



Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi

ORDINE DEI MEDICI CHIRURGHI ED ODONTOIATRI DI REGGIO EMILIA

VIA DALMAZIA 101 – 42124 REGGIO EMILIA

Area Organizzativa Omogenea: SEGRETERIA

AZIONE	NOMINATIVO	FUNZIONE
Redazione	Federica Bosi	Responsabile e Coordinatore gestione documentale
	Federica Artioli	Vicaria
Verifica	Aldo Sangermano	Consigliere Segretario
Approvazione	Consiglio direttivo	Organo di controllo

IL PRESENTE MANUALE È STATO APPROVATO E ADOTTATO CON DELIBERAZIONE N. 61 DEL
16/06/2021

INDICE

Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi	1
1 PRINCIPI GENERALI	5
1.1 Premessa	5
1.1.1 Peculiarità dell'Ordine professionale.....	6
1.2 Ambito di applicazione e struttura del Manuale di Gestione	6
1.2.1 Ambito di applicazione.....	6
1.2.2 Struttura del manuale	7
1.3 Definizioni e norme di riferimento.....	7
1.4 Aree organizzative omogenee (AOO) e modelli organizzativi	9
1.5 Servizio archivistico per la gestione informatica del protocollo informatico, dei flussi documentali e degli archivi	9
1.5.1 Il delegato per la conservazione	11
1.5.2 Firma digitale	11
1.6 Sistema di protocollo informatico unico e strumenti per il suo funzionamento.....	11
1.7 Politiche di gestione e conservazione documentale.....	12
2 PIANO DI SICUREZZA.....	12
2.1 Formazione dei documenti – aspetti di sicurezza	12
2.2 Gestione dei documenti informatici – aspetti di sicurezza	12
2.2.1 Componente organizzativa della sicurezza.....	13
2.2.1 Componente fisica e infrastrutturale della sicurezza	13
2.2.3 Componente logica della sicurezza.....	14
2.2.4 Gestione delle registrazioni di protocollo e di sicurezza	17
2.2.5 Criteri di utilizzo degli strumenti tecnologici	17
2.3 Accesso ai documenti informatici	18
2.4 Politiche di sicurezza adottate dall'Ente	18
2.5 Servizio archivistico (doc. analogici).....	18
3 MODALITÀ DI FORMAZIONE DEI DOCUMENTI	19
3.1 I documenti dell'Ente	19
3.1.1 I requisiti minimi del documento.....	19
3.1.2 Produzione dei documenti informatici	19

3.1.3	Tipologie di formato del documento informatico	20
3.1.4	Documenti contenenti collegamenti ipertestuali.....	21
4	FLUSSI DI LAVORAZIONE DEI DOCUMENTI	21
4.1	Documenti in entrata	22
4.1.1	Ricevuti o prodotti su supporto analogico.....	22
4.1.2	Ricevuti o prodotti su supporto informatico	22
4.2	Documenti inviati	22
4.2.1	Inviati su supporto analogico	22
4.2.2	Inviati su supporto informatico.....	23
4.2.3	Documento Cartaceo inviato elettronicamente.....	23
4.2.4	Documento Digitale inviato elettronicamente	23
5	MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO.....	24
5.1	Registrazione dei documenti.....	24
5.2	Registro di protocollo	24
5.3	Modalità di registrazione di protocollo.....	26
5.4	La segnatura di protocollo.....	26
5.5	Documenti soggetti a registrazione particolare (Repertoriazione)	27
5.6	Procedure specifiche nella registrazione di protocollo.....	27
5.6.1	Protocollazione di documenti riservati.....	27
5.6.1.1	Modifica della gestione della sicurezza per documenti classificati come “riservati”	27
5.6.2	Documenti esclusi dalla registrazione di protocollo.....	28
5.6.3	Annullamento delle registrazioni di protocollo	28
5.7	Casi particolari di registrazioni di protocollo	28
5.7.1	Lettere anonime e comunicazioni prive di firma autografa (e-mail).....	28
5.7.2	Corrispondenza personale o riservata	28
5.7.3	Integrazioni documentarie.....	28
5.7.4	Documenti pervenuti per errore all’Ordine.....	28
5.7.5	Documenti in partenza con più destinatari	29
5.7.6	Flussi documentali informatici.....	29
5.7.6.1	Flusso FNOMCeO-ENPAM	29

5.8	Regole di smistamento e di assegnazione	29
6	MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA.....	30
7	SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE	31
7.1	Protezione e conservazione degli archivi pubblici	31
7.2	Titolario o piano di classificazione	32
7.2.1	Classificazione dei documenti.....	33
7.3	Formazione del fascicolo	33
7.3.1	Il fascicolo.....	33
7.3.2	Famiglie e tipologie di fascicolo	34
7.3.3	Processo di assegnazione dei fascicoli	35
7.3.4	Repertorio dei fascicoli	35
7.3.5	Il fascicolo personale dell'iscritto.....	36
7.4	Serie archivistiche e repertori	36
7.5	Organizzazione, gestione e strumenti dell'archivio unico corrente, di deposito e storico ..	37
7.5.1	Piano di conservazione	37
7.5.2	Strumenti per la gestione dell'archivio di deposito.....	37
7.5.3	Obbligo di conservazione, ordinamento e inventariazione dell'archivio storico	38
8	APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI	38
8.1	Modalità di approvazione e aggiornamento del Manuale.....	38
8.2	Pubblicità del presente Manuale	38
9	ALLEGATI.....	39
9.1	Allegato 1 Modello del Registro di emergenza	39
9.2	Allegato 1 Piano di classificazione.....	39
9.3	Allegato 2 Documenti esclusi dalla protocollazione	39
9.4	Allegato 3 Massimario di conservazione e di scarto dei documenti.....	39

1 PRINCIPI GENERALI

1.1 Premessa

Il Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 concernente le “Regole tecniche per il protocollo informatico” ai sensi del Codice dell’Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005, all’art. 3, comma 1, lettera d), prevede per tutte le amministrazioni di cui all’art. 2, comma 2, del Codice l’adozione del Manuale di gestione.

Il Manuale di gestione, disciplinato dal successivo art. 5, comma 1, “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”.

In questo ambito è previsto che ogni Amministrazione Pubblica individui una o più Aree Organizzative Omogenee, all’interno delle quali sia nominato un Responsabile del Servizio per la tenuta del protocollo informatico, così come già previsto dall’art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa – **Decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000**.

Obiettivo del manuale di gestione è descrivere il sistema di gestione documentale a partire dalla fase di registrazione dei documenti; elencare le ulteriori funzionalità disponibili nel sistema, finalizzate alla gestione di particolari tipi di documenti, alla pubblicità legale degli atti e documenti nelle modalità previste dalla normativa vigente e alla acquisizione e gestione di documenti redatti mediante i moduli e formulari disponibili sul portale istituzionale dell’Ordine.

Il documento Manuale di gestione dovrà, quindi, essere periodicamente aggiornato sulla base delle evoluzioni organizzative, normative, tecnologiche e degli strumenti informatici utilizzati.

Il protocollo informatico, anche con le sue funzionalità minime, costituisce l’infrastruttura di base tecnico-funzionale sulla quale avviare il processo di ammodernamento e di trasparenza dell’attività dell’amministrazione.

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

Il protocollo informatico e il sistema di gestione documentale costituiscono il fulcro della struttura tecnologica e organizzativa dell’Ente con riferimento alla gestione dei documenti, dei flussi documentali, dei processi e dei procedimenti amministrativi, nel rispetto della normativa vigente.

Il registro di protocollo è atto di fede privilegiata¹ perché prodotto durante l’espletamento dell’attività di un pubblico ufficiale e questo lo qualifica come atto pubblico che non necessita, tra i requisiti essenziali per la sua efficacia, di una sottoscrizione (firma).

¹Il Consiglio di Stato (sent. 1993, I, 838) ha riconosciuto il protocollo come atto pubblico di “fede privilegiata”. Nella gerarchia dei mezzi probatori documentali, al documento regolarmente protocollato è assegnato un rango superiore rispetto agli altri mezzi di prova, in quanto si presenta come atto pubblico gerarchicamente più elevato.

I fattori che garantiscono il valore probatorio del registro di protocollo informatico sono:

- L'appartenenza del fatto attestato alla sfera di attività direttamente compiuta dal pubblico ufficiale
- Il dirigente o funzionario che presiede alla sua compilazione attestandone il contenuto
- Il requisito di immodificabilità imposto nelle operazioni di registrazione e il tracciamento delle azioni di annullamento o correzione
- I requisiti di sicurezza del sistema.

1.1.1 Peculiarità dell'Ordine professionale

L'Ordine dei Medici Chirurghi e degli Odontoiatri di Reggio Emilia, di seguito "Ordine", è un ente pubblico non economico dotato di una struttura organizzativa semplice e poco ramificata. Inoltre la limitata presenza di personale e relativa concentrazione delle funzioni/attività, riduce notevolmente le esigenze gestionali. Gli iter amministrativi avvengono quasi sempre all'interno dello stesso ufficio e i documenti vengono presi in carico spesso dagli stessi addetti che effettuano le registrazioni di protocollo.

Ciò premesso l'Ordine intende adempiere agli obblighi normativi applicando le prescrizioni, in un'ottica di semplificazione dei processi, degli strumenti e riduzione dei costi.

Coordinano gli uffici di Segreteria due dipendenti di area C e due dipendenti di area B part time; svolgono le varie attività dell'ufficio in maniera sinergica e coordinata. L'organizzazione degli uffici in considerazione della tipologia e della funzione svolta presenta esigenze di semplificazione della gestione documentale, che pertanto viene svolta in maniera coordinata e unitaria da un'unica AREA ORGANIZZATIVA OMOGENEA (AOO).

1.2 Ambito di applicazione e struttura del Manuale di Gestione

1.2.1 Ambito di applicazione

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per la corretta gestione dei documenti, che comprende le attività di:

- Formazione
- Registrazione
- Classificazione
- Fascicolazione
- Archiviazione
- Conservazione

dei documenti.

Come prescritto **dall'art. 5, comma 3 del DPCM 13 novembre 2013 Regole tecniche per il protocollo informatico**, è pubblicato sul sito istituzionale dell'Ordine.

Esso disciplina:

- il piano di sicurezza dei documenti
- le modalità di formazione e scambio dei documenti
- l'utilizzo del sistema di protocollo informatico e gestione documentale
- la gestione dei flussi documentali, sia cartacei che digitali, e le aggregazioni documentali (fascicoli)
- l'uso del titolario di classificazione e del piano di conservazione
- le modalità di accesso ai documenti e alle informazioni e le relative responsabilità
- la gestione dei procedimenti amministrativi

Il presente Manuale di gestione è adottato dall'Ordine ai sensi dell'art. 3, comma 1, lettera d) del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante le regole tecniche per il protocollo informatico.

L'adozione del Manuale di gestione si pone l'obiettivo di raggiungere, attraverso i sistemi che l'Ordine ha a disposizione per la gestione documentale, una corretta ed uniforme metodologia per il trattamento dei documenti sia analogici che digitali, una serie di procedure condivise per la gestione dei procedimenti amministrativi, l'accesso agli atti ed alle informazioni e l'archiviazione e la conservazione dei documenti.

1.2.2 Struttura del manuale

L'attuale manuale di gestione è organizzato in 8 capitoli ed include n. 4 allegati.

1.3 Definizioni e norme di riferimento

Ai fini delle definizioni del presente Manuale si è fatto riferimento alla seguente normativa e documentazione:

- Decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- Decreto legislativo 7 marzo 2005 n. 82 – *Codice dell'Amministrazione Digitale*
- Decreto legislativo 26 agosto 2016, n.179 – *Modifiche e integrazioni al Codice dell'Amministrazione Digitale in materia di riorganizzazione delle amministrazioni pubbliche.*
- Decreto legislativo 22 gennaio 2004, n. 42 – *Codice dei beni culturali e del paesaggio*
- Decreto legislativo 30 giugno 2003, n. 196 – *Codice in materia di protezione dei dati personali*
- Legge 7 agosto 1990 n. 241 – *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*
- Legge 11 febbraio 2005, n. 15 – Modifiche ed integrazioni alla legge 7 agosto 1990, n. 241, concernenti norme generali sull'azione amministrativa

- Decreto del presidente del Consiglio dei Ministri 3 dicembre 2013 – *Regole tecniche per il protocollo informatico*
- Decreto del presidente del Consiglio dei Ministri 3 dicembre 2013 – *Regole tecniche in materia di sistema di conservazione*
- Decreto del presidente del Consiglio dei Ministri 11 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*
- Decreto del presidente del Consiglio dei Ministri 22 febbraio 2013 – *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*
- Quaderno 21 CNIPA, febbraio 2006 – *Manuale di gestione del protocollo informatico, dei documenti e dell'archivio delle Pubbliche amministrazioni – Modello di riferimento*
- disposizioni integrative e correttive al d.lgs. 26 agosto 2016, n. 179, del 13 dicembre 2017, n. 217, concernente modifiche ed integrazioni al Codice dell'Amministrazione Digitale (CAD), di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche

Ai fini del presente manuale si intende per:

- **“Ordine”**, l'Ordine dei Medici Chirurghi e degli Odontoiatri della provincia di Reggio Emilia
- **“Testo Unico”**, il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- **“Regole tecniche”**, il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le “Regole tecniche per il protocollo informatico”
- **“Codice”** o **“CAD”**, il decreto legislativo 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale e successive modificazioni (aggiornato a dicembre 2017).

Di seguito si riportano gli acronimi utilizzati più frequentemente:

- **AOO** – Area Organizzativa Omogenea
- **MdG** – Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi (il presente documento)
- **RPA** – Responsabile del Procedimento Amministrativo – il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare
- **RSP** – Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi

1.4 Aree organizzative omogenee (AOO) e modelli organizzativi

Ai fini della gestione unica e coordinata dei documenti l'Ordine è costituito da un'unica Area organizzativa omogenea (AOO unica), formalmente definita con Deliberazione del 21.03.2018. Denominazione dell'AOO = Ufficio Protocollo

All'interno della AOO viene utilizzato un unico sistema di protocollazione per la registrazione della corrispondenza in entrata ed in uscita.

1.5 Servizio archivistico per la gestione informatica del protocollo informatico, dei flussi documentali e degli archivi

A norma dell'art. 61 del DPR 445/2000, Il Consiglio direttivo ha istituito, con Deliberazione del 19/06/2019, l'ufficio denominato "Servizio archivistico dell'Ordine dei Medici chirurghi e degli odontoiatri di Reggio Emilia", con il compito di gestire il protocollo informatico, i flussi documentali e gli archivi.

Al Servizio archivistico è demandata la gestione dell'archivio (corrente, di deposito e storico), che svolge le seguenti funzioni:

- a) attribuire il livello di autorizzazione per l'accesso alle funzioni del sistema di protocollo informatico, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- b) garantire che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
- c) garantire la corretta produzione e la conservazione del registro giornaliero di protocollo;
- d) conservare le copie dei dati di protocollo e dei documenti archiviati su supporto informatico, in luoghi sicuri e differenti;
- e) garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione dell'archivio;
- f) autorizzare le operazioni di annullamento delle registrazioni di protocollo;
- g) vigilare sull'osservanza delle disposizioni del presente regolamento da parte del personale dell'Ente interessato;
- h) esercitare competenza sull'intera documentazione dell'Archivio corrente e di deposito;
- i) mantenere costantemente aggiornato il manuale di gestione dei documenti, provvedendo anche alla sua pubblicazione, comunicazione e diffusione negli Uffici.

Con la medesima deliberazione è stata individuata la figura del Responsabile del Servizio per la tenuta del protocollo informatico che, a norma dell'art. 61, comma 2 del DPR 445/2000, è definito come un **"dirigente, ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente"**.

In mancanza di una figura dirigenziale, si individua il dipendente che, in possesso di idonei requisiti di cui sopra, sia nelle condizioni di poter assolvere all'incarico.

In assenza del responsabile e vicario, le decisioni vengono assunte dal Segretario dell'Ordine ovvero dal Presidente e legale rappresentante.

Ai sensi dell'art. 4, comma 1 del DPCM 13 novembre 2013 *Regole tecniche per il protocollo informatico* sono compiti del Responsabile del Servizio:

- predisporre lo schema del Manuale di gestione di cui all'art. 5 delle Regole tecniche per il protocollo
- curare la redazione e l'aggiornamento del Titolario, del Piano di fascicolazione e degli altri strumenti archivistici previsti
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni e dalla circolare AgID del 18 aprile 2017 n. 2/201 che definisce le misure di sicurezza, d'intesa con il responsabile della conservazione, con i preposti ai sistemi informativi (Amministratore di sistema) e con il responsabile del trattamento dei dati personali di cui al suddetto decreto;

Sono inoltre compiti del Servizio:

- abilitare gli addetti dell'amministrazione all'utilizzo del sistema di protocollo informatico e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, registrazione, modifica ecc.)
- 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
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile
- conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema
- garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali
- autorizzare le operazioni di annullamento delle registrazioni di protocollo;
- aprire e chiudere il registro di emergenza
- definire e assicurare criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna, ai sensi dell'art. 50, comma 4, del testo unico
- autorizzare, aprire, chiudere e assicurarsi della corretta compilazione dell'eventuale protocollo di emergenza

1.5.1 Il delegato per la conservazione

Il servizio di conservazione digitale dei documenti è affidato a fornitore esterno.

Il delegato interno per la conservazione svolge i seguenti compiti:

- si accerta che il fornitore sia fra quelli accreditati AGID
- verifica il manuale della conservazione redatto dal fornitore
- interagisce con il fornitore per la definizione dei metadati da utilizzare per ogni tipologia documentale da portare in conservazione
- definisce contrattualmente i tempi di conservazione dei documenti
- effettua verifiche periodiche di mantenimento dei requisiti del fornitore (esempio controlli a campione sui documenti e richieste di pacchetti di distribuzione)

Il delegato si avvale di sostituti in caso di sua assenza o impedimento.

Quando non vi sia la nomina del delegato, tali funzioni sono assunte dal responsabile del servizio di archivistica e protocollo informatico

1.5.2 Firma digitale

L'Ordine utilizza la firma digitale per l'espletamento delle attività istituzionali e gestionali con la finalità, ai sensi del CAD, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Tutti i dipendenti dell'Ordine che ne avessero necessità, per motivi di servizio, sono muniti di firma digitale.

Nella gestione delle firme digitali si tiene conto che il loro rinnovo (ogni 3 anni) deve avvenire prima della loro scadenza. Al fine di minimizzare la possibilità di superare tale limite temporale, le procedure di rinnovo vengono avviate almeno 30 gg prima della scadenza di ogni certificato di firma.

1.6 Sistema di protocollo informatico unico e strumenti per il suo funzionamento

L'Ordine, avendo individuato un'unica AOO, dispone di un unico sistema di protocollo informatico e gestione documentale denominato Jente prodotto da Infor (Arezzo) (di seguito software di protocollo)

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

Al protocollo informatico unico sono di supporto, oltre al presente Manuale, i seguenti strumenti di gestione:

- Titolario di classificazione comprensivo del piano di fascicolazione e di conservazione
- Oggettario

1.7 Politiche di gestione e conservazione documentale

L'Ente ha adottato politiche di gestione e conservazione in linea con la normativa vigente e, con riferimento specifico al Manuale di gestione qui proposto, coerenti con il Codice dei beni culturali e con il Codice dell'amministrazione digitale (CAD).

La gestione e la conservazione hanno come obiettivo la tutela dei documenti nel loro valore giuridico-probatorio mantenendone l'integrità e affidabilità, e la valorizzazione finalizzata alla fruibilità a scopi storici delle informazioni e dei dati contenuti nei documenti.

L'Ente si avvale di un conservatore esterno scelto dall'elenco dei conservatori attivi accreditati presso AgID, secondo i criteri e le modalità descritte nella Circolare AgID n. 65/2014. Il Software di gestione del protocollo e dei documenti consente il riversamento con modalità semplificate.

2 PIANO DI SICUREZZA

Il presente capitolo, ai sensi **dell'art. 4, comma c, e dell'art. 7 del DPCM 3 dicembre 2013**, riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto delle misure minime di sicurezza previste nell'allegato B del D.lgs. 196/2003 e dalla circolare AgID del 18 aprile 2017 n. 2/201 che definisce le misure di sicurezza che ogni PA deve obbligatoriamente adottare entro il 31/12/2017.

2.1 Formazione dei documenti – aspetti di sicurezza

Le risorse strumentali e le procedure atte a garantire la sicurezza nella formazione dei documenti informatici, con particolare riferimento alla loro immodificabilità e integrità, sono descritte nel cap.3.

2.2 Gestione dei documenti informatici – aspetti di sicurezza

Il sistema di gestione informatica dei documenti:

- Garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- Assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- Fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Ente e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- Consente il reperimento delle informazioni riguardanti i documenti registrati;
- Permette, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;

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

2.2.1 Componente organizzativa della sicurezza

La gestione della sicurezza si realizza con specifici interventi tecnici e organizzativi finalizzati a prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia e con attività di controllo e verifica essenziali ad assicurare l'efficacia nel tempo del sistema informatico.

2.2.1 Componente fisica e infrastrutturale della sicurezza

La sede è organizzata in due diverse aree:

1. Area di accesso al pubblico
2. Area di lavoro riservata

Il controllo degli accessi fisici alle risorse dell'area di lavoro riservata, è regolato secondo i seguenti principi:

- l'accesso è controllato e consentito soltanto al personale autorizzato per motivi di servizio
- gli utenti dei servizi dell'Ente, i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti, possono accedere esclusivamente alle aree pubbliche. Gli accessi alle aree protette avvengono con accompagnamento da parte del personale dell'Ente;
- ogni persona che accede alle risorse della sede in locali protetti è identificata in modo certo.

Le misure di sicurezza fisica hanno un'architettura multilivello così articolata:

- a livello di edificio, attengono alla sicurezza perimetrale e sono atte a controllare l'accesso alla sede in cui sono ospitate risorse umane e strumentali;
- a livello di locale, sono finalizzate a controllare l'accesso ai locali interni alla sede.

Il controllo degli accessi fisici alle risorse della sede dell'amministrazione/AOO è regolato secondo i principi stabiliti dell'Ente.

Si garantisce la sicurezza fisica degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico attraverso locali dotati di:

- porte blindate
- impianti elettrici verificati
- luci di emergenza
- sistemi di condizionamento per il raffreddamento delle apparecchiature
- continuità elettrica del server garantita da apposito UPS (gruppo di continuità),
- continuità elettrica per i soli computer client degli uffici operativi ...
- controllo periodico di efficienza degli UPS
- estintori

-
- controllo dell'attuazione del piano di verifica periodica sull'efficacia dei sistemi di sorveglianza e degli estintori

Essendo la Sede Operativa lontana da insediamenti industriali e posta all'interno di un edificio adibito ad uffici, le sue condizioni ambientali per quanto riguarda polvere, temperatura, umidità, vibrazioni meccaniche, interferenze elettriche e radiazioni elettromagnetiche e livelli di inquinamento chimico e biologico, sono tali da non richiedere misure specifiche di prevenzione oltre quelle già adottate per le sedi di uffici di civile impiego.

2.2.3 Componente logica della sicurezza

La componente logica della sicurezza 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 stata realizzata attraverso:

- identificazione e autenticazione utente
- profilazione degli accessi (ACL – Access Control List)
- sistemi antivirus
- firma digitale (da applicare)
- disponibilità del software e dell'hardware
 - ridondanza dei sistemi di salvataggio
 - replica del salvataggio in Cloud

Policy di backup

Del contenuto di tutti i database del server viene effettuato il dump notturno in formato SQL Plain Text tramite l'utilità "pgdump" e mantenuta una ultima copia nella directory /home/db_repository Contestualmente viene eseguito anche un dump sempre suddiviso per database mantenendo una policy di retention settimanale/mensile/annuale nella directory /home/history-backup (ogni giorno viene eseguito il backup sovrascrivendo i backup oltre la settimana, mantengo anche una copia mensile sovrascrivendoli dopo un'anno, viene mantenuta anche una copia annuale)

l'elenco dei db mantenuti in copia sono:

- nome
- jente
- DbServiziApp
- ed alcuni piccoli db utilizzati in fase di recupero/migrazione dati dalla precedente versione del software.

Queste copie sono mantenute nella stessa macchina virtuale contenente il database

Backup su macchina differente

A sua volta la macchina virtuale è sottoposta a backup su una ulteriore macchina virtuale dedicata al mantenimento delle copie tramite software URBACKUP, sempre ospitata nel cluster delle macchine virtuali Aruba.

La policy di retention delle copie su quest'ultima macchina è la seguente:

Vengono effettuati i backup delle directory contenete i dump giornalieri dei db, dei documenti di stampa, delle effigi per i cartellini, degli applicativi compresi i files di configurazione (/var/lib/tomcat per NOME e /app per JENTE)

Viene eseguito un backup file completo ogni 30 giorni, successivamente ogni 24 ore un backup incrementale, vengono mantenuti da un minimo da di 2 backup completi fino a 10, un minimo di 4 fino ad un massimo di 100 backup incrementali (il tutto in base allo spazio disponibile sulla periferiche di backup)

Le realizzazioni sono in parte in carico al software specifico e in parte all'infrastruttura in cui il software è stato installato e viene utilizzato, come meglio chiarito in seguito.

Nello specifico, Jente è una **applicazione web** e come tale presenta una architettura di tipo **client/server**.

La struttura informativa implementata è basata su un server Linux Centos 6.7, il server è implementato in ambiente Aruba Private Cloud ed offre come storage il servizio di storage gold, raid in replica.

Il software è progettato e sviluppato secondo l'architettura **a tre livelli** che prevede la suddivisione dell'applicazione in tre diversi moduli (livelli):

1. Interfaccia utente
2. Logica funzionale/business (logicapplication server)
3. Dati persistenti (**database/repository file**)

Le possibili interazioni fra i livelli sono vincolate secondo quanto segue:

- interfaccia utente ↔ logica funzionale
- logica funzionale ↔ dati persistenti

Il livello "interfaccia utente" non può quindi relazionarsi direttamente con il livello "dati persistenti" (e viceversa).

Gli utenti (**clients**) usufruiscono dell'applicazione interagendo con l'interfaccia utente per mezzo di un **browser** installato nella propria postazione di lavoro (PdL) e della rete locale (intranet) dell'Ente.

Il software (logica funzionale) e le informazioni gestite (dati persistenti) risiedono in un sistema centralizzato presso l'Ente e costituito da server condivisonel quale, insieme ad altre, sono attivate le seguenti funzioni:

- server applicativo
- DBMS + Repository file

Un server applicativo è una tipologia di server che fornisce l'infrastruttura necessaria all'esecuzione di un software in un contesto "distribuito" mediante la rete.

All'interno del server applicativo server sono presenti una serie di applicazioni e procedure funzioni) che vengono rese disponibili contemporaneamente (distribuite) a più client mediante i protocolli standard previsti per la tecnologia web.

Il server applicativo è in sintesi il servizio di rete che ospita il software di protocollo ed è quindi responsabile della pubblicazione ed esecuzione delle funzioni previste. I **client** richiedono l'esecuzione di una determinata funzione per mezzo del browser e dell'interfaccia utente. Tali richieste giungono al server attraverso l'intranet dell'Ente.

Un database (DB) permette la memorizzazione di un insieme di informazioni in modo strutturato ed integro costituendo in tal modo un archivio di dati (base di dati). Il **DatabaseManagement System** (DBMS) è il software che permette la creazione, manipolazione e interrogazione di un DB. In Jente il DB gestisce anche il **repository dei file**, cioè l'area di memoria persistente che contiene i documenti gestiti dal sistema.

La scrittura ed l'interrogazione del DB avviene da parte del server applicativo interagendo con il DBMS attraverso la rete locale.

L'architettura precedentemente descritta permette di aumentare la modularità ed il livello di sicurezza del sistema.

L'utilizzo delle PdL e della rete intranet è garantito ai soli utenti dotati di apposite credenziali d'accesso (user ID + password) al sistema informatico dell'Ente.

L'operatore può accedere unicamente al livello "interfaccia utente" e solamente se dotato di specifiche credenziali e autorizzazioni al sistema protocollo.

L'interfaccia viene generata in funzione delle autorizzazioni in possesso dell'utente connesso.

Le ridotte dimensioni dell'Ente e la necessità di distribuire le attività di protocollo e gestione documentale a tutti i dipendenti, rendono di fatto non necessaria la stratificazione di diversi livelli di autorizzazione fatta a livello di documenti. Quindi tutti i dipendenti abilitati alla protocollazione, hanno accesso a tutti i documenti gestiti dal sistema documentale. Per questo sono stati opportunamente edotti sulle responsabilità e formati in merito agli aspetti della sicurezza informatica. Sono gestiti livelli di autorizzazione differenziati per quegli utenti che devono accedere al sistema per la sola consultazione (visualizzazione). Anche in questo caso disponibile in modo indifferenziato a tutti i documenti.

Ciò nonostante il sistema di gestione del protocollo e gestione documentale consente di stratificare le autorizzazioni alla visualizzazione di documenti ritenuti particolarmente sensibili. Tale configurazione può avvenire in relazione alla classe documentale o al singolo documento.

Nessun sistema, componente, servizio ed interfaccia inerente al sistema Jente è direttamente accessibile e fruibile dalla rete pubblica **internet**.

Quanto sopra potrebbe cambiare in relazione al posizionamento in cloud del software. In quel caso andranno svolte specifiche analisi per la sicurezza.

2.2.4 Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) – presenti o transitati su Jente o altri indipendenti sistemi di supporto – che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza possono essere costituite:

- dai log di sistema generati dal Sistema Operativo
- dai log dei dispositivi di protezione periferica del sistema informatico (IntrusionDetection System(IDS), sensori di rete e firewall)
- dalle registrazioni di Jente

Le registrazioni di sicurezza sono soggette almeno ad una delle seguenti misure:

- scrittura su database in modalità sincrona (scrittura logica che coincide con scrittura fisica sul disco)
- sistemi di backup riportati nel paragrafo precedente.

2.2.5 Criteri di utilizzo degli strumenti tecnologici

Il sistema informatico garantisce agli utenti interni dell'Ente, l'accesso ai servizi previsti, mediante l'adozione di un insieme di misure organizzative e tecnologiche.

Gli utenti interni autorizzati ad utilizzare il software di protocollo, operano nel rispetto dei vincoli posti dall'Ente, che prevede quanto segue:

- ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi e dei programmi a cui ha accesso, nonché dei dati trattati ai fini istituzionali
- ogni utente è responsabile, civilmente e penalmente, del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali, anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio e della normativa per la tutela dei dati personali
- ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico. È vietato l'utilizzo di supporti per la memorizzazione dei dati (CD, DVD, memorie USB, etc.) non sicuri e/o provenienti dall'esterno, al fine di non diffondere eventuali virus
- i dati archiviati informaticamente devono essere esclusivamente quelli attinenti alle proprie attività lavorative
- tutti i dati sensibili riprodotti su supporti informatici, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da terzi. Altrettanta cautela deve essere riposta in fase di stampa dei documenti contenenti dati sensibili: la stampa va effettuata su stampanti presidiate dall'addetto
- l'account del sistema Jente è costituito da un codice identificativo personale (username) e da una parola chiave (password)

-
- la password che viene associata a ciascun utente è personale, non cedibile e non divulgabile
 - le password dovranno avere le seguenti caratteristiche:
 - lunghezza minima 8 caratteri
 - caratteri di tipo alfanumerico e deve contenere almeno un numero, una lettera minuscola e una lettera maiuscola e un carattere speciale

2.3 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata o PIN nel caso di un dispositivo rimovibile in uso esclusivo all'utente) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

2.4 Politiche di sicurezza adottate dall'Ente

Le politiche di sicurezza sono riportate nella documentazione predisposte ai sensi del GDPR (Regolamento Europeo 2016/679).

Come previsto dal provvedimento 393, 2 luglio 2015 del Garante della protezione dei dati personali, le amministrazioni pubbliche sono tenute a comunicare al Garante le violazioni dei dati personali (data breach) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. p del Codice in materia di protezione dei dati personali 196 del 2003) di cui sono titolari, secondo la compilazione del modulo predisposto dal Garante (**Modello di segnalazione data breach PA**).

È compito dei responsabili della sicurezza, del sistema informativo e della tutela dei dati personali, procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza.

Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni secondo quanto previsto dalla normativa o a seguito dei risultati delle attività di audit.

2.5 Servizio archivistico (doc. analogici)

La sede dell'archivio dell'Ente è individuata nei locali al piano primo e a piano terra della sede istituzionale dell'amministrazione medesima.

3 MODALITÀ DI FORMAZIONE DEI DOCUMENTI

3.1 I documenti dell'Ente

3.1.1 I requisiti minimi del documento

I documenti dell'Ente sono di norma prodotti con sistemi informatici, ai sensi dell'articolo 3 del D. Lgs. 12 febbraio 1993, n. 39 e successive modificazioni ed integrazioni.

2. I documenti prodotti dall'Ente devono riportare, al minimo, le seguenti informazioni:

- a) denominazione e Logo dell'Ordine
- b) indirizzo completo con numero di telefono, e-mail, PEC
- c) data completa, luogo, giorno, mese, anno
- d) indice di classificazione: titolo e classe
- e) numero e data di protocollo
- f) dati del destinatario: Cognome e nome (per le persone) Denominazione (per gli enti e le imprese), Indirizzo completo: via/piazza, numero civico, CAP, città o Indirizzo informatico (e-mail/Pec...)
- g) numero degli allegati se presenti
- h) oggetto del documento
- i) sigla dell'estensore del documento
- l) sottoscrizione (firma autografa o digitale)

3.1.2 Produzione dei documenti informatici

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

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

Il documento informatico viene formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico o derivante da consultazioni web o a seguito di processi telematici, acquisizione della copia informatica di un documento analogico

Le caratteristiche di immutabilità e di integrità sono determinate da una o più delle seguenti operazioni:

- sottoscrizione con firma digitale
- trasferimento a soggetti terzi con Posta Elettronica Certificata con ricevuta completa
- memorizzazione su sistemi di protocollo e gestione documentale che adottino idonee politiche di sicurezza

Nel caso specifico del documento amministrativo informatico l'insieme di metadati minimi è costituito da:

- A. numero di protocollo
- B. data di protocollo
- C. mittente – destinatario
- D. oggetto
- E. data e protocollo del documento ricevuto, se disponibili
- F. impronta del documento informatico
- G. metadati aggiuntivi stabiliti dall'Ente a fini amministrativi, gestionali e conservativi, inclusi dell'indice di classificazione

3.1.3 Tipologie di formato del documento informatico

L'Ente, in considerazione di quanto previsto dal DPCM 3 dicembre 2013 in materia di conservazione, al fine di garantire le caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo e diffusione, adotta i seguenti formati:

FORMATO	ESTENSIONE	STANDARD DI RIFERIMENTO
PDF – PDF/A	.pdf	ISO 32000-1 (PDF) ISO 19005-1 :2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
File grafici	.tif, .jpeg, .jpg, .bmp, .png	ISO 12639 ISO 12234 ISO/IEC 10918:1
Office Open XML (OOXML)	.docx, .xlsx, .pptx	ISO/IEC DIS 29500:2008
Open Document Format	.odt, .ods, .odp, .odg, .odb	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
XML	.xml Derivati da XML: .svg	ISO 8879 – SGML Specifiche W3C
TXT	.txt	/
Formati messaggi di posta elettronica	.eml	RFC 2822 – MIME RFC 1847 – S/MIME
File audio	.mp3	
File video	.avi .mpeg4	

File compressi	.zip, .rar	
Documento firmato con firma elettronicaCAdeS	.p7m	

I file compressi o che contengono altri formati devono contenere esclusivamente file con formato incluso nella tabella di cui sopra.

La scelta dei formati è stata effettuata considerando che essa, come da previsione normativa, deve garantire la leggibilità e la reperibilità del documento informatico nell'intero ciclo di vita dello stesso. Eventuali integrazioni al presente elenco sono definite in considerazione di specifiche previsioni normative o tecniche.

Nel caso pervengano documenti su formati diversi da quelli elencati:

- l'Ente provvede alla conversione del documento in uno dei formati adottati, mantenendone inalterati i contenuti. Qualora non sia possibile la conversione del formato, il servizio di gestione documentale avrà cura di avvisare il soggetto produttore in modo da permettere un nuovo invio con formato tra quelli previsti.

3.1.4 Documenti contenenti collegamenti ipertestuali.

Nel caso pervengano documenti contenenti collegamenti ipertestuali (link) a pagine web o file in qualsiasi formato, il servizio gestione documentale avrà cura di avvisare il soggetto produttore affinché provveda ad un nuovo invio, inserendo in allegato (in formato consentito) i file e/o la stampa in formato PDF delle pagine web di destinazione dei collegamenti ipertestuali.

4 FLUSSI DI LAVORAZIONE DEI DOCUMENTI

Il presente capitolo fornisce indicazioni sulle modalità di lavorazione dei documenti ricevuti e prodotti dall'Ente.

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

- ricevuto
- inviato
- interno

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 *“le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche”*.

La redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità.

Pertanto, soprattutto nella fase transitoria di migrazione verso l'adozione integrale delle tecnologie digitali da parte dell'amministrazione, il documento amministrativo può essere disponibile anche nella forma analogica.

4.1 Documenti in entrata

La corrispondenza in ingresso può essere acquisita dall'Ente con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

4.1.1 Ricevuti o prodotti su supporto analogico

I documenti ricevuti su supporto analogico possono essere recapitati attraverso:

- a mezzo posta convenzionale. La Responsabile di segreteria provvede a separare i documenti esclusi dalla registrazione di protocollo (**Allegato 3 – Documenti esclusi dalla registrazione di Protocollo**) e all'apertura della corrispondenza
- a mezzo posta raccomandata
- fax
- brevi manu: consegna diretta presso gli sportelli aperti al pubblico durante l'orario di apertura.

4.1.2 Ricevuti o prodotti su supporto informatico

I documenti informatici possono essere recapitati/trasmessi tramite:

- posta elettronica convenzionale o certificata (la casella mail istituzionale dell'Ente info@odmeo.re.it, casella PEC dell'Ente segreteria.re@pec.omceo.it, pubblicate sul sito istituzionale www.odmeo.re.it)
- su supporto rimovibile quale, ad esempio, cd rom, dvd, pen drive, consegnato direttamente alla Segreteria o inviato per posta convenzionale o corriere

4.2 Documenti inviati

Le comunicazioni verso i privati avvengono sia attraverso i canali analogici che informatici, le comunicazioni verso le altre pubbliche amministrazioni avvengono mediante l'uso dei canali informatici a meno che l'Ente destinatario non richieda esplicitamente una modalità diversa.

4.2.1 Inviati su supporto analogico

I documenti analogici sono trasmessi attraverso:

- Servizi postali
- Brevi manu
- Notifica

Il documento in uscita viene normalmente redatto in unica copia, sottoscritta dal Legale rappresentante dell'Ente o da un suo delegato, registrata nel sistema di protocollo e spedita. La minuta di tale documento viene conservata presso l'Ente e inserita nel fascicolo.

Il documento analogico viene sempre scansionato e associato al relativo protocollo compilando manualmente i metadati necessari e associandolo al relativo fascicolo informatico, al fine di consentire che il sistema di gestione documentale informatizzato costituisca il sistema unico anche dei documenti analogici e ne permetta l'inclusione nei relativi fascicoli informatici.

4.2.2 Inviati su supporto informatico

I documenti informatici sono trasmessi attraverso:

- Posta elettronica certificata (PEC)
- Caselle di Posta elettronica
- Canali digitali

I documenti sono trasmessi per posta elettronica certificata e/o per posta elettronica convenzionale. Solo la trasmissione dalla casella di PEC istituzionale ad una casella PEC del destinatario costituisce, infatti, evidenza giuridico-probatoria dell'invio e della consegna del messaggio (art. 47 CAD).

4.2.3 Documento Cartaceo inviato elettronicamente

Se il documento cartaceo è inviato tramite posta elettronica certificata o canali digitali, viene redatto in un unico esemplare, sottoscritto, registrato, acquisito tramite scansione nel sistema di protocollo, associato al protocollo stesso e al fascicolo relativo. L'operatore provvede poi all'invio del file alla posta elettronica certificata o tramite i canali digitali del destinatario. Viene quindi conservato presso l'Ente e inserito nel fascicolo.

4.2.4 Documento Digitale inviato elettronicamente

Se il documento informatico inviato tramite posta elettronica certificata o canali digitali, viene redatto tramite un software adeguato (es. elaborazione testi), sottoscritto con firma digitale, registrato, acquisito nel sistema di protocollo, associato al protocollo stesso e al fascicolo relativo, è archiviato solo in formato digitale. L'operatore provvede poi all'invio del file alla posta elettronica certificata o canali digitali del destinatario.

5 MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

L'Ente utilizza il sistema di protocollo informatico e di gestione documentale indicato al cap. 1.

5.1 Registrazione dei documenti

Tutti i documenti dell'Ente, con particolare riferimento a quei documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi, devono essere registrati sul protocollo informatico unico dell'Ente, 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.

Tale operazione serve a identificare in modo univoco un documento individuandone data, forma e provenienza certa.

Anche i documenti soggetti a repertoriatura, forma particolare di registrazione, vengono registrati sul protocollo informatico unico dell'Ente.

Al fine di ottenere un unico punto di ricerca e gestione dei documenti, si dà particolare rilevanza alla registrazione di protocollo.

La registrazione a protocollo riguarda il singolo documento; non può riguardare per alcun motivo il fascicolo. Quindi il numero di protocollo individua un singolo documento.

I documenti sono poi raccolti in fascicoli informatici o ibridi o in aggregazioni documentarie per tipologie di documenti (serie).

5.2 Registro di protocollo

Il registro di protocollo², è un documento informatico prodotto e redatto secondo le modalità previste dalla vigente normativa.

²La giurisprudenza, sia civile, che penale che amministrativa, ha affrontato in numerose occasioni la tematica della natura giuridica e del valore probatorio del registro di protocollo all'interno di un ente pubblico, giungendo sempre alla medesima conclusione: si tratta di un atto pubblico di fede privilegiata (tra le altre, si vedano Cons. Stato, sez. VI, sentenza 26.5.1999, n. 693, Cass. pen., sez. V, sentenza 2.5.1994, Cons. Stato, ad. plen., sentenza 5.8.1993, n. 10). Da ciò deriva non solo che qualunque pubblico dipendente operi nel sistema di protocollazione lo fa in qualità di pubblico ufficiale, ma anche che chiunque intenda contestare la veridicità di una o più registrazioni contenute nel protocollo di un'Amministrazione è tenuto a proporre querela di falso, in base all'art. 221 del codice di procedura civile

Nell'ambito dell'Ente, il registro di protocollo è unico e la sua numerazione, unica, progressiva e costituita da 7 cifre numeriche, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

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

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

Nel caso di ricezione dello stesso documento da parte di più destinatari dell'Ente occorre evitare una molteplice registrazione dello stesso documento.

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

Il registro di protocollo giornaliero riporta tutti i protocolli generati nell'arco della singola giornata.

Il "registro di protocollo"³ deve ricomprendere le informazioni minime richieste dall'art. 53, comma 1, del DPR 445/2000 e dalla Circolare AGID n. 60 del 2013.

In particolare, la registrazione di protocollo per ogni documento ricevuto o spedito richiede la memorizzazione delle seguenti informazioni:

- A. il numero di protocollo del documento generato automaticamente dal sistema
- B. la data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile
- C. il mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti
- D. l'oggetto del documento
- E. l'impronta del documento informatico, se trasmesso per via telematica o se il documento analogico è scansionato ed associato al protocollo
- F. indicazione del registro nell'ambito del quale è stata effettuata la registrazione;

Gli elementi non obbligatori, ma funzionali qualora disponibili sono:

- numero di protocollo del documento ricevuto
- data del documento ricevuto
- annotazioni

Di conseguenza, il registro giornaliero di protocollo contiene, in modo ordinato e progressivo, l'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

³ Conformemente anche a quanto indicato nel documento AGID "PRODUZIONE E CONSERVAZIONE DEL REGISTRO GIORNALIERO DI PROTOCOLLO"

http://www.agid.gov.it/sites/default/files/documenti_indirizzo/istruzioni_per_la_produzione_e_conservazione_registro_giornaliero_di_protocollo.pdf

Ai sensi dell'art. 7 comma 5 del DPCM 3 dicembre 2013, il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

5.3 Modalità di registrazione di protocollo

Per registrazione di protocollo si intende l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. La registrazione si effettua di norma entro la giornata di arrivo o comunque entro 24 ore lavorative dal ricevimento o, se intercorrono dei giorni festivi o di chiusura programmata dell'Ente, nel primo giorno lavorativo utile. Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immodificabile. Contestualmente alla registrazione i documenti analogici vengono acquisiti nel sistema di protocollo tramite procedura di scansione. I documenti informatici vengono acquisiti nel sistema di protocollo attraverso le modalità descritte nel capitolo 4.

5.4 La segnatura di protocollo

La segnatura di protocollo avviene contemporaneamente all'operazione di registrazione mediante l'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.

Le informazioni minime previste ai sensi del DPCM 3 dicembre 2013 sono:

- A. codice identificativo dell'amministrazione
- B. codice identificativo dell'area organizzativa omogenea
- C. codice identificativo del registro
- D. progressivo registrazione
- E. data di registrazione

Ulteriori informazioni previste sono:

- A. identificazione degli allegati
- B. anno
- C. titolo
- D. classe

Quando il documento è indirizzato ad altre amministrazioni ed è sottoscritto con firma digitale e trasmesso con strumenti informatici, la segnatura di protocollo può includere le informazioni di registrazione del documento purché siano adottate idonee modalità di formazione dello stesso in formato pdf (preferibilmente pdf/a).

Qualora il documento venga prodotto su formato analogico, al termine della registrazione, la segnatura viene apposta direttamente sul supporto cartaceo. Questa riporterà il numero e la data di protocollo, la classificazione, il numero di fascicolo.

Qualora il documento venga prodotto e spedito in formato nativo digitale:

- il numero di protocollo è indicato nel nome del file e nell'oggetto della mail nel caso di trasmissione con posta elettronica.

5.5 Documenti soggetti a registrazione particolare (Repertoriazione)

Possono essere esclusi dall'obbligo di registrazione di protocollo generale le tipologie di documenti soggetti a registrazione particolare (*ad esempio i mandati e le reversali*).

Questi documenti costituiscono delle serie di interesse archivistico e devono essere opportunamente identificati, datati e conservati coerentemente con la tipologia di supporto adottata.

5.6 Procedure specifiche nella registrazione di protocollo

5.6.1 Protocollazione di documenti riservati

I documenti di carattere riservato sono trattati esclusivamente dal personale autorizzato.

I documenti vengono caricati nel sistema di gestione documentale e vengono poi protocollati e classificati in modo da garantirne la condizione di riservatezza.

Tale accesso può essere esteso anche a cariche istituzionali dell'Ente (es. presidente, consiglieri, ecc.) purché ne abbiano facoltà.

Un controllo nel rilascio delle credenziali di accesso consente un adeguato livello di sicurezza.

5.6.1.1 Modifica della gestione della sicurezza per documenti classificati come "riservati"

Le tipologie di documenti da registrare nel protocollo riservato saranno codificate all'interno del sistema di protocollo informatico a cura del responsabile del Servizio archivistico dell'Ordine, di concerto con il responsabile/direttore dell'Ordine. Le procedure adottate per la gestione dei documenti e dei procedimenti amministrativi ad accesso riservato, comprese la registrazione, la segnatura, la classificazione e la fascicolazione, saranno le stesse adottate per gli altri documenti e procedimenti amministrativi. L'operatore che effettua la registrazione di protocollo di un documento attribuisce allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal sistema. Il sistema può associare il livello di riservatezza in relazione alla classe documentale assegnata al protocollo/documento.

5.6.2 Documenti esclusi dalla registrazione di protocollo

Il DPR 445/2000 prevede che tutti i documenti in entrata e in uscita e tutti i documenti informatici siano registrati a protocollo, con alcune eccezioni. Tra le eccezioni troviamo i documenti soggetti a registrazione particolare e i documenti di cui all'**allegato 2– Documenti esclusi dalla registrazione di Protocollo**.

5.6.3 Annullamento delle registrazioni di protocollo

Le informazioni non modificabili della registrazione a protocollo sono annullabili ai sensi dell'art. 54 del DPR 445/2000 ma devono rimanere memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data e l'ora.

La procedura di annullamento di una registrazione avviene su autorizzazione del Responsabile del servizio archivistico.

5.7 Casi particolari di registrazioni di protocollo

5.7.1 Lettere anonime e comunicazioni prive di firma autografa (e-mail)

La lettera anonima e la comunicazione con mittente, priva di firma, vanno protocollate, su autorizzazione del Responsabile del servizio archivistico.

5.7.2 Corrispondenza personale o riservata

La corrispondenza personale (es. Mario Rossi c/o Ordine dei Medici ...) è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale" o "s.p.m".

In quest'ultimo caso, la corrispondenza con la dicitura "riservata" o "personale" o "s.p.m" non è aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti debbano essere comunque protocollati provvede a trasmetterli all'ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

5.7.3 Integrazioni documentarie

L'addetto al protocollo è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta e, in caso di mancanze, è tenuto a richiederne l'integrazione.

5.7.4 Documenti pervenuti per errore all'Ordine

I documenti pervenuti per errore all'Ente non devono essere protocollati e devono essere spediti immediatamente al destinatario con la dicitura «Erroneamente pervenuto all'Ordine dei Medici Chirurghi e degli Odontoiatri di Reggio Emilia in data.....».

5.7.5 Documenti in partenza con più destinatari

Qualora i destinatari del documento siano molteplici nella registrazione di protocollo, questi vanno tutti riportati nel campo “destinatario”.

Solo in casi eccezionali e qualora i destinatari siano in numero superiore a 10, si utilizza uno dei destinatari particolari, esempio: “ISCRITTI/DESTINATARI ALLA DATA DELL’INVIO”.

5.7.6 Flussi documentali informatici

5.7.6.1 Flusso FNOMCeO-ENPAM

L’Ordine è tenuto periodicamente all’invio delle posizioni degli iscritti alla FNOMCeOe all’ENPAM. Tale invio avviene con una procedura semiautomatica:

- generazione a partire dal gestionale Albi di 2 file in formato xml
- protocollazione del file “Anagrafica” indicando come destinatari FNOMCeO ed ENPAM
- protocollazione del file “Datirifnom” indicando come destinatario FNOMCeO
- procedura di upload effettuato con software FNOMCeO/ENPAM

Il sistema si occupa poi di instradare i 2 File ai sistemi FNOMCeO o ENPAM.

La procedura dovrà essere revisionata in relazione delle nuove disposizioni in materia di trattamento dati (GDPR).

5.8 Regole di smistamento e di assegnazione

L’operazione di smistamento consiste nell’assegnazione di un documento registrato all’attenzione del Presidente o della Segreteria e al conseguente conferimento di responsabilità del relativo procedimento amministrativo.

Si adottano le modalità operative di seguito illustrate:

- tutti i documenti analogici in entrata o in uscita registrati devono essere acquisiti in copia per immagine e associati alla registrazione di protocollo. Fanno eccezione i documenti che materialmente non possono essere sottoposti a scansione (a titolo meramente esemplificativo: volumi, registri, plichi, planimetrie di formato superiore all’A3, plastici, monete, ecc.). In questi casi si deve segnalare l’assenza degli allegati, nel campo “Note”
- nel caso di documento analogico, l’originale è conservato nell’archivio generale dell’Ente;
- nel caso di documenti informatici, l’originale è acquisito direttamente (salvo procedura di caricamento manuale) nel sistema di protocollo attraverso i canali previsti;
- il responsabile/direttore dell’Ente visualizzano i documenti attraverso l’utilizzo del software di gestione documentale dell’Ente.

6 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico, ogni evento deve essere registrato su un supporto alternativo, denominato Registro di emergenza (**Allegato 1 Modello del Registro di emergenza**).

Per emergenza si intende una situazione in cui la sospensione del servizio si protragga oltre le **otto ore** o che sia comunque tale da pregiudicare la registrazione a protocollo in giornata, nel caso in cui vi siano scadenze inderogabili e prescrittive (es: bandi, concorsi, ecc.).

L'utilizzo del registro di emergenza deve essere autorizzato dal Responsabile del Servizio per la tenuta del protocollo informatico. In caso di assenza del responsabile del servizio provvede all'autorizzazione il Vicario o, in assenza di entrambi, il Segretario dell'Ordine ovvero dal Presidente e legale rappresentante così come descritto al cap. 1.

Per la registrazione di emergenza si utilizza un modulo cartaceo di cui si allega fac simile al Manuale di gestione che verrà compilato manualmente.

In condizione di emergenza si applicano le seguenti modalità di registrazione e di recupero dei dati:

a) sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema di gestione informatica dei documenti

b) qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile del Servizio Archivistico può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana.

d) la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve essere unica per ciascun anno e deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea;

e) le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

f) Il file per il recupero dall'emergenza può essere compilato sia preassegnando manualmente i numeri (operando sulla gestione dei numeratori) che lasciandoli vuoti (il sistema li assegnerà in automatico). Il numero e la data del registro di emergenza vengono registrati negli "estremi" dei protocolli che saranno assegnati. Il registro di emergenza viene citato negli estremi della registrazione di protocollo del registro generale.

Sul registro di emergenza devono essere riportate codice registro, numero di protocollo, arrivo/partenza, la data, l'oggetto, numero degli allegati, classe documentale, nonché eventuali note ritenute rilevanti dal responsabile del protocollo informatico e della gestione documentale. Il registro di emergenza viene gestito esclusivamente in forma cartacea.

Prima di autorizzare l'avvio della procedura, il RSP deve impostare e verificare la correttezza di data e ora sui rispettivi registri di emergenza. In caso di vicinanza alla data di fine anno solare, si tenga

presente che ogni registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo senza soluzione di continuità la numerazione del protocollo informatico unico raggiunta al momento dell'interruzione del servizio. A tale registrazione sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza. L'utente adibito alla protocollazione, alla ripresa della piena funzionalità del sistema di protocollo informatico, provvede a riversare sul programma stesso tutte le registrazioni già eseguite sul registro di emergenza.

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 informatico unico.

7 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

7.1 Protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti degli Enti Pubblici sono beni culturali inalienabili ai sensi dell'art. 10, comma 2 del Decreto legislativo 42/2004.

Quindi, tutti i documenti acquisiti e prodotti (compresi quelli interni) nel sistema di gestione documentale dall'Ente, sono inalienabili e appartengono ad un unico complesso archivistico, che è l'archivio dell'Ente.

L'archivio non può essere smembrato e deve essere conservato nella sua organicità. Lo scarto dei documenti, siano essi cartacei o informatici, è subordinato all'autorizzazione della Soprintendenza archivistica competente per la regione di appartenenza ai sensi degli artt. 20 e 21 del Decreto legislativo 42/2004.

Per l'archiviazione e la custodia nella sezione di deposito, o storica, dei documenti contenenti dati personali, si applicano le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che di supporti convenzionali.

Ai sensi dell'art. 30 del Decreto legislativo 42/2004 **Codice dei beni culturali e del paesaggio (ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137)**, dell'art. 30 del DPR 30 settembre 1963, n. 1409 **Norme relative all'ordinamento ed al personale degli archivi di Stato** e degli artt. 67 e 69 del DPR 445/2000 **Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa**, L'Ente, in quanto ente pubblico, ha l'obbligo di:

- garantire la sicurezza e la conservazione del proprio archivio e procedere al suo ordinamento
- costituire uno, o più archivi di deposito nei quali trasferire annualmente i fascicoli relativi agli affari conclusi

-
- istituire una sezione separata d'archivio per i documenti relativi ad affari esauriti da più di 40 anni (archivio storico) e di redigerne l'inventario

L'archivio è quindi un'entità unitaria, che conosce tre fasi:

- **Archivio corrente**⁴, composto dai documenti relativi ad affari in corso, conservati presso gli uffici (comprende fascicoli di persona fisica o giuridica)
- **Archivio di deposito**⁵, composto dai documenti relativi ad affari cessati da meno di 40 anni conservati presso l'archivio di deposito presso l'Archivio generale dell'Ente, a determinate condizioni
- **Archivio storico**⁶, composto dai documenti relativi ad affari cessati da più di 40 anni, selezionati per la conservazione permanente conservati presso l'Archivio generale dell'Ente, che funge da sezione separata

Il trattamento del sistema documentale dell'Ente implica la predisposizione di strumenti di gestione dell'archivio corrente che consentano un'efficace organizzazione e consultazione della documentazione, a prescindere dai supporti dei documenti

Il presente capitolo descrive il sistema di classificazione dei documenti, di formazione del fascicolo e di conservazione dell'archivio, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto della documentazione e di consultazione e movimentazione dei fascicoli.

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (titolario).

Il piano di conservazione, collegato con il titolare ed elaborato tenendo conto dei flussi documentali dipendenti dai procedimenti e dalle prassi seguiti dall'Ente nell'espletamento delle funzioni istituzionali, definisce i tempi di conservazione dei documenti e dei fascicoli.

Titolario e piano di conservazione, in quanto strumenti che consentono la corretta gestione e conservazione, sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di registrazione di protocollo e di archiviazione. Il titolare e il piano di conservazione sono adottati con atti formali dai vertici dell'amministrazione.

7.2 Titolare o piano di classificazione

La classificazione consiste nell'attività di organizzazione logica in base alla quale ciascun documento, prodotto e conservato su qualsiasi tipo di supporto, protocollato e non (spediti, ricevuti, interni) viene ricondotto, alla voce del titolare che individua la funzione cui si riferisce.

⁴ In ambito informatico si può assumere che appartengano a questa fase i documenti o fascicoli non chiusi.

⁵ In ambito informatico si può assumere che appartengano a questa fase i documenti o fascicoli chiusi (indipendentemente dal fatto che siano stati inviati o meno in conservazione digitale)

⁶ In ambito informatico si può assumere che appartengano a questa fase tutti i documenti o i fascicoli che, con anzianità superiori ai 40 anni, siano presenti nel sistema di gestione del protocollo informatico a valle di tutte le fasi di sfolgimento avvenute nel tempo.

L'Ente utilizza un titolario, adottato con deliberazione del 20/03/2019 organizzato a 2 livelli suddiviso in titoli e classi. Titoli e classi sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del Consiglio Direttivo dell'Ente sentito il RSP. L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RSP. Dopo ogni modifica del titolario, il RSP 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; le eventuali modifiche e integrazioni entrano in vigore il 1° gennaio dell'anno seguente. Il titolario non è retroattivo: non si applica cioè, ai documenti protocollati prima della sua introduzione.

Tutti i documenti ricevuti e prodotti dagli Uffici utenti dell'AOO, sono classificati in base al titolario o piano di classificazione che costituisce **allegato n. 2** al presente Manuale.

7.2.1 Classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo l'ordinamento del Titolario. Viene effettuata su tutti i documenti ricevuti e prodotti dell'Ente, indipendentemente dal supporto sul quale vengono formati.

La classificazione (apposizione/associazione di titolo e classe al documento) è necessaria e preliminare all'attività di fascicolazione.

7.3 Formazione del fascicolo

7.3.1 Il fascicolo

Il fascicolo è l'unità archivistica di base indivisibile di un archivio, deve essere inteso come la raccolta ordinata della documentazione che si è prodotta durante la trattazione di un affare, inserita nel complesso documentario costituente l'archivio, sulla scorta del sistema di classificazione previsto dal titolario.

L'operazione di fascicolazione attiene all'inserimento di un documento nell'unità archivistica relativa all'oggetto, procedimento amministrativo, persona fisica o giuridica, a cui si riferisce.

Tutti i documenti registrati nel sistema di gestione informatica dei documenti, indipendentemente dal supporto sul quale sono formati, devono essere riuniti in fascicoli con l'operazione di fascicolazione.

La formazione di un nuovo fascicolo comporta la registrazione sul sistema di gestione informatica dei documenti, al minimo, delle seguenti informazioni:

- a. data di apertura
- b. indice di classificazione c. numero del fascicolo
- d. oggetto del fascicolo

I fascicoli possono essere organizzati in sottofascicoli e inserti, i quali sono numerati progressivamente nell'ambito delle unità archivistiche che li compongono.

Sul frontespizio di un fascicolo cartaceo devono essere riportate le informazioni di cui al comma 4

La formazione dei fascicoli avviene nell'ambito degli uffici di competenza, a cura dei responsabili dei procedimenti amministrativi.

7.3.2 Famiglie e tipologie di fascicolo

I fascicoli sono suddivisi in 2 macro-categorie:

1. fascicoli inerenti persone fisiche o giuridiche
2. fascicoli inerenti procedimenti, affari o attività

All'interno dei fascicoli di persona, si distinguono 2 tipologie:

- fascicoli relativi a persone fisiche (ad esempio: personali dipendente, assistiti, etc.)
- fascicoli inerenti persone giuridiche (ad esempio: Enti, attività economiche, etc.)

Per ogni persona fisica o giuridica deve essere istruito un fascicolo nominativo. Il fascicolo viene generato automaticamente dal sistema documentale alla prima associazione di un documento/sottofascicolo.

L'apertura prevede la registrazione di alcune informazioni essenziali:

- anno
- identificativo progressivo
- indice di classificazione, (cioè titolo, classe)
- oggetto del fascicolo
- data di apertura del fascicolo
- nominativo del responsabile del procedimento/fascicolo

All'interno della famiglia dei fascicoli inerenti procedimenti, si distinguono 2 tipologie:

- fascicoli relativi ad attività
- fascicoli relativi procedimenti amministrativi

I documenti sono archiviati all'interno di ciascun fascicolo, ed eventuale 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/attività. **La data di chiusura si riferisce alla data dell'ultimo documento prodotto.**

Tutti i fascicoli sono generati all'interno del software di gestione documentale.

In caso di fascicolo cartaceo (analogico) o ibrido (analogico-digitale), sulla camicia del fascicolo vengono riportate le informazioni descrittive del fascicolo.

I dati identificativi del fascicolo analogico, al fine della sua identificazione e archiviazione, includono:

- anno
- identificativo progressivo
- indice di classificazione, (cioè titolo, classe)
- oggetto del fascicolo

-
- data di apertura del fascicolo
 - data di scadenza
 - data di chiusura
 - nominativo del responsabile del procedimento/fascicolo

7.3.3 Processo di assegnazione dei fascicoli

Quando un nuovo documento viene formato o ricevuto dall'amministrazione, il responsabile del procedimento o suo delegato abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso debba essere inserito in un fascicolo già esistente, oppure sia necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

- Se il documento si riferisce a un fascicolo aperto, l'addetto:
 - seleziona il relativo fascicolo
 - collega la registrazione di protocollo del documento al fascicolo selezionato (Se si tratta di un documento su supporto cartaceo, assicura l'inserimento fisico dello stesso nel relativo fascicolo cartaceo)
- Se il documento non è riferito ad alcun fascicolo aperto, il soggetto preposto:
 - esegue l'operazione di apertura del fascicolo
 - collega la registrazione di protocollo del documento al fascicolo appena creato

7.3.4 Repertorio dei fascicoli

Ogni Fascicolo ha un proprio "IDENTIFICATIVO", costituito da un codice che consente di identificare univocamente un'entità dal punto di vista amministrativo. Tale identificativo è strutturato conformemente a quanto indicato nella **CIRCOLARE AGID N. 60 DEL 23 GENNAIO 2013** (Pag. 71)⁷

Il repertorio dei fascicoli, ripartito per ciascun titolo del titolare, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio quindi rispecchia quella del titolare di classificazione e 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 al proprio mandato istituzionale, il repertorio dei fascicoli rappresenta, in concreto, le attività svolte e i documenti prodotti in relazione a tali attività.

Gli elementi costitutivi del repertorio di fascicoli sono:

- l'anno di riferimento

⁷ La forma dell'Identificativo può essere stabilita dall'amministrazione che lo attribuisce. Un Identificativo deve essere compatibile con la formazione di un identificativo telematico come URI, cioè Uniform Resource Identifier (RFC 1738).

Regole aggiuntive:

- Un Identificativo è codificato mediante caratteri previsti dalla specifica US-ASCII a 8 bit ed è composto da una sequenza di lettere maiuscole ([A-Z]), lettere minuscole ([a-z]), cifre decimali ([0-9]) e dai caratteri '.', '!' e '_'.
Un Identificativo deve avere una lunghezza non superiore a 16 caratteri.

-
- l'indice di classificazione completo (titolo, classe, sottoclasse, etc.)
 - identificativo(es. 2016-0000002)
 - la data/anno di apertura
 - la data/anno di chiusura
 - l'oggetto del fascicolo
 - le note sullo stato del fascicolo, cioè se è aperto o chiuso
 - eventuali note

Le ricerche dei fascicoli si effettuano a partire dalla gestione informatizzata.

In caso di fascicoli ibridi e analogici è indispensabile indicare e tenere aggiornata la collocazione fisica dei fascicoli.

7.3.5 Il fascicolo personale dell'iscritto

Il fascicolo dell'iscritto riguarda tutta la gestione della documentazione relativa alla vita del medico, dell'odontoiatra e della società tra professionisti.

All'interno del titolo "tenuta albi" si distinguono tre voci di classificazione fondamentali per la tenuta degli Albi:

- Albo medici chirurghi
- Albo odontoiatri
- Albo società tra professionisti

Le prime due voci danno origine a fascicolo di persona fisica mentre nella terza si generano fascicoli di persona giuridica.

Si distinguono due differenti sottofascicoli:

- il sotto fascicolo denominato DATI ISTITUZIONALI che comprende tutti i documenti relativi a titoli e requisiti necessari per l'effettiva iscrizione all'albo e per l'esercizio della professione
- il sotto fascicolo denominato QUALIFICHE E ATTIVITA' che comprende tutti i documenti relativi all'attività professionale

Nel caso dei doppi iscritti i fascicoli devono essere duplicati con i dati necessari per la tenuta dei rispettivi Albi.

Nel caso in cui sia necessaria la gestione massiva di informazioni riferite a più iscritti (es. richiesta verifica autocertificazione del casellario giudiziario) viene generato un fascicolo unico annuale di attività da classificare nel titolo principale 3.0.

7.4 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, attività o al procedimento al quale afferiscono.

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

7.5 Organizzazione, gestione e strumenti dell'archivio unico corrente, di deposito e storico

Il sistema di protocollo informatico conserva nel suo archivio elettronico tutti i documenti originati e ricevuti ivi caricati dalla messa in esercizio dello stesso e pertanto funge da archivio corrente.

Il citato sistema informatico consente la gestione dell'archivio elettronico e ne garantisce l'accesso.

I documenti che costituiscono l'archivio di deposito e storico sono conservati presso l'Archivio generale che è parte integrante del Servizio archivistico.

7.5.1 Piano di conservazione

Il piano di conservazione è uno strumento finalizzato a individuare le disposizioni di massima e definire i criteri e le procedure attraverso i quali i documenti e i fascicoli, non rivestendo interesse storico ai fini della conservazione permanente e avendo esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della soprintendenza archivistica e bibliografica (**allegato n. 3 Massimario di conservazione e di scarto dei documenti**).

Le operazioni di selezione, necessarie a garantire la corretta gestione e la conservazione del complesso documentale dell'Ente, avvengono principalmente nella fase di deposito, in modo tale da sedimentare solo la documentazione ritenuta rilevante ai fini della conservazione a lungo termine.

La proposta di scarto formulata su apposito modulo, cioè "l'elenco di scarto" in cui sono indicate le tipologie documentarie, gli estremi cronologici, il volume e le motivazioni dell'eliminazione corredata dall'autorizzazione del Consiglio Direttivo, viene inviata alla soprintendenza archivistica e bibliografica nelle modalità concordate.

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

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

7.5.2 Strumenti per la gestione dell'archivio di deposito

Periodicamente e secondo un apposito piano di versamento (di norma una volta all'anno), ogni singolo RPA (Responsabile del procedimento amministrativo) conferisce al RSP i fascicoli relativi ad affari e procedimenti amministrativi conclusi o comunque non più necessari a una trattazione corrente.

7.5.3 Obbligo di conservazione, ordinamento e inventariazione dell'archivio storico

I documenti che costituiscono l'archivio storico (quelli relativi ad affari esauriti da oltre quarant'anni, giudicati degni di conservazione permanente) sono conservati presso l'Ente e affidati alla gestione del Servizio archivistico. Essi devono essere ordinati e inventariati.

Anche se dichiarato bene culturale a tutti gli effetti dall'art. 10, comma 2, lettera b), del D.lgs 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, l'organizzazione tecnico-scientifica dell'archivio storico, data la specificità del materiale, non può essere demandata alle strutture che si occupano di altri beni culturali (biblioteche, musei, etc.).

La consultazione dell'archivio storico è gestita direttamente dal Servizio archivistico.

8 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

8.1 Modalità di approvazione e aggiornamento del Manuale

Il presente Manuale è approvato dal Consiglio direttivo con propria deliberazione ed è aggiornato, su proposta del RSP o del gruppo di progetto incaricato della revisione, con le medesime modalità.

Gli aggiornamenti potranno rendersi necessari a seguito di:

- adeguamenti normativi che rendano superate le prassi definite nel Manuale
- 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

Gli allegati al presente Manuale, che contengono indicazioni di dettaglio sulle procedure operative e sulle modalità di funzionamento dei sistemi gestionali, sono modificati con apposita deliberazione del Consiglio.

Entra in vigore alla data di esecutività della deliberazione che lo approva. Con l'entrata in vigore del presente Manuale viene abrogato l'eventuale Manuale di gestione già approvato con Deliberazione precedente.

8.2 Pubblicità del presente Manuale

In ottemperanza a quanto disposto dal comma 3 dell'art. 5 del DPCM 3 dicembre 2013, il Manuale di gestione è reso pubblico dall'Ordine mediante la pubblicazione sul proprio sito istituzionale.

Al fine di assicurarne adeguata conoscenza al personale dell'Ente il Manuale di gestione è inserito nei percorsi di formazione del personale in tema di gestione documentale.

9 ALLEGATI

9.1 Allegato 1 Modello del Registro di emergenza

9.2 Allegato 2 Piano di classificazione

9.3 Allegato 3 Documenti esclusi dalla protocollazione

9.4 Allegato 4 Massimario di conservazione e di scarto dei documenti