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

Lecco, 14 Maggio 2024 2024

AZIONE	DATA	NOMINATIVO	FUNZIONE
Redazione		Sig. Massimo Iacobuzio	Funzionario Capo RTD
Verifica		Dr. Massimo Bergamini	Segretario
Approvazione		Consiglio Direttivo	Organo di controllo

IL PRESENTE MANUALE È STATO APPROVATO E ADOTTATO CON DELIBERAZIONE N. 44 DEL 14 Maggio 2024.

Sommario

Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi 1
1 PRINCIPI GENERALI 6
1.1 Premessa 6
1.1.1 Peculiarità dell'Ordine professionale 7
1.2 Ambito di applicazione e struttura del Manuale di Gestione 7
1.2.1 Ambito di applicazione 7
1.2.2 Struttura del manuale 8
1.3 Definizioni e norme di riferimento 9
1.4 Aree organizzative omogenee (AOO) -Unità Organizzative Responsabili (UOR) e modelli organizzativi 11
1.5 Servizio archivistico per la gestione informatica del protocollo informatico, dei flussi documentali e degli archivi 11
1.5.1 Il delegato per la tenuta del protocollo informatico 13
1.5.2 Il delegato per la conservazione 14
1.5.3 Firma digitale (vedi anche cap. 3.5) 14
1.5.4 Firma elettronica (vedi anche cap. 3.5) 14
1.5.5 Firma remota automatica (vedi anche cap. 3.5) 15
1.6 Sistema di protocollo informatico unico e strumenti per il suo funzionamento 15
1.7 Politiche di gestione e conservazione documentale 15
2 PIANO DI SICUREZZA 17
2.1 Formazione dei documenti - aspetti di sicurezza 17
2.2 Gestione dei documenti informatici - aspetti di sicurezza 17
2.2.1 Componente organizzativa della sicurezza 17
2.2.2 Componente fisica e infrastrutturale della sicurezza 18
2.2.3 Componente logica della sicurezza 19
2.2.4 Gestione delle registrazioni di protocollo e di sicurezza 21
2.2.5 Criteri di utilizzo degli strumenti tecnologici 21
2.3 Trasmissione e interscambio dei documenti informatici - aspetti di sicurezza 23
2.4 Accesso ai documenti informatici 23
2.5 Politiche di sicurezza adottate dall'Ente 23

2.6 Servizio archivistico (doc. analogici) 24
3 MODALITÀ DI FORMAZIONE DEI DOCUMENTI 25
3.1 I documenti dell'Ente 25
3.2 Formazione dei documenti 25
3.2.1 Elementi informativi essenziali dei documenti prodotti 25
3.2.2 Formazione dei documenti - aspetti operativi generali 26
3.3 Formazione del documento analogico 26
3.4 Formazione del documento informatico 26
3.5 La firma elettronica (avanzata, qualificata, digitale, automatica) e la validazione temporale 28
3.6 La Firma Elettronica Remota Automatica Massiva (FERAM) 28
3.7 La validazione temporale 29
3.8 Tipologie di formato del documento informatico 29
3.9 Documenti contenenti collegamenti ipertestuali. 30
3.10 Documenti contenenti video o audio o social 30
4 FLUSSI DI LAVORAZIONE DEI DOCUMENTI 30
4.1 Documenti in entrata 30
4.1.1 Ricevuti o prodotti su supporto analogico 31
4.1.2 Ricevuti o prodotti su supporto informatico 31
4.2 Documenti in uscita 31
4.2.1 Inviati su supporto analogico 31
4.2.2 Inviati su supporto informatico 31
4.3 Descrizione del flusso di lavorazione dei documenti 32
4.4 Flusso in entrata 32
4.5 Flusso in uscita 33
5 MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO 33
5.1 Registrazione dei documenti 33
5.1.1 Modalità di registrazione di protocollo 34
5.1.2 Documento analogico inviato elettronicamente 35
5.1.3 Documento digitale inviato elettronicamente 35
5.2 Registri di protocollo periodici 35

5.2.1 Invio in conservazione del registro giornaliero di protocollo 35
5.3 La segnatura di protocollo 36
5.4 Procedure specifiche nella registrazione di protocollo 37
5.4.1 Protocollazione di documenti riservati 37
5.4.2 Documenti esclusi dalla registrazione di protocollo 38
5.4.3 Modifica delle registrazioni di protocollo 38
5.4.4 Annullamento delle registrazioni di protocollo 38
5.5 Casi particolari di registrazioni di protocollo 39
5.5.1 Lettere anonime 39
5.5.2 Documenti privi di firma 39
5.5.3 Corrispondenza personale o riservata 39
5.5.4 Integrazioni documentarie 39
5.5.5 Documenti pervenuti per errore all'Ente 39
5.5.6 Trattamento dei documenti con oggetto o smistamento plurimo 40
5.5.7 Documenti in partenza con più destinatari 40
5.5.8 Flussi documentali informatici 41
5.6 Regole di smistamento e di assegnazione 43
6 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA 44
7 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE 45
7.1 Protezione e conservazione degli archivi pubblici 45
7.2 Titolario o piano di classificazione 47
7.3 Formazione del fascicolo 48
7.3.1 Il fascicolo 48
7.3.2 Famiglie e tipologie di fascicolo 48
7.3.3 Repertorio dei fascicoli 49
7.3.4 Il fascicolo personale dell'iscritto/S.T.P. 50
7.3.5 Dossier 50
7.4 Repertori e fascicoli annuali 51
7.5 Tipologie di registri 51
7.6 Organizzazione, gestione e strumenti dell'archivio unico corrente, di deposito e storico .. 52
7.7 Piano di conservazione 52
7.7.1 Strumenti per la gestione dell'archivio di deposito 52

7.7.2 Obbligo di conservazione, ordinamento e inventariazione dell'archivio storico 52
8 PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA. 53
8.1 Premessa 53
8.2 Procedure di accesso ai documenti e di tutela della riservatezza 53
9 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI 54
9.1 Modalità di approvazione e aggiornamento del Manuale 54
9.2 Pubblicità del presente Manuale 54
Elenco allegati 55

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 presente documento 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 Manuale è redatto dal personale afferente all'Ufficio Protocollo. E' rivolto ai dirigenti, ai funzionari, agli operatori di protocollo ed agli istruttori delle pratiche quale strumento di lavoro e di riferimento per la gestione dei documenti, degli affari e dei procedimenti amministrativi, in tutte le fasi di vita della documentazione.

Il presente Manuale è frutto di un lavoro pluriennale congiunto di un Gruppo di Lavoro di Funzionari appartenenti a diversi Ordini Provinciali dei Medici Chirurghi e degli Odontoiatri, col supporto della Prof.ssa Maria Guercio in qualità di Presidente del Comitato tecnico-scientifico dell'Associazione Nazionale Archivistica Italiana (ANAI) ed è un documento work in progress, al fine di migliorarlo e adeguarlo alle nuove indicazioni operative.

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'ente.

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/collaboratori e ai soggetti esterni che si relazionano con l'Ente.

Il protocollo informatico e il sistema di gestione documentale costituiscono assieme 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 privilegiata[1] 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).

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 Provinciale dei Medici Chirurghi e degli Odontoiatri di Lecco, di seguito "Ente", è un ente pubblico non economico sussidiario dello Stato dotato di una struttura organizzativa semplice e poco ramificata tanto che molto spesso i documenti vengono presi in carico spesso dagli stessi addetti che effettuano le registrazioni di protocollo.

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

Coordina gli uffici un Funzionario Amministrativo con incarico di Responsabile per la transizione al digitale che coadiuva l'attività di 2 assistenti amministrativi che svolgono le varie attività dell'ufficio in maniera sinergica e connessa. 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).

L'Ente, con deliberazione consiliare n. 27/2017, ha formalizzato un'unica Area Organizzativa Omogenea per la gestione dei documenti e dei flussi documentali dell'Amministrazione. Esiste un'altra AOO creata di default dal portale IPA per l'Ufficio per la transizione digitale.

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:

[1]Il 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.

- Formazione
- Gestione
- 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'Ente.

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'Ente 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'Ente 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 sia in un'ottica di trasparenza amministrativa che di transizione al digitale.

1.2.2 Struttura del manuale

L'attuale Manuale di gestione è organizzato in 9 capitoli ed include n. 11 allegati:

1. Glossario dei termini e degli acronimi
2. Individuazione Area Organizzativa Omogenea
3. Istituzione servizio Archivistico e Nomina del Responsabile del Servizio
4. Titolario di Classificazione
5. Piano fascicolazione
6. Oggettario
7. Organigramma
8. Organigramma privacy

9. Documenti esclusi dalla registrazione di protocollo
10. Modello registro di emergenza
11. Formati di file e riversamento

1.3 Definizioni e norme di riferimento

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

- RD 1163/1911, Regolamento per gli archivi di Stato;
- DPR 1409/1963, Norme relative all'ordinamento ed al personale degli archivi di Stato;
- Legge 241/1990, Nuove norme sul procedimento amministrativo;
- DPR 445/2000, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- DPR 37/2001, Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato;
- D.lgs 196/2003 recante il Codice in materia di protezione dei dati personali;
- D.lgs 42/2004, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
- Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106, Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici;
- D.lgs 82/2005 e ss.mm.ii., Codice dell'amministrazione digitale;
- D.lgs 33/2013, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- DPCM 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- DPCM 21 marzo 2013, Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- Reg. UE 910/2014, 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;
- Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013;

- Reg. UE 679/2016 (GDPR), 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;
- Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- Circolare n. 2 del 9 aprile 2018, recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
- Circolare n. 3 del 9 aprile 2018, recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
- Reg. UE 2018/1807, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;
- DPCM 19 giugno 2019, n. 76, Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.

Linee guida AGID richiamate

- Linee guida del 15 aprile 2019 dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi;
- Linee guida del 6 giugno 2019 contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.
- Linee guida del 09/01/2020 sull'Accessibilità degli strumenti informatici.
- Linee guida del Maggio 2021 sulla formazione, gestione e conservazione dei documenti informatici.

Ai fini del presente manuale si intende per:

- "**Ente**", l'Ordine dei Medici Chirurghi e degli Odontoiatri della provincia di Lecco
- "**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
- **DPO/RPD** – Data Protection Officer /Responsabile Protezione Dati
- **MdG** - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi (il presente documento)

- **RPA** - Responsabile del Procedimento Amministrativo – in riferimento alla peculiarità dell'Ente si evidenzia come da Delibera n. 32 del 24/02/2021 che l'incarico di Dirigente dell'Ordine dei Medici Chirurghi e degli Odontoiatri della provincia di Lecco è assegnato con attribuzione delle funzioni di responsabile dei procedimenti individuati dalla deliberazione consiliare n. 27 del 24/02/2021; le funzioni di responsabile e di incaricato dei procedimenti amministrativi da attribuire al personale dipendente sono da considerarsi relative alla fase istruttoria e preparatoria dei procedimenti stessi, preordinata all'adozione dei provvedimenti finali, la cui emanazione, quindi, resta di esclusiva competenza e responsabilità degli Organi elettivi istituzionali dell'Ente salvo per il Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi e Il Rup nell'ambito dell'espletamento delle gare.
- **RSP** - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi
- **RTD** – Responsabile Transizione al Digitale
- **SGD** – Servizio gestione documentale
- **UOR** - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato

Per altre definizioni si faccia riferimento all'*Allegato 1 - Glossario dei termini e degli acronimi*

1.4 Aree organizzative omogenee (AOO) -Unità Organizzative Responsabili (UOR) e modelli organizzativi

Ai fini della gestione unica e coordinata dei documenti l'Ente è costituito da un'unica Area organizzativa omogenea (AOO unica), formalmente definita con Deliberazione n. 27/2017. ***(Allegato 2 - Individuazione Area organizzativa omogenea (AOO unica)***.

Sigla dell'AOO =SEGRETERIA

All'interno della AOO viene utilizzato un unico sistema di protocollazione che consente l'autonomia di ogni UOR per la registrazione della corrispondenza in entrata, in uscita ed interna.

Le Unità organizzative responsabili (UOR) sono individuate dall'organigramma dell'Ente (vedi ***Allegato n. 6 - Organigramma***).

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 n. 28/2017, l'ufficio denominato "Servizio archivistico dell'Ordine Provinciale dei Medici chirurghi e degli odontoiatri di Lecco", 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 comprende:

- **la gestione e il coordinamento del sistema di protocollo informatico** - registrazione, classificazione, assegnazione dei documenti, costituzione e repertoriazione dei fascicoli, autorizzazione per l'accesso alle funzioni della procedura, gestione del registro di emergenza, annullamento di registrazioni
- **la gestione e il coordinamento degli archivi:**
  - **corrente:** riguarda i documenti necessari alle attività correnti;
  - **di deposito:** riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
  - **storico:** riguarda i documenti storici selezionati per la conservazione permanente.

Con la medesima deliberazione si individua il 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.

La gestione dell'Ufficio Protocollo è attualmente affidata con deliberazione n. 28/2017 al Sig. Massimo Iacobuzio, Funzionario Capo che ricopre fra l'altro anche il ruolo di Responsabile per la Transizione al Digitale (RTD).

(Allegato 3 - Istituzione del Servizio archivistico dell'Ordine dei medici chirurghi e degli odontoiatri e individuazione del responsabile).

L'attuale Responsabile del Servizio è stato individuato con Delibera n. 28/2017; in assenza del responsabile le decisioni vengono assunte da un suo delegato o alternativamente dal Segretario dell'Ente 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. 2/2017 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'ente 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 tenuta del protocollo informatico

Il Responsabile si avvale di delegati per la tenuta del protocollo informatico i cui compiti sono:

- garantire il rispetto delle disposizioni normative e delle procedure durante le operazioni di registrazione e di segnatura di protocollo
- autorizzare le operazioni di annullamento della registrazione di protocollo
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo
- conservare le copie di salvataggio del registro giornaliero di protocollo e del registro di emergenza in sistemi diversi da quello in cui opera il sistema di gestione del protocollo
- aprire e chiudere il registro di protocollazione di emergenza

I delegati individuati attualmente, stante la ridotta struttura organica dell'Ente, sono le 2 Assistenti Amministrative in servizio.

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 archivistico e protocollo informatico.

1.5.2 Il delegato per la conservazione

Il servizio di conservazione digitale dei documenti è attualmente affidato per quanto riguarda la conservazione del registro di protocollo a 2C Solution SRL, società appartenente al gruppo Namirial SPA, conservatore certificato AGID.

È intenzione dell'Ente procedere con la sottoscrizione di un accordo tra pubbliche amministrazioni, ai sensi dell'art. 15 della Legge 241/1990, correlato all'art. 7 comma 4 del D.Lgs. 36/2023 per la conservazione dei documenti informatici dell'Ente produttore e al trasferimento dei documenti, ai sensi dell'art. 21 lettera e) del D. Lgs. n. 42/2004 (Codice dei Beni Culturali e del Paesaggio) col ***Polo archivistico dell'Emilia-Romagna (ParER)****, previo il prescritto nulla osta espresso dalla Soprintendenza Archivistica della Lombardia. Si evidenzia come dal 2022* ***Regione Emilia-Romagna sia un conservatore iscritto nel Marketplace dei servizi di conservazione gestito da AgID.***

Il delegato interno per la conservazione svolge i seguenti compiti:

- Affianca il RUP nella verifica dei requisiti di legge nella scelta del fornitore di conservazione
- verifica il manuale della conservazione redatto dal fornitore da integrare con il manuale di conservazione dell'organizzazione
- 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.

1.5.3 Firma digitale (vedi anche cap. 3.5)

L'Ente 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.

I dipendenti dell'Ente sono tutti attualmente dotati per motivi di servizio di firma digitale.

Nella gestione delle firme digitali si tiene conto che il loro rinnovo (di solito 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.

1.5.4 Firma elettronica (vedi anche cap. 3.5)

In conformità alla normativa vigente in materia di amministrazione digitale, le credenziali di accesso costituiscono la "firma elettronica" dell'utente che utilizza il sistema e qualsiasi azione e attività svolta nel sistema documentale e del protocollo, costituisce atto valido ai fini amministrativi. Si sottolinea l'importanza della segretezza delle credenziali e del cambio password periodico, in base alle politiche

di sicurezza dell'Ente (si raccomanda il cambio password ogni 3 mesi e comunque da indicazioni dell'Amministratore di sistema e DPO).

1.5.5 Firma remota automatica (vedi anche cap. 3.5)

L'ente individua i soggetti che devono essere dotati di firma automatica per l'espletamento delle procedure di firma massiva connesse al sistema di riversamento del registro giornaliero in conservazione digitale, per procedura di attestazione di conformità o per procedure di firma singola o multipla di documenti generati automaticamente.

Attualmente sono dati di firma remota automatica il Presidente, il Vicepresidente, il Segretario e il Funzionario Capo

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

L'Ente, avendo individuato un'unica AOO, dispone di un unico sistema di protocollo informatico e gestione documentale denominato IrideDoc (di seguito software di protocollo) prodotto da TecSis srl.

Il protocollo informatico unico è lo strumento attraverso il quale l'Ente garantisce l'effettiva ricezione e trasmissione dei documenti. Con la messa a regime di tale sistema è cessata di fatto la necessità di mantenere altri protocolli interni (protocolli di settore, servizio, ufficio, etc., protocolli multipli, etc.) o altri sistemi di registrazione diversi dal protocollo unico, che sono stati eliminati.

Al protocollo informatico unico sono di supporto i seguenti strumenti di gestione se presenti:

- Titolario di classificazione (***Allegato 4 - Titolario di classificazione***)
- Oggettario (***Allegato 5 – Oggettario documento in continua evoluzione ed ampliamento***)
- Organigramma (***Allegato 6 - Organigramma***)
- Repertorio dei fascicoli (da produrre a fine anno)
- Piano di fascicolazione **(*Allegato n. 5 – Piano di fascicolazione*)**
- Piano di conservazione e scarto (*in fase di definizione*)
- Elenco dei formati di file e riversamento **(Allegato n. 11 – Formato di file e riversamento)**

1.7 Politiche di gestione e conservazione documentale

L'Ente ha adottato e programmerà nel futuro 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) anche in accordo con le indicazioni del RTD, dell'Amministratore di Sistema e del DPO.

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 qualificati presso AgID, secondo i criteri e le modalità descritte nella Linee guida Agid maggio 2021. Il Software di gestione del protocollo e dei documenti consente il riversamento con modalità semplificate.

Il tavolo tecnico sta portando avanti un lavoro di ricerca per la conservazione con Il Polo archivistico dell’Emilia-Romagna (ParER), che è stato riconosciuto come conservatore accreditato dall’Agenzia per l’Italia Digitale (AgID) e ha individuato nell’Ordine dei Medici Chirurghi e degli Odontoiatri di Venezia l’ente capofila del progetto di ricerca.

I termini di conservazione minimi previsti devono sempre essere verificati alla luce di nuove possibili normative di settore che obbligano ad un periodo di conservazione maggiore rispetto a quello indicato alla data di emanazione del Massimario (ad esempio per i documenti contabili e fiscali).

I termini minimi di conservazione vanno intesi dalla data di chiusura del fascicolo e in via generale salvo contenzioso in essere si rimanda inoltre alla responsabilità e al margine di discrezionalità del singolo archivista come di ogni Ente nel decidere di conservare tutta quella documentazione che si ritiene utile ai fini della comprensione sul piano storico dell’attività dell’Ente.

La documentazione per la quale non è prescritto il termine di conservazione si intende da poter avviare allo scarto dopo un periodo di anni cinque.

2 PIANO DI SICUREZZA

Il presente capitolo, ai sensi **delle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017 e ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)**, 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.

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

Tale componente consiste nella definizione di una struttura operativa dedicata alla gestione della sicurezza nell'ambito delle attività svolte per il protocollo e gestione documentale.

In tale contesto 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.

Conseguentemente vengono adottate le seguenti misure di sicurezza, la cui competenza è posta a carico di figure che sono appositamente individuate come prevista dalla normativa vigente.

Le nomine nell'ambito della sicurezza sono indicate nell'allegato n. 8 Organigramma Privacy

2.2.2 Componente fisica e infrastrutturale della sicurezza

La sede fa parte del complesso condominiale sito nella città di Lecco denominato “condominio FAPIS”; L’accesso principale alla sede è Corso martiri della Liberazione, 86, con ingresso dal livello stradale pedonabile.

Gli Uffici sono distribuiti su un unico piano.

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 ovvero dipendenti /collaboratori/organi istituzionali per motivi di servizio che deve seguire le indicazioni previste dal Codice di comportamento;
- i meccanismi di controllo dell'accesso sono più selettivi all'aumentare della sensibilità dei dati custoditi e quindi del livello di protezione del locale necessario
- 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 possono avvenire solo a seguito di motivata richiesta. Essi non possono entrare e trattenersi nelle aree protette se non accompagnati da personale dell'Ente autorizzato a quel livello di protezione;
- ogni persona che accede alle risorse della sede in locali protetti è identificata.

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'Ente/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 per l’accesso alla sede
- armadi con chiusura a chiave
- impianti elettrici verificati
- luci di emergenza
- sistemi di condizionamento per il raffreddamento delle apparecchiature
- continuità elettrica del server garantita da apposito UPS
- controllo periodico di efficienza degli UPS
- estintori e porte antipanico
- controllo dell’attuazione del piano di verifica periodica sull’efficacia dei sistemi di sorveglianza e degli estintori
- sistema di allarme antiintrusione con videosorveglianza collegato a servizio di pronto intervento garantito da azienda di vigilanza contrattualizzata
- essendo la Sede Operativa lontana da insediamenti industriali e posta all'interno di un edificio adibito a condominio , 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 (dove necessario)
- monitoraggio sessioni di lavoro
- disponibilità del software e dell'hardware
  - ridondanza dei sistemi di salvataggio
  - replica del salvataggio in Cloud (in area geografica diversa da quella dell'Ente ma comunque in Paese della UE)

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

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 condiviso nel 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 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 IrideDoc 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 ***Database Management System*** (DBMS) è il software che permette la creazione, manipolazione e interrogazione di un DB. In IrideDoc il DB gestisce anche il ***repository dei file***, cioè l’area di memoria persistente che contiene i documenti gestiti dal sistema.

La scrittura e 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” solamente se dotato di specifiche credenziali e autorizzazioni al sistema IrideDoc.

L'interfaccia viene generata in funzione delle autorizzazioni in possesso dell'utente connesso e quindi con permessi diversificati.

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 anche secondo le indicazioni del RTD e DPO. Sono gestiti livelli di autorizzazione differenziati per quegli utenti che devo accedere al sistema per la sola consultazione (visualizzazione). Anche in questo caso disponibile in modo indifferenziato a tutti i documenti.

E’ sempre possibile prevedere la protocollazione riservata secondo quanto previsto dal Manuale al paragrafo 5.4.1.

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.

Nel caso vi fosse una evoluzione nel sistema organizzativo e fossero identificati utenti “generici” dell’Ente, non sarà loro consentito:

- interrogare direttamente il DBMS
- interagire direttamente con il repository dei file

- accedere direttamente ai server fisici e virtualizzati

Le precedenti operazioni sono possibili:

- per il personale dell'Ente in possesso delle adeguate credenziali amministrative
- per i tecnici informatici autorizzati, per le sole attività sistemistiche di amministrazione, aggiornamento e manutenzione delle componenti di sistema
- per i collaboratori esterni titolari di specifici incarichi professionali conferiti con atto amministrativo.

Nessun sistema, componente, servizio ed interfaccia inerente al sistema IrideDoc 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 IrideDoc 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 (Intrusion Detection System(IDS), sensori di rete e firewall)

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)
- copie di backup realizzate su dischi RAID in mirroring e RAID 5
- consegna di una copia di sicurezza dei backup in un locale diverso come previsto dalla normativa
- scrittura asincrona dei file su storage ospitato in altra sede o in cloud.

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 definite sia all'interno del Regolamento per l'utilizzo degli strumenti informatici sia nel registro dei trattamenti dell'Ente.

Gli utenti interni autorizzati ad utilizzare il software di protocollo, operano nel rispetto del Codice di Comportamento e del "Regolamento per l'utilizzo degli strumenti informatici e telematici dell'Ente", che in riferimento alla sicurezza nell'utilizzo delle risorse tecnologiche, 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. É 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
- la tutela dei dati archiviati su personal computer che gestiscono localmente documenti e/o dati è demandata all'utente finale, il quale dovrà effettuare con frequenza opportuna i salvataggi su supporti dedicati e idonei, nonché la conservazione degli stessi in luoghi adatti
- 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 IrideDoc 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
- la password può essere affiancata da rilevatore di impronte digitali presenti in alcune tipologie di tastiera dei PC che garantisca la sicurezza dell'Utente
- le password dovranno avere le caratteristiche definite dal Regolamento per l'utilizzo degli strumenti informatici:

è necessario che ciascun utente scelga una password "robusta" e che tale password sia mantenuta rigorosamente segreta. A questo scopo è necessario scegliere la propria password seguendo i seguenti requisiti minimi, comuni a tutti i sistemi:

- non è possibile impostare password di lunghezza inferiore a 12 caratteri;
- la password deve includere, di regola, almeno tre delle seguenti caratteristiche: lettera maiuscola, lettera minuscola, cifre, caratteri speciali da selezionare fra quelli messi a disposizione dal sistema di autenticazione;
- la password non deve far riferimento ad informazioni personali o al servizio al quale si accede, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa.

2.3 Trasmissione e interscambio dei documenti informatici - aspetti di sicurezza

L'Ente predilige l'utilizzo di tecnologie di trasmissione sicure.

In riferimento al cap.3, le modalità previste per la trasmissione hanno il seguente livello di sicurezza:

Tipologia di trasmissione	Caratteristiche	Livello di sicurezza	Attivo?
Posta elettronica Certificata	• Identità sicura e accertata del titolare della casella /mittente • Transito del messaggio attraverso il protocollo S/STTP Mime che garantisce la piena riservatezza • Sicurezza dell'accettazione e consegna del messaggio attraverso l'utilizzo delle ricevute • Tracciamento delle attività nel file di Log a carico del gestore del servizio e conservazione dei registri per 30 mesi	Alto	si
Canali Web - Istanze online	• Accesso ai servizi previa autenticazione sicura del mittente attraverso SPID/CIE • Utilizzo del protocollo HTTPS che garantisce la piena riservatezza	Alto	si
Interoperabilità	• Meccanismo di trasmissione attraverso la Posta elettronica certificata con funzionalità interoperabili	Alto	no
Posta elettronica ordinaria/standard	• Identità del titolare della casella non accertata da un ISP (Internet server provider) accreditato. • Transito del messaggio attraverso un protocollo SMTP che non garantisce la riservatezza della trasmissione	Basso	si

2.4 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.

2.5 Politiche di sicurezza adottate dall'Ente

Le politiche di sicurezza vengono riportate nel Codice di Comportamento, nel Regolamento per l'utilizzo degli strumenti informatici e nella procedura in caso di Data Breach e stabiliscono sia le

misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.

Le politiche illustrate sono corredate dalle procedure sanzionatorie che l'Ente intende adottare in caso di riscontrata violazione delle prescrizioni dettate in materia di sicurezza da parte di tutti gli utenti che, a qualunque titolo, interagiscono con il servizio di protocollo, gestione documentale ed archivistica.

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/servizio online predisposto dal Garante al link https://servizi.gpdp.it/databreach/s/ .

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 minime di sicurezza richieste dall'Agenzia per l'Italia digitale o a seguito dei risultati delle attività di audit.

2.6 Servizio archivistico (doc. analogici)

La sede dell'archivio dell'Ente è individuata nei locali e negli armadi ubicati negli uffici della sede istituzionale dell'Ente medesimo.

La scelta è stata effettuata alla luce dei vincoli logistici imposti dall'edificio e della valutazione dei fattori di rischio che incombono sui documenti. L'obiettivo è stato quello di prevenire o contenere eventuali danni conseguenti a situazioni di emergenza.

Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità, nel tempo, di tutti i documenti trasmessi o ricevuti, adottando i formati previsti dalle regole tecniche vigenti.

Per un maggiore dettaglio si può fare riferimento anche a quanto scritto al 2.2.2 .

Alla luce della quasi totale digitalizzazione dei procedimenti di iscrizione, cancellazione, trasferimento nonché della tenuta ed aggiornamento degli Albi professionali, nonché all'adozione dell'Ordinativo Informatico all'interno dello stabile la documentazione cartacea/riservata presente è limitata alla seguente:

Presso l'Ufficio si trova tutta la documentazione che, a diverso titolo, è stata acquisita in formato nativo cartaceo. Le pratiche vengono custodite in armadi chiusi a chiave a cui solo il personale autorizzato ha accesso; tutti gli uffici dove si trovano suddette pratiche vengono chiusi a chiave alla fine della giornata di lavoro, prima di chiudere ed impostare il sistema di allarme. La quasi totalità del cartaceo esistente è stato comunque digitalizzato ed acquisito al sistema di protocollazione grazie anche al contributo di un archivista che ha operato nel corso del 2022-23 con un contratto interinale.

3 MODALITÀ DI FORMAZIONE DEI DOCUMENTI

3.1 I documenti dell'Ente

I documenti dell'Ente (d'ora in poi chiamati semplicemente documenti) sono quelli prodotti (spediti e ricevuti), in uno dei modi previsti dal CAD in vigore, dagli organi e uffici dell'Ente medesimo nello svolgimento dell'attività istituzionale.

In ottemperanza a quanto indicato dal vigente Codice dell'amministrazione digitale, che prevede l'uso delle tecnologie dell'informazione e della comunicazione per organizzare la propria attività amministrativa, l'Ente predilige la formazione, gestione, e trasmissione dei documenti in formato nativo digitale.

Per agevolare il processo di formazione dei documenti informatici e favorire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'Ente rende disponibili per via telematica moduli e formulari, alcuni anche compilabili attraverso servizi webservice.

Ciò premesso, il documento amministrativo va distinto in:

- Documento analogico
- Documento informatico

3.2 Formazione dei documenti

I documenti, indipendentemente dalla forma nella quale sono redatti, devono sempre riportare gli elementi essenziali, elencati di seguito.

Dev'essere curata, per quanto possibile, la standardizzazione della forma e dei contenuti dei documenti.

3.2.1 Elementi informativi essenziali dei documenti prodotti

I documenti in uscita devono riportare le seguenti informazioni, organizzate per blocchi logici:

1. Individuazione dell'autore del documento
   - Logo dell'Ente
   - Indirizzo completo: via/piazza, numero civico, CAP, città
   - Codice fiscale
   - Numero di telefono
   - Indirizzo istituzionale di posta elettronica
   - Indirizzo istituzionale di posta elettronica certificata
2. Individuazione e descrizione del documento:
   - Data ricavata dalla firma digitale
   - Numero e descrizione degli allegati se presenti
   - Numero e data del documento cui si risponde se necessario

- Oggetto del documento

3. Individuazione del destinatario del documento:

   Cognome e nome (per le persone) Denominazione (per gli enti e le imprese)
   A seconda dei casi:
   - Indirizzo completo: via/piazza, numero civico, CAP, città
   - Indirizzo informatico (Pec…)

4. Individuazione del Responsabile del Procedimento Amministrativo[2] (RPA) ove necessario:

   Cognome, nome e recapito digitale

5. Individuazione del Responsabile dell'istruttoria ove necessario:

   - Cognome, nome
   - Eventuali dati di contatto

3.2.2 Formazione dei documenti - aspetti operativi generali

I documenti e i fascicoli dell'Ente sono prodotti con adeguati sistemi informatici e solo in casi eccezionali in modalità analogica.

Ogni documento:

- tratta un unico argomento indicato in maniera sintetica ma esaustiva a cura dell'autore nello spazio riservato all'oggetto
- è riferito ad un solo protocollo
- è riconducibile almeno ad un fascicolo o ad un'aggregazione documentaria

3.3 Formazione del documento analogico

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

Si definisce "originale" il documento nella sua redazione definitiva corredato degli aspetti diplomatistici sopra descritti.

Un documento analogico può essere convertito in documento informatico corredato da firma digitale ed eventuale attestazione di conformità ai sensi dell'art. 22 del D.lgs. 82/2005 e del capitolo 2.2 delle Linee Guida AGID 2021.

3.4 Formazione del documento informatico

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

[2] In conformità alla legge 241/90

Gli atti formati dall'Ente 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 è formato mediante una delle seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 delle linee guida AGID;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico viene identificato in modo univoco e persistente mediante registrazione di protocollo univocamente associata al documento con contestuale generazione dell'impronta crittografica basata su funzioni di hash che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle linee guida nella tabella 1 del paragrafo 2.2 regole di processamento.

L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti che prevede la generazione dell'impronta crittografata come descritto nel paragrafo precedente.

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

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di protocollo e gestione documentale che adottino idonee politiche di sicurezza

Al documento informatico immodificabile vengono associati i metadati che sono stati generati durante l'inserimento nel sistema di gestione documentale. L'insieme minimo dei metadati è costituito da:

A. numero di protocollo
B. data di protocollo
C. oggetto
D. mittente – destinatari
E. data e protocollo del documento ricevuto, se disponibili
F. impronta del documento informatico
G. Numero degli allegati
H. Classe documentale

3.5 La firma elettronica (avanzata, qualificata, digitale, automatica) e la validazione temporale

La sottoscrizione dei documenti informatici è ottenuta con processi di firma elettronica conformi alle disposizioni dettate dalla normativa vigente.

Per l'apposizione delle firme digitale e automatiche, l'Ente si avvale dei servizi di autorità di certificazione iscritte nell'elenco pubblico dei certificatori qualificati tenuto dall'Agenzia per la Cybersicurezza Nazionale (ACN).

I documenti informatici prodotti dall'Ente, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale eseguita al fine di garantirne l'immodificabilità e la corretta archiviazione, sono convertiti nei formati standard previsti dalla norma indicati nell'allegato11 Formati di file e di riversamento .

La firma digitale viene utilizzata dall'Ente come forma di sottoscrizione per garantire i requisiti di integrità, riservatezza e non ripudiabilità nei confronti di entità esterne e viene apposta prima della protocollazione del documento.

La verifica della firma digitale dei documenti prodotti o ricevuti avviene:

- attraverso verifica manuale dell'operatore o specifiche funzioni integrate nel software di protocollo/gestione documentale nel rispetto della normativa vigente

Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna l'Ente, nella propria autonomia organizzativa, adotta forme diverse dalla firma digitale previste dal DPCM 22 febbraio 2013.

3.6 La Firma Elettronica Remota Automatica Massiva (FERAM)

Qualora fosse richiesta la firma dei documenti da conferire in conservazione o per la firma di documenti generati automaticamente, questa viene apposta in forma automatica dal software di gestione documentale a mezzo **Firma elettronica remota automatica massiva.**

Si tratta di una particolare tipologia di firma, che rientra nella qualifica di "firma forte"[3], utilizzata in tutti i casi nei quali vi sia il trattamento automatico di grandi quantità di documenti, da ottenere quindi automaticamente e senza presidio.

Al fine di garantire la sicurezza del sistema, il software di protocollo adotta il seguente schema:

- Il RSP può delegare altro utente del protocollo per firmare a suo nome il registro giornaliero di protocollo
- solo l'utente abilitato può inserire le credenziali di firma all'interno della sua area amministrativa.
- le credenziali di cui al precedente punto sono criptate al momento dell'inserimento.

IrideDoc consente la firma remota automatica anche su un singolo documento.

[3] Fonte documenti Namirial

3.7 La validazione temporale

Per tutte le casistiche per cui la normativa prevede l'apposizione di un riferimento o validazione temporale, l'Ente adotta almeno una delle seguenti modalità di marcatura:

- registrazione di protocollo
- posta elettronica certificata (PEC)
- eventuale sistema di marcatura temporale, nei casi in cui non sia possibile utilizzare uno di quelli precedenti

3.8 Tipologie di formato del documento informatico

L'Ente, in considerazione di quanto previsto dalle linee guida Agid del maggio 2021 in materia di conservazione (e successive modificazioni ed integrazioni), al fine di garantire le caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo e diffusione, tende verso l'applicazione delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici emanata da AGID (allegato 2 – Formati di file e riversamento).

L'Ente gestisce esclusivamente formati di file indicati nell'allegato 11 Formati di file e riversamento dell'Ente.

I file compressi o che contengono altri formati devono contenere esclusivamente file con formato incluso nell'allegato 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 all'elenco presente nell'allegato sono definite in considerazione di specifiche previsioni normative o tecniche.

Nel caso pervengano documenti su formati diversi da quelli elencati:

- L'Ente avrà cura di avvisare il soggetto produttore in modo da permettere un nuovo invio con formato tra quelli previsti

oppure

- Qualora il soggetto produttore non ne sia in grado entro il termine richiesto, l'Ente provvede ad effettuare una copia del documento informatico come previsto dal paragrafo 2.3 delle Linee Guida AGID 2021 secondo il seguente schema:
    - Convertire il documento in uno dei formati adottati ed indicati nell'allegato 9, verificando che vengano mantenuti inalterati i contenuti
    - Apporre la firma digitale dell'operatore che intende attestare la conformità della copia all'originale

3.9 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.

3.10 Documenti contenenti video o audio o social

Nel caso pervengano documenti contenenti video, audio o riferimenti a link a social media, il servizio gestione documentale avrà cura di estrapolare l'impronta Hash degli stessi indicando - in una dichiarazione sostitutiva allegata al protocollo – che la sequenza di bit, detta digest (o stringa) è strettamente correlata ai dati in ingresso.

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

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"* e successive Linee Guida Agid 2021.

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, il documento amministrativo può essere disponibile anche nella forma analogica nei casi previsti dalla legge.

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, corriere o telegramma
- a mezzo posta raccomandata
- brevi manu

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@omceolecco.it , casella PEC dell'Ente segreteria.lc@pec.omceo.it , pubblicate sul sito istituzionale www.omcelecco.it)
- piattaforme accreditate per la gestione delle acquisizioni per la Pubblica Amministrazione come : CONSIP e MEPA (www.acquistinretepa.it).
- La piattaforma della Banca Popolare di Sondrio (https://gestes.popso.it), per trasmissione OIL e pagamento stipendi/compensi.
- Piattaforma del MEF (https://area.rgs.mef.gov.it) per ricognizione dello stock del debito e indicatore tempestività pagamenti

4.2 Documenti in uscita

La trasmissione dei documenti in uscita avviene mediante l'uso dei canali informatici a meno che il destinatario non richieda motivandola una modalità diversa.

4.2.1 Inviati su supporto analogico

I documenti analogici sono trasmessi attraverso:

- Servizi postali attraverso un servizio di posta ibrida
- Brevi manu
- Notifica atti

4.2.2 Inviati su supporto informatico

I documenti informatici sono trasmessi attraverso:

- Posta elettronica certificata (PEC)
- Flussi informatici
- Caselle di Posta elettronica ordinaria
- Servizi di spedizione massiva di email ordinarie o PEC integrati nel software gestionale
- Messa a disposizione del destinatario nell'Area Riservata del sito istituzionale

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).

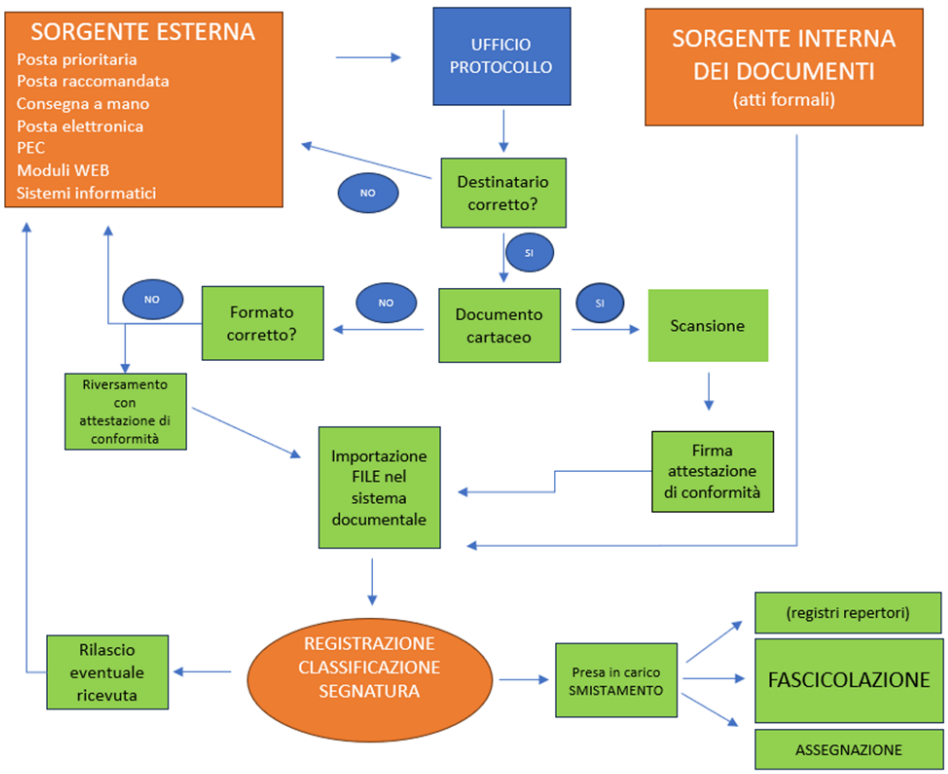
4.3 Descrizione del flusso di lavorazione dei documenti

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti e spediti attraverso i diagrammi di flussi riportati nelle pagine seguenti.

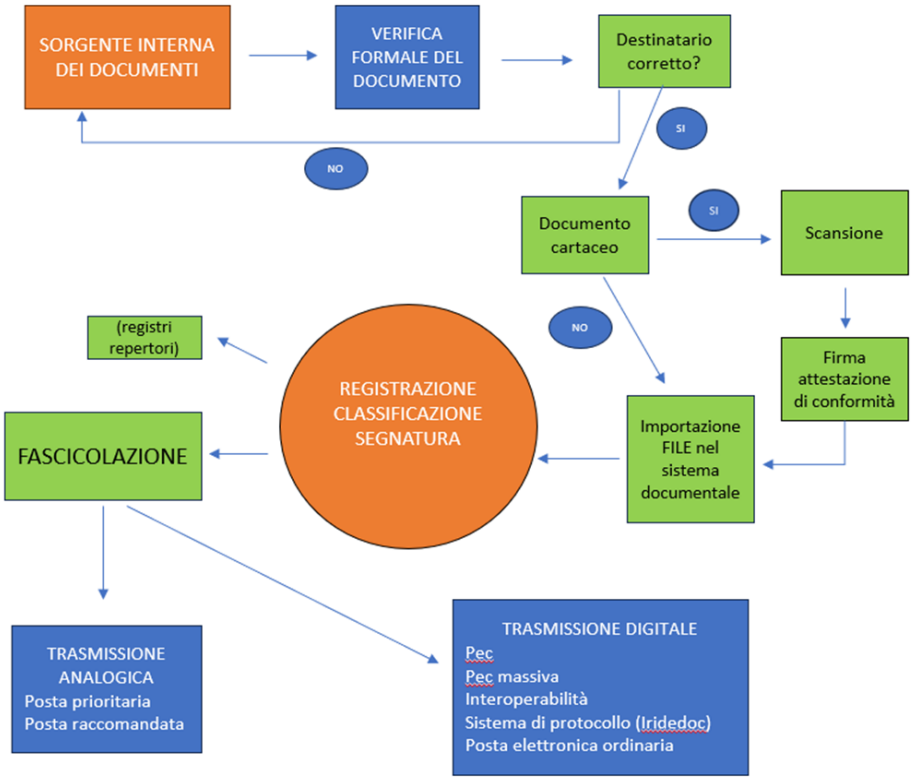
Essi si riferiscono ai documenti:

- ricevuti dall'Ente
- spediti dall'Ente

4.4 Flusso in entrata



4.5 Flusso in uscita



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. 1.6.

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 previste dalla normativa vigente.

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

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

La registrazione di 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 documentali per tipologie di documenti (serie).

5.1.1 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. In caso di particolari ed eccezionali carichi di lavoro contingenti, la registrazione può avvenire entro 48 ore dal ricevimento.

Il Protocollo generale provvede all'apertura/lettura della corrispondenza e a separare i documenti esclusi dalla registrazione di protocollo ***(Allegato 9 - Documenti esclusi dalla registrazione di Protocollo)*** ricordando che solo la corrispondenza che transita dall'email istituzionale è soggetta a protocollazione, mentre le email di servizio nominative per il personale **DEVONO** trattare messaggi non soggetti a protocollazione (messaggi interlocutori, programmatori, prodromici).

Nel caso in cui pervengano all'indirizzo personale documenti di rilevante valore giuridico che necessitino la protocollazione è cura dell'ufficio ricevente, dopo aver verificato l'aderenza della comunicazione e degli atti alle norme e diposizioni vigenti, provvedere ad inoltrare la corrispondenza alla email istituzionale.

Nell'ambito dell'Ente, il registro di protocollo è unico e la sua numerazione progressiva è 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 principale ed eventuali allegati e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immodificabile.

Contestualmente alla registrazione i documenti analogici vengono sempre acquisiti nel sistema di protocollo tramite procedura di scansione e attestazione di conformità anche acquisendo il certificato di firma se necessario come file di supporto.

Nel caso di ricezione dello stesso documento da parte di più destinatari interni all'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.

Tutti i documenti analogici in entrata o in uscita registrati devono essere acquisiti in copia rispettando i requisiti di accessibilità (es. formato PDF/A) 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.) che devono essere elencati e descritti in un documento che verrà acquisito come documento principale.

5.1.2 Documento analogico inviato elettronicamente

Se il documento analogico è inviato tramite posta elettronica certificata o canali digitali, viene gestito come segue:

- Redatto in un unico esemplare
- Sottoscritto con firma autografa
- Acquisito tramite scansione nel sistema di protocollo
- Firmato digitalmente dall'operatore di protocollo, il quale provvederà anche ad apporre l'attestazione di conformità
- Associato al protocollo stesso e al fascicolo relativo.
- L'operatore provvede poi all'invio del file all'indirizzo telematico del destinatario.
- Viene quindi conservato presso l'Ente secondo le modalità descritte nel Manuale e inserito nel fascicolo relativo.

5.1.3 Documento digitale inviato elettronicamente

Se il documento digitale è inviato tramite posta elettronica certificata o canali digitali, viene gestito come segue:

- redatto tramite un software adeguato (es. elaborazione testi)
- sottoscritto con firma digitale ove necessario
- acquisito nel sistema di protocollo
- associato al protocollo stesso e al fascicolo relativo
- L'operatore provvede poi all'invio del file all'indirizzo telematico del destinatario o reso disponibile con webservice

5.2 Registri di protocollo periodici

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

5.2.1 Invio in conservazione del registro giornaliero di protocollo

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

Il "registro di protocollo"[4] ricomprendere i metadati minimi indicati nell'allegato 5 delle Linee Guida AGID 2021 ma anche gli ulteriori metadati indicati nella circolare AGID art. 53, comma 1, del DPR 445/2000 e dalla Circolare AGID n. 60 del 2013.

- Anno
- Numero della prima registrazione effettuata sul registro
- Numero dell'ultima registrazione effettuata sul registro
- Data della prima registrazione effettuata sul registro
- Data dell'ultima registrazione effettuata sul registro

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
B. la data di registrazione di protocollo
C. il mittente o i destinatari
D. l'oggetto del documento
E. l'impronta del documento principale
F. indicazione del registro di protocollo

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.

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

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.

Oltre al registro giornaliero di protocollo è previsto l'invio in conservazione del registro dei protocolli sia mensile (entro 7 giorni lavorativi dalla fine del mese precedente) che annuale (entro il 31 gennaio dell'anno successivo) dei protocolli.

Questo al fine di riportare nei registri le eventuali variazioni intercorse.

5.3 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,

[4] Conformemente anche a quanto indicato nel documento AGID "PRODUZIONE E CONSERVAZIONE DEL REGISTRO GIORNALIERO DI PROTOCOLLO"
https://www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/istruzioni_per_la_produzione_e_conservazione_registro_giornaliero_di_protocollo.pdf

delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.

Le informazioni previste sono indicate all'interno dell'allegato 6 delle comunicazioni tra AOO di documenti amministrativi protocollati delle linee guida AGID del Maggio 2021 sulla formazione, gestione e conservazione dei documenti informatici.

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 tramite timbro o etichetta (le cui informazioni sono il risultato dell'estrazione delle informazioni minime contenute nella segnatura informatica). Questa riporterà il numero e la data di protocollo.

Qualora il documento venga prodotto in formato nativo digitale il numero di protocollo è indicato solitamente:

- nel nome del file
- nell'oggetto della mail nel caso di trasmissione con posta elettronica.
- Nel file di segnatura in formato xml nel caso di trasmissione con posta elettronica

5.4 Procedure specifiche nella registrazione di protocollo

5.4.1 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.

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

Il RSP monitora periodicamente l'adeguatezza del sistema organizzativo e del software utilizzato per la registrazione di protocollo e gestione documentale.

Il monitoraggio è favorito anche dallo stretto rapporto collaborativo con l'Amministratore di sistema e dal gruppo di lavoro interregionale tra gli Ordini di Pisa, Venezia e Lecco che, in ossequio alle previsioni di AGID sulla digitalizzazione, rivolgono particolare riguardo agli aspetti della sicurezza e riservatezza anche secondo le indicazioni dei DPO e RTD vista la particolare natura dei dati trattati.

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 RPCT e/o Dirigente Amministrativo. 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.

Il sistema può associare il livello di riservatezza anche in relazione alla classe documentale assegnata al protocollo/documento.

Il RPA o un suo delegato che effettua l'operazione di apertura di un nuovo fascicolo può stabilire anche il livello di riservatezza applicando, tramite le apposite funzioni, le autorizzazioni a livello di ruolo oppure di singolo utente.

Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi sia stato assegnato un livello di riservatezza minore o uguale. I documenti che invece hanno un livello di riservatezza superiore lo mantengono.

Per approfondimenti su altri aspetti di riservatezza e privacy vedere capitolo 2.

5.4.2 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 di cui all'allegato ***(Allegato 9 - Documenti esclusi dalla registrazione di Protocollo).***

5.4.3 Modifica delle registrazioni di protocollo

Le uniche informazioni modificabili della registrazione di protocollo sono la classe documentale e l'assegnazione oppure i fascicoli e dossier/ di riferimento o file di supporto.

Tali modifiche vengono storicizzate e rese visibili e comparabili ai sensi dell'art. 54 del DPR 445/2000 e ss.mm.ii.

5.4.4 Annullamento delle registrazioni di protocollo

La procedura di annullamento di una registrazione è di competenza del Responsabile del servizio archivistico o del suo delegato.

L'annullamento della registrazione di protocollo prevede la memorizzazione dei seguenti dati:

- data di annullamento
- operatore
- motivo dell'annullamento
- estremi del provvedimento di autorizzazione

Tali modifiche vengono storicizzate e rese visibili e comparabili ai sensi dell'art. 54 del DPR 445/2000 e ss.mm.ii.

5.5 Casi particolari di registrazioni di protocollo

5.5.1 Lettere anonime

La lettera anonima, una volta aperta e attestata l'assenza di ogni riferimento al mittente, viene posta all'attenzione del Segretario/Dirigente o di persona dallo stesso delegata, che fornirà istruzioni in merito al suo trattamento agli addetti del Protocollo, i quali provvederanno secondo le indicazioni ricevute, alla sua registrazione e assegnazione (indicando nel campo mittente "anonimo") ovvero alla sua eliminazione.

Una disciplina particolare è prevista per le procedure di whistleblowing. Oltre la procedura telematica potrebbero pervenire segnalazioni cartacee dagli utenti che devono necessariamente seguire l'iter previsto dal Piano Anticorruzione predisposto dall'Ente e seguite esclusivamente da RPCT.

5.5.2 Documenti privi di firma

I documenti con mittente, privi di firma, vanno protocollati. La funzione notarile del protocollo (cioè della registrazione) è quella di attestare data e provenienza certa di un documento senza interferire su di esso.

5.5.3 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".

5.5.4 Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.

Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) o suo delegato che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente.

I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati oppure integrati come documenti secondari nella registrazione di protocollo originaria secondo la valutazione del RPA e sono inseriti nel fascicolo relativo.

5.5.5 Documenti pervenuti per errore all'Ente

I documenti pervenuti per errore all'Ente non devono essere protocollati e devono essere spediti immediatamente al mittente con la dicitura «Erroneamente pervenuto all'Ordine provinciale dei Medici Chirurghi e degli Odontoiatri di Lecco il (giorno.mese.anno)».

5.5.6 Trattamento dei documenti con oggetto o smistamento plurimo

Ogni documento, anche se in più esemplari, deve essere individuato da un solo e unico numero di protocollo, indipendentemente dal fatto che sia indirizzato, per competenza o per conoscenza, a una o più strutture amministrative e/o organi politici all'interno dell'Ente. Di conseguenza, qualora pervenga un documento nel quale risultano evidenti più destinatari, l'addetto alla registrazione, prima di protocollarlo, deve verificare, attraverso il sistema informatico, che esso non sia già stato registrato precedentemente.

Nel caso in cui, oltre alla pluralità di destinatari, il documento tratti anche una pluralità di argomenti (pluralità di oggetti), afferenti a procedimenti diversi e – conseguentemente – a fascicoli diversi, si individua la classe principale anche in considerazione del Piano di Conservazione e si inserisce nei relativi fascicoli da cui ne ereditano la classe.

Ogni documento in uscita deve obbligatoriamente trattare un solo oggetto (un solo argomento) e deve necessariamente riferirsi ad un solo procedimento.

5.5.7 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 collettivi, esempio: "TUTTI GLI ISCRITTI".

Al fine di permettere una corretta protocollazione, nei casi di invio massivo di un documento ed utilizzo dei "destinatari collettivi", l'Ufficio di protocollo associa come documento secondario del protocollo un file contenente l'elenco dei destinatari individuati con nome, cognome o Ragione Sociale, codice fiscale e il recapito pervenuto dal RPA o delegato.

Nel caso di invio di comunicazioni massive quando il documento è identico questo sarà il documento principale del protocollo, nel caso in cui il documento è personalizzato il documento principale sarà il modello definito per la generazione dei singoli file personalizzati.

Le ricevute di consegna relative ad invii effettuati tramite PEC sono gestite come segue:

- Le ricevute di consegna relative all'Avviso di Convocazione per le Assemblee elettorali spedito in forma massiva sono conservate nel software gestionale della posta elettronica per 30 giorni dalla data di proclamazione dei risultati elettorali, in armonia a quanto previsto dall'art. 6 del Decreto del Ministero della Salute del 15/03/2018 inerente le procedure elettorali degli Ordini sanitari. Decorso tale termine, possono essere scartate;
- Le ricevute di consegna relative a lettere di messa in mora spedite in forma massiva sono conservate nel software gestionale della posta elettronica fino al termine del procedimento amministrativo. Nel caso in cui il procedimento amministrativo, al suo perfezionamento, comporti l'adozione di un provvedimento limitativo o pregiudizievole per il destinatario, la ricevuta di consegna è registrata nel dossier del destinatario. Viceversa, nel caso in cui il procedimento amministrativo, al suo perfezionamento, non comporti alcun provvedimento limitativo o pregiudizievole per il destinatario, la ricevuta di consegna può essere scartata;

- Le ricevute di consegna relative a comunicazioni singole (non massive) sono sempre registrate nel dossier/fascicolo del destinatario, indipendentemente dal tipo di procedimento amministrativo sottostante.

Gli avvisi di spedizione o lettura relativi all'invio di email ordinarie, sia massive che singole, non sono di norma soggetti a registrazione e vengono gestiti dagli uffici competenti al solo scopo di monitoraggio, controllo e verifica dei dati.

5.5.8 Flussi documentali informatici

5.5.8.1 Flusso FNOMCeO-ENPAM

L'Ente è tenuto periodicamente all'invio delle posizioni degli iscritti alla FNOMCeO e all'ENPAM. Tale invio avviene solitamente dopo le variazioni occorse nelle sedute consiliari con una procedura semiautomatica:

- generazione a partire dal gestionale Albi di 2 file in formato xml
- verifica della correttezza formale dei file
- protocollazione del file "Anagrafica" indicando come destinatari FNOMCeO ed ENPAM
- protocollazione del file "Datirifnom" indicando come destinatario FNOMCeO

I due file vengono inviati tramite il software fornito da FNOMCeO e ENPAM.

5.5.8.2 Flusso Fnomceo Onaosi

L'Ente provvede a inviare circa due volte l'anno le variazioni alla Fondazioni Onaosi. Al riguardo si sta valutando una modalità omogenea per tutti gli OMCeO che utilizzando il medesimo software gestionale.

5.5.8.3 Flusso OIL (ordinativo informatico)

Anche in questo caso viene generato un flusso xml dall'applicativo TecSis Conto che poi viene firmato digitalmente da: Presidente, Segretario e Tesoriere, quindi inviato telematicamente alla banca che funge da Cassiere e infine protocollato.

5.5.8.4 Fatture elettroniche

Le fatture elettroniche e le notifiche vengono protocollate con una procedura automatica che giornalmente, per mezzo di un job eseguito dal server in orario serale, le riversa nel software del protocollo inserendo i seguenti metadati:

- Numero e data protocollo
- Data riferimento del documento: viene impostata la data di emissione della fattura
- Oggetto: viene composto secondo uno standard predefinito - Fatt. [Num Fattura] del [Data emissione] emessa da [Ragione sociale fornitore e partita IVA]
- Classe documentale: 07.04 per le fatture e 07.05 per le notifiche

- Direzione: entrata
- Mittente: viene caricato il soggetto corrispondente sulla base del codice fiscale inserito nell'anagrafica o, se non presente, viene anche anagrafato il soggetto
- Mezzo di trasmissione: quello configurato nel software di protocollo per questa tipologia di documenti
- Documento primario: fattura elettronica
- Documento secondario: metadati allegati alla fattura

5.5.8.5 Casellario Massivo

Il sistema CERPA (CERtificati Pubbliche Amministrazioni) consente la consultazione diretta del Sistema Informativo del Casellario (SIC) da parte delle amministrazioni pubbliche e dei gestori di pubblici servizi, ai fini dell'acquisizione dei certificati del casellario giudiziale e dell'anagrafe delle sanzioni amministrative dipendenti da reato.

La consultazione può avvenire qualora, per lo svolgimento dei propri compiti istituzionali, le PP.AA. e i gestori di pubblici servizi abbiano necessità di procedere:

- alle acquisizioni d'ufficio di informazioni concernenti stati, qualità e fatti (art. 43 e 46 D.P.R. 445/2000)
- ai controlli delle dichiarazioni sostitutive di certificati (art. 71 D.P.R. 445/2000):

tramite:

- un servizio di cooperazione tra sistemi informativi
- Posta Elettronica Certificata (PEC)

Presupposto per accedere al sistema è l'aver sottoscritto una convenzione con il Ministero della Giustizia.

La stipula di tale convenzione, per quanto concerne gli Ordini dei Medici spetta alla Federazione Nazionale degli Ordini dei Medici (FNOMCEO) che ad oggi non ha ancora adempiuto.

Fino a quando le pubbliche amministrazioni ed i gestori di pubblici servizi non avranno stipulato le relative convenzioni o fino a quando tali soggetti non si saranno accreditati al sistema AVCPass, i certificati in premessa andranno richiesti agli uffici locali del casellario giudiziario, tramite due appositi moduli: uno per richieste riferite a singoli soggetti, l'altro per richieste riguardanti un numero significativo di persone, compilabile attraverso apposito applicativo (procedura certificazione massiva).

La procedura utilizzata dall'Ente nel caso di richieste che superino il nr. di 20 casellari è pertanto la procedura di richiesta massiva, una procedura informatica che prevede prima l'estrazione dei nominativi dal gestionale Albo e successivamente l'inserimento all'interno di un programma scaricabile dal sito del Ministero con il quale si inoltra con protocollo la richiesta all'Ufficio del Casellario che evade le richieste all'incirca entro 24 ore.

5.5.8.6 Istanze telematiche

Le istanze telematiche (domanda di prima iscrizione e domanda di cancellazione) vengono protocollate dall'operatore per mezzo di un connettore presente nel software di protocollo che recupera i dati direttamente dall'istanza effettuata in cloud.

L'operatore dovrà quindi solo dare l'input di protocollazione, una volta verificata l'istanza da parte del RPA o delegato, ed il software provvederà a protocollare la singola istanza impostando automaticamente i seguenti dati:

- Numero e data protocollo
- Data riferimento del documento: viene impostata la data di invio dell'istanza
- Oggetto: viene composto secondo uno standard predefinito - ...
- Classe documentale: 03.19 per le istanze di prima iscrizione e cancellazione Albo medici e 03.20 per le istanze di prima iscrizione e cancellazione Albo odontoiatri
- Direzione: entrata
- Mittente: viene caricato il soggetto corrispondente sulla base del codice fiscale inserito nell'anagrafica o, se non presente, viene anche anagrafato il soggetto
- Mezzo di trasmissione: quello configurato nel software di protocollo per questa tipologia di documenti
- Documento primario: istanza telematica
- Documento secondario: eventuali allegati all'istanza (a titolo esemplificativo documento d'identità, ricevute di pagamento, ecc)

Successivamente viene inserito nel fascicolo relativo e assegnato.

5.6 Regole di smistamento e di assegnazione

L'operazione di smistamento consiste, da parte dell'operatore di protocollo, nell'assegnazione al personale addetto all'attività preposta.

Si adottano le modalità operative di seguito illustrate:

- quotidianamente gli operatori e/o i responsabili verificano i documenti a loro assegnati;
- ogni soggetto provvede alla visione e alla gestione del documento assegnato e alla sua riassegnazione ad altro collega con eventuali note ove necessario.

Le assegnazioni hanno di regola scadenza 30 giorni come previsto dalle norme sul procedimento amministrativo.

Il sistema di gestione documentale prevede l'assegnazione soltanto ad un singolo utente per cui di norma le registrazioni in arrivo vengono assegnate al Responsabile dell'Ufficio individuato come da Allegato n. 6 Organigramma e secondo le indicazioni del Segretario tenendo conto degli incarichi di Posizione Organizzativa e di eventuali altri incarichi speciali e specifici conosciuti dall'operatore di Protocollo. Il Responsabile poi eventualmente provvede ad assegnare la registrazione ad altra persona.
Le registrazioni in uscita vengono assegnate al soggetto che ha chiesto la protocollazione dell'istanza.

5.6.1.1 Processo di assegnazione delle registrazioni di protocollo ai fascicoli

Quando un nuovo documento viene formato o ricevuto dall'Ente, il RPS 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 sulla base del piano di fascicolazione (allegato n. 5)
  - collega la registrazione di protocollo del documento al fascicolo appena creato

Il soggetto che ha in carico l'assegnazione provvederà inoltre alla revisione del processo di fascicolazione e provvederà se opportuno ad assegnare la registrazione anche in altri fascicoli ovvero alla variazione della classe documentale se ritiene di doverla assegnare ad una più opportuna il tutto anche alla luce del Piano di Conservazione

6 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico, ogni documento in entrata o in uscita deve essere registrato su un supporto alternativo, denominato Registro di emergenza (***Allegato 8: Modello del Registro di emergenza***).

Per emergenza si intende una situazione in cui la sospensione del servizio si protragga oltre le **8 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 o suo delegato come descritto al cap. 1.5.

Per la registrazione di emergenza si utilizza:

1. nel caso di disponibilità dei PC un modulo in formato Excel disponibile tra la modulistica amministrativa dell'Ente; il modulo potrà essere compilato mediante l'immissione dei dati direttamente sulla tabella;
2. nel caso di impossibilità ad utilizzare i PC ci si avvarrà del modulo cartaceo di cui al fac simile allegato al Manuale di gestione che verrà compilato manualmente.

Sul registro di emergenza 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 note ritenute rilevanti dal responsabile del protocollo informatico e della gestione documentale.

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.

Ogni documento è individuato dal numero assegnato nel Registro di emergenza, anno di registrazione, numero di protocollo nel formato stabilito; ad esempio:

RE01-2023-0000005.

Una volta ripristinata la piena funzionalità del sistema, il RSP provvede alla chiusura dei registri di emergenza, annotando su ciascuno il numero di registrazioni effettuate e la data e ora di chiusura e dovrà protocollare il registro di emergenza attivato.

I dati delle registrazioni di emergenza dovranno essere inseriti nel sistema informatico di protocollo e si configurano come un repertorio dello stesso.

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.

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

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 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 dev'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.

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**[5],composto dai documenti relativi ad affari correnti ,
- **Archivio di deposito**[6],riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- **Archivio storico**[7],composto dai documenti relativi ad affari cessati da più di 40 anni, selezionati per la conservazione permanente

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 titolario 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 titolario e il piano di conservazione sono adottati con atti formali dai vertici dell'Ente.

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

[6] 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)

[7] 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 sfoltimento avvenute nel tempo.

7.2 Titolario o piano di classificazione

7.2.1.1 Titolario

Il Titolario o Piano di classificazione è un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'Ente, al quale viene ricondotta la molteplicità dei documenti prodotti.

L'Ente utilizza un titolario, adottato con deliberazione N. 16/2017 e approvato dalla Soprintendenza dei Beni Archivistici e Bibliografici della Regione Lombardia unitamente alla precedente versione del manuale di gestione (vedi ***Allegato 4 -Titolario di classificazione***) organizzato a 2 livelli suddiviso in titoli e classi. Il titolo (o la voce di I° livello) individua per lo più funzioni primarie e di organizzazione dell'Ente (macrofunzioni); le successive partizioni (classi) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

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 su proposta del RSP.

L'Ente di norma sottopone il Titolario all'approvazione della Sopraindentenza di riferimento.

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.

Il sistema di protocollazione garantisce 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.

Per ogni specifica voce viene riportata la data di inserimento e la data di variazione.

7.2.1.2 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.

Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti medesimi.

7.3 Formazione del fascicolo

7.3.1 Il fascicolo

Il fascicolo costituisce l'unità archivistica di base, che permette, nel tempo, la gestione ottimale della documentazione detenuta istituzionalmente da qualsiasi Ente.

Il fascicolo rappresenta una delle unità archivistiche elementari (documento, fascicolo, registro) e può essere definito come "*un insieme organico di documenti raggruppati o dal soggetto produttore per le esigenze della sua attività corrente o nel corso dell'ordinamento dell'archivio, in base al comune riferimento allo stesso oggetto, attività o negozio giuridico*".

I documenti registrati e classificati nel sistema informatico (protocollati) sono riuniti in fascicoli o in aggregazioni documentali.

I fascicoli vengono creati secondo le indicazioni riportate nel piano di fascicolazione (All. 5) dove vengono riportate le tipologie di fascicoli (o l'eventuale gestione in repertori) e l'indicazione se il fascicolo ha durata annuale o per singola attività o per procedimento.

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

Qualora un documento dia luogo all'avvio di un procedimento amministrativo, il RPA o suo delegato assegnatario del documento stesso, deve provvedere all'apertura (istruzione) di un nuovo fascicolo che comprende la registrazione dei relativi metadati.

Ogni fascicolo è caratterizzato dai seguenti metadati:

- indice di classificazione, (cioè titolo, classe)
- identificativo progressivo
- oggetto del fascicolo
- data di apertura del fascicolo
- data di chiusura
- nominativo del responsabile
- tipologia

7.3.2 Famiglie e tipologie di fascicolo

I fascicoli sono suddivisi in 4 categorie:

1. fascicoli inerenti persone fisiche
2. fascicoli inerenti persone giuridiche
3. fascicoli inerenti procedimenti amministrativi
4. fascicoli inerenti affari o attività

Per ogni persona fisica o giuridica deve essere istruito un fascicolo nominativo. Il fascicolo viene generato dall'operatore di protocollo secondo le indicazioni riportate al paragrafo 5.7.1.1.

L'apertura prevede la registrazione di alcune informazioni essenziali:

- identificativo progressivo

- indice di classificazione
- oggetto del fascicolo
- data di apertura del fascicolo
- nominativo del responsabile del procedimento/fascicolo
- tipologia

I documenti sono archiviati all'interno di ciascun fascicolo, 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. I fascicoli classificati come annuali vengono chiusi di norma alla fine dell'anno solare e possono essere riaperti con modalità automatica per l'anno successivo. La data di chiusura si riferisce alla data dell'ultimo documento prodotto.

Per quanto riguarda i fascicoli di persona questi verranno chiusi nel momento in cui il ruolo giuridico di quella persona viene meno (per es. quando un iscritto si cancella o quando un dipendente cessa l'attività lavorativa) sempre considerando la data dell'ultimo documento prodotto.

7.3.3 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)[8].

Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio, quindi, rispecchia quella del titolario di classificazione e varia in concomitanza con l'aggiornamento di quest'ultimo. Mentre il titolario rappresenta in astratto le funzioni e le competenze che l'Ente può esercitare, in base 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
- 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

[8] 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.

- eventuali note
- tipologia

7.3.4 Il fascicolo personale dell'iscritto/S.T.P.

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.

Ognuno di questi fascicoli è suddiviso in due differenti sottofascicoli:

- il sottofascicolo 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 sottofascicolo denominato QUALIFICHE E ATTIVITA' che comprende tutti i documenti relativi all'attività professionale

Nel caso dei doppi iscritti deve essere aperto un fascicolo per ogni albo all'atto della presentazione dell'istanza di iscrizione.

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.

7.3.5 Dossier

Il sistema di gestione del protocollo consente anche di accorpare fascicoli e documenti anche di classi diverse di un particolare soggetto in un'entità denominata Dossier.

Esso comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica o giuridica. Per spiegare meglio, nel DOSSIER personale di un iscritto all'Ordine o del personale dipendente ciascun documento viene classificato a seconda della classe di riferimento prevista e viene inserito nel fascicolo o nel repertorio di competenza

Il dossier si configura così come aggregazione di documenti e si apre indipendentemente dalle classi. Si apre a livello di titolo (ad esempio, per gli iscritti nel titolo III oppure per il personale nel titolo VI).

7.4 Repertori e fascicoli annuali

Il repertorio aggrega documentazione omogenea dal punto di vista formale, ma eterogenea sotto il profilo del contenuto giuridico e amministrativo: ad esempio verbali e deliberazioni di organi collegiali o monocratici, registrature contabili, ecc.

Si tratta di un peculiare tipo di aggregazione documentale che raccoglie documenti identici per forma e provenienza, ma difformi per contenuto, disposti in sequenza cronologica. Ciascun documento, in base a tale ordine, è identificato con un numero progressivo cui viene riconosciuta una valenza probatoria.

Il fascicolo annuale può raccogliere documentazione eterogenea sotto il profilo formale ma conservata insieme perché risultato di un medesimo processo di sedimentazione, o di una medesima attività, o perché relativa alla stessa materia.

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 di protocollo ed inseriti in un repertorio. I documenti possono essere altresì conservati in un fascicolo annuale, insieme ai documenti che afferiscono al medesimo argomento.

7.5 Tipologie di registri

L'Ente gestisce altri registri, oltre a quello di protocollo informatico. Tali registri sono:

VERIFICARE SE LI ABBIAMO E SE LI UTILIZZIAMO ALTRIMENTI TOGLIERE

- albo medici
- albo odontoiatri
- albo società tra professionisti
- psicoterapeuti
- medicine complementari
- Registro unico fatture
- Registro cronologico mandati
- Registro cronologico reversali
- Inventario beni mobili ed immobili
- Verbali e delibere del Consiglio Direttivo
- Verbali e delibere della Comm. MED. e della CAO
- Verbali delle Assemblee degli iscritti (ordinarie, straordinarie, elettorali)
- Delibere del Consiglio Direttivo
- Determine del Presidente
- Verbali di altre Commissioni e/o Gruppi di lavoro
- Convenzioni e Protocolli d'intesa fra l'Ordine ed altri Enti.

L'Ente ha in corso un processo di valutazione dei registri e delle dinamiche di gestione al fine di uniformare e centralizzare la gestione all'interno del software di gestione documentale e del protocollo informatico.

7.6 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.

7.7 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.

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

La proposta di scarto viene formulata secondo la procedura indicata dalla soprintendenza archivistica Lombardia che prevede la presentazione di un'istanza dove deve essere indicato l'elenco degli atti che si propongono per l'eliminazione corredati da

- Numero unità
- Descrizione degli atti
- Estremi cronologici
- Peso in Kg.
- Motivo della eliminazione

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

7.7.1 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 chiusi o comunque non più necessari a una trattazione corrente.

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

I documenti che costituiscono l'archivio storico sono conservati presso depositi dell'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.).

8 PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA

8.1 Premessa

L'Ente, recependo le prescrizioni e i principi espressi dalla normativa in materia, ha disciplinato le attività e i procedimenti amministrativi definendo le responsabilità in ordine agli stessi.

Attraverso appositi regolamenti garantisce da un lato l'accesso il più ampio possibile ai documenti amministrativi e dall'altro la tutela dei dati personali e sensibili, riconoscendo in tal modo i diritti entrambi costituzionalmente fondati.

Le specifiche procedure sono definite nei documenti di seguito indicati: **DA RECUPERARE**

- regolamento per l'individuazione dei termini e responsabili dei procedimenti amministrativi approvato con Deliberazione n. 79 del 17.09.1996 e secondo la Delibera n. 27 del 24/02/2021
- regolamento sul diritto di accesso dei cittadini agli atti e ai documenti amministrativi, approvato con Deliberazione n. 74 del 17/06/2019

In adempimento alla recente normativa in tema di trasparenza e accesso civico (Decreto legislativo n. 33 del 14 marzo 2013) l'Ente ha costituito apposita sezione di "Amministrazione trasparente" nel sito istituzionale, nella quale sono pubblicati dati, informazioni e documenti che riguardano l'organizzazione e le attività dell'ente.

8.2 Procedure di accesso ai documenti e di tutela della riservatezza

Merita chiarire preliminarmente alcuni principi e procedure che costituiscono un punto di riferimento per chi opera presso l'Ente, tenendo conto che le problematiche connesse all'accesso e alla tutela della riservatezza riguardano tutte le fasi di vita dei documenti.

L'accesso/consultazione dei documenti si può così suddividere:

1. Consultazione per fini amministrativi, per la quale si fa riferimento allo specifico regolamento dell'Ente già citato, che può riguardare tutta la documentazione prodotta dall'Ente nell'esercizio della sua attività amministrativa, ivi compresa quella conservata nell'archivio storico.
2. Consultazione per fini di ricerca storico-scientifica, che è disciplinata dal Capo III del Codice dei Beni Culturali e del Paesaggio, in base al quale i documenti sono liberamente consultabili, ad eccezione:

    - di quelli di carattere riservato relativi alla politica estera o interna dello Stato, che divengono consultabili 50 anni dopo la chiusura del fascicolo che li contiene
    - di quelli contenenti dati sensibili, che diventano consultabili 40 anni dopo la chiusura del fascicolo che li contiene

- di quelli contenenti taluni dati sensibili (noti in gergo come “sensibilissimi”), idonei a rivelare lo stato di salute o la vita sessuale o i rapporti riservati di tipo familiare, che diventano consultabili 70 anni dopo la chiusura del fascicolo che li contiene.

La consultazione dei documenti contenenti dati sensibili può essere autorizzata dalla Soprintendenza archivistica competente per territorio anche prima della scadenza dei termini prescritti dalla legge.

In ogni caso gli utenti che accedono alla documentazione conservata negli archivi storici sono tenuti al rispetto delle prescrizioni del Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici.

9 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

9.1 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 delegato, 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, possono essere aggiornati e modificati con determina del Presidente, se non prevedono modifiche organizzative rilevanti altrimenti con apposita deliberazione di Consiglio.

Entra in vigore alla data di esecutività della deliberazione che lo approva.

9.2 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 pubblicato sull’area amministrazione trasparente e la sua conoscenza è inserita nei percorsi di formazione del personale in tema di gestione documentale.

Elenco allegati

1. Glossario dei termini e degli acronimi
2. Individuazione Area Organizzativa Omogenea
3. Istituzione servizio Archivistico e Nomina del Responsabile del Servizio
4. Titolario di Classificazione
5. Piano fascicolazione
6. Oggettario
7. Organigramma
8. Organigramma privacy
9. Documenti esclusi dalla registrazione di protocollo
10. Modello registro di emergenza
11. Formati di file e riversamento