

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO

EMISSIONE DEL DOCUMENTO

AZIONE	DATA	NOMINATIVO	FUNZIONE
<i>Redazione</i>		Emanuela Diamantini	Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi
<i>Verifica</i>		Emanuela Diamantini	
<i>Approvazione</i>	29/12/2017	Luca Ferrucci	Commissario straordinario

REGISTRO DELLE VERSIONI

N°VER/REV/BOZZA	DATA EMISSIONE	MODIFICHE APPORTATE	OSSERVAZIONI
1°		Adeguamento del Piano di sicurezza al D.Lgs. n. 196/2003 – Codice in materia di protezione di dati personali, come da ultimo modificato e integrato con D.Lgs. 101/2018“Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679	
		Inserimento dell'allegato III “Regolamento per la gestione, la consultazione, l'accesso ai documenti dell'archivio di deposito” (Cap. 6)	
		Modifica del Titolare di classificazione	

INDICE

1. PRINCIPI GENERALI.....	4
1.1 PREMESSA	4
1.2 DEFINIZIONI.....	4
1.3 MODELLO ORGANIZZATIVO - AREA ORGANIZZATIVA OMOGENEA	8
1.4 SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO LA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI.	9
1.5 REGISTRO DI PROTOCOLLO	10
1.6 FORMAZIONE.....	11
1.7 ELIMINAZIONE DEI REGISTRI DI PROTOCOLLO DI SETTORE	11
1.8 TUTELA DEI DATI PERSONALI	11
2. PIANO DI SICUREZZA.....	12
2.1 OBIETTIVI DEL PIANO DI SICUREZZA	12
2.2 GENERALITÀ.....	12
2.3 AGGIORNAMENTO E MANUTENZIONE DEL SISTEMA GESTIONE DOCUMENTALE.....	13
2.4 FORMAZIONE DEI DOCUMENTI - ASPETTI ATTINENTI ALLA SICUREZZA.....	14
2.5 GESTIONE DEI DOCUMENTI INFORMATICI	14
2.5.1 COMPONENTE FISICA DELLA SICUREZZA	15
2.5.2 COMPONENTE LOGICA DELLA SICUREZZA	16
2.6 ACCESSO AI DOCUMENTI INFORMATICI.....	16
2.6.1 UTENTI INTERNI ALLA AOO.....	17
2.6.2 ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI ALLA AOO.....	17
2.6.3 UTENTI ESTERNI ALLA AOO- ALTRE AOO/AMMINISTRAZIONI.....	18
2.6.4 UTENTI ESTERNI ALLA AOO- PRIVATI.....	18
2.7 CONSERVAZIONE DEI DOCUMENTI INFORMATICI	18
3. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI	19
3.1 DOCUMENTO AMMINISTRATIVO	19
3.2 DOCUMENTO ANALOGICO	19
3.3 DOCUMENTO INFORMATICO.....	20
3.4 ULTERIORI FORMATI UTILIZZATI PER LA FORMAZIONE DEL DOCUMENTO	

INFORMATICO	20
3.5 DOCUMENTO RICEVUTO	21
3.6 DOCUMENTO INVIATO	21
3.7 DOCUMENTO INTERNO FORMALE	21
3.8 DOCUMENTO INTERNO INFORMALE	22
3.9 FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI	22
3.10 FIRMA DIGITALE	23
3.11 MARCA TEMPORALE	25
3.12 USO DELLA POSTA ELETTRONICA CERTIFICATA (PEC).....	25
4. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI	27
4.1 RICEZIONE E TRASMISSIONE DEI DOCUMENTI	27
4.1.1 RICEZIONE DI DOCUMENTI CARTACEI.....	27
4.1.2 RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI CARTACEI	28
4.1.3 RICEZIONE DI DOCUMENTI INFORMATICI.....	28
4.1.4 RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI INFORMATICI....	29
4.1.5 RICEZIONE DI DOCUMENTI INFORMATICI SU SUPPORTI REMOVIBILI.....	29
4.1.6 TRASMISSIONE DI DOCUMENTI CARTACEI TRAMITE POSTA/CORRIERE	29
4.1.7 TRASMISSIONE DI DOCUMENTI CARTACEI TRAMITE FAX	30
4.1.8 TRASMISSIONE DI DOCUMENTI INFORMATICI	30
4.2 REGISTRAZIONE E SEGNATURA DEI DOCUMENTI.....	31
4.2.1 REGISTRAZIONE DI PROTOCOLLO	31
4.2.2 SEGNATURA DI PROTOCOLLO	32
4.2.3 ACQUISIZIONE DELLE RAPPRESENTAZIONI DIGITALI DI DOCUMENTO CARTACEI.....	33
4.2.4 DIFFERIMENTO DEI TERMINI DI REGISTRAZIONE	33
5. <u>REGOLE DI SMISTAMENTO ED ASSEGNAZIONE DEI DOCUMENTI RICEVUTI</u>	
_____ 34	
5.1 DESCRIZIONE FUNZIONALE ED OPERATIVA	34
5.2 MODIFICA DELLE ASSEGNAZIONI	35
5.3 ANNULLAMENTO DI UNA REGISTRAZIONE DI PROTOCOLLO.....	35
5.4 REGISTRO GIORNALIERO DI PROTOCOLLO	35
5.5 REGISTRO DI EMERGENZA	36
5.6 DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE	36
5.7 DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO	37
5.8 RICEZIONE DI LETTERE ANONIME E PRIVE DI FIRMA	38

5.9	REGISTRAZIONI DI PROTOCOLLO URGENTI.....	38
5.10	RILASCIO DELLE ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI	38

6. CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE DEI DOCUMENTI

40

6.1	TITOLARIO O PIANO DI CLASSIFICAZIONE.....	40
6.2	ARCHIVIO	41
6.3	MISURE DI PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI.....	41
6.4	MASSIMARIO DI SELEZIONE E SCARTO.....	42
6.5	FASCICOLAZIONE DEI DOCUMENTI.....	42
6.6	REPERTORIO DEI FASCICOLI	44
6.7	SERIE ARCHIVISTICHE E REPERTORI	44

7. NORME TRANSITORIE E FINALI.....

7.1	MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE.....	45
7.2	OPERATIVITÀ DEL PRESENTE MANUALE	45
	NORMATIVA DI RIFERIMENTO	46

1. PRINCIPI GENERALI

1.1 Premessa

Il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - recante *“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”*, prevede l’obbligo per le pubbliche amministrazioni di cui all’art. 2 del D.lgs. n. 165/2001 di “adottare il *Manuale di gestione del protocollo informatico, dei documenti e dell’archivio* (di seguito Manuale), su proposta del Responsabile della gestione documentale”(art. 3).

Il Manuale, redatto secondo quanto previsto dall’art. 5, comma 1, del suddetto DPCM, descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del *Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi* dell’ADiSU per il Diritto allo studio universitario dell’Umbria (di seguito ADiSU). Il documento è composto da disposizioni di carattere generale, che presumibilmente rimarranno invariate nel tempo, e specificazioni di natura operativa o di dettaglio, che invece richiederanno un continuo adeguamento al contesto organizzativo e tecnologico dell’ADiSU e alla normativa sopravvenuta.

Il Manuale è destinato alla più ampia diffusione e conoscenza interna ed esterna, in quanto fornisce le istruzioni necessarie per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti; pertanto, si rivolge non solo agli operatori di protocollo, ma, in generale, a tutti i dipendenti e anche ai soggetti esterni che si relazionano con l’ADiSU.

Il presente documento sostituisce dal 1° gennaio 2018 il precedente manuale approvato con delibera del Commissario straordinario n. 61 del 9 dicembre 2008.

1.2 Definizioni

Ai fini del presente Manuale si intende per:

- I. Amministrazione: l’ADiSU per il Diritto allo Studio Universitario dell’Umbria (ADiSU)
- II. Area Organizzativa Omogenea (AOO): un insieme di funzioni e di strutture, individuate dall’Amministrazione che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato
- III. Archivio corrente: la parte di documentazione relativa agli affari ed ai procedimenti in

corso di trattazione, o comunque verso i quali sussiste un interesse corrente

- IV. Archivio di deposito: la parte di documentazione relativa ad affari esauriti, non più occorrenti quindi alla trattazione degli affari in corso, ma non ancora destinata istituzionalmente alla conservazione permanente e alla consultazione da parte del pubblico
- V. Archivio storico: il complesso di documenti relativi ad affari esauriti e destinati, previa operazioni di scarto, alla conservazione permanente per garantirne in forma adeguata la consultazione al pubblico
- VI. Codice dell'amministrazione digitale (CAD): il decreto legislativo 7 marzo 2005, n. 82
- VII. Conservazione elettronica dei documenti informatici: è un processo che si serve di soluzioni informatiche al fine di assicurare a lungo termine il mantenimento del valore giuridico, delle caratteristiche di integrità ed autenticità, ma anche l'accesso e la leggibilità ai documenti informatici oggetto di conservazione
- VIII. Cooperazione applicativa: la parte del Sistema Pubblico di Connettività finalizzata all'interazione tra i sistemi informatici dei soggetti partecipanti, per garantire l'integrazione dei metadati, delle informazioni, dei processi e procedimenti amministrativi
- IX. Documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
- X. 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 (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - «Regolamento eIDAS», valido ai fini delle comunicazioni elettroniche aventi valore legale
- XI. Fascicolo: l'unità di base indivisibile di un archivio che raccoglie i documenti relativi ad un procedimento amministrativo o ad un affare; aggregazione organizzata di documenti prodotti o ricevuti dalle unità organizzative dell'Amministrazione
- XII. Firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario 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

- XIII. Flusso documentale: il movimento dei documenti sia all'interno dell'archivio che tra le unità organizzative che compongono una AOO
- XIV. Gestione dei documenti: l'insieme delle attività finalizzate alla formazione, ricezione, registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dall'Amministrazione, nell'ambito del sistema di classificazione d'archivio adottato; essa è effettuata mediante sistemi informativi automatizzati
- XV. Impronta di un documento informatico: una sequenza di simboli binari in grado di identificarne univocamente il contenuto
- XVI. Indice PA: l'indice delle amministrazioni pubbliche e delle Aree Organizzative
- XVII. Interoperabilità: la possibilità di trattamento automatico, da parte del sistema di protocollo ricevente, delle informazioni trasmesse dal sistema di protocollo mittente, allo scopo di automatizzare le attività ed i procedimenti amministrativi conseguenti
- XVIII. Massimario di selezione: il componente del piano di conservazione che definisce le disposizioni e i criteri di massima per attuare la selezione ed elenca le serie e i documenti la cui conservazione deve essere illimitata
- XIX. Piano di conservazione di un archivio: il piano, integrato con il titolario di classificazione, contenente i criteri di organizzazione dell'archivio, di selezione periodica e conservazione permanente dei documenti ai sensi dell'art. 68 del DPR 445/2000
- XX. Posta elettronica certificata: il servizio di posta elettronica che, ai sensi del D.P.R. 11 febbraio 2005, n. 68, garantisce la riservatezza, l'integrità e la consegna dei messaggi
- XXI. Registrazione di protocollo: l'operazione di registrazione quotidiana dei documenti ricevuti e spediti dall'amministrazione, assegnando contestualmente a ciascuno di essi un numero progressivo, che comincia dal n. 1 (uno) all'inizio di ogni anno solare. La registrazione a protocollo attesta in modo inoppugnabile l'esistenza all'interno dell'archivio e la data archivistica del singolo documento, che viene identificato in modo univoco dal numero progressivo assegnatogli
- XXII. Registro di protocollo: il registro su cui si annotano quotidianamente i documenti ricevuti o spediti dall'Amministrazione
- XXIII. Repertorio: il registro su cui si trascrivono e nel quale si inseriscono in sequenza determinata (in genere cronologica) documenti ai quali si attribuisce un numero

identificativo progressivo con valenza probatoria

- XXIV. Scarto: la eliminazione fisica e irreversibile di documenti
- XXV. Segnatura di protocollo: l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile, delle informazioni che consentono di identificare in modo inequivocabile il documento stesso
- XXVI. Serie: ciascun raggruppamento, operato dall'Amministrazione stessa, di documenti o fascicoli con 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'Amministrazione
- XXVII. Servizio archivistico: l'ambito organizzativo preposto alla tenuta del protocollo informatico, alla gestione dei flussi documentali e degli archivi
- XXVIII. Sistema pubblico di identità digitale (SPID): è il sistema unico di login per l'accesso ai servizi on line della pubblica amministrazione italiana e dei privati aderenti
- XXIX. Testo unico: il DPR 28 dicembre 2000, n° 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- XXX. Titolario di classificazione: un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'Amministrazione, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la sedimentazione secondo un ordine logico che rispecchi storicamente lo sviluppo dell'attività svolta
- XXXI. Ufficio Utente: un ufficio dell'area organizzativa omogenea che utilizza i servizi messi a disposizione dal sistema di gestione informatica dei documenti
- XXXII. Unità archivistica: un documento o un insieme di documenti, aggregati secondo un nesso logico di collegamento organico, che li individua come unità indivisibile: fascicolo, registro, repertorio
- XXXIII. Versamento: l'operazione con cui ciascuna unità organizzativa trasferisce periodicamente alla struttura deputata alla conservazione permanente la parte di archivio non più occorrente alla trattazione degli affari

Si riportano di seguito gli acronimi utilizzati più frequentemente:

- AOO - Area Organizzativa Omogenea (ADiSU);
- IPA - Indice delle Pubbliche Amministrazioni - elenco di tutti gli uffici pubblici con casella di posta elettronica a disposizione del pubblico;
- MdG – Manuale

- RPA - Responsabile del Procedimento Amministrativo;
- RGD - Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi;
- SGD - Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi
- UP - UP;
- UU - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.

1.3 Modello organizzativo - Area organizzativa omogenea

Ai fini della gestione dei documenti e dell'archivio, è individuata una sola Area Organizzativa Omogenea (AOO) denominata: **ADiSU per il diritto allo studio universitario dell'Umbria** (ADiSU).

L'organigramma dell'ADiSU è pubblicato sul sito istituzionale nella sezione "*Amministrazione trasparente*" – sottosezione "*Organizzazione*".

L'ADiSU, nell'ambito degli adempimenti previsti, è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) tenuto e reso pubblico da AGID.

Il codice IPA dell'ADiSU è: adsu_pg.

Il sistema di protocollazione è di tipo accentrato e tutta la corrispondenza, in ingresso e in uscita, è gestita dal UP.

L'ADiSU/AOO è dotata:

- di una casella di Posta Elettronica Certificata istituzionale adisu@pec.it, pubblicata sull'IPA;
- di una casella di posta elettronica di tipo tradizionale adisu@adisu.umbria.it.

L'Amministrazione può istituire ulteriori caselle di posta elettronica certificata, disciplinandone la gestione per uffici e procedimenti specifici.

In attuazione di quanto previsto dalla Direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'ADiSU ha creato per tutti i dipendenti una casella di posta elettronica del tipo: nome.cognome@adisu.umbria.it.

Le suddette e-mail sono indicate sul sito istituzionale dell'ADiSU nella sezione "*Amministrazione trasparente*" - sottosezione "*Organizzazione*": *articolazione degli uffici*,

secondo quanto stabilito dal D.Lgs. 33/2013.

La descrizione dettagliata di tutte le funzioni e delle modalità di utilizzo del software per la gestione del protocollo informatico è contenuta nel manuale del software disponibile in IntrADiSU – Sezione Modulistica.

1.4 Servizio per la tenuta del protocollo informatico la gestione dei flussi documentali e degli archivi.

Nella AOO è istituito il *Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi* (di seguito SGD), funzionalmente incardinato nella Sezione II “Affari generali e servizi comuni” del Servizio II “Organizzazione e gestione delle risorse umane, finanziarie e servizi comuni”.

Il protocollo informatico unico è lo strumento attraverso il quale l'ADiSU garantisce l'effettiva ricezione e trasmissione dei documenti

Al SGD è preposto il Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RGD).

Nei casi di assenza, impedimento o vacanza del RGD, la responsabilità del SGD è affidata al Responsabile della Conservazione digitale o suo vicario.

Al Servizio sono assegnati i seguenti compiti:

- predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del Manuale sul sito istituzionale dell'ADiSU;
- richiedere alla Sezione “Sistema informativo” di abilitare gli utenti dell'ADiSU all'utilizzo del Sistema di protocollo informatico, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;
- garantire il buon funzionamento degli strumenti interni all'AOO e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le

- attività di gestione degli archivi;
- autorizzare le eventuali operazioni di annullamento della registrazione di protocollo;
 - curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza;
 - curare la gestione, conservazione e fruizione dell'archivio dell'ADiSU in conformità alla normativa vigente;
 - predisporre in collaborazione con la Sezione "Sistema informativo" il *Piano per la sicurezza* relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso e alla conservazione dei documenti informatici.

1.5 Registro di protocollo

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.

Tale registro soggiace alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa in materia.

La numerazione delle registrazioni di protocollo è unica e progressiva; si conclude il 31 dicembre di ogni anno ed inizia il 1 gennaio dal numero 0000001.

Ai sensi dell'articolo 57 del Testo Unico il numero di protocollo è costituito da sette cifre numeriche seguito dal simbolo "/" e dalle ultime due cifre dell'anno (Es: 0001234/17).

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.

Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in uscita.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale o informatica di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se collegati tra loro.

Non è consentita la protocollazione di un documento già protocollato.

La documentazione che non è stata registrata presso l'UP viene considerata giuridicamente inesistente.

Entro il 31 gennaio dell'anno successivo a quello di riferimento, il RGD esegue la stampa del registro annuale di protocollo in formato PDF/A e la sottopone al Dirigente competente che

la sottoscrive digitalmente.

1.6 Formazione

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni dalla direttiva del 13 dicembre 2001 del Ministro della funzione pubblica sulla formazione e la valorizzazione del personale delle pubbliche amministrazioni, l'ADiSU stabilisce percorsi formativi specifici e generali che coinvolgono tutte le figure professionali. In particolare, per quanto concerne il processo di dematerializzazione dell'azione amministrativa, saranno pianificati specifici percorsi formativi in materia archivistica, imprescindibili per poter creare e gestire fascicoli digitali.

1.7 Eliminazione dei registri di protocollo di settore

In coerenza con quanto previsto e disciplinato, i documenti inviati e ricevuti dall'ADiSU sono registrati all'interno del registro di protocollo informatico. Pertanto tutti i registri particolari di protocollo sono aboliti ed eliminati.

1.8 Tutela dei dati personali

L'ADiSU titolare dei dati di protocollo e dei dati personali contenuti nella documentazione amministrativa di propria pertinenza dà attuazione al dettato del Regolamento EU 2016/679 e del D.Lgs. 196/2003, come da ultimo modificato e integrato con D.Lgs. 101/2018 con atti formali aventi rilevanza interna ed esterna.

Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, sono stati autorizzati dal titolare dei dati.

Le regole e le modalità operative stabilite dall'ADiSU sono riportate nel Piano di sicurezza di cui al successivo capitolo 2.

2. PIANO DI SICUREZZA

Il presente capitolo riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

2.1 Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'ADiSU siano, su base permanente, riservati, l'integri e disponibili;
- i dati personali vengano trattati in modo da ridurre al minimo, mediante l'adozione di misure tecniche e organizzative *adeguate*, i rischi di distruzione o perdita, anche accidentale, di trattamento non autorizzato o illecito, *"(...) tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche"*.

2.2 Generalità

Il piano di sicurezza si basa sui risultati delle analisi dei rischi a cui sono esposti i dati e i documenti trattati e definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al sistema di protocollo, di gestione documentale ed archivistico;
- le misure di sicurezza operative adottate sotto il profilo organizzativo, procedurale e tecnico;
- i piani specifici di formazione degli addetti;
- le modalità con cui deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione formale con cadenza almeno biennale. Esso può essere modificato anticipatamente oppure ove lo si ritenga opportuno.

Le valutazioni di sicurezza riguardano non solo i dati, ma l'intero ciclo del trattamento.

In ossequio alle disposizioni normative e regolamentari in materia, il Responsabile della Sezione "Sistema informativo" unitamente al RGD dell'ADiSU fissano le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto

tecnologico dell'ADiSU, la riservatezza e l'integrità delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- invio al sistema di conservazione del registro giornaliero di protocollo, da effettuare entro la giornata lavorativa successiva a quella della sua produzione, garantendone l'immodificabilità del contenuto, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema;
- cambio delle password con frequenza almeno semestrale durante la fase di esercizio;

Per quanto riguarda la password, occorre osservare le seguenti regole:

- non scrivere la propria password, meno che mai vicino alla postazione di lavoro;
- non comunicare a nessuno la password: lo scopo principale della password è assicurare che nessun altro possa utilizzare le risorse di un altro utente o possa farlo a suo nome;
- non usare password banali o facilmente identificabili come, ad esempio, il proprio nome, quello della moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

[2.3 Aggiornamento e manutenzione del Sistema gestione documentale](#)

L'implementazione, la gestione operativa, l'aggiornamento e la manutenzione del Sistema di gestione informatica dei documenti è assicurata dalla Sezione "Sistema informativo" dell'ADiSU.

Il Responsabile di tale struttura garantisce:

- la puntuale esecuzione delle operazioni di backup dei dati e dei documenti archiviati;
- il monitoraggio quotidiano dell'operatività del Sistema e l'intervento in caso di anomalie;
- l'integrità del patrimonio documentario e informativo memorizzato dal Sistema, anche in caso di migrazione dello stesso per obsolescenza tecnologica.

2.4 Formazione dei documenti - Aspetti attinenti alla sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- identificabilità del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l' idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno dell'Amministrazione.

L'ADiSU utilizza applicativi che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

Di norma i documenti redatti sono convertiti, prima della loro sottoscrizione con firma digitale, nel formato PDF/A al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento. Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici attualmente vigenti.

2.5 Gestione dei documenti informatici

Il server che ospita i file utilizzati come deposito dei documenti è configurato in maniera tale che:

- gli utenti non possano mai accedere ai documenti al di fuori del sistema di gestione documentale;
- avvenga la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione documentale:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata e in

uscita;

- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'ADiSU e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di protezione dei dati personali, con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

2.5.1 Componente fisica della sicurezza

OBIETTIVO: prevenire l'accesso fisico non autorizzato, il danneggiamento e l'intromissione nelle aree e nei locali che custodiscono il patrimonio informativo dell'ADiSU.

MISURE:

- l'accesso è consentito soltanto al personale autorizzato per motivi di servizio, mediante un sistema di autenticazione (tastiera con codice);
- i visitatori occasionali e gli ospiti devono esplicitare la procedura di registrazione. Essi non possono entrare e trattenersi nelle aree protette se non accompagnati da personale autorizzato;
- la sala server è dotata di sistemi di condizionamento per il raffreddamento delle apparecchiature;
- l'isolamento della sala server assicura la protezione delle apparecchiature da danneggiamenti accidentali o intenzionali. Il suo impianto di alimentazione è protetto da un gruppo di continuità.

La sicurezza degli Uffici dell'ADiSU è garantita dalle seguenti MISURE/AZIONI:

- porte degli uffici che si possono chiudere a chiave;
- accesso consentito ai soli visitatori autorizzati ed identificati;
- distruzione della documentazione contenente dati personali in modo da non essere più ricomponibile (sminuzzata), oppure mediante appositi apparecchi "distruggi documenti";
- sistemazione della documentazione e delle pratiche trattate o da trattare in armadi chiusi a chiave nel periodo di intervallo meridiano o al termine della giornata lavorativa;
- non lasciare documentazione sulle scrivanie o postazioni di lavoro a disposizione di

chiunque entri nell'ufficio/locale;

- ritiro delle stampe inviate alla stampante di piano quanto prima affinché non abbiano accesso alle stampe persone non autorizzate;
- gli addetti preposti alla duplicazione di documentazione o alla sostituzione della documentazione cartacea con registrazione ottica devono prestare attenzione a non dimenticare l'originale del documento all'interno della macchina fotocopiatrice e/o dello scanner.

2.5.2 Componente logica della sicurezza

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

Tale componente, nell'ambito del sistema di protocollo informatico e di gestione documentale è realizzata attraverso:

- identificazione, autenticazione ed autorizzazione utente;
- profilazione degli accessi;
- politica antivirus;
- firma digitale;
- monitoraggio sessioni di lavoro;
- riservatezza dei dati;
- integrità dei dati.

2.6 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso, pubblica (UserID) e privata (Password) ed un sistema di autorizzazione basato sulla profilazione preventiva degli utenti.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Queste, in sintesi, sono:

- Consultazione - per visualizzare in modo selettivo le registrazioni di protocollo eseguite da altri;
- Inserimento - per inserire gli estremi di protocollo, effettuare una registrazione di protocollo ed associare i documenti;
- Modifica - per modificare i dati opzionali di una registrazione di protocollo;

- Annullamento - per annullare una registrazione di protocollo autorizzata dal RSP.

Il Sistema di gestione documentale fruito dall'AOO:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una Access Control List (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

Considerato che il Sistema di gestione documentale segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo Servizio, o alle Sezioni ad esso subordinate.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca full text.

2.6.1 Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal Responsabile della Sezione "Sistema informativo", sentito il RGD.

Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti principi operativi:

- gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta esplicita dell'amministratore dell'AOO o per errori di inserimento);
- la credenziale privata degli utenti e dell'amministratore AOO non transita in chiaro sulla rete, ne' al momento della prima generazione, ne' successivamente, al momento del login.

2.6.2 Accesso al registro di protocollo per utenti interni alla AOO

L'autorizzazione all'accesso ai registri di protocollo è regolata tramite i seguenti strumenti:

- liste di competenza, gestite dall'amministratore di AOO, per la definizione degli utenti abilitati ad accedere a determinate voci del Titolare;

- ruoli degli utenti, gestiti dall'amministratore di ente, per la specificazione delle macrofunzioni alle quali vengono abilitati;
- protocollazione "particolare o riservata", gestita dall'amministratore di ente, relativa a documenti sottratti alla consultazione da parte di chi non sia espressamente abilitato.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di "RGD".

L'operatore che gestisce lo smistamento dei documenti può definire "riservata" una registrazione di protocollo ed assegnarla per competenza ad un utente assegnatario.

Nel caso in cui sia effettuata una protocollazione riservata, la visibilità completa del documento è possibile solo all'utente assegnatario per competenza e agli operatori di protocollo che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo).

2.6.3 Utenti esterni alla AOO- Altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui agli art. 72 e ss. del d.lgs 7 marzo 2005 n. 82.

Le AOO che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC, utilizzano funzioni di accesso per ottenere le seguenti informazioni:

- numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
- identificazione dell'UU di appartenenza del RPA.

2.6.4 Utenti esterni alla AOO- Privati

Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso agli atti.

2.7 Conservazione dei documenti informatici

Per il dettaglio del processo di conservazione si rinvia al "Manuale della Conservazione Digitale" di prossima emanazione.

3. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'AOO.

Prima di entrare nel merito, occorre caratterizzare l'oggetto di scambio: il documento amministrativo

3.1 Documento amministrativo

I documenti dell'ADiSU sono quelli prodotti e acquisiti nello svolgimento della propria attività istituzionale.

Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini tecnologici, è classificabile in:

- analogico;
- informatico.

In termini operativi, è classificabile in:

- ricevuto;
- inviato;
- interno formale;
- interno informale.

3.2 Documento analogico

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

Il documento amministrativo cartaceo può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura).

In quest'ultimo caso si definisce "originale" il documento cartaceo, comprendente tutti gli elementi sostanziali e formali di garanzia e di informazione del mittente e destinatario, stampato su carta intestata e dotato di firma autografa.

La "copia informatica di documento analogico" identifica un file che ha lo stesso contenuto del documento analogico da cui è tratto, ma diverso nella forma.

La “copia per immagine su supporto informatico di documento analogico” risulta dalla scansione del documento analogico da cui è tratto, rispetto al quale appare identico, come forma e come contenuto.

La copia ha la stessa efficacia probatoria dell'originale da cui è tratta se la conformità all'originale non è espressamente disconosciuta.

3.3 Documento informatico

Per documento informatico si intende il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, lett. p) del CAD).

Il documento informatico soddisfa il requisito della forma scritta ed ha l'efficacia prevista dall'art. 2702 del Codice Civile, ovverosia quella di fare piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto, *quando vi e' apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, e' formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.* (art. 20, co. 1-bis CAD).

Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

3.4 Ulteriori formati utilizzati per la formazione del documento informatico

L'ADiSU si avvale , per l'erogazione dei servizi agli studenti, di una piattaforma informatica che realizza un data base relazionale, alimentato dalla procedura on line di domanda della borsa di studio ed iscrizione all'anagrafe, disponibile in modalità web e dalle funzionalità fornite dalla piattaforma per l'editing dei dati associati ad ogni studente e per l'elaborazione e la pubblicazione delle graduatorie della Borsa di studio.

Le istanze telematiche sono registrate al protocollo in maniera automatica in formato PDF.

Le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di registrazione dell'esito delle procedure on line e dall'applicazione di misure per la protezione dell'integrità dei data base e per la produzione e conservazione dei log di sistema, ovvero

con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

3.5 Documento ricevuto

La corrispondenza in ingresso può essere acquisita dalla AOO con diversi mezzi e modalità in base alla tecnologia utilizzata dal mittente.

Un **documento informatico** può essere recapitato:

1. a mezzo posta elettronica convenzionale o certificata;
2. su supporto rimovibile, ad esempio CD ROM, DVD, pen drive;
3. tramite appositi **form** predisposti nel sito web istituzionale ai quali si accede mediante un sistema di autenticazione sicura, oppure tramite Sistema Pubblico di Identità Digitale (SPID).

Un **documento analogico** può essere recapitato:

1. a mezzo servizio postale convenzionale o privato;
2. a mezzo corriere;
3. per telefax o telegramma;
4. con consegna diretta da parte dell'interessato o tramite persona dallo stesso delegata allo sportello dell'UP.

3.6 Documento inviato

Per documenti inviati si intendono i documenti che hanno rilevanza giuridico-probatoria prodotti dal personale dell'ADiSU nell'esercizio delle proprie funzioni e destinati ad essere trasmessi ad altra amministrazione, ovvero ad altro ufficio interno o all'utenza esterna.

Se il documento supera la dimensione massima prevista dal sistema di posta utilizzato, il documento viene riversato, su supporto digitale rimovibile, non modificabile e trasmesso con altri mezzi di trasporto al destinatario, oppure messo a disposizione in download attraverso un apposito servizio esposto sul sito Web dell'ADiSU.

3.7 Documento interno formale

Si tratta di documenti di preminente carattere giuridico-probatorio redatti dai dipendenti dell'ADiSU nell'esercizio delle proprie funzioni per documentare fatti relativi all'attività svolta o documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi. Questi debbono essere classificati e protocollati.

Lo scambio tra uffici di documenti interni formali avviene di norma per mezzo del sistema di gestione documentale.

3.8 Documento interno informale

Documenti prevalentemente a carattere informativo, ossia appunti, memorie informali e comunicazioni per i quali non è prevista la protocollazione.

La trasmissione di questa tipologia di documenti interni tra gli uffici e/o tra dipendenti può essere effettuata tramite le caselle di posta elettronica assegnate dall'ADiSU ai dipendenti oppure mediante il sistema di gestione documentale.

3.9 Formazione dei documenti – aspetti operativi

Secondo quanto previsto dall'art. 40 del D.Lgs. n. 82/2005, modificato dal D.Lgs. n. 179/2016 *“Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le Linee guida”*.

Di norma i documenti informatici sono convertiti, prima della loro sottoscrizione con firma digitale, nel formato PDF/A.

Al fine di curare la standardizzazione della forma e dei contenuti, i documenti, formati per essere inoltrati all'esterno in modo formale, devono essere redatti sui modelli ufficiali reperibili nella intranet dell'ADiSU.

Oltre agli elementi presenti nei suddetti modelli, il documento deve inoltre recare le seguenti informazioni:

- il luogo di redazione;
- la data e il numero di protocollo (riportata all'interno della segnatura di protocollo);
- l'oggetto, indicato in maniera sintetica ma esaustiva;
- il numero degli allegati, se presenti;
- sottoscrizione digitale del soggetto abilitato alla sottoscrizione del documento di cui trattasi;
- modalità di spedizione (se l'invio avviene per posta elettronica tradizionale o PEC occorre indicare i relativi indirizzi);
- la sigla di chi lo redige (in maiuscolo).

Le firme e le sigle necessarie alla redazione e perfezione giuridica del documento devono essere apposte prima della sua protocollazione.

Al documento informatico immutabile vengono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo dei metadati, come definiti nell'allegato 5 al DPCM 13 novembre 2014 "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici", è costituito da:

- a) l'identificativo univoco e persistente;
- b) data di chiusura;
- c) l'oggetto;
- d) il soggetto che ha formato il documento;
- e) l'eventuale destinatario;
- f) l'impronta del documento informatico

Eventuali ulteriori metadati sono definiti in funzione del contesto e delle necessità gestionali e conservative.

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

3.10 Firma digitale

La firma digitale è il risultato di una procedura informatica – detta validazione – che conferisce al documento informatico le seguenti caratteristiche:

- autenticità: garantisce l'identità del sottoscrittore del documento;
- integrità: assicura che il documento non sia stato modificato dopo la sottoscrizione;
- non ripudio: il documento non può essere ripudiato dal sottoscrittore.

I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità. Tale processo si realizza con modalità conformi a quanto prescritto dalla normativa vigente in materia.

L'ADiSU si avvale dei servizi di un'autorità di certificazione iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'ADiSU per l'Italia Digitale.

L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

I documenti informatici prodotti dall'ADiSU, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti di norma nel formato PDF/A al fine di garantire la leggibilità per altri sistemi e la non alterabilità durante

le fasi di accesso e conservazione, e l'immutabilità nel tempo del contenuto e della struttura. Una firma digitale può essere apposta: in modalità CADES o in modalità PAdES.

Di per sé, la firma digitale consiste sempre nella creazione di un file associato ad un documento, creato dal software di firma in base al documento da firmare e al certificato del firmatario. Tecnicamente, la differenza tra una firma di tipo CADES e una firma di tipo PAdES consiste nel modo in cui questo nuovo file viene associato al documento.

Nel caso di una firma digitale apposta con **modalità CADES**, il documento firmato e il file con la firma digitale vengono inseriti insieme in una busta. Tale busta, che contiene il documento e il file della firma, è anch'essa un file con estensione .p7m. Infatti, tutti i file firmati digitalmente con modalità CADES hanno una seconda estensione .p7m.

Le principali caratteristiche di questa modalità di firma sono:

- la modalità CADES permette di firmare qualsiasi tipo di documento (docx, .xlsx, ecc.);
- un documento, una volta firmato con modalità CADES modifica il suo nome. Ad esempio un documento **Prova.docx**, una volta firmato digitalmente con modalità CADES modificherà il suo nome in **Prova.docx.p7m**;
- per verificare una firma digitale apposta con modalità CADES e per visualizzare il documento firmato, occorre utilizzare uno degli appositi software specifici come Dike 6, ArubaSign, ecc. .

Nel caso di firma digitale apposta con **modalità PAdES**, invece, vengono sfruttate le caratteristiche dei documenti in formato .pdf e il file contenente la firma digitale viene inglobato insieme al documento stesso.

Le principali caratteristiche di questa modalità di firma sono:

- la modalità PAdES permette di firmare solo documenti in formato .pdf;
- un documento, una volta firmato con modalità PAdES, mantiene il suo nome;
- per verificare una firma digitale apposta con modalità PAdES e per visualizzare il documento firmato, è possibile utilizzare un qualsiasi software per la lettura dei file .pdf come Acrobat Reader.

L'ADiSU utilizza la firma digitale sia in modalità CADES che PADES.

Nel software di gestione informatica dei documenti adottato, integrato con la casella di posta elettronica certificata, sono previste funzioni di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare.

3.11 Marca temporale

A differenza della firma digitale che riporta data e ora dell'hardware utilizzato, la **marca temporale** è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi.

Il servizio di marcatura temporale può essere utilizzato anche su file non firmati digitalmente, garantendone una collocazione temporale certa e legalmente valida.

Sui documenti informatici sui quali è stata apposta una firma digitale, la marca temporale attesta il preciso momento in cui il documento è stato creato, trasmesso o archiviato. Apporre una marca temporale ad un documento firmato digitalmente pertanto fa sì che la firma digitale risulti sempre e comunque valida anche nel caso in cui il relativo Certificato risulti scaduto, sospeso o revocato, purché la marca sia stata apposta in un momento precedente alla scadenza, revoca o sospensione del Certificato di firma stessa.

Come sancito dall'articolo 49 del DPCM del 30.03.2009, le marche temporali emesse devono essere conservate in appositi archivi per un periodo non inferiore a 20 anni.

L'apposizione di una marca temporale a un documento firmato digitalmente, quindi, ne garantisce la validità nel tempo.

3.12 Uso della Posta Elettronica Certificata (PEC)

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.

Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo.

Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno: denominazione, indirizzo, casella di posta elettronica);
- firmare il documento (ed eventualmente associare il riferimento temporale al documento firmato);

- notificare il messaggio contenente il documento firmato digitalmente all'UP.

L'UP assegna il numero di protocollo in uscita al documento firmato digitalmente e invia il messaggio contenente il documento firmato e protocollato in uscita alla casella di posta istituzionale del destinatario.

L'utilizzo della Posta Elettronica Certificata - PEC - consente di:

- firmare elettronicamente il messaggio;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con AOO appartenenti ad altre amministrazioni.

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema di protocollazione della AOO ricevente. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato. Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa, vigente e alle relative regole tecniche sono opponibili ai terzi. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale, nei casi consentiti dalla legge, alla notifica per mezzo della posta.

4. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

4.1 Ricezione e trasmissione dei documenti

4.1.1 Ricezione di documenti cartacei

I documenti cartacei possono pervenire all'AOO attraverso:

1. SERVIZIO POSTALE TRADIZIONALE, CORRIERE O RACCOMANDATA.

I documenti pervenuti a mezzo posta sono consegnati dall'addetto al servizio postale presso lo sportello dell'UP.

Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti. Di norma la corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta. La busta delle raccomandate viene allegata al documento per la parte recante i timbri postali. Le ricevute di ritorno delle raccomandate non devono essere protocollate.

La corrispondenza presentata o ricevuta in busta chiusa riportante la dicitura "personale e/o riservata e/o s.p.m. (sue proprie mani) non viene aperta né protocollata, ma è consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare compiti istituzionali, provvederà a consegnarla all'UP per la registrazione.

Per motivi organizzativi tutte le Sezioni sono tenute ad informare preventivamente il SGD in merito alle scadenze di concorsi, gare, bandi di ogni genere.

Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.

Nel caso in cui pervengano erroneamente all'ADiSU buste indirizzate ad altri soggetti, le stesse vengono restituite all'addetto al servizio postale.

Se il documento è stato erroneamente acquisito al registro di protocollo generale, la protocollazione viene annullata inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si rinvia al mittente accompagnato da lettera di restituzione.

2. CONSEGNA A MANO DA PARTE DELL'INTERESSATO O PER TRAMITE DI PERSONA DALLO STESSO DELEGATA.

Per la corrispondenza recapitata a mano da utenti esterni, l'addetto al protocollo, su richiesta dell'interessato, rilascia apposita ricevuta (v. successivo paragrafo (4.1.2)).

Qualora un utente si presenti presso l'UP per consegnare un documento riguardante un

altro soggetto, è necessario che costui sia munito di delega con copia del documento di identità della persona delegante.

3. APPARECCHI TELEFAX (SOLO DA SOGGETTI PRIVATI AI SENSI ART. 14 L. 9.08.2013 N. 98) o TELEGRAMMA.

La corrispondenza ricevuta via telegramma o via telefax, per ciò che concerne la registrazione di protocollo, è trattata come un documento cartaceo.

Dopo aver accuratamente separato i documenti esclusi dalla registrazione del protocollo di cui all'art. 53, comma 5, del Testo Unico e aver apposto il timbro di ricezione dell'ADiSU, il personale dell'UP consegna la corrispondenza in ingresso al Dirigente per l'individuazione della corretta assegnazione alle strutture dell'ADiSU.

4.1.2 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Qualora venga richiesta il rilascio di una ricevuta attestante l'avvenuta consegna a mano di un documento cartaceo e non fosse possibile effettuare la protocollazione al momento della ricezione, l'addetto al protocollo rilascia una fotocopia del primo foglio sulla quale verrà apposto lo specifico timbro di ricezione con la data e la sigla del ricevente. In alternativa, l'addetto esegue la registrazione di protocollo in arrivo e rilascia la fotocopia del documento con gli estremi della segnatura.

La semplice apposizione del timbro datario attesta la ricezione ma non ha valore giuridico.

4.1.3 Ricezione di documenti informatici

Di norma, la ricezione dei documenti informatici è assicurata tramite la caselle di posta elettronica certificata istituzionale dell'ADiSU adis@pec.it che è accessibile solo al personale del SGD.

Gli addetti all'UP controllano frequentemente durante lo stesso giorno, i messaggi pervenuti nelle caselle di posta istituzionale tradizionale/certificata.

Quando i documenti informatici pervengono all'UP, talea stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento, procedono alla registrazione di protocollo ed all'assegnazione al Servizio/Sezione di competenza.

Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario, lo stesso viene rispedito al mittente con la dicitura "Messaggio pervenuto per errore, non di competenza di questa amministrazione".

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle

regole tecniche vigenti, recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.

I documenti informatici ricevuti attraverso canali Web appositamente creati per la redazione e l'inoltro di specifiche istanze sono resi disponibili al sistema di gestione informatica dei documenti, unitamente ai dati immessi da chi li ha prodotti, ad opera del software che realizza l'interazione con l'utenza, utilizzando i meccanismi standard della cooperazione applicativa tra sistemi.

Qualora i messaggi di posta elettronica non siano conformi agli standard indicati dalla normativa vigente ovvero non siano dotati di adeguata sottoscrizione elettronica, il messaggio viene comunque acquisito nel sistema di gestione documentale. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quello di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA). Il messaggio ricevuto su una casella di posta elettronica non istituzionale, deve essere inoltrato alla casella di posta istituzionale per la protocollazione.

4.1.4 Rilascio di ricevute attestanti la ricezione di documenti informatici

Nel caso di ricezione di documenti informatici mediante la casella di posta elettronica certificata, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dagli specifici standard del servizio di posta elettronica certificata dell'Agenzia.

4.1.5 Ricezione di documenti informatici su supporti removibili

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

4.1.6 Trasmissione di documenti cartacei tramite posta/corriere

L'UP esegue le verifiche di conformità della documentazione cartacea ricevuta dagli Uffici Utente (per essere spedita) agli standard formali, ovvero, verifica:

- che siano indicati correttamente il mittente e il destinatario;
- che il documento sia sottoscritto;
- la presenza di allegati se dichiarati;

- che siano compilate le ricevute di ritorno (per le raccomandate A.R.);
- che sia allegata la busta personalizzata con logo aziendale, completa di indirizzo del destinatario;

In caso contrario il documento è rispedito all'Ufficio di provenienza con le osservazioni del caso.

4.1.7 Trasmissione di documenti cartacei tramite fax

La documentazione da inviare via fax deve essere necessariamente protocollata prima della trasmissione. L'addetto al protocollo non può protocollare, successivamente, una lettera che è già stata inviata per fax. L'etichetta del protocollo (segnatura) è apposta sul documento e non sulla copertina. L'art. 47 comma 2 del Codice, dispone che non possono essere inviati fax alle pubbliche amministrazioni.

4.1.8 Trasmissione di documenti informatici

I documenti informatici, compresi gli eventuali allegati anch'essi informatici, sono inviati per mezzo di un servizio di "Posta Elettronica Certificata".

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla circolare AGID 23 gennaio 2013, n. 60.

Ai sensi della normativa vigente, per la spedizione dei documenti informatici, la data di protocollo assegnato al documento prodotto dall'ADiSU costituisce un riferimento temporale certo per la verifica delle firme digitali ad esso apposte. In alternativa l'AOO si avvale dei servizi di autenticazione e marcatura temporale offerti da certificatore accreditato iscritto nell'elenco pubblico tenuto da AGID.

Così come previsto per il documento analogico, gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.

4.2 Registrazione e segnatura dei documenti

4.2.1 Registrazione di protocollo

Tutti i documenti documento ricevuti o spediti dall'ADiSU dai quali possano nascere diritti, doveri o legittime aspettative di terzi, devono essere registrati sul protocollo informatico unico dell'ADiSU con le modalità e le eccezioni di seguito illustrate. La registrazione è l'operazione di memorizzazione delle informazioni fondamentali relative al contenuto, alla forma, all'autore e alla modalità di trasmissione di un documento.

L'assegnazione delle informazioni nelle operazioni di registrazione di protocollo e' effettuata dal sistema in unica soluzione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c) mittente per i documenti ricevuti o, in alternativa, destinatario o destinatari per i documenti spediti, registrati in forma non modificabile;
- d) oggetto del documento, registrato in forma non modificabile;
- e) codice di classificazione, secondo il Titolario vigente;
- f) data e numero di protocollo del documento ricevuto, se disponibili;

Gli elementi accessori che assicurano una migliore utilizzazione dei documenti sotto il profilo giuridico, gestionale ed archivistico sono:

- a) data di arrivo;
- b) luogo di provenienza, o di destinazione del documento;
- c) numero degli allegati;
- d) descrizione sintetica degli allegati;
- e) mezzo di ricezione o, in alternativa, mezzo di spedizione.

La registrazione di protocollo dei documenti informatici è eseguita dopo che l'operatore addetto ne ha verificato l'autenticità, la provenienza e l'integrità. Per i documenti informatici è prevista la registrazione delle stesse informazioni indicate per i documenti su supporto cartaceo con l'aggiunta, tra i dati obbligatori di protocollo, dell'impronta del documento

informatico, registrata in forma non modificabile.

La registrazione di documenti con particolare livello di riservatezza è gestita garantendo l'accesso alle informazioni ai soli utenti coinvolti nel processo e/o procedimento.

4.2.2 Segnatura di protocollo

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo. Essa consente di individuare ciascun documento in modo inequivocabile.

La registrazione e la segnatura costituiscono un'operazione unica e contestuale avente entrambe la natura di atto pubblico. Non potranno, quindi, essere effettuate registrazioni di protocollo senza disporre del documento a cui la registrazione si riferisce.

La segnatura di protocollo di un documento su supporto cartaceo è realizzata attraverso l'apposizione su di esso di un'etichetta di protocollo sul quale sono riportate le seguenti informazioni:

- denominazione dell'Amministrazione;
- tipo di documento (arrivo o uscita)
- data e numero di protocollo del documento
- codice a barre identificante il progressivo assoluto

Per i documenti informatici le informazioni minime incluse nella segnatura sono quelle elencate negli articoli 9 e 21 del DPCM 3 dicembre 2013¹.

I dati relativi alla segnatura di protocollo di un documento trasmesso da un'area organizzativa omogenea sono associati al documento stesso e contenuti, nel messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition), definito e aggiornato periodicamente

¹ DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico"

art. 9 "Formato della segnatura di protocollo"

1. Le informazioni apposte o associate ai documenti informatici, registrati nel registro di protocollo, negli altri registri di cui all'art. 53, comma 5, del testo unico, nei repertori e negli archivi, nonché negli albi, negli elenchi e in ogni raccolta di dati concernente stati, qualità personali e fatti con le modalità descritte nel manuale di gestione, mediante l'operazione di segnatura di cui all'art. 55 del testo unico che ne garantisce l'identificazione univoca e certa, sono espresse nel seguente formato:

- a) codice identificativo dell'amministrazione;
- b) codice identificativo dell'area organizzativa omogenea;
- c) codice identificativo del registro;
- d) data di protocollo secondo il formato individuato in base alle previsioni di cui all'art. 20, comma 2;
- e) progressivo di protocollo secondo il formato specificato all'art. 57 del testo unico.

dall'ADiSU per l'Italia Digitale con provvedimento reso disponibile sul proprio sito (DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico" art. 20 - Segnatura di protocollo dei documenti trasmessi).

4.2.3 Acquisizione delle rappresentazioni digitali di documento cartacei

I documenti cartacei, dopo le operazioni di registrazione e segnatura, devono essere acquisiti in formato immagine attraverso un processo di scansione integrato con il sistema di gestione documentale

Il processo di scansione avviene in diverse fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico file;
- verifica della leggibilità e della qualità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- collegamento delle immagini alle rispettive registrazioni di protocollo in modo non modificabile;
- memorizzazione delle immagini su supporto informatico, in modo non modificabile.

E' compito dell'operatore dell'UP assicurarsi che il documento venga acquisito correttamente. Qualora il documento sia difficilmente leggibile in origine e non vi sia possibilità di contattare il mittente per una nuova trasmissione, l'operatore è tenuto ad acquisirlo nel migliore dei modi possibile dandone evidenza nelle "annotazioni" della scheda di protocollo. Gli originali dei documenti cartacei ricevuti, di norma non vengono inviati alle UU ma rimangono alla UP che provvede ad archivarli in ordine sequenziale di protocollo.

4.2.4 Differimento dei termini di registrazione

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e comunque non oltre due giorni lavorativi dal ricevimento, nel caso di oggettive impossibilità.

Nel caso di eccezionale carico di lavoro, che non permette di evadere la corrispondenza ricevuta nei tempi sopra indicati e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa risultare lesa un diritto di terzi (es. partecipazione concorso), eccezionalmente, il RGD può autorizzare la registrazione in tempi successivi, conferendo valore, nel caso di scadenze predeterminate, al timbro datario di arrivo.

5. REGOLE DI SMISTAMENTO ED ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

5.1 Descrizione funzionale ed operativa

La descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'AOO, con particolare riferimento alle modalità di utilizzo dello stesso, consente di riprodurre informaticamente i processi tipici dell'attività amministrativa dell'ADiSU.

La descrizione completa delle funzionalità dell'applicativo di protocollo è disponibile e consultabile insieme ai manuali operativi nella intranet dell'ADiSU.

L'attività di smistamento consiste nell'operazione di inviare un documento protocollato al Servizio competente in base alla classificazione del documento.

Lo smistamento dei documenti segue di norma il criterio di "competenza" e di "gerarchia".

Tramite l'applicativo è possibile distinguere:

- la spedizione con notifica
- la spedizione senza notifica (comprendendo in essa anche la visibilità predefinita).

La spedizione con notifica consente al destinatario di visualizzare il documento in evidenza nella cassetta della posta dell'applicativo. Il documento apparirà in neretto. Effettuando il "click" sul medesimo, l'applicativo registrerà la "presa visione" nella storia della relativa scheda di protocollo.

La spedizione senza notifica comporta che la scheda di protocollo sarà visualizzabile solo tramite l'apposita funzionalità di ricerca e non ne sarà data evidenza nella cassetta della posta dell'applicativo: di norma tale funzionalità viene utilizzata non nello smistamento ma nell'attribuzione della visibilità predefinita delle schede di protocollo.

I Dirigenti, ad esempio, pur non avendo la notifica, hanno la visibilità completa su tutti i documenti di competenza del proprio Servizio.

Il sistema di gestione informatica dei documenti in arrivo e in partenza memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.

La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

I documenti ricevuti per via telematica sono resi disponibili agli UU, attraverso il sistema di gestione documentale subito dopo l'operazione di smistamento e di assegnazione.

Particolare attenzione va rivolta allo smistamento di quei documenti indirizzati a dipendenti, qualora la funzione cui fa riferimento tale atto sia distinta da quella stabilmente ricoperta dallo stesso (Es. R.U.P., Presidente di Gara, Presidente Commissione Disciplinare, etc...).

Nel caso in cui, ad esempio, un documento debba essere inoltrato al Presidente della commissione gara, l'invio al soggetto non deve tenere presente la funzione che svolge, ad es. Responsabile di Sezione, ma deve essere fatto all'utente "nome e cognome".

5.2 Modifica delle assegnazioni

Nel caso di assegnazione errata di un documento, l'ufficio a cui perviene il documento stesso lo restituisce nell'immediatezza all'UP e comunque non oltre le 24 ore. L'UP ne curerà la modifica dell'assegnazione. 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.

5.3 Annullamento di una registrazione di protocollo

In base all'art. 8 del DPCM del 3 dicembre 2013, recante le regole tecniche sul protocollo informatico, l'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immutabile determina l'automatico e contestuale annullamento della intera registrazione.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RGD e da questi autorizzato. Ai sensi degli artt. 54 e 61 del "Testo Unico", i dati annullati e/o modificati rimangono memorizzati nella procedura del protocollo informatico unitamente alle informazioni relative all'ora, alla data, al nominativo dell'operatore che effettua l'operazione.

5.4 Registro giornaliero di protocollo

Il sistema di registrazione deve consentire la produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Il registro giornaliero di protocollo è trasmesso entro la giornata successiva al sistema di conservazione, garantendone l'immutabilità del contenuto, secondo le modalità consentite dal sistema di gestione software del protocollo informatico.

5.5 Registro di emergenza

Qualora non fosse possibile utilizzare il protocollo informatico a causa di una sospensione del servizio accidentale o programmata, il RGD autorizza l'apertura del registro di emergenza.

Per emergenza si intende una situazione in cui la sospensione del servizio sia tale da pregiudicare la registrazione a protocollo in giornata nel caso in cui vi siano scadenze inderogabile e prescrittive (es: bandi, concorsi, ecc...). Sul registro devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, la data e l'ora di ripristino della piena funzionalità del sistema, nonché eventuali annotazioni ritenute rilevanti dal RGD.

Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno. Qualora nel corso di un anno non venga utilizzato, il RGD annota sullo stesso il mancato uso.

Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite sul protocollo generale. Al termine dell'emergenza, l'addetto alla protocollazione, provvede a riversare sul sistema di protocollo informatico tutte le registrazioni già eseguite sul registro di emergenza, continuando la numerazione raggiunta al momento dell'interruzione del servizio.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo informatico unico recheranno, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo generale.

Al numero attribuito dal registro di emergenza si fa riferimento per l'avvio dei termini del procedimento amministrativo.

5.6 Documenti soggetti a registrazione particolare

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le seguenti tipologie documentali:

- Fatture
- Determinazioni Dirigenziali
- Decreti dell'Amministratore unico/Commissario straordinario
- Mandati e Reversali
- Contratti

Tale tipo di registrazione particolare consente comunque di eseguire su tali documenti tutte

le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione e la fascicolazione; anche questi documenti appartengono al complesso archivistico dell'ADiSU e concorrono al popolamento del sistema di gestione documentale nell'ottica di una gestione uniforme e coordinata.

Questi documenti costituiscono delle serie di interesse archivistico e sono collegate a registri o repertori che contengono almeno le seguenti informazioni:

- tipologia del registro o repertorio
- numero di registro o repertorio (cronologico e progressivo)
- data
- elementi identificativi dell'atto (soggetto o soggetti; oggetto)
- eventuali dati di classificazione e di fascicolazione
- annotazioni

Ai sensi dell'art. 5 del DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico", l'elenco dei metadati associati ai documenti soggetti a registrazione particolare sono riportati nell'ALLEGATO I al presente Manuale.

5.7 Documenti esclusi dalla registrazione di protocollo

L'art. 53 comma 5 del Testo Unico stabilisce che *"sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione."*

Sono altresì esclusi dalla protocollazione:

- le comunicazioni relative a corsi di aggiornamento
- i certificati di malattia
- le comunicazioni di variazione sede ed anagrafe delle ditte fornitrici
- le convocazioni ad incontri o riunioni interne
- la pubblicità in generale
- le offerte commerciali e i listini prezzi
- gli aggiornamenti di fascicoli del personale dipendente

5.8 Ricezione di lettere anonime e prive di firma

Ai sensi dell'art. 240 del c.p.p. (codice di procedura penale), i documenti che contengono dichiarazioni anonime non possono essere acquisiti né in alcun modo utilizzati, salvo che costituiscano corpo di reato. Le lettere anonime vengono inoltrate, se contengono informazioni o dati di interesse dell'ADiSU, al Dirigente competente per materia, il quale valuta l'opportunità di dare seguito alle comunicazioni ed individua le eventuali procedure da sviluppare.

I documenti privi di firma o con firma illeggibile, ma riconducibili ad un mittente certo (ente, studio privato, fornitore, ecc..), vengono protocollati ed inoltrati ai Servizi competenti.

5.9 RegISTRAZIONI DI PROTOCOLLO URGENTI

La richiesta di protocollare urgentemente un documento è collegata ad una necessità indifferibile e di tipo straordinario, considerato che nella protocollazione deve essere rispettato l'ordine di arrivo o di redazione dei documenti.

In questo caso il RGD si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale o cartaceo da acquisire al registro di protocollo generale.

Per i documenti in partenza è assolutamente vietato predisporre la protocollazione dei documenti prima della loro sottoscrizione e prima della loro acquisizione per i documenti in arrivo. Il mancato rispetto di tale disposizione configura un grave reato in quanto l'acquisizione al registro di protocollo generale, nella sua qualità di atto pubblico di fede privilegiata, attesta ufficialmente l'effettiva ricezione e/o l'invio di un documento.

5.10 Rilascio delle abilitazioni di accesso alle informazioni documentali

Gli utenti del servizio di protocollo, in base agli uffici di appartenenza, ovvero in base alle rispettive competenze hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza.

Ad ogni utente è assegnata:

- a) una credenziale di accesso, costituita, ad esempio, da una componente:
 - pubblica che permette l'identificazione dell'utente da parte del sistema (userID);
 - privata o riservata di autenticazione (password);

- b) una autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene. I diversi livelli di autorizzazione sono assegnati agli utenti dal RGD, e stabilite di concerto con i responsabili dei rispettivi procedimenti. Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione degli UU e del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'AOO, sono costantemente aggiornate a cura del RGD ed effettuate dalla Sezione "Sistemi Informativi".

6. CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE DEI DOCUMENTI

6.1 Titolario o piano di classificazione

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordine logico, in relazione alle funzioni e alle competenze dell'ADiSU ed è sancita dall'art. 30, comma 4 del Codice dei beni culturali.

La classificazione dei documenti si avvale del Piano di classificazione o "TITOLARIO", facente parte del Piano di conservazione dell'archivio

Il Piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, o, più in generale, in voci di I livello, II livello, III livello.

Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

Titoli, classi, sottoclassi sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto.

Il titolario 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 titolario compete esclusivamente al RGD ed è assicurato quando se ne presenta la necessità e cioè al momento dell'attribuzione all'Amministrazione di nuove funzioni.

Dopo ogni modifica, il SGD 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 titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Viene garantita la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.

Il Piano di classificazione adottato dall'ADiSU si articola in 8 voci di primo livello. Nell'ambito di ciascuna voce di primo livello, si articolano un numero variabile di classi che consentono di

identificare lo specifico procedimento cui il documento da classificare afferisce.

A decorrere dal 1/1/2018 è prevista l'introduzione del nuovo Titolario (ALLEGATO II).

6.2 Archivio

L'archivio è il complesso dei documenti prodotti, acquisiti o utilizzati dall'ADiSU nell'esercizio delle proprie funzioni e nello svolgimento della propria attività.

L'archivio generale è unico (anche se conservato in luoghi differenti).

In relazione alla sua gestione, si suddivide in:

- Archivio corrente
- Archivio di deposito
- Archivio storico

L'archivio corrente è il complesso di documenti relativi ad affari ed a procedimenti amministrativi:

- in corso di istruttoria o di trattazione;
- conclusi da breve periodo e pertanto aventi ancora un forte interesse ai fini dello svolgimento dell'attività corrente.

L'archivio di deposito è il complesso di documenti relativi ad affari ed a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione o verso i quali sussistono saltuarie esigenze di consultazione ai fini dell'attività corrente.

L'archivio storico è il complesso di documenti relativi ad affari ed a procedimenti amministrativi conclusi e destinati, previa effettuazione delle operazioni di scarto, alla conservazione permanente.

6.3 Misure di protezione e conservazione degli archivi pubblici

Il D.Lgs. 22 gennaio 2004, n. 42 impone precise disposizioni inerenti la tutela e la conservazione degli archivi, stabilendo che l'archivio è un bene culturale e come tale soggetto alle disposizioni in materia di tutela e valorizzazione dei beni culturali (art. 10 comma 2 lettera b).

I singoli documenti (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'AOO, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di

conservazione senza l'autorizzazione della Soprintendenza archivistica competente per territorio.

L'ADiSU è stata istituita, in sostituzione dell'E.R.S.U., ai sensi dell'art. 8 *“Istituzione dell'Agenzia per il diritto allo studio universitario”* della L. R. 26 agosto 1997, n. 26 *“Norme sul diritto allo studio universitario”* che al comma 1 recita *“Per la gestione degli interventi previsti dalla presente legge, la Regione istituisce l'Agenzia per il diritto allo studio universitario, ente pubblico dotato di autonomia amministrativa e gestionale.”*

Pertanto, nell'Archivio generale dell'Agenzia è presente la sezione “corrente” e la sezione di “deposito”. La gestione, la consultazione e l'accesso all'archivio di deposito è disciplinata dal “Regolamento” allegato al presente MdG (ALLEGATO III).

6.4 Massimario di selezione e scarto

La normativa impone alle amministrazioni pubbliche la predisposizione di un massimario di selezione e scarto di atti dell'archivio (ALLEGATO IV).

Le operazioni di selezione e scarto sono effettuate sotto la vigilanza del RGD o da persona da questi delegata.

Pertanto, periodicamente, viene effettuata la selezione della documentazione da conservare perennemente e lo scarto degli atti che non sono soggetti a conservazione, allo scopo di garantire il corretto mantenimento e la funzionalità dell'archivio.

6.5 Fascicolazione dei documenti

Tutti i documenti registrati nel sistema di protocollo informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.

Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento.

I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza sottofascicolo, secondo l'ordine cronologico di registrazione.

Si distinguono due tipologie di fascicolo:

- Fascicoli relativi ad affari o procedimenti amministrativi
- Fascicoli relativi a persone fisiche (ad esempio: personale dipendente, studente)

Fascicoli relativi ad affari o procedimenti amministrativi

Nel caso in cui un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'AOO, il Responsabile del Procedimento provvede all'apertura

di un nuovo fascicolo. La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali se non già esistenti:

- indice di classificazione;
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'AOO;
- data di apertura del fascicolo;
- collocazione fisica, di eventuali documenti cartacei;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Qualora insorgano esigenze pratiche, il fascicolo può essere distinto in sottofascicoli.

I documenti sono archiviati all'interno di ciascun fascicolo, sottofascicolo secondo l'ordine cronologico di registrazione, in base cioè al numero di protocollo ad essi attribuito.

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto. Esso va archiviato rispettando l'ordine del repertorio, vale a dire l'anno di apertura.

Fascicoli relativi a persone fisiche

Per ogni persona fisica deve essere istruito un fascicolo nominativo.

Il fascicolo viene aperto al momento dell'inizio del rapporto con l'ADiSU e viene chiuso al momento della cessazione del rapporto.

Il fascicoli delle persone fisiche costituiscono una serie archivistica autonoma per ciascuna delle categorie di persone fisiche. All'interno di ciascuna serie i fascicoli vanno conservati nell'ordine prestabilito secondo criteri che rispondano ad opportunità ed efficacia (es. ordine cronologico di instaurazione del rapporto, ordine alfabetico, ...).

L'ADiSU realizza il fascicolo informatico e l'aggregazione documentale informatica in maniera conforme ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico, secondo quanto stabilito dal D. lgs n. 82/2005.

L'insieme minimo dei metadati del fascicolo informatico e dell'aggregazione documentale informatica è il seguente:

- Identificativo
- Amministrazione titolare

- Amministrazioni partecipanti
- Responsabile del procedimento
- Oggetto
- Elenco degli identificativi dei documenti contenuti nel fascicolo

6.6 Repertorio dei fascicoli

I fascicoli, sono annotati nel repertorio dei fascicoli. Il repertorio dei fascicoli, ripartito per ciascun titolo del titolare, è lo strumento di gestione e di reperimento dei fascicoli.

La struttura del repertorio rispecchia quella del titolare di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo.

Mentre il titolare rappresenta in astratto le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività.

Il repertorio dei fascicoli deve essere costantemente aggiornato.

6.7 Serie archivistiche e repertori

La serie archivistica consiste in un raggruppamento di unità archivistiche (documenti, fascicoli, registri) riunite o per caratteristiche omogenee, quali la natura e la forma dei documenti oppure in base alla materia trattata, all'affare o al procedimento al quale afferiscono.

Ai fini del loro facile reperimento, alcuni documenti, come i verbali, le deliberazioni degli organi di governo dell'amministrazione o i contratti, sono soggetti a registrazione particolare (repertorio). I documenti repertoriati costituiscono una serie archivistica; possono essere altresì conservati in un fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

digitale”.

7. NORME TRANSITORIE E FINALI

7.1 Modalità di approvazione e aggiornamento del manuale

Il presente “Manuale di gestione” è approvato con Decreto dell’organo di indirizzo politico-istituzionale di vertice su proposta del RGD.

Il presente Manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;
- 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;
- modifiche apportate negli allegati dal Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

7.2 Operatività del presente manuale

Il presente Manuale è operativo il primo giorno del mese successivo a quello della sua approvazione.

Normativa di riferimento

- Legge 7 agosto 1990, n. 241 s.m.i. - Nuove norme in materia di procedimento amministrativo di diritto di accesso ai documenti amministrativi. (G.U. del 18 agosto 1990, n. 192) .
- Legge 15 marzo 1997, n. 59 - Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa.
- DPR 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (G.U. 20 febbraio 2001, n. 42).
- D.Lgs. n. 165/2001 - Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.
- D.Lgs. n. 196/2003 – Codice in materia di protezione di dati personali, come da ultimo modificato e integrato con D.Lgs. 101/2018 “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- D.Lgs. n. 42/2004 - Codice dei beni culturali e del paesaggio.
- DLgs. n. 82/2005 - Codice per l'Amministrazione Digitale
- LR n.8 /2011 – Semplificazione amministrazione e normativa regionale e degli Enti locali territoriali
- DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 . Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
- DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 13 NOVEMBRE 2014 Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi

degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. (15A00107) (GU Serie Generale n.8 del 12-1-2015)

ALLEGATI

Allegato I: Elenco dei metadati minimi associati ai documenti soggetti a registrazione particolare

Allegato II: Titolario o Piano di classificazione

Allegato III: Regolamento per la gestione, la consultazione, l'accesso ai documenti dell'Archivio di deposito

Allegato IV: Massimario di selezione e scarto