il dettaglio, si rimanda al "Modello dei processi di gestione documentale" riportato in allegato al presente Manuale (Allegato 3) in cui sono riportate anche le disposizioni impartite dal Direttore Generale per la **gestione dei flussi documentali presso i Dipartimenti e i relativi Uffici**.

8.2. Flussi documentali in entrata

8.2.1. Descrizione generale

I documenti, analogici oppure informatici, in ingresso ad una data UOR dell'Amministrazione possono essere di tipo "Entrata" se inviati da un soggetto esterno all'AOO (altra PA, cittadino, società esterna, professionista, dipendente) oppure possono



essere originati da altra UOR/UE dell'Ateneo (in tal caso sono definiti "Tra Uffici"). In ogni caso, i documenti ricevuti da una UOR possono essere trattati, per competenza, all'interno della UOR stessa (intendendo anche le UE ad essa afferenti), oppure da questa smistati alla UOR di competenza.

Un documento informatico può, in generale, essere recapitato:

1. a mezzo posta elettronica convenzionale (PEO) o certificata (PEC) inviata a un indirizzo istituzionale, di servizio o personale (assegnato, cioè, a un dipendente);
2. a mezzo interoperabilità applicativa, mediante l'invocazione dei WebServices messi a disposizione delle applicazioni esterne al sistema di gestione informatica dei documenti da parte di SPI e SD;
3. su supporto rimovibile quale, ad esempio, cd rom, dvd, floppy disk, tape, pen drive, etc., consegnato direttamente alla UOP o inviato per posta convenzionale o corriere;
4. mediante sistema di gestione informatica dei documenti (SPI o SD), nel caso di documenti interni "intra-AOO", come sarà diffusamente descritto più avanti.

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. con consegna diretta da parte dell'interessato o consegnato tramite una persona dallo stesso delegata alle UOP e/o agli UOR aperti al pubblico.

Ai sensi dell'art. 53, comma 1, del DPR 445/2000, come detto in precedenza, tutti i documenti che provengono da soggetti esterni alla AOO dell'Università devono essere protocollati.

Ogni UOR è autorizzata dall'Amministrazione, per il tramite dei propri UOP, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in entrata di propria competenza.

Il ciclo di vita dei documenti in entrata si articola, in generale, salvo casi particolari regolamentati con apposito provvedimento, oppure flussi automatizzati gestite con logiche predeterminate da componenti informatici interoperabili, nelle seguenti fasi:

A. Accettazione: il Servizio smistamento posta della UOR riceve il documento proveniente da un mittente esterno all'Amministrazione (altro ente, privato cittadino etc.) e stabilisce se il documento è di competenza della propria UOR. Nel caso in cui sul plico sia riportata la dicitura "offerta", "gara d'appalto" o simili, sul plico viene apposta la data e l'ora di arrivo e il plico viene quindi inviato all'UOP per la registrazione di protocollo e, infine, da questi al Responsabile del procedimento.

Nel caso dei documenti informatici che riguardino procedimenti dell'Università pervenuti a caselle PEC o PEO non istituzionali, il destinatario (il titolare della

casella PEC o PEO) inoltra il messaggio ricevuto alla propria UOR. La UOR garantisce una diligente consultazione della propria casella istituzionale (PEO) e del proprio domicilio digitale (PEC) e la selezione dei messaggi oggetto di protocollazione;

- B. Smistamento:** nel caso in cui il plico o il suo contenuto/il messaggio di posta elettronica o il documentale siano di competenza di un'altra UOR, viene effettuata uno smistamento alla UOR destinataria per posta interna o PEC, a seconda dei casi;
- C. Assegnazione:** il documento/il messaggio viene inviato alla Segreteria UOR (nel caso dell'Amministrazione Centrale, alla Segreteria del Direttore Generale) che stabilisce se il documento è da inviare al dirigente delegato alla sigla, oppure no. Nel primo caso, la Segreteria invia il documento/il messaggio al delegato, altrimenti, sottopone il documento al Direttore Generale/Responsabile UOR. Il responsabile di sigla (Direttore Generale o Responsabile UOR o Delegato alla sigla) provvede a identificare il "primo assegnatario", cioè la propria UOR/UE destinataria del documento in oggetto, oppure altra UOR dell'Ateneo, al quale è assegnata la responsabilità del procedimento amministrativo (RPA) e gli eventuali ulteriori assegnatari, nonché, verificata la presenza di particolari categorie di dati nel contenuto del documento (quali quelli personali o riservati), stabilisce se il documento debba essere contrassegnato come riservato o contenente dati particolari oppure, nel caso della Amministrazione Centrale, se la registrazione del documento debba essere gestita nell'ambito del Protocollo Particolare. Nel caso di assegnazione ad altra UOR, questa si occuperà dell'eventuale assegnazione e smistamento alle proprie UE. In linea di principio, salvo il caso di iter di presa in carico semplificata, le strutture assegnatarie sono UOR di primo livello, ragion per cui, nel caso dell'Amministrazione Centrale, sarà quest'ultima a occuparsi della assegnazione e smistamento del documento alle proprie UOR/UE.
- D. Protocollazione e Classificazione:** in questa fase la UOR/UE destinataria inoltra il documento cartaceo, oppure invia una mail al proprio UOP con dati e metadati di registrazione di protocollo e i documenti da registrare. L'UOP mediante le funzioni del SPI provvede a:
- attribuire un numero e una data di protocollo al documento;
 - nel caso dei documenti analogici l'UOP procede a,
 - apporre la segnatura al documento cartaceo e, contestualmente, effettuare l'acquisizione dell'immagine del documento completa di segnatura. Di norma, la scansione viene effettuata in bianco e nero, ove tale procedura non infici la leggibilità del documento. Le medesime procedure sono previste per gli eventuali allegati al documento principale protocollato. Si ricorda che, le copie per immagine tratte dai documenti originali analogici, acquisite nel sistema di protocollo in fase di registrazione, non costituiscono copie conformi. Quindi, permane l'obbligo di conservazione dei documenti originali cartacei, come descritto nei paragrafi 5.2 e 5.3 del presente Manuale;

- registrare nel sistema SPI il documento completo della copia per immagine;
- nel caso di documenti informatici, ricevute via mail le disposizioni sulla registrazione di protocollo, l'UOP procede a:
 - selezionare il documento principale da protocollare (eventualmente, il .pdf/a contenente il testo del messaggio) e gli eventuali allegati, tra cui, nel caso PEC, anche il messaggio PEC originale in formato .eml;
 - a registrare e classificare il documento, inserendo gli assegnatari in copia/copia conoscenza del documento, mantenendo l'ordine apposto dal Responsabile UOR/UE.

Se la UOR/UE è abilitata alla interoperabilità di protocollo, i due passi precedenti sono gestiti grazie al sistema MC che si occuperà di valorizzare gran parte dei metadati di registrazione, sulla base delle informazioni contenute nel messaggio (ad esempio, il file *segnatura.xml*). I dettagli sono riportati in **Allegato 3**.

- E. Consegna documento (cartaceo) ai destinatari:** l'originale cartaceo è inoltrato al primo assegnatario, insieme al rapporto di consegna. Tutte le restanti UE assegnatarie (compresa la prima), accedendo al SPI, dispongono dell'immagine scansionata del documento originale. Nel caso di competenza trasversale, il documento può essere assegnato ad altra UOR che di occuperà dell'eventuale assegnazione e smistamento alle proprie UE. In linea di principio, salvo il caso di iter di ordinaria amministrazione, la protocollazione avviene tra UOR di primo livello, ragion per cui, nel caso dell'Amministrazione Centrale, sarà questa UOR a occuparsi della assegnazione e smistamento del documento alle UOR afferenti (le Aree, nel caso della Amministrazione Centrale) e alle UE sottostanti.

Nel caso in cui il destinatario non sia utente del SPI, viene inviato all'interessato da parte dell'UOP competente (oppure, in funzione della specificità del procedimento, in modo concordato, dalla UOR/UE assegnataria) un messaggio di posta elettronica o di PEC (a seconda del tipo di procedimento) con allegata la copia per immagine del documento o una copia con contrassegno dello stesso, oppure, nel caso di documento analogico, una copia cartacea consegnata a mano mediante posta interna.

- F. Fascicolazione:** l'UOR/UE/RPA destinatario della registrazione di protocollo acquisisce, importandolo, il documento protocollato nel corrispondente fascicolo procedimentale creato in SD.

8.2.2. Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica.

Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, l'Amministrazione si riserva la facoltà di acquisire e trattare tutti i documenti

informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a sua disposizione.

Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

8.2.3. Ricezione di documenti sulla casella istituzionale

L'Ufficio di Segreteria del Direttore Generale, oltre a gestire i propri indirizzi di posta elettronica ordinaria e PEC, gestisce anche i corrispondenti indirizzi istituzionali dell'intera AOO: ateneo@unina.it e ateneo@pec.unina.it.

La casella ateneo@pec.unina.it, domicilio digitale della AOO riportato in IPA (PEI), è consultata almeno con frequenza giornaliera, fermo restando che è attivo un meccanismo di notifica per l'invio di notifiche di arrivo nuovo messaggio sulla PEO dell'Ufficio di Segreteria del Direttore Generale.

I messaggi PEC recapitati su PEI sono gestiti mediante il modulo MC, come descritto in precedenza e le operazioni di assegnazione, classificazione e registrazione di protocollo dei messaggi pervenuti su PEI sono effettuate, di norma, direttamente dalla Segreteria del Direttore Generale

8.2.4. Modifica delle assegnazioni

Di seguito, si riporta il flusso della gestione del cambio di assegnazione di un documento in entrata registrato nel sistema SPI che la UOR destinataria ha assegnato a una o più sotto-UO, con riferimento al caso (più complesso) della UOR Amministrazione Centrale.

Ciascun ufficio (UOR/UO) si collega con frequenza almeno giornaliera al SPI e verifica la presenza di documenti da prendere in carico.

Prima di prendere in carico i documenti presenti in "lista di lavoro", l'UO assegnataria controlla che il documento, salvo il caso descritto più avanti di "iter semplificato di presa in carico", sia siglato, cioè che gli sia stato inviato dalla propria UOR padre (oppure, nel caso di UO dell'Amministrazione Centrale, dalla UOR di primo livello Amministrazione Centrale).

In caso affermativo (documento siglato), l'UO potrà:

- prendere in carico il documento, se il documento è di propria competenza; oppure,
- richiedere il cambio assegnatario, se il documento non è di propria competenza. In tal caso,
 - smisterà il documento alla struttura del Responsabile di Sigla mittente (Amministrazione Centrale o Area o, più in generale, UOR gerarchicamente superiore), senza prenderlo in carico;
 - se è primo assegnatario, invierà al Responsabile di Sigla anche il documento cartaceo.

Il Responsabile di Sigla dovrà quindi collegarsi al sistema SPI, accedere alla propria "lista di lavoro" e smistare il documento al nuovo assegnatario. Se il cambio è relativo al primo



assegnatario, il Responsabile di Sigla dovrà, infine, stampare il “rapporto di consegna” e trasmetterlo, insieme al documento cartaceo originale all’UOP per le ordinarie operazioni di consegna al nuovo ufficio destinatario.

Se il documento non è siglato e, come già detto, non è di ordinaria amministrazione, la UO dovrà controllare se:

- a. il documento ha tra i destinatari di registrazione anche l’Amministrazione Centrale, oppure la UOR padre. In tal caso, attenderà la ricezione della propria copia siglata (tale copia sarà elettronica per gli assegnatari diversi dal primo, cartacea ed elettronica solo per il primo assegnatario);
oppure,
- b. il documento non ha tra i destinatari anche l’Amministrazione Centrale, oppure la UOR padre. In tal caso, l’ufficio smisterà la propria copia elettronica all’Amministrazione Centrale o alla UOR padre per far avviare il procedimento di sigla ed assegnazione ed invierà contestualmente anche l’eventuale documento cartaceo.

Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l’identificativo dell’utente che effettua l’operazione con la data e l’ora di esecuzione.

8.2.5. Errata ricezione di documenti

Nel caso in cui pervengano sulla casella di posta istituzionale dell’Amministrazione (certificata o meno) messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l’operatore addetto alla consultazione della PEO o PEC rispedisce il messaggio al mittente con la dicitura “Messaggio pervenuto per errore - non di competenza di questa Amministrazione”.

Nel caso di documenti pervenuti alla UOR/UO mediante SPI o SD, il documento dovrà essere restituito al mittente (interno) mediante le funzionalità informatiche messe a disposizione dalle due applicazioni SPI o SD, a seconda dei casi.

Nel caso in cui pervengano erroneamente alla UOP dell’Amministrazione documenti analogici indirizzati ad altri soggetti, possono verificarsi le seguenti possibilità:

- busta indirizzata ad altra UOR della stessa Amministrazione:
 - a. se per errore la corrispondenza viene recapitata ad una UOR non destinataria del plico, quest’ultima, a tutela dei dati personali eventualmente contenuti nella missiva, non apre le buste o i contenitori ricevuti ma rilascia ricevuta al mittente e invia, nella stessa giornata, prima della chiusura del protocollo, il plico alla UOR interessata, affinché possa essere sottoposto al processo di apertura, sigla ed assegnazione da parte del Responsabile della UOR o dal Responsabile di Sigla, se designato;
 - b. se la busta viene aperta per errore, il documento è protocollato in entrata, inserendo nel campo oggetto una nota del tipo “documento pervenuto per

errore”, si pone come destinataria la UOR responsabile del procedimento e si invia alla UOR stessa il plico, apponendo sulla busta la dicitura “Pervenuta ed aperta per errore”;

- busta indirizzata ad altra amministrazione:
 - a. viene restituita alla posta;
 - b. se la busta viene aperta per errore, il documento è protocollato prima in entrata e quindi in uscita (collegando le due registrazioni), inserendo nel campo oggetto una nota del tipo “documento pervenuto per errore” e si invia al mittente apponendo sulla busta la dicitura “Pervenuta ed aperta per errore”.

8.2.6. Rilascio di ricevute attestanti la ricezione di documenti

Gli addetti alle UOP non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione.

Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata all’Amministrazione ed è richiesto il rilascio di una ricevuta attestante l’avvenuta consegna, viene rilasciata una ricevuta di presa in carico/consegna. Se l’incaricato dell’Amministrazione preposto alla consegna è un addetto a una UOP di protocollo, la UOP che lo riceve è autorizzata a rilasciare ricevuta con gli estremi della segnatura, se contestualmente alla ricezione avviene anche la protocollazione. Tale operazione è svolta mediante un’apposita funzionalità del SPI che consente di produrre una ricevuta di avvenuta protocollazione, in cui sono riportate la data di consegna, la data e l’ora di registrazione di protocollo, la posizione organizzativa dell’ufficio mittente e la sigla dell’operatore.

La ricezione di documenti informatici ricevuti via PEC comporta l’invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, una al servizio di protocollazione informatica.

Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell’avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall’Amministrazione con gli standard specifici.

Nel caso di ricezione di messaggi di protocollo interoperabili da parte di altra amministrazione pubblica, ai sensi dell’Allegato 6 alle LLGG AgID, il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvederà alla formazione e all’invio al mittente di uno dei seguenti messaggi:

- messaggio di conferma di protocollazione: un messaggio che contiene la conferma dell’avvenuta protocollazione in ingresso di un documento ricevuto. Si differenzia da altre forme di ricevute di recapito generate dal servizio di posta elettronica dell’AOO in quanto segnala l’avvenuta protocollazione del documento, e quindi l’effettiva presa in carico;
- messaggio di notifica di eccezione: un messaggio che notifica la rilevazione di una anomalia in un messaggio ricevuto;

- messaggio di annullamento di protocollazione: un messaggio che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza;
- messaggio di aggiornamento di protocollazione: un messaggio che contiene una comunicazione di aggiornamento riguardante un documento protocollato ricevuto in precedenza.

In tutti gli altri casi, l'eventuale consegna della ricevuta di avvenuta protocollazione di un documento informatico proveniente dall'esterno della AOO dovrà essere rilasciata con modalità concordate tra UOP e interessato.

Nel caso di documenti "intra AOO" (trattato più avanti) sarà l'evento di "presa in carico" nel sistema SPI o SD a testimoniare al mittente l'effettiva consegna e avvio del procedimento amministrativo da parte del destinatario.

Infine, nel caso di utilizzo della interoperabilità, la ricevuta di avvenuta protocollazione/acquisizione del documento da parte del sistema di gestione informatica dei documenti viene inviata all'applicazione client chiamante, in risposta alla invocazione del servizio.

8.3. Flussi documentali in uscita

Per la trasmissione dei documenti in formato digitale è previsto l'utilizzo della casella PEI associata alla AOO dell'Università, che è integrata nel sistema di protocollo grazie al modulo Mail Connect (MC) integrato nel sistema SPI, oppure le caselle PEC assegnate alle UOR di I livello e ad alcune UO, anch'esse gestite tramite MC per consentire la trasmissione automatica dei protocolli ai destinatari esterni, oppure altre caselle PEC istituzionali non interoperabili o di servizio (assegnate a RPA). La procedura prevista, nelle sue varianti da scegliere a seconda di esigenze organizzative e della tipologia dei destinatari, è la seguente:

A. Sottoscrizione del documento, fascicolazione e Registrazione di protocollo

Il documento con i suoi allegati, sottoscritto digitalmente, viene prima classificato e fascicolato in SD e quindi protocollato secondo le modalità riportate di seguito:

- l'UOR/UO o l'RPA (se abilitato) procede con l'acquisizione, classificazione e fascicolazione del documento nel sistema SD, compresi gli eventuali allegati. In accordo con quanto riportato nel paragrafo 5.6 del presente Manuale, il documento potrà essere già firmato dal responsabile della UOR o del procedimento o da eventuali altri soggetti, oppure potrà essere firmato direttamente utilizzando l'applicazione centralizzata di firma.
- L'UOR/UO o l'RPA (se abilitato) seleziona i destinatari del protocollo e procede con la registrazione di protocollo in uscita, utilizzando l'apposita funzionalità disponibile nel SD, oppure potrà:

- inviare all'UOP il riferimento ipertestuale al documento importato in SD. L'UOP utilizzerà quindi le funzionalità di protocollazione messe a disposizione da SD, oppure,
- se i destinatari sono AOO iscritte in IPA, inviare via PEO il documento, gli allegati e i metadati all'UOP. L'UOP procederà quindi a registrare il documento in SPI.

In alternativa al caso A., la sequenza può essere la seguente:

B. Sottoscrizione del documento, registrazione di protocollo e fascicolazione

Il documento con i suoi allegati, sottoscritto digitalmente, viene prima protocollato in SPI e quindi fascicolato in SD, secondo le modalità riportate di seguito:

- l'UOR/UE o l'RPA sottoscrive digitalmente il documento e gli eventuali allegati e invia al proprio UOP un messaggio PEO, trasmettendo i documenti firmati (indicando il documento primario), l'oggetto della registrazione, la voce di classificazione e i destinatari (con gli eventuali indirizzi PEC). UOP esegue in SPI la registrazione in uscita del documento.
- L'UOR/UE o l'RPA (se abilitato) procede in SD con l'importazione da SPI del documento protocollato in uscita, compresi gli eventuali allegati nel fascicolo creato per il procedimento in esame.

Infine, come ultima fase, viene effettuata la trasmissione del documento protocollato alla casella PEC del destinatario (o alle caselle dei destinatari, se più di uno) a partire dalla casella PEC istituzionale associata alla UOR/UE protocollante:

➤ Trasmissione del messaggio via PEC

Tale operazione può essere effettuata in una delle modalità di seguito riportate:

- direttamente dal sistema SPI (se la UOR/UE è dotata di casella PEC interoperabile) da utenti abilitati all'invio di mail. Il messaggio, oltre al documento sottoscritto con firma digitale, potrà recare in allegato anche il file *segnatura.xml* e rispettare gli standard previsti dall'Allegato 6 alle LLGG AgID e le ricevute PEC di avvenuta consegna e accettazione saranno collegate alla registrazione. Se il destinatario è una AOO iscritta in IPA, il protocollo di colloquio sarà quello previsto per l'interoperabilità tra AOO. Maggiori dettagli sono riportati nell'**Allegato 3** al presente MdG.

In alternativa,

- il documento potrà essere inviato dalla UOR/UE/RPA utilizzando funzionalità SD, eventualmente apponendo al documento (protocollato al passo precedente) il contrassegno elettronico, e l'applicazione riconcilerà quindi nel fascicolo procedimentale in cui risiede il documento le ricevute di accettazione e consegna PEC. Maggiori dettagli sono riportati nell'**Allegato 3** al presente MdG.

In alternativa,

- il documento (con gli eventuali allegati) potrà essere inviato via webmail dalla casella PEC della UOR/UU o RPA.

Nei casi residuali di trasmissione di documenti in formato analogico, questi devono essere predisposti secondo le modalità descritte nel par. 5.1 del presente Manuale e devono essere registrati nel sistema SPI, con acquisizione della copia per immagine del documento originale. Al termine della procedura di protocollazione, il documento originale analogico completo di segnatura di protocollo viene trasmesso al destinatario mediante corriere o servizi postali. La copia per immagine del documento registrato nel sistema SPI potrà essere successivamente importata nel sistema SD nel fascicolo relativo al procedimento in esame.

8.4. Flussi documentali interni

Come già evidenziato al punto 6.4 del presente Manuale, ai sensi dell'art. 53, comma 5, del DPR 445/2000, per i documenti scambiati internamente a ciascuna AOO non sussistendo l'obbligo di protocollazione, si effettua la registrazione particolare mediante la **fascicolazione** e la classificazione con il sistema a norma di gestione documentale e dei flussi (SD) utilizzato dall'Amministrazione e l'invio alla UOR/UO destinataria mediante gli strumenti di condivisione e/o workflow messi a disposizione da SD. L'obbligo di registrazione di protocollo sancito dall'articolo 53, comma 5, del DPR 445/2000 si riferisce infatti principalmente ai **documenti informatici che costituiscono comunicazioni esterne** (istanze, dichiarazioni, corrispondenza con altri enti o cittadini) ricevute o inviate dalla AOO. Per i **documenti informatici interni**, la **regola generale prevede la loro gestione attraverso il sistema di gestione documentale e dei flussi**. La protocollazione viene effettuata **eccezionalmente** per quei casi specifici in cui si ravveda una particolare necessità di certificazione formale per particolari ragioni giuridiche o amministrative, ad esempio quando un atto interno acquisisce rilevanza verso terzi o deve essere formalmente comunicato a soggetti esterni, ragion per cui la sua protocollazione diventa obbligatoria, ai sensi del citato articolo 53, comma 5, del DPR 445/2000.

Bisogna infatti considerare che:

- I. l'obiettivo primario per i documenti interni è garantirne la **corretta organizzazione, conservazione e tracciabilità** all'interno dell'AOO: la fascicolazione e la classificazione nel sistema di gestione documentale assolvono pienamente a questa funzione, permettendo di ricostruire i procedimenti e individuare rapidamente i documenti pertinenti.
- II. richiedere la protocollazione sistematica di ogni atto interno andrebbe contro i principi di **semplificazione, efficienza e proporzionalità**, in quanto stendere l'obbligo di protocollazione a ogni singolo documento informatico interno

creerebbe un appesantimento burocratico eccessivo e non giustificato dalla necessità di certezza giuridica verso l'esterno.

- III. il sistema **SD adottato dall'Ateneo è conforme alle LLGG AgID sulla formazione, gestione e conservazione dei documenti informatici** e garantisce, tra l'altro, data certa alle operazioni di creazione, acquisizione, modifica e ogni altra operazione rilevante sul documento informatico, nonché meccanismi di sicurezza e autenticazione del sistema, segnatura archivistica univoca, classificazione, collegamento ai procedimenti, assegnazione alle unità documentali di un ricco set di metadati, nel rispetto dei principi di trasparenza, accessibilità, integrità e immutabilità ed è pertanto idoneo fornire un livello adeguato di data certa e autenticità per gli atti amministrativi interni, rendendo superflua la protocollazione sistematica per ogni documento.

Tali principi suggeriscono quindi di adottare per la gestione dei documenti interni un approccio più flessibile, **ferma restando la possibilità di procedere alla registrazione di protocollo, in funzione della specificità del procedimento amministrativo e di valutazioni di opportunità organizzativa.**

La precedente raccomandazione non si applica a flussi interni specifici che sono attualmente ancora gestiti nell'ambito del sistema SPI, sulla base di decreti e circolari attuative specifiche, quale ad esempio l'iter di approvazione ai fini della successiva emanazione dei Decreti e degli Ordini di servizio.

Di seguito si descrive la procedura per la gestione e lo scambio dei documenti interni alla AOO basata sull'utilizzo del sistema SD e dei servizi di interoperabilità con SPI:

- a. il responsabile della UOR o del procedimento predispone e sottoscrive digitalmente il documento interno, secondo i formati e le modalità descritte nel paragrafo 5.6 del presente Manuale;
- b. la UOR/UE procede con la registrazione nel sistema SD del documento nel fascicolo (precedentemente creato) relativo al procedimento in questione, con la valorizzazione dei metadati (con particolare riguardo a quello relativo alla tipologia documentale) e al caricamento degli eventuali allegati;
- c. lo scambio di documenti avviene, di norma tra UOR di primo livello che provvedono alla assegnazione alle proprie sotto UE, salvo il caso di iter semplificato riportato più avanti. Pertanto, la UE mittente invia mediante work-flow o condivide il documento/il fascicolo procedimentale con le UOR destinatarie (eventualmente per il tramite della propria UOR);
- d. tuttavia, nel caso di documenti per i quali non sorgono dubbi sulla determinazione della competenza, principalmente quando i documenti sono riferiti a procedimenti che hanno carattere ripetitivo e di ordinaria amministrazione e con unica UE competente assegnataria, può essere seguito l'**iter semplificato di presa in carico** (già avviato nel 2007 dalla Amministrazione Centrale, il cui principio è stato successivamente ripreso nella definizione del "Flusso per la gestione dei documenti presso i Dipartimenti e gli Uffici afferenti" illustrato nell'**Allegato 3**): i documenti



- potranno essere infatti inviati direttamente alla UO competente che sarà infatti autorizzata a prendere in carico tali documenti senza dover necessariamente attendere formale ed esplicita assegnazione da parte del proprio responsabile UOR;
- e. il documento sarà immediatamente reso disponibile al destinatario in piattaforma SD e, se necessario, potrà essere quindi collocato, con l'operazione di copia, nel fascicolo procedimentale da questo ritenuto più idoneo.
 - f. nel caso in cui sia necessario per la rilevanza amministrativa giuridico-probatoria dell'atto o per considerazioni di carattere organizzativo, il documento può essere anche protocollato utilizzando l'apposita funzionalità di SD oppure essere oggetto di registrazione in un repertorio tenuto da SPI o da SD.

Per lo scambio dei documenti di carattere informale/endo-procedimentale, per i quali non è prevista la acquisizione nel sistema di gestione documentale, si prevede invece il ricorso alla sola posta elettronica ordinaria, in conformità alle disposizioni di cui all'art. 47, comma 3, del CAD, utilizzando l'indirizzo PEO istituzionale associato a ciascuna UOR/UO UniNA, oppure l'utilizzo di sistemi istituzionali di collaborazione.

9. CONSERVAZIONE

Come riportato nel documento “Poli di conservazione”¹, il Codice dei beni culturali (il D.Lgs. n. 42 del 22 gennaio 2004) all’art. 10, comma 2, lett. b), definisce senza alcuna distinzione cronologica tutti “gli archivi e i singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico” come beni culturali, cioè testimonianze aventi valore di civiltà, facenti parte del patrimonio culturale tutelato e valorizzato in attuazione dell’art. 9 della Costituzione. La tutela e la valorizzazione del patrimonio culturale concorrono a preservare la memoria della comunità nazionale e a promuovere lo sviluppo della cultura.

Lo Stato, le regioni e gli altri enti territoriali debbono assicurare e sostenere la conservazione di tale patrimonio e favorirne la pubblica fruizione.

In conformità alle disposizioni di cui all’art. 34, comma 1-bis, del CAD, UniNA procede alla conservazione dei documenti informatici all’interno della propria struttura organizzativa.

In attuazione di quanto previsto dall’art. 44, comma 1, del CAD e dalle LLGG AgID, il sistema di conservazione dell’Ateneo (SD-C), modulo del sistema SD realizzato come componente funzionalmente autonomo nell’ambito del sistema di gestione documentale di Ateneo, assicura, dalla presa in carico fino all’eventuale scarto, la conservazione degli oggetti digitali in esso conservati e, tramite l’adozione di regole, procedure e tecnologie, il mantenimento delle loro caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità. Ne garantisce inoltre l’accesso, per il periodo di tempo previsto dal Piano di conservazione e nel rispetto della normativa sulla tutela dei dati personali.

Per ulteriori dettagli si rimanda al Manuale di conservazione UniNA v.1.2, approvato con delibera del CdA UniNA n. 39 del 26.09.2016, consultabile all’indirizzo:

<https://www.praxis.unina.it/documentaleguidemanuali>

9.1. Archivio dell’Ateneo

L’archivio dell’Ateneo è costituito dall’insieme di documenti prodotti, ricevuti e acquisiti nello svolgimento delle proprie funzioni, o per fini pratici di auto-documentazione.

Ai fini di una corretta organizzazione del sistema documentario e di una sua adeguata tenuta anche per finalità di ricerca storica, l’Ateneo, in qualità di soggetto produttore di documenti, ha organizzato per l’esercizio di tale funzione una idonea struttura di gestione dotata di risorse umane, strumentali e informatiche, nonché di regole e prassi

¹ Documento redatto a giugno 2021 da un tavolo di lavoro coordinato da AgID con la partecipazione dell’Archivio centrale dello Stato, il Consiglio nazionale del Notariato e il l’Agenzia industrie difesa.



per la formazione, tenuta, reperimento e uso dei documenti nella loro fase corrente e di deposito.

L'archivio è unico, ma la sua gestione si suddivide in tre fasi:

- ❑ archivio corrente
- ❑ archivio di deposito
- ❑ archivio storico

9.1.1. Archivio corrente

L'archivio corrente dell'Ateneo è costituito dai documenti relativi ad affari ancora in corso. Include documentazione prevalentemente in formato digitale, gestita mediante le funzionalità dei sistemi SPI e SD e organizzata secondo i criteri definiti nel presente Manuale, mediante gli strumenti archivistici in esso gestiti (Titolario di classificazione, Piano di fascicolazione e Piano di conservazione, Catalogo dei procedimenti ed elenco delle Tipologie documentali).

L'attuazione operativa delle disposizioni inerenti al funzionamento dell'archivio corrente spetta ai responsabili UOR, in qualità di RGD della propria struttura, in collaborazione con i Capi Ufficio delle UO afferenti alla UOR, con gli RPA e con il supporto e l'azione di coordinamento svolta da RCGD, RSI e RPD, al fine di assicurare la corretta gestione e conservazione dei documenti relativi ai procedimenti e agli affari in corso di propria competenza e di competenza delle UO afferenti.

I criteri di organizzazione dell'archivio corrente sono finalizzati a rendere efficace la gestione dei flussi documentali e la ricerca dei documenti per garantire la certezza dell'attività giuridico-amministrativa dell'Amministrazione e l'accesso alla documentazione di cui l'Ateneo è titolare e depositario. Inoltre, come già ribadito in precedenza, è opportuno attuare i necessari accorgimenti finalizzati a una corretta e diligente metadattazione degli oggetti, alla scelta dei formati (prediligendo quelli ad alto indice di interoperabilità e, dunque, più adatti alla conservazione di lungo termine), alla riduzione delle ridondanze e al caricamento dei soli documenti essenziali ai fini del procedimento trattato.

Inoltre, visto che, ai sensi delle LLGG AgID e dell'art. 44, comma 1-bis, del CAD, il sistema di gestione documentale deve assicurare la possibilità di trasferire in conservazione:

- fascicoli e serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito;
- fascicoli informatici e serie non ancora chiuse, trasferendo i singoli documenti in essi contenuti in relazione alle specifiche esigenze dell'Ente e al fine di contrastare i rischi legati all'obsolescenza tecnologica, garantendo l'integrità e l'autenticità dei documenti;

in alcuni contesti archivistici il versamento nel sistema di conservazione viene effettuato in modo "precoco", cioè anche prima della conclusione del procedimento. Tale prassi

viene infatti spesso seguita in ambito informatico per timore di incorrere nella obsolescenza tecnologica o nella perdita di integrità e autenticità dei documenti firmati con firma digitale o, ancora, per apporre un riferimento temporale certo e opponibile a terzi.

A tal riguardo, è fatta raccomandazione agli utenti del sistema SD UniNA di non ricorrere alla conservazione “precoca” dei documenti per una serie di motivi, tra i quali:

- I pacchetti informativi versati (metadati e contenuti binari) sono conservati in una fase in cui i documenti non presentano ancora caratteristiche di stabilità e staticità;
- Le unità documentarie versate precocemente, risultando ancora in fase attiva, potrebbero risultare sprovviste di tutti i metadati e delle informazioni necessarie a costruire l’archivio informatico dell’ente, una delle finalità principali di un sistema di conservazione di “lungo termine”, con conseguente difficoltà a mantenere allineate il contenuto informativo dell’archivio corrente con quello del sistema di conservazione;
- I documenti versati singolarmente, spesso non ancora inseriti in fascicoli procedurali e neppure tipizzati rispetto alla tipologia documentale, risultano non correttamente gestibili nell’ambito del processo di selezione e scarto;

Per estendere la autenticità dei documenti oltre il periodo di validità tecnologica dei certificati digitali di sottoscrizione a valle dell’acquisizione dei documenti firmati nel sistema documentale di Ateneo, operazione complessa gestionalmente e onerosa sotto il profilo computazionale, come anche riportato nel Manuale di Conservazione, il sistema di gestione documentale UniNA realizza il modello della “**catena di sistemi fidati**”: il documento sottoscritto digitalmente viene, cioè, acquisito e verificato dal “validation service” del sistema qualificato di SD o SPI (considerati sistemi “fidati” e riportati nell’apposito registro tenuto da SD e consultato da SD-C) che registra, **a data certa e in modo indissolubile rispetto al documento stesso**, l’esito della verifica di validità della firma digitale e l’integrità del documento. In fase di versamento, SD-C, pur riportando l’esito del controllo di validità dei certificati alla data del versamento, riterrà superato il controllo in quanto il documento era stato acquisito da un sistema “fidato”.

9.1.2. Archivio di deposito

La documentazione che si riferisce a procedimenti esauriti, ma che risulta ancora utile per lo svolgimento delle attività amministrative in corso, è trasferita nell’archivio di deposito, dove permane per un determinato periodo di tempo, in attesa che termini del tutto la sua utilità amministrativa.

In conformità alle disposizioni di cui all’art. 67 del DPR 445/2000, almeno una volta l’anno il RGD di ciascuna UOR/UO e gli RPA provvedono a trasferire “in senso logico” fascicoli e le serie documentarie relativi a pratiche e procedimenti conclusi nell’archivio di deposito. A tal fine, è prevista un’attività di verifica per l’individuazione dei fascicoli già chiusi o afferenti a pratiche concluse. Tale verifica può essere effettuata:

- alla fine dell’anno solare, in modo tale che i fascicoli delle pratiche ancora in corso vengano mantenuti nell’archivio corrente;



- durante il corso dell'anno, per selezionare periodicamente i fascicoli afferenti a pratiche già concluse.

In questa fase, è opportuno, prima di effettuare la chiusura dei fascicoli procedurali, effettuare lo sfoltoimento dei documenti non più utili ai fini del procedimento, nonché valorizzare con cura i metadati, soprattutto quello relativo alla tipologia documentale. L'attività di chiusura dei fascicoli procedurali ha, tra l'altro, il vantaggio immediato di rendere più efficiente la ricerca e il reperimento dei documenti e dei fascicoli attivi e non ancora chiusi.

Una volta individuati i fascicoli e le serie da conservare, il versamento deve essere effettuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.

Il processo di versamento e i ruoli coinvolti in tale processo, coerenti con le LLGG AgID, sono descritti nel Manuale di Conservazione dell'Università.

Al termine del processo di versamento in conservazione, i fascicoli e le serie di documenti versati all'archivio di deposito gestito dal sistema di conservazione SD-C continuano a essere disponibili nel sistema di gestione documentale in forma imm modificabile e ai fini della mera consultazione, ma saranno accessibili (previa autorizzazione del RC) previa presentazione di una richiesta di esibizione da parte dell'interessato.

Coerentemente ai criteri definiti nel Piano di conservazione e in conformità alla normativa sulla tutela dei beni culturali, la fase di deposito dell'archivio termina con un'attività di selezione dei documenti che è finalizzata all'individuazione della documentazione da destinare allo scarto, in quanto ha perso totalmente la sua rilevanza amministrativa e non ha assunto alcuna rilevanza storica rispetto a quella di interesse storico-documentario da destinare alla conservazione permanente. A tal riguardo, il sistema SD-C offre a RC la possibilità di selezionare la documentazione da scartare, produrre un report da allegare alla proposta di scarto da inviare a RCGD e, quindi, alla Soprintendenza competente.

Il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione dalla Soprintendenza (che può essere concessa anche solo su una parte dell'elenco proposto), può procedere alla distruzione dei pacchetti di archiviazione. Al termine dell'attività di distruzione, viene redatto un verbale che attesta l'avvenuta eliminazione logica e fisica della documentazione, come descritto al paragrafo 4.11 delle LLGG AgID.

Alla data, sono versati in conservazione da RCGD e, ove nominati, dai responsabili del versamento RV, solo i repertori versati in SD a partire da SPI ove sono gestiti, oppure i repertori creati e gestiti nell'ambito di SD. I tempi di conservazione dei documenti versati, per ciascun repertorio, dipendono dalla tipologia documentaria che caratterizza



il repertorio e sono coerenti con il Massimario di selezione e scarto dell'Università, di cui al successivo punto 9.2.

Il versamento in conservazione, salvo casi particolari², avviene nel corso dell'anno solare successivo all'anno solare di registrazione dei documenti. Per ciascuna operazione di versamento, il sistema produce il rapporto di versamento, registrato nel repertorio "RV" tenuto dal sistema SD e accessibile a SCGD.

A seguire, UniNA, con il coinvolgimento del SCGD, organizzerà ed avvierà presso le UOR/UO il processo di versamento anche dei fascicoli procedurali, nei casi in cui sia richiesto per legge il versamento in conservazione a lungo termine della documentazione in essi contenuta.

La figura 4 riportata più avanti illustra lo schema del processo di versamento in conservazione dei repertori.

9.1.3. Archivio storico

La normativa sui beni culturali indica dei percorsi conservativi differenti per gli archivi pubblici statali (cioè, prodotti e/o accumulati per acquisizione di funzioni istituzionali dalle Amministrazioni dello Stato) rispetto agli archivi pubblici non statali.

In particolare, le Regioni, gli altri enti pubblici territoriali nonché ogni altro ente ed istituto pubblico, quindi anche l'Università, al fine di garantire la sicurezza e la conservazione dei beni culturali di loro appartenenza, hanno l'obbligo di conservare i propri archivi nella loro organicità e di ordinarli e di inventariare i propri archivi storici, costituiti dai documenti relativi agli affari esauriti da oltre 40 anni ed istituiti in sezioni separate.

Tale sezione, per quanto attiene ai documenti originali informatici, non è stata ancora costituita, visto che l'Archivio digitale dell'Ateneo è stato costituito formalmente a partire dal 1° gennaio 2007.

² Ad esempio, nel caso del repertorio RRM delle richieste di rimborso spese missione, il versamento in conservazione avviene entro sei mesi dalla data di registrazione in SD e, trascorso tale periodo, l'interessato è autorizzato a distruggere gli originali cartacei delle ricevute e degli scontrini.

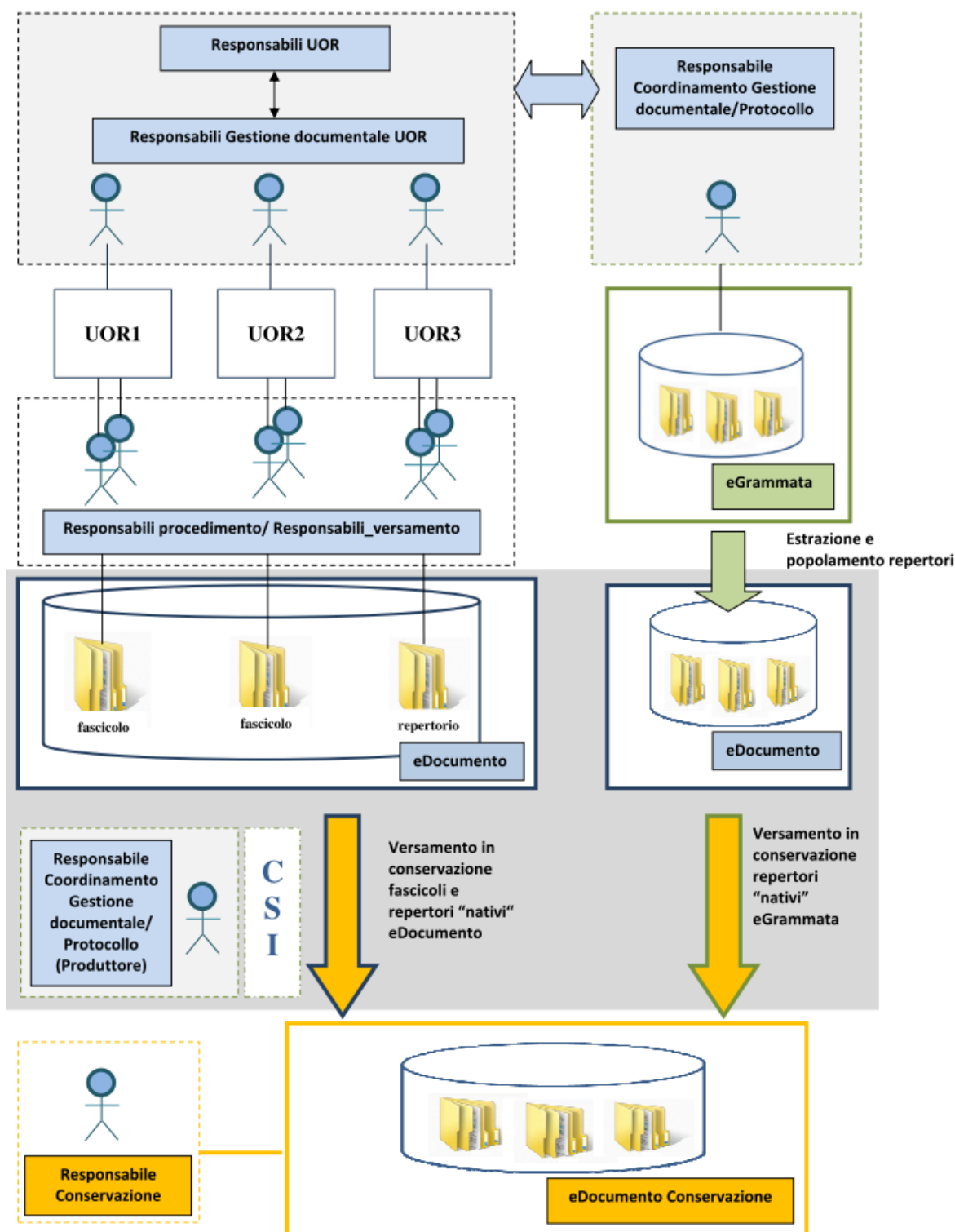


Figura 5 – Il processo di versamento in conservazione



9.2. Piano di conservazione

L'art. 68 del DPR 445/2000 pone l'obbligo per i soggetti pubblici di dotarsi di un "piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni contenute in materia di tutela dei beni culturali e successive modificazioni ed integrazioni". Il Piano di conservazione è il documento che pianifica le procedure di selezione e i tempi per il trasferimento nel sistema di conservazione e che contiene l'elenco (il c.d. Massimario di scarto) delle tipologie documentarie con l'indicazione, per ciascuna di esse, dei tempi di conservazione, superati i quali, un documento di tale tipologia, previa valutazione ed approvazione della competente Soprintendenza archivistica, può essere distrutto.

Il "Massimario di Selezione per la conservazione e lo scarto dei documenti prodotti e/o detenuti dall'Università degli Studi di Napoli Federico II", approvato sezione per sezione dalla Soprintendenza Archivistica e Bibliografica della Campania e dal CdA di questo Ateneo con delibera n. 243 del 21.02.2023, è pubblicato al seguente indirizzo:

<http://www.unina.it/ateneo/statuto-e-normativa/massimario>

Tale documento è dunque il riferimento nell'ambito dell'Amministrazione per guidare le attività per la conservazione e/o lo scarto dei documenti analogici e informatici. Il sistema SD gestisce infatti l'entità delle tipologie documentali (ottenute dalla aggregazione effettuata in base a criteri di analogia delle tipologie di dettaglio contenute nel Massimario) in cui a ciascuna tipologia viene attribuito il periodo di conservazione.

Ciascun RPA (o suo incaricato opportunamente abilitato), dal momento della acquisizione di un documento in un fascicolo fino alla chiusura del fascicolo stesso, consultando tale tabella potrà selezionare la corretta tipologia da attribuire a ciascun documento. Tale informazione, riportata per ciascun documento versato, sarà quindi successivamente utilizzata dal processo di selezione e scarto periodicamente eseguito da RC nel sistema di conservazione.

Per quanto riguarda i repertori tenuti da SPI, come già riportato, questi vengono versati prima in SD e da questo in SD-C con cadenza annuale, a cura di SCGD. Analogamente, i repertori tenuti da SD sono versati in SD-C con cadenza annuale da SCGD. SCGD, in quanto soggetto produttore, si occupa di monitorare l'intero processo e di verificare, attraverso i report di versamento, la corretta validazione dei pacchetti versati e la loro acquisizione nel sistema di conservazione.

10. MISURE DI SICUREZZA

10.1. Finalità e contesto normativo

Ai sensi dell'art. 51, comma 2, del CAD, l'Università garantisce il controllo e la custodia dei documenti informatici di cui è Titolare e depositaria, con modalità tali da ridurre al minimo i rischi di distruzione, di perdita, di accesso non autorizzato o non consentito, oppure non conforme alle finalità della raccolta. A tal fine, in accordo con quanto riportato nelle LLGG, RCGD predispone il piano della sicurezza del sistema di gestione informatica dei documenti, in accordo con RC, con RTD e acquisito il parere di RPD, prevedendo idonee misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali e di sicurezza dei dati e dei sistemi informatici.

Le misure di sicurezza sono adottate in coerenza con:

- ✓ il Regolamento (UE) 2016/679 (GDPR);
- ✓ il D.Lgs. 82/2005 e successive modificazioni (CAD);
- ✓ il D.P.R. 445/2000;
- ✓ le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici;
- ✓ la Circolare AgID n. 2/2017 recante "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni";
- ✓ la Direttiva NIS2 (UE 2022/2555) è la normativa europea sulla cybersicurezza, in vigore in Italia tramite il D.Lgs. 138/2024;
- ✓ il Regolamento dell'Università degli Studi di Napoli Federico II in materia di trattamento dei Dati Personali (DR/2026/111 del 15/01/2026);
- ✓ le politiche di sicurezza informatica, continuità operativa e protezione dei dati personali adottate dall'Ateneo.

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento affidato per suo conto ad altri soggetti esterni, ai responsabili del trattamento, individuati sulla base dell'art. 28 del GDPR.

10.2. Protezione dei dati personali e gestione degli incidenti

L'Università assicura che il trattamento dei dati personali effettuato nell'ambito del Sistema di Gestione Documentale avvenga nel rispetto del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 196/2003 e successive modificazioni, del Codice dell'Amministrazione Digitale, delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici e delle ulteriori disposizioni applicabili in materia di protezione dei dati personali. L'Università assicura il coordinamento tra il presente Manuale, il Registro delle attività di trattamento, le politiche di sicurezza informatica, il Piano della



Sicurezza ICT, il Manuale di Conservazione e le procedure di gestione dei data breach, al fine di garantire un approccio integrato alla sicurezza delle informazioni e alla protezione dei dati personali.

Nell'ambito del Sistema di Gestione Documentale sono adottate misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato ai rischi derivanti dal trattamento dei dati personali, tenendo conto della natura dei dati trattati, delle finalità perseguite, del contesto operativo e dell'evoluzione tecnologica.

La progettazione e la gestione dei processi documentali si conformano ai principi di privacy by design e privacy by default, assicurando che l'accesso ai documenti e alle informazioni sia consentito esclusivamente ai soggetti autorizzati in ragione delle funzioni svolte e nel rispetto dei principi di necessità, pertinenza e minimizzazione dei dati personali.

Particolare attenzione, come sarà riportato più avanti, è riservata alla protezione dei documenti contenenti dati personali, dati appartenenti a categorie particolari ai sensi dell'articolo 9 del GDPR e dati relativi a condanne penali e reati di cui all'articolo 10 del GDPR, mediante adeguati sistemi di autorizzazione, profilazione degli utenti, tracciamento degli accessi e monitoraggio delle operazioni effettuate.

Gli eventi che possano compromettere la riservatezza, l'integrità, la disponibilità o l'autenticità dei documenti informatici e dei dati personali trattati sono gestiti secondo procedure formalizzate di gestione degli incidenti di sicurezza, in coordinamento con le strutture competenti in materia di sicurezza informatica, gestione documentale e protezione dei dati personali.

Qualora un incidente comporti una violazione dei dati personali (personal data breach), l'Università procede alla relativa gestione secondo le procedure interne adottate, assicurando la tempestiva valutazione dell'evento, la registrazione delle informazioni rilevanti, l'adozione delle misure di contenimento e mitigazione e, ove ricorrano i presupposti previsti dagli articoli 33 e 34 del GDPR, la notifica all'Autorità Garante per la protezione dei dati personali e la comunicazione agli interessati.

Il Responsabile della Protezione dei Dati (RPD), in riferimento al presente Manuale, svolge le funzioni di cui all'art. 39 del GDPR.

10.3. Piano della sicurezza del sistema di gestione informatica dei documenti

Come precedentemente detto, il piano della sicurezza costituisce parte integrante del sistema di governo documentale dell'Ateneo e definisce le misure tecniche e organizzative e procedurali volte a garantire la sicurezza del sistema di protocollo informatico, del sistema documentale e dei processi di versamento dei documenti informatici nel sistema di conservazione, mediante i seguenti meccanismi di sicurezza:



- l'identificazione univoca degli utenti e l'autenticazione degli accessi;
- la profilazione preventiva degli utenti mediante assegnazione di ruoli e privilegi coerenti con le funzioni svolte;
- il controllo degli accessi ai documenti e alle aggregazioni documentali sulla base del principio di necessità e minimizzazione;
- la protezione dei documenti contenenti dati riservati o dati personali appartenenti alle categorie particolari di cui all'art. 9 del GDPR e dei dati relativi a condanne penali e reati di cui all'art. 10 del GDPR;
- l'audit logging e il monitoraggio delle operazioni effettuate dagli utenti;
- la protezione dei sistemi mediante misure di aggiornamento, manutenzione e gestione delle vulnerabilità;
- l'esecuzione di copie di sicurezza e procedure di ripristino periodicamente verificate;
- la gestione degli incidenti di sicurezza e degli eventuali eventi di data breach secondo le procedure adottate dall'Ateneo;
- il mantenimento nel tempo dell'integrità, dell'autenticità e della leggibilità dei documenti trasferiti in conservazione.

L'Ateneo assicura inoltre il coordinamento tra il presente Manuale, il Manuale di Conservazione, il Registro dei Trattamenti, le Politiche di sicurezza, il Piano di Gestione del rischio ai sensi della direttiva NIS2, il Piano di business continuity e le procedure di gestione degli incidenti di sicurezza e delle violazioni dei dati personali. Con particolare riguardo all'attuazione della direttiva NIS2, l'Università degli Studi di Napoli Federico II è classificata come soggetto NIS importante (settore Istruzione superiore e Ricerca, Allegato II del D.Lgs. 138/2024) e il MUR è autorità NIS di settore.

I trattamenti di dati personali effettuati mediante il Sistema di Gestione Documentale sono censiti nel Registro delle attività di trattamento dell'Ateneo ai sensi dell'art. 30 del GDPR.

Le misure di sicurezza, di seguito più dettagliatamente descritte, sono soggette a verifica periodica e ad aggiornamento in occasione di modifiche normative, organizzative, procedurali o tecnologiche che possano incidere sul livello di rischio associato al trattamento dei dati e alla gestione dei documenti informatici. Il processo di risk assessment segue l'approccio metodologico e implementa, secondo le indicazioni riportate dai responsabili di Ateneo per la governance della sicurezza, le contromisure riportate nel Piano di Gestione del rischio ai sensi della direttiva NIS2, dal momento che il sistema di gestione informatica dei documenti è compreso nel perimetro NIS2 ed è stato categorizzato dall'Ateneo nella macro-area "Servizi amministrativi e finanziari", con rilevanza assegnata di livello "Medio", in accordo con quanto proposto dall'ACN. |



10.3.1. Criteri di identificazione e autenticazione per l'accesso al sistema

L'accesso al sistema SPI e al sistema SD è consentito ai soli dipendenti dell'Ateneo abilitati che si autenticano mediante le proprie credenziali IAM (Identity and Access Management) di Ateneo.

10.3.2. Policy di visibilità dei dati e dei documenti e di abilitazione alle funzionalità

Le policy di visibilità implementate nel sistema sono riconducibili sia ai parametri di autorizzazione definiti dall'Amministrazione, sia a funzionalità di base configurate nel sistema stesso, in quanto conforme alle disposizioni di legge sul diritto di accesso e sulla tutela della riservatezza.

In particolare, la visibilità dei dati e dei documenti è determinata da:

- logiche di visibilità gerarchica;
- liste di competenza (Access Control List – ACL);
- flussi di assegnazione dei documenti e dei fascicoli e operazioni di condivisione;
- la profilatura degli utenti per l'abilitazione all'accesso ai dati e alla documentazione registrata nel sistema di gestione documentale, nonché all'abilitazione all'uso delle funzionalità del sistema.

L'attribuzione delle autorizzazioni avviene secondo il principio del minimo privilegio (least privilege), limitando l'accesso ai documenti e alle funzionalità strettamente necessari allo svolgimento delle attività istituzionali attribuite all'utente.

Le logiche di visibilità gerarchica impostate di default nel sistema garantiscono alle strutture organizzative superordinate della AOO (le UOR complesse, caratterizzate da sotto UOR oppure sotto UO) di accedere ai dati e di controllare le attività svolte dalle strutture sottostanti. Viceversa, è inibita la possibilità da parte degli uffici di livello gerarchico inferiore di accedere a dati e documenti gestiti dalle strutture superordinate.

La gestione degli accessi si basa da una parte su una profilatura funzionale che abilita o meno agli utenti determinate azioni e dall'altra su una serie di ACL sugli oggetti (in primis documenti e fascicoli, ma non solo) che abilitano gli stessi utenti ad utilizzare quelle funzionalità solo sugli oggetti a cui hanno accesso.

Un concetto peculiare di SPI e SD è quello di scrivania: un utente non può entrare nel sistema se non ha almeno una scrivania associata, la quale è la rappresentazione virtuale del ruolo all'interno del sistema. Nel sistema di gestione documentale UniNA si è scelto di rendere centrale il ruolo delle scrivanie associando ad esse la profilatura e le ACL in modo da rendere semplice gestire gli avvicendamenti delle persone nei vari ruoli dell'Ateneo, in questo modo infatti sarà sufficiente associare l'utente alla scrivania lasciata libera dal precedente utente per fargli ereditare tutti i suoi fascicoli/documenti e/o compiti di workflow. A ciascun utente, può quindi essere attribuito più di un profilo applicativo, ciascuno collegato a una Unità Organizzativa e, a valle della autenticazione, l'utente deve selezionare il profilo attraverso il quale operare nell'ambito della rispettiva UO.



Le attività di configurazione dei profili applicativi e di abilitazione degli utenti sono di competenza degli utenti in possesso del ruolo di Amministratore di Sistema e sono regolate da criteri organizzativi e autorizzativi interni all'Amministrazione. Per ulteriori dettagli sui profili e sul processo di autorizzazione si rimanda all'**Allegato 6** al presente Manuale.

Gli Amministratori di Sistema sono abilitati a fronte di uno specifico atto di nomina, così come previsto dall'art. 16 del Regolamento di Ateneo in materia di trattamento dei dati personali.

10.3.3. Accesso alla documentazione riservata e contenente dati particolari

Ai sensi dell'art. 32 del Regolamento UE 2016/679, l'Amministrazione, tenendo conto dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali di cui è titolare e depositaria, mette in atto adeguate misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tali misure sono garantite sia dal ricorso a specifiche funzionalità del sistema di gestione documentale che consentono una corretta gestione della documentazione riservata contenente dati personali, sia dall'individuazione, all'interno dell'Università, di determinate figure di responsabilità incaricate del trattamento dei dati, le quali dispongono di particolari permessi applicativi per gestirne la registrazione o per autorizzarne e monitorarne gli accessi.

La configurazione dei profili autorizzativi e delle funzionalità di accesso al Sistema di Gestione Documentale è effettuata secondo i principi di privacy by design e privacy by default di cui all'art. 25 del Regolamento (UE) 2016/679, assicurando che siano trattati esclusivamente i dati necessari rispetto alle finalità perseguite.

In particolare, per la gestione dei documenti contenenti dati personali di tipo particolare il sistema di gestione documentale (sia SPI che SD) mette a disposizione una funzionalità attivabile in fase di protocollazione/acquisizione del documento, che consente sia di impedirne l'accesso agli utenti non abilitati o non opportunamente autorizzati, sia di oscurarne i dati relativi all'oggetto e ai corrispondenti negli elenchi di ricerca.

Nel sistema SD, l'attributo relativo alla presenza di dati ad accesso limitato, cioè riservati e/o personali particolari, oltre che al singolo documento, può essere attribuito a un

intero fascicolo procedimentale, di fatto oscurandone il contenuto agli utenti non dotati di idonea autorizzazione alla visualizzazione di tale fattispecie di documenti.

10.3.4. Funzioni di logging e monitoraggio

I sistemi SPI e SD dispongono di specifiche funzionalità per il monitoraggio e la storicizzazione delle operazioni effettuate all'interno dello stesso. In particolare, tali funzioni garantiscono:

- Audit log: la registrazione di tutte le attività svolte dagli utenti, il tracciamento delle singole operazioni e l'identificazione dei rispettivi responsabili;
- Monitoraggio accessi: il controllo degli accessi al sistema e alla documentazione in esso registrata.

I log applicativi e di accesso sono conservati secondo le policy di sicurezza adottate dall'Ateneo e sono accessibili esclusivamente ai soggetti autorizzati per finalità di sicurezza, audit, controllo e gestione degli incidenti.

Presso il CSI è inoltre operativo il SIEM centralizzato per raccogliere, aggregare e analizzare in tempo reale alert su eventi di sicurezza significativi generati dall'intera infrastruttura IT di Ateneo e viene assicurata dal Referente CSIRT la tenuta e l'aggiornamento in tempo reale del registro incidenti e "near-miss".

10.3.5. Continuità operativa, backup e disaster recovery

Per garantire la continuità operativa del sistema e delle operazioni indispensabili per i servizi erogati, le risorse sono ridondate al fine di un loro ripristino in caso di malfunzionamento. Tra tali funzioni vi sono quelle di salvataggio periodico (back-up), mirroring dei dischi, adozione di architetture di sistema configurate in HA (Alta disponibilità).

Il salvataggio dei dati del sistema documentale avviene con frequenza giornaliera. In particolare, per quanto riguarda i server su cui risiedono DB, il sistema SAN, il back-up del sistema è eseguito quotidianamente in modalità incrementale dei dati su libreria centralizzata; il sabato viene eseguito il dump completo del sistema. Inoltre, viene eseguito ogni notte il back-up incrementale del DB e settimanalmente quello totale.

Dal punto di vista applicativo, il sistema SPI mette a disposizione una funzionalità per la gestione delle interruzioni di servizio fino al ritorno alla normale operatività del sistema e il recupero dei dati al termine della fase di emergenza, come illustrato nel par. 6.9.2.

Dal punto di vista della architettura, i sistemi sono ridonati in configurazione HA, garantendo sia un bilanciamento di carico che la continuità operativa (seppur con prestazioni degradate) in caso di guasto di un componente.

Infine, a livello infrastrutturale, la adeguata gestione di interruzioni di corrente elettrica o di picchi di tensione viene assicurata dalla presenza dei seguenti dispositivi:

- Sistema UPS
(Continuità di alimentazione)
- Inverter per stabilizzazione
(Continuità di alimentazione)

10.3.6. Sistemi che evidenziano eventi anomali

La funzione permette di investigare sugli eventi che, discostandosi da determinate soglie, possono rappresentare una minaccia alla sicurezza. Devono essere presenti e documentati appositi strumenti per esaminare e gestire gli archivi registrati. Tali strumenti devono consentire di identificare selettivamente le azioni eseguite da uno o più utenti. Periodicamente controllano le registrazioni, per verificare casi anomali o sospetti. Permettono l’alert online o differito al superamento di opportune soglie di sicurezza predefinite.

I sistemi SPI e SD, al pari dei restanti sistemi infrastrutturali e applicativi gestiti dal CSI, sono sottoposti a monitoraggio mediante il sistema Nagios in grado di inviare alert (anche preventivi) a console di sistema, mailing list e cellulari, al verificarsi di eventi anomali o al raggiungimento di prefissate soglie (ad es., di occupazione disco).

10.3.7. Rilevazione e ripristino affidabilità software

La funzione permette l’analisi del software al fine di identificare, segnalare e correggere violazioni dell’integrità. Fra tali funzioni vi sono quelle di identificazione ed eliminazione dei virus, bombe logiche e “cavalli di troia”, analisi del codice per verificare l’integrità degli eseguibili, la correttezza delle chiamate ai dati, etc.

Il software di sistema sui server viene aggiornato manualmente, a fronte di ogni nuovo annuncio di vulnerabilità dei sistemi.

Inoltre, i server sono protetti da una soluzione centralizzata antimalware costantemente aggiornata automaticamente ogni ora, configurata secondo le policy di sicurezza dell’Ateneo. Anche i PC degli utenti sono protetti dall’attacco di virus, in quanto sono dotati di programma antivirus, centralizzato per i PC collegati in rete dell’Amministrazione Centrale, e aggiornato automaticamente con cadenza giornaliera.

Il corretto deployment dell’applicazione dei sistemi SPI e SD è assicurato mediante preventiva verifica da parte dei gruppi di lavoro tecnici UniNA competenti prima del rilascio in produzione, nonché il prelevamento del software da installare da repository opportunamente allestiti, a cui hanno accesso solo gli Amministratori di Sistema. In particolare, gli unici soggetti abilitati a eseguire le operazioni di deployment in ambiente di produzione sono esclusivamente gli Amministratori di sistema SYS e DBA del CSI.

10.3.8. Manutenzione del software applicativo

Per quanto riguarda l'aggiornamento delle versioni del software, questo è previsto sia in caso di variazioni di carattere normativo, dalle quali deriva la necessità di effettuare interventi adeguativi, sia in caso di interventi evolutivi richiesti dall'Amministrazione per l'implementazione di nuove funzionalità. Nella prima casistica rientra, ad esempio, l'intervento di aggiornamento del software a seguito dell'entrata in vigore delle LLGG AgID nel gennaio 2022, che ha riguardato lo sviluppo e l'implementazione di specifiche funzionalità volte a garantire la conformità ai requisiti di legge in termini di:

- metadatazione (Allegato 5 alle LLGG AgID);
- interoperabilità via PEC con sottoscrizione mediante sigillo elettronico qualificato del file *segnatura.xml* (Allegato 6 alle LLGG AgID);
- revisione delle procedure per la storicizzazione delle modifiche dei dati;
- adeguamento alle firme europee, supporto delle firme remote e dei formati Cades-T, Pades-T, Xades-T.

Infine, l'Università ha provveduto a nominare le ditte che si occupano della manutenzione delle applicazioni Responsabili del trattamento, richiedendo i nominativi dei loro incaricati individuati quali Amministratori di Sistema. Nel rispetto della normativa in materia di protezione dei dati personali, in caso di malfunzionamento, per consentire l'attività di *problem determination & solving*, UniNA autorizza solo tali soggetti ad accedere agli ambienti di produzione, per periodi limitati e con rilascio di rapporti tecnici sull'intervento svolto.

In accordo con la Direttiva NIS2, i fornitori dei servizi ICT per la manutenzione del sistema di gestione informatica dei documenti (dai servizi infrastrutturali sistemistici e di rete a quelli applicativi) rientrano nel programma di gestione e presidio della supply-chain.

10.3.9. Qualità dei dati

È l'insieme di misure da intraprendere al fine di elevare la qualità dei dati, con particolare riferimento ai dati entranti nel Sistema Informatico dell'Ateneo. Tali misure consistono in funzioni di valorizzazione, funzioni di integrità semantica, funzioni di integrità referenziale, funzioni di integrità logica, funzioni di non ridondanza e funzioni di aggiornamento.

Per quanto concerne il sistema di gestione documentale, in fase progettuale di sviluppo sono stati previsti meccanismi di controllo da realizzare e applicare a livello di DBMS e/o applicativo al fine di garantire: *accuratezza* (garanzia che il contenuto di ogni dato, in ciascuno dei suoi attributi, sia dettagliato in maniera significativa e priva di errori); *completezza* (garanzia che un determinato dato sia previsto nello schema strutturale e sia valorizzato in tutti i suoi elementi in base ai requisiti informativi); *conformità* (garanzia che il contenuto del dato sia in armonia col contenuto degli altri dati, rispettando l'insieme dei vincoli logici e referenziali che legano i dati tra loro); *interpretabilità* (garanzia che il valore del dato sia comprensibile per tutti i possibili utenti, senza adito ad alcuna ambiguità); *tempestività* (garanzia che il valore del dato



risultati aggiornato al momento in cui viene reso disponibile all'utente finale in ragione delle esigenze di utilizzo).

Il rispetto di tali requisiti è reso possibile, sotto il profilo tecnologico, dall'utilizzo della tecnologia Oracle su appliance ODA (che utilizza la funzionalità integrata di crittografia dei dati persistenti) e SAN per quanto attiene al file system, cioè di infrastrutture tecnologiche e sistemi di archiviazione che garantiscono cifratura, integrità, disponibilità e resilienza dei dati secondo le policy di sicurezza dell'Ateneo.

Per quanto riguarda i pacchetti di archiviazione materializzati su file system, qualsiasi oggetto presentato al sistema viene archiviato in modo tale da essere inalterabile, autenticato e trasparente all'applicazione. Inoltre, configurando le impostazioni per la conservazione dei dati è possibile impedire che le informazioni vengano cancellate prima della scadenza del periodo di conservazione definito. Il controllo per la protezione, la conservazione e l'eliminazione avviene a livello di singolo oggetto, in funzione del tempo di conservazione per la sua tipologia documentale, dopo che è scaduto il rispettivo periodo di conservazione.

10.3.10. Controllo interscambio dati

Funzione che assicura la sicurezza nelle trasmissioni di dati attraverso: autenticazione dell'originatore, integrità e riservatezza del contenuto del messaggio, non ripudio dell'originatore e del destinatario. Tale funzione può essere articolata conformemente allo standard X.509, nelle seguenti categorie di servizi di sicurezza:

- Autenticazione
- Controllo autorizzazioni
- Riservatezza dei dati
- Integrità dei dati
- Non ripudio

Di seguito se ne riporta una breve descrizione:

- Autenticazione: garanzia che un'entità di pari livello in una comunicazione è quella che dichiara di essere;
- Controllo autorizzazioni: impedimento dell'uso non autorizzato di una risorsa, incluso l'utilizzo di una risorsa in una maniera non autorizzata. In particolare, per ogni transazione via internet bisogna sempre utilizzare un sistema filtro di tipo "firewall";
- Riservatezza dei dati: protezione dei dati da accessi non autorizzati, mediante sistemi di crittografia;
- Integrità dei dati: la proprietà dei dati non deve essere alterata o distrutta; devono, cioè, essere riconosciute le manipolazioni non autorizzate di dati;
- Non ripudio:
 - Non ripudio di origine dei dati: il servizio garantisce al destinatario dei dati la prova della loro origine e protegge dal tentativo del mittente di negare falsamente la spedizione dei dati o il loro contenuto;



- Non ripudio del destinatario: il servizio garantisce al mittente dei dati l'avvenuta ricezione dei dati e protegge dal tentativo del destinatario di negare falsamente di aver ricevuto i dati o il loro contenuto.

In particolare, l'integrità dei documenti è assicurata mediante associazione univoca e persistente al documento registrato di una sua impronta crittografica basata su funzioni di hash SHA-256. Inoltre, per i documenti firmati digitalmente, il sistema di gestione documentale effettua il controllo di integrità e di autenticità prima della registrazione e blocca la registrazione nel caso in cui non sia superata la verifica di integrità e validità del documento.

Per quanto riguarda la trasmissione e interscambio dei documenti informatici, il sistema di gestione documentale è accessibile da web esclusivamente con protocollo https e inoltre, previa autorizzazione dei server coinvolti basata su ACL, dialoga con le applicazioni interoperabili mediante protocollo TLS con autenticazione forte mediante certificati digitali oppure basic authentication, a seconda dei casi.

Infine, entrambi i sistemi per la gestione informatica dei documenti utilizzano la PEC come mezzo trasmissivo per lo scambio di documenti amministrativi: in questo caso, l'infrastruttura certificata garantisce la provenienza del messaggio e, oltre alla data e ora certa, fornisce certezza dell'integrità.