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" 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 della gestione documentale, così come già previsto dall'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - **Decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000**.

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

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

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

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

Il protocollo informatico e il sistema di gestione documentale costituiscono il fulcro della struttura tecnologica ed 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 dei Medici Chirurghi e degli Odontoiatri, di seguito "Ente", è un Ente Pubblico non economico dotato di una struttura organizzativa semplice e poco ramificata. Inoltre la limitata presenza di personale e relativa concentrazione delle funzioni/attività, riduce notevolmente le esigenze gestionali. Gli iter amministrativi avvengono quasi sempre all'interno dello stesso ufficio e i documenti vengono presi in carico spesso dagli stessi addetti che effettuano le registrazioni di protocollo.

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

Coordina gli uffici un funzionario in posizione organizzativa e tre funzionari amministrativi svolgono le varie attività dell'ufficio in maniera sinergica e coordinata, quindi 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 ed unitaria da un'unica AREA ORGANIZZATIVA OMOGENEA.

1.2 Ambito di applicazione del Manuale di Gestione

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

- Formazione
- Registrazione
- Classificazione
- Fascicolazione

[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.

- 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.

1.3 Definizioni e norme di riferimento

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

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

- Legge 11 febbraio 2005, n. 15 - Modifiche ed integrazioni alla legge 7 agosto 1990, n. 241, concernenti norme generali sull'azione amministrativa
- Decreto del presidente del Consiglio dei Ministri 3 dicembre 2013 - *Regole tecniche per il protocollo informatico*
- Decreto del presidente del Consiglio dei Ministri 3 dicembre 2013 - *Regole tecniche in materia di sistema di conservazione*
- Decreto del presidente del Consiglio dei Ministri 11 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni
- Decreto del presidente del Consiglio dei Ministri 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali
- Quaderno 21 CNIPA, febbraio 2006 - Manuale di gestione del protocollo informatico, dei documenti e dell'archivio delle Pubbliche amministrazioni - Modello di riferimento.

Ai fini del presente manuale si intende per:

- "**amministrazione**", l'Ordine dei Medici Chirurghi e degli Odontoiatri della provincia di Genova.
- "**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 settembre 2016).
- Di seguito si riportano gli acronimi utilizzati più frequentemente:
- **AOO** - Area Organizzativa Omogenea;
- **CGD** – Coordinatore della Gestione Documentale;
- **MdG** - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi (il presente documento);
- **RPA** - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- **RSP** - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **SdP** – Servizio di protocollo informatico;

- **UOP** - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **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;
- **UU** - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal servizio di protocollo informatico; ovvero il soggetto, destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Per altre definizioni si faccia riferimento allegato 01

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

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

Sigla dell'AOO = omceoge

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'Ordine (vedi cap. 14).

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

A norma dell'art. 61 del DPR 445/2000, Il Consiglio Direttivo ha istituito, con Deliberazione del 27 marzo 2018, l'ufficio denominato "Servizio archivistico dell'Ordine dei Medici chirurghi e degli odontoiatri di Genova", 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;
- **Il coordinamento degli archivi** di deposito (procedure di versamento e scarto documentale, consultazione) e la gestione dell'archivio storico dell'Ente (conservazione, inventariazione, accesso e valorizzazione).

Con la medesima deliberazione si individua il Responsabile del Servizio, 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.

(Allegato 3 - Istituzione del Servizio archivistico dell'Ordine e individuazione del responsabile: delibera del 27 marzo 2018).

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

Per il dettaglio si veda la tabella dei delegati al cap. 11.

Ai sensi dell'art. 5, comma 3 del DPCM 13 novembre 2013 *Regole tecniche per il protocollo informatico* sono compiti del Responsabile del Servizio e/o del delegato:

- 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, d'intesa con il responsabile della conservazione, con i preposti ai sistemi informativi (Amministratore di sistema) e con il responsabile del trattamento dei dati personali di cui al suddetto decreto;
- Sono inoltre compiti del Servizio:
    - Abilitare gli addetti dell'amministrazione all'utilizzo del sistema di protocollo informatico e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, registrazione, modifica ecc.);
    - Garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
    - Garantire la corretta produzione e conservazione del registro giornaliero di protocollo;

- Curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- Conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- Garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali;
- Autorizzare le operazioni di annullamento delle registrazioni di protocollo;
- Aprire e chiudere il registro di emergenza.
- Definire e assicurare criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna, ai sensi dell'art. 50, comma 4, del testo unico.
- Curare le attività di registrazione di protocollo affinché, in caso di guasti o anomalie, ne sia ripristinata la funzionalità entro max ventiquattro ore dal blocco e, comunque, nel più breve tempo possibile
- Autorizza, apre, chiude e si assicura della corretta compilazione dell'eventuale protocollo di emergenza

1.5.1 Il delegato per la tenuta del protocollo informatico

I compiti del delegato per la tenuta del protocollo informatico 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.

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.

Per il dettaglio si veda la tabella dei delegati al cap.11

1.5.2 Il delegato per la conservazione

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

Il delegato interno per la conservazione svolgerà i seguenti compiti:

- Si accerta che il fornitore sia fra quelli accreditatati AGID;
- Verifica il manuale della conservazione redatto dal fornitore;
- Interagisce con il fornitore per la definizione dei metadati da utilizzare per ogni tipologia documentale da portare in conservazione
- Definisce contrattualmente i tempi di conservazione dei documenti.
- Effettua verifiche periodiche di mantenimento dei requisiti del fornitore (esempio controlli a campione sui documenti e richieste di pacchetti di distribuzione)

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

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

1.5.3 Firma digitale (vedi anche cap. 3.5.1)

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.

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

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

1.5.4 Firma elettronica (vedi anche cap. 3.5.1)

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. Va sottolineata l'importanza della segretezza delle credenziali e del cambio password periodico, in base alle politiche di sicurezza dell'Ente (si raccomanda cambio password ogni 3 mesi).

1.5.5 Firma Remota Automatica (vedi anche cap. 3.5.1)

L'Ente è dotato di firma automatica per l'espletamento delle procedure di firma massiva connesse al sistema di riversamento dei documenti in conservazione digitale.

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

L'Ente, avendo individuato un'unica AOO, si serve di un unico sistema di protocollo informatico e gestione documentale denominato IRIDEDOC prodotto da TecSis S.r.l. (di seguito software di protocollo)

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, protocolli del telefax, 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)*
- Organigramma *(Allegato 6 – Organigramma)*
- Repertorio dei fascicoli
- Piano di fascicolazione e di conservazione

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).

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

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

2 PIANO DI SICUREZZA

Il presente capitolo, ai sensi **dell'art. 4, comma c, e dell'art. 7 del DPCM 3 dicembre 2013**, riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto delle misure minime di sicurezza previste nell'allegato B del D.lgs. 196/2003.

2.1 Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- I documenti e le informazioni trattati dall'Ente siano resi disponibili, autentici e integri;
- I dati personali, i dati sensibili e quelli giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2.2 Contesto di riferimento

Il piano di sicurezza, basato sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

- Le politiche generali e particolari di sicurezza da adottare all'interno dell'ente
- Le modalità di accesso al sistema di protocollo e gestione documentale
- Le misure di sicurezza operative adottate sotto il profilo organizzativo, procedurale e tecnico
- Le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

Al fine di garantire la sicurezza dell'impianto tecnologico, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, l'Ente ha adottato le misure tecniche e organizzative di seguito specificate:

- Protezione periferica della Intranet dell'amministrazione a mezzo firewall fisico;
- Protezione dei sistemi di accesso e conservazione delle informazioni;
- Assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- Cambio delle password con frequenza almeno trimestrale durante la fase di esercizio
- Piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- Conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e lontani da quelli in cui è installato il sistema di elaborazione di esercizio;
- Gestione delle situazioni di emergenza informatica attraverso risorse qualificate;
- Monitoraggio del sistema server e client con agent di controllo continuo.
- Impiego e manutenzione di un adeguato sistema antivirus;
- Uso di codici identificativi (o altre soluzioni) dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli inintelligibili a chi non è autorizzato ad accedervi;
- Impiego di idonee misure di sicurezza anche nel caso di supporti analogici contenenti banche di dati sensibili e giudiziari;
- Archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log contenenti le informazioni sulle operazioni effettuate da

ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali riferiti agli accessi registrati nel log del sistema operativo, e quelli registrati dal sistema di controllo delle modifiche sui dati più importanti dal sistema di protocollazione e gestione dei documenti, saranno consultabili in caso di necessità dalle forze dell'ordine.

2.3 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.

2.4 Gestione dei documenti informatici - aspetti di sicurezza

I documenti dell'Ente sono gestiti attraverso il sistema di protocollo e gestione documentale IRIDEDOC.

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato nelle modalità descritte nel precedente paragrafo 2.2.

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'amministrazione e gali 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.

2.4.1 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 del Dirigente, Funzionario in posizione organizzativa o del dipendente ritenuto più idoneo.

Nella conduzione del sistema informativo è responsabile del trattamento dei dati il Dirigente, Funzionario in posizione organizzativa o del dipendente ritenuto più idoneo.

È in facoltà del Responsabile di avvalersi della delega di funzioni a dipendenti dell'Ente o a terzi, in possesso dei necessari requisiti di competenza e professionalità tecnica.

2.4.2 Componente fisica e infrastrutturale della sicurezza

La sede è organizzata in due diverse aree:

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

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

- L'accesso è controllato e consentito soltanto al personale autorizzato per motivi di servizio;
- 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 procedura di registrazione. 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 in modo certo con sistemi di autenticazione forte;

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

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

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

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

- Porte blindate
- Armadi ignifughi
- Impianti elettrici verificati
- Luci di emergenza

- Sistemi di condizionamento per il raffreddamento delle apparecchiature
- Continuità elettrica del server garantita da apposito UPS,
- Continuità elettrica per i soli computer client degli uffici operativi;
- Controllo periodico di efficienza degli UPS
- Estintori
- Controllo dell'attuazione del piano di verifica periodica sull'efficacia dei sistemi di sorveglianza e degli estintori

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

2.4.3 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)

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

Il server applicativo è in sintesi il servizio di rete che ospita il software di 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" e solamente se dotato di specifiche credenziali e autorizzazioni al sistema IRIDEDOC.

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

Le ridotte dimensioni dell'Ordine e la necessità di distribuire le attività di protocollo e gestione documentale a tutti i dipendenti, rendono di fatto non necessaria la stratificazione di diversi livelli

di autorizzazione fatta a livello di documenti. Quindi tutti i dipendenti abilitati alla protocollazione, hanno accesso a tutti i documenti gestiti dal sistema documentale. Per questo sono stati opportunamente edotti sulle responsabilità e formati in merito agli aspetti della sicurezza informatica. Sono gestiti livelli di autorizzazione differenziati per quegli utenti che devo accedere al sistema per la sola consultazione (visualizzazione). Anche in questo caso disponibile in modo indifferenziato a tutti i documenti.

Ciò nonostante il sistema di gestione del protocollo e gestione documentale consente di stratificate 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'ordine 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.

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.

2.4.4 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)
- Dalle registrazioni di IRIDEDOC

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 sincrona dei file su storage ospitato in altra sede o in cloud.

2.4.5 Criteri di utilizzo degli strumenti tecnologici

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

Gli utenti interni autorizzati ad utilizzare il software di protocollo, operano nel rispetto 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 ed 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;
- Le password dovranno avere le seguenti caratteristiche:
  - Lunghezza minima 8 caratteri
  - Caratteri di tipo alfanumerico e deve contenere almeno un numero, una lettera minuscola e una lettera maiuscola (non si possono usare simboli)
  - Non deve essere riconducibile a:
  - Nome o cognome proprio o di un collega o di un famigliare
  - Identificativi di ufficio, di area, di servizio o del Comune, in modo parziale o completo
  - Date di nascita, codici fiscali o altri elementi che ne facilitino l'individuazione
  - Validità 90 giorni.

2.5 Trasmissione e interscambio dei documenti informatici - aspetti di sicurezza

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

In riferimento al cap. 4, 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 • Utilizzo del protocollo HTTPS che garantisce la piena riservatezza	Alto	no
Interoperabilità	• Meccanismo di trasmissione attraverso la Posta elettronica	Alto	no

	certificata con funzionalità interoperabili		
Posta elettronica ordinaria	• 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
Fax server	• Meccanismo di trasmissione che utilizza la tecnologia della posta elettronica ordinaria	Basso	si

2.6 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.

Per le specifiche relative alla sicurezza per l'accesso al Software di protocollo e di gestione documentale, si fa riferimento al ***cap. 7 DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO.***

2.7 Politiche di sicurezza adottate dall'Ente

Le politiche di sicurezza sono riportate nel Documento programmatico sulla sicurezza 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 predisposto dal Garante *(Allegato 10 - Modello di segnalazione data breach PA).*

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

Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dall'Agenzia per l'Italia digitale o a seguito dei risultati delle attività di audit.

2.8 Servizio archivistico (doc. analogici)

La sede dell'archivio dell'Ente è individuata nei locali al piano primo e secondo e negli armadi ubicati negli uffici della sede istituzionale dell'amministrazione medesima.

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.

Sono state altresì regolamentate le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.

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.

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 dalla normativa vigente, dagli organi ed uffici dell'Ente medesimo nello svolgimento dell'attività istituzionale.

In ottemperanza a quanto indicato dal Codice dell'Amministrazione Digitale, che prevede l'uso delle tecnologie dell'informazione e della comunicazione per organizzare la propria attività amministrativa, l'Ente sta progressivamente evolvendo verso la formazione, gestione, e trasmissione dei documenti informatici.

Per agevolare il processo di formazione dei documenti informatici e favorire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'Ente tenderà a rendere disponibili per via telematica moduli, formulari elettronici e non elettronici.

Ciò premesso, il documento amministrativo va distinto in:

- Documento analogico
- Documento informatico

Tutti i documenti originali, indipendentemente dal loro supporto, sono tra loro connessi da speciale vincolo originario, necessario e determinato e costituiscono l'archivio dell'Ente.

3.2 Formazione dei documenti - aspetti diplomatici

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

Deve essere curata, per quanto possibile, la standardizzazione della forma e dei contenuti dei documenti, attenendosi a formulari tipici, sottoposti ad approvazione del dirigente/funzionario competente.

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 e dicitura "Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Genova" nelle forme stabilite dall'amministrazione.
   - Indirizzo completo: via/piazza, numero civico, CAP, città
   - Codice fiscale (e partita IVA se presente)
   - Numero di telefono ed eventuale fax
   - Indirizzo istituzionale di posta elettronica
   - Indirizzo di posta elettronica certificata
2. Individuazione e descrizione del documento: (queste informazioni sono già presenti nei metadati del protocollo)
   - Numero di protocollo
   - Data di protocollo (giorno, mese, anno)
   - Eventuale numero del registro (repertorio)
   - Indice di classificazione: titolo, classe
   - Numero degli allegati
   - Numero e data del documento cui si risponde
   - Oggetto del documento
3. Individuazione del destinatario del documento (se è un documento in uscita):
   - Cognome e nome (per le persone) Denominazione (per gli enti e le imprese) e il Codice Fiscale/P.I.
   - A seconda dei casi:
     Indirizzo completo: via/piazza, numero civico, CAP, città
     Indirizzo informatico (Pec…)
4. Individuazione del Responsabile del Procedimento Amministrativo (RPA):
   - Cognome, nome e qualifica del Responsabile del Procedimento Amministrativo che nel caso dell'Ordine dei medici di Genova è sempre il Presidente, che dirige l'attività degli uffici (art. 29 dpr 221/50)
   - Sottoscrizione (firma autografa o digitale)

3.3 Formazione dei documenti - aspetti operativi generali

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

Ogni documento amministrativo:

- 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
- Normalmente fa riferimento ad uno o più fascicoli

3.4 Formazione del documento amministrativo 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 diplomatici sopra descritti.

Un documento analogico può essere convertito in documento informatico ai sensi dell'art. 22 del D.lgs. 82/2005.

3.5 Formazione del documento informatico e del documento amministrativo informatico

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

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

Il documento informatico viene formato mediante una delle seguenti principali modalità:

- Redazione tramite l'utilizzo di appositi strumenti software;
- Acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- Registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- Generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

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

- Sottoscrizione con firma digitale, ovvero con firma elettronica qualificata

- Apposizione di una validazione temporale
- Trasferimento a soggetti terzi con Posta Elettronica Certificata con ricevuta completa
- Memorizzazione su sistemi di protocollo e gestione documentale che adottino idonee politiche di sicurezza
- Versamento ad un sistema di conservazione

Al documento informatico immodificabile e ai documenti soggetti a registrazione particolare vengono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo dei metadati è costituito da:

A. Identificativo univoco e persistente
B. Riferimento temporale
C. Oggetto
D. Soggetto che ha formato il documento
E. Destinatario
F. Impronta del documento informatico
G. Metadati aggiuntivi stabiliti dall'Ente a fini gestionali e conservativi

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

H. Numero di protocollo
I. Data di protocollo
J. Mittente - destinatario
K. Oggetto
L. Data e protocollo del documento ricevuto, se disponibili
M. Impronta del documento informatico
N. Metadati aggiuntivi stabiliti dall'Ordine a fini amministrativi, gestionali e conservativi

3.5.1 La firma elettronica (avanzata, qualificata, digitale, automatica)

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

Per l'apposizione della firma digitale, L'Ente si avvale dei servizi di un'autorità di certificazione iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'Agenzia per l'Italia Digitale (AgID).

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 ed in particolare, dove possibile, nel formato standard PDF (quando possibile PDF/A).

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.

Le verifiche delle firme digitali dei documenti prodotti o ricevuti avviene attraverso l'utilizzo di software rilasciati gratuitamente, secondo la normativa, da enti certificatori.

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.

3.5.1.1 La Firma Elettronica Remota Automatica Massiva (FERAM)

Qualora fosse richiesta la firma dei documenti da conferire in conservazione, 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"[2], 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:

- Solo il responsabile della gestione documentale può attribuire potere di firma ad un utente del sistema
- Solo il responsabile della gestione documentale ha accesso alle configurazioni di sistema per l'assegnazione dell'utente per le fasi di firma massiva
- 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 ad un singolo documento

3.5.2 La marcatura 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)

3.5.3 Tipologie di formato del documento informatico

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

FORMATO	ESTENSIONE	STANDARD DI RIFERIMENTO
PDF - PDF/A	.pdf	ISO 32000-1 (PDF)

[2] Fonte documenti Namirial

		ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
File grafici	.tif, .jpeg, .jpg, .bmp, .png	ISO 12639 ISO 12234 ISO/IEC 10918:1
Office Open XML (OOXML)	.docx, .xlsx, .pptx	ISO/IEC DIS 29500:2008
Open Document Format	.odt, .ods, .odp, .odg, .odb	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
XML	.xml Derivati da XML: .svg	ISO 8879 – SGML Specifiche W3C
TXT	.txt	/
Formati messaggi di posta elettronica	.eml	RFC 2822 - MIME RFC 1847 - S/MIME
File audio	.mp3	
File video	.avi .mpeg4	
File compressi	.zip, .rar	
Documento firmato con firma elettronicaCAdES	.p7m	

Eventuali integrazioni al presente elenco vengono definite in considerazione di specifiche previsioni normative o tecniche.

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

La scelta dei formati è stata effettuata considerando che essa, come da previsione normativa, deve garantire la leggibilità e la reperibilità del documento informatico nell'intero ciclo di vita dello stesso

Eventuali integrazioni al presente elenco sono definite in considerazione di specifiche previsioni normative o tecniche.

Nel caso pervengano documenti su formati diversi da quelli elencati, questi non saranno presi in considerazione dall'Uff. di protocollo, il quale avrà cura di avvisare il soggetto produttore in modo da permettere un nuovo invio con formato tra quelli previsti.

3.5.4 Documenti contenenti collegamenti ipertestuali

Nel caso pervengano documenti contenenti collegamenti ipertestuali (link) a pagine web o file in qualsiasi formato, il servizio gestione documentale avrà cura di avvisare il soggetto produttore

affinché provveda ad un nuovo invio, inserendo in allegato (in formato consentito) i file e/o la stampa in formato PDF delle pagine web di destinazione dei collegamenti ipertestuali.

3.5.5 Interoperabilità

L'Ente deve sempre effettuare una valutazione di interoperabilità che tenga conto dei seguenti fattori: formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo, garantendo sempre la gestione dei formati classificati nell'Allegato 2 "Formati di file e riversamento" come "generici", secondo la distinzione introdotta nell'Allegato 2 tra formati di file generici e specifici.

Qualora l'ordinamento giuridico preveda, per particolari categorie di documenti elettronici, degli obblighi relativamente all'uso di formati di file specifici ovvero di vincoli aggiuntivi su formati generici (quali, ad esempio, l'uso di particolari dialetti o specializzazioni per formati generici), l'Ente accetterà i suddetti documenti elettronici solo se prodotti nei formati o con i vincoli aggiuntivi obbligatori.

La valutazione di interoperabilità è effettuata in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento" delle linee guida di AGID. La valutazione di interoperabilità, in quanto parte della gestione documentale, viene effettuata periodicamente e, comunque, ogni anno, allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati.

A seguito della valutazione di interoperabilità, l'Ente valuterà l'esigenza o l'opportunità di effettuare o pianificare il riversamento dei file da un formato di file ad un altro formato, sempre tenendo in considerazione quanto previsto nel punto precedente. Il riversamento è effettuato in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento".

4 MODALITÀ DI SCAMBIO DEI DOCUMENTI

Il presente capitolo fornisce indicazioni per lo scambio di documenti all'interno ed all'esterno dell'Ente (AOO).

Tutti i documenti pervenuti all'Ente devono essere registrati, segnati, classificati e smistati alla Persona/Ufficio di competenza contestualmente alla loro ricezione nella stessa giornata in cui sono pervenuti.

La corrispondenza in ingresso può essere acquisita dall'Ente con diversi mezzi e modalità, in base alla modalità di trasporto utilizzata dal mittente. Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in:

- Ricevuto (in entrata)
- Inviato (in uscita)
- Interno

4.1 Documenti in entrata

4.1.1 Ricevuti o prodotti su supporto analogico

I documenti ricevuti su supporto analogico possono essere recapitati attraverso:

- **Posta convenzionale e posta raccomandata:** I documenti analogici ricevuti tramite il servizio postale presso la casella postale dell'Ente pervengono al Protocollo generale al più tardi entro le ore 14.00 di ogni giorno lavorativo. Il Protocollo generale provvede a separare i documenti esclusi dalla registrazione a protocollo *(per le tipologie di esclusione si rimanda allegato 7)* e all'apertura della corrispondenza. Provvede immediatamente alla registrazione a protocollo attraverso il sistema di protocollo informatico e gestione documentale e alla segnatura a mezzo etichetta dei singoli documenti dando priorità a quelli individuabili come urgenti.
- **Fax:** I documenti ricevuti tramite fax sono da considerarsi a tutti gli effetti analogici, poiché solo la loro modalità di trasmissione è telematica. Tuttavia l'Ente sta evolvendo verso la tecnologia del fax server, che presuppone il trattamento del documento in modalità esclusivamente digitale, prevedendo l'inoltro dello stesso sul sistema di gestione documentale.
- **Brevi manu:** consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata allo sportello del Protocollo generale aperto al pubblico durante l'orario di apertura. Gli operatori provvedono alla registrazione, segnatura e scansione dei documenti, con relativo smistamento alle UOR di competenza nello stesso giorno di ricezione. Su richiesta dell'interessato viene rilasciata apposita ricevuta della avvenuta registrazione mediante il programma di protocollo informatico o, in alternativa, viene apposta la segnatura di protocollo sulla copia già in possesso dell'utente apponendo la dicitura "copia per l'utente".

In tutte e tre le casistiche avviene un processo di scansione e inserimento del documento all'interno del sistema di protocollo informatico.

4.1.2 Ricevuti o prodotti su supporto informatico

I documenti informatici possono essere recapitati/trasmessi tramite:

- **Caselle di posta elettronica istituzionale**. La casella istituzionale dell'Ente è protocollo@omceoge.org;
- **Posta elettronica certificata**: la casella PEC dell'Ente è ordinemedici@pec.omceoge.eu; inoltre sono istituite una o più caselle PEC per ogni settore, pubblicate sull'Indice delle Pubbliche Amministrazioni e sul sito istituzionale www.omceoge.org.

4.2 Documenti inviati

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

4.2.1 Inviati su supporto analogico

I documenti analogici sono trasmessi attraverso:

A. Posta convenzionale o posta raccomandata
B. Brevi manu
C. Notifica
D. Posta tradizionale
E. Fax

Il documento in uscita viene normalmente redatto in unica copia, sottoscritta dal Legale rappresentante dell'ente o da un suo delegato, registrata nel sistema di protocollo e spedita. Copia di tale documento viene trattenuta presso il produttore ed inserito nel fascicolo relativo all'affare o al procedimento amministrativo trattato.

Il documento analogico viene sempre scansionato ed associato al relativo protocollo compilando manualmente i metadati necessari ed associandolo al relativo fascicolo elettronico, questo per consentire che il sistema di gestione documentale informatizzato sia il contenitore univoco anche dei documenti analogici e ne permetta l'inclusione nei relativi fascicoli elettronici.

4.2.2 Inviati su supporto informatico

I documenti informatici sono trasmessi attraverso:

A. Posta elettronica certificata (PEC)
B. Caselle di Posta elettronica

I documenti sono trasmessi sempre per posta elettronica certificata e solo quando non possibile con altri sistemi tra quelli elencati. Infatti solo la trasmissione dalla casella di PEC istituzionale ad una casella PEC del destinatario costituisce evidenza giuridico-probatoria dell'invio e della consegna del messaggio (art. 47 CAD).

4.2.2.1 Documento Cartaceo inviato elettronicamente

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

4.2.2.2 Documento Digitale inviato elettronicamente

Se informatico inviato tramite posta elettronica certificata o canali digitali, viene redatto tramite un software adeguato (es. elaborazione testi), sottoscritto con firma digitale, registrato,

acquisito nel sistema di protocollo, associato al protocollo stesso ed al fascicolo relativo. L'operatore provvede poi all'invio del file alla posta elettronica certificata del destinatario.

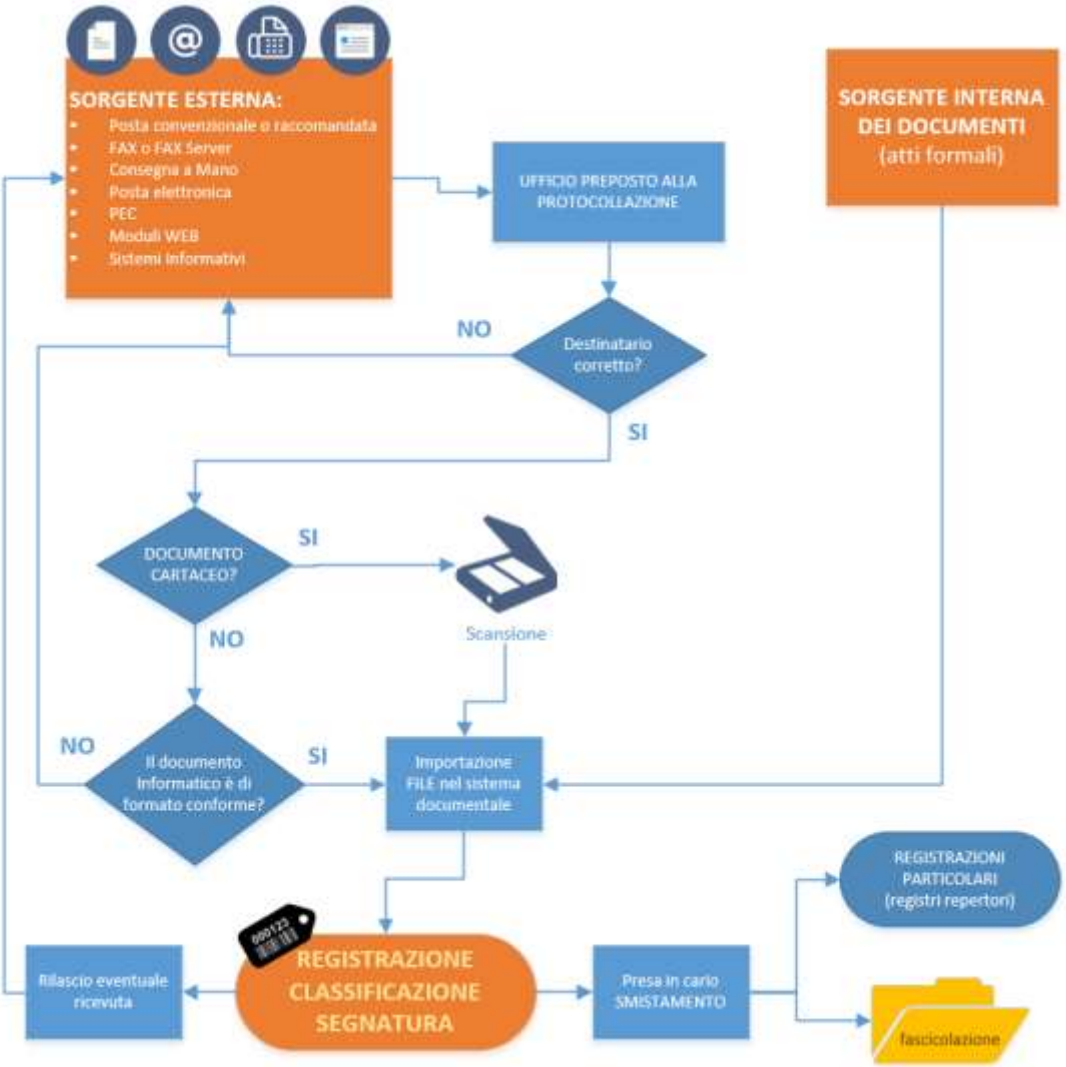
4.3 Descrizione del flusso di lavorazione dei documenti

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

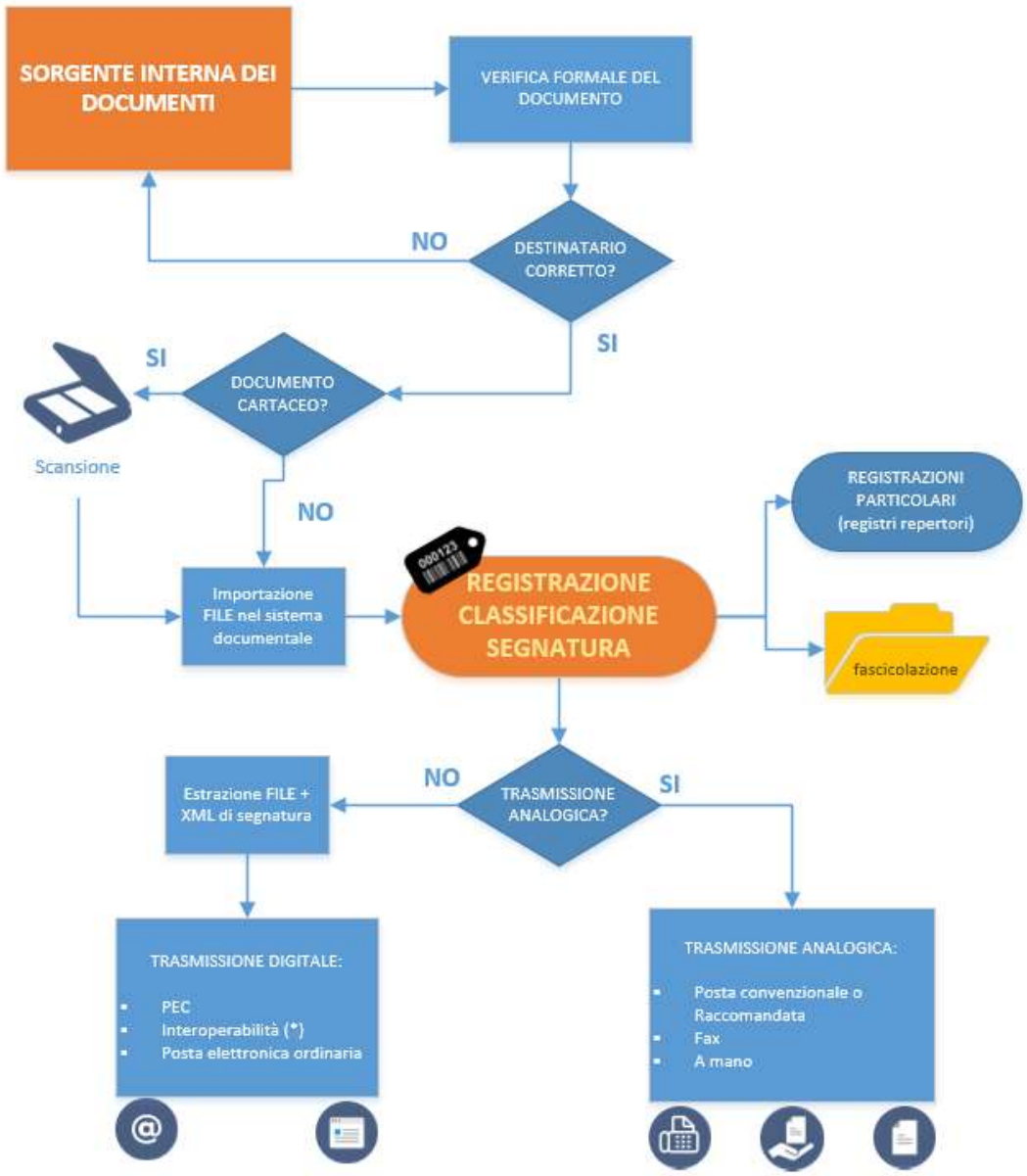
Essi si riferiscono ai documenti:

- Ricevuti dall'Ordine, dall'esterno
- Inviati dall'Ordine, all'esterno

4.4 Flusso in entrata



4.5 Flusso in uscita



(*) non ancora implementato o in fase di implementazione

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, dai quali possano nascere diritti, doveri o legittime aspettative di terzi, devono essere registrati sul protocollo informatico unico dell'Ordine, con le modalità e le eccezioni di seguito illustrate.

La registrazione è l'operazione di memorizzazione delle informazioni fondamentali relative al contenuto, alla forma, all'autore e alla modalità di trasmissione di un documento.

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

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

Al fine di ottenere un unico punto di ricerca e gestione dei documenti, si dà particolare spinta alla registrazione di protocollo, anche dei documenti sottoposti ad altre particolari registrazioni. Pratica che diventa obbligatoria in caso di documento digitale, al fine di poter poi procedere al conferimento dei documenti in Conservazione Digitale.

La registrazione a protocollo riguarda il singolo documento; non può riguardare per alcun motivo il fascicolo, in quanto è vietata la registrazione cosiddetta "sintetica". Quindi il numero di protocollo individua un singolo documento.

I documenti potranno essere poi raccolti in fascicoli elettronici o ibridi.

5.2 Registro di protocollo

Il registro di protocollo[3], è un documento informatico prodotto e redatto secondo le modalità previste dalla vigente normativa.

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

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

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

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

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

Non è consentita la protocollazione di un documento già protocollato, salvo casi inevitabili di invii multipli da parte del mittente.

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

Il registro di protocollo giornaliero riporta tutti i protocolli generati nell'arco della singola giornata come indicato nel documento AGID dal titolo "PRODUZIONE E CONSERVAZIONE DEL REGISTRO GIORNALIERO DI PROTOCOLLO" del 01/10/2015, tale registro deve ricomprendere le informazioni minime richieste dall'art. 53, co. 1, del DPR 445/2000 e dalla Circolare n. 60 del 2013.

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

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

Di conseguenza, il registro giornaliero di protocollo deve contenere, 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 alla giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Il software di gestione del protocollo e dei documenti, prevede la possibilità di stampare anche registri inerenti più giorni, da utilizzare a bisogno.

Per finalità di consultazione e ricerca interna viene inoltre prodotta una stampa annuale e consolidata del registro di protocollo. Il termine "consolidata" si riferisce al fatto che, in caso di eventuali modifiche ai dati di protocollo (oggetto, classificazione, mittente/destinatario, direzione), fermo restando la tracciatura della modifica da parte del sistema di gestione documentale, nel registro annuale verranno riportati i dati inerenti l'ultima revisione/modifica.

5.2.1 Altri registri presenti nel sistema di gestione documentale

Il sistema di gestione documentale è in grado di gestire diversi registri oltre a quello di protocollo. Di seguito ne viene schematizzato l'elenco:

Codice	Registro	Descrizione
001	PROTOCOLLO	Registro ufficiale di protocollo
002	REGISTRAZIONI INTERNE	Registro non formale che consente di inserire nel sistema di gestione documentale documenti che non hanno necessità di protocollazione ma che si vuole reperibile nel sistema di gestione generale dei documenti. Questo anche nella necessita di associare tali documenti ad un fascicolo.
003	REGISTRO DEI FASCICOLI NON PERSONALI (repertorio)	Registro che raccoglie i fascicoli non personali generati (d'affare, di attività, di procedimento amministrativo)
004	REGISTRO DEI FASCICOLI PERSONALI (repertorio)	Registro che raccoglie i fascicoli personali (persona fisica, persona giuridica)

5.3 Elementi della registrazione di protocollo

Gli elementi obbligatori, in quanto giuridicamente rilevanti della registrazione a protocollo sono:

- **Il numero di protocollo**, generato automaticamente dal sistema e registrato in forma non modificabile;
- **La data di registrazione di protocollo**, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- **Il mittente** per i documenti ricevuti o, in alternativa, **il destinatario o i destinatari** per i documenti spediti, registrati in forma non modificabile;
- **L'oggetto del documento**, registrato in forma non modificabile;
- **La data e il numero di protocollo del documento ricevuto**, se disponibili;
- **L'impronta del documento informatico**, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il

contenuto, registrata in forma non modificabile. Come descritto a cap. 5.2 punto F, l'impronta viene calcolata anche per i documenti analogici scansionati ed associati al protocollo.

- **Indice di classificazione (classe documentale)**

Gli elementi non obbligatori, ma funzionali qualora disponibili sono:

- Livello di riservatezza
- Numero di protocollo del documento ricevuto
- Data del documento ricevuto
- Modalità di trasmissione
- Numero degli allegati
- Numero raccomandata
- Annotazioni

5.4 Modalità di registrazione di protocollo

I documenti pervenuti all'Ordine da altri soggetti giuridici sono registrati una sola volta, salvo casi di invii multipli non individuabili da parte del mittente, come documenti in entrata.

I documenti inviati dall'Ente ad altri soggetti giuridici sono registrati una sola volta come documenti in uscita.

Qualora fosse necessario, possono essere protocollati anche "documenti Interni" al fine di darne esistenza giuridica e data certa.

In seguito alla registrazione i documenti analogici vengono sempre acquisiti nel sistema di protocollo tramite procedura di scansione. I documenti informatici vengono acquisiti nel sistema di protocollo attraverso le modalità descritte nel capitolo 4.

Il responsabile del procedimento o funzionario/direttore dell'Ente, prende visione quotidianamente, tramite il sistema informatico, dei documenti pervenuti e procede alla loro fascicolazione o assegnazione.

In caso di documenti con particolari caratteristiche di urgenza o rilevanza, potrà essere data notifica del nuovo protocollo anche attraverso mail interne.

5.5 La segnatura di protocollo

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

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

A. Codice identificativo dell'amministrazione
B. Codice identificativo dell'area organizzativa omogenea
C. Codice identificativo del registro

D. Progressivo registrazione
E. Data di registrazione

Ulteriori informazioni previste sono:

A. Indicazione della UOR dell'Ordine responsabile del documento prodotto.
B. Identificazione degli allegati
C. Anno
D. Titolo
E. Classe

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, la classificazione, il numero di fascicolo.

Opzionalmente potrà riportare un codice a barre o Qrcode, che permetterà l'associazione del documento acquisito mediante lo scanner, alla registrazione di protocollo.

Qualora il documento venga prodotto in formato nativo digitale il numero di protocollo è indicato nel nome del file e nell'oggetto della mail nel caso di trasmissione con posta elettronica.

5.5.1 Funzionalità non attive ma programmate dall'Ordine

Al fine di facilitare l'interoperabilità tra le PA, l'Ente si attiverà per garantire che i dati relativi alla segnatura di protocollo di un documento trasmesso da una AOO siano associati al documento stesso e contenuti, nel messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema, definito e aggiornato periodicamente dall'Agenzia per l'Italia digitale.

All'interno del file XML dovranno essere contenute anche le seguenti informazioni minime:

A. L'oggetto
B. Il mittente
C. Il destinatario o i destinatari

La segnatura di protocollo è prerequisito per permette di realizzare un sistema per l'interoperabilità tra i sistemi di gestione informatica dei documenti di amministrazioni diverse, automatizzando, fino al massimo livello possibile, la registrazione di protocollo di documenti informatici provenienti da altri sistemi interoperabili.

5.6 Documenti soggetti a registrazione particolare (Repertoriazione)

Possono essere esclusi dall'obbligo di registrazione di protocollo generale le tipologie di documenti soggetti a registrazione particolare.

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

- Tipologia del registro o repertorio
- Numero di registro o repertorio (cronologico e progressivo)
- Data
- Elementi identificativi dell'atto (soggetto o soggetti; oggetto)
- Eventuali dati di classificazione e di fascicolazione
- Annotazioni

5.7 PROCEDURE SPECIFICHE NELLA REGISTRAZIONE DI PROTOCOLLO

5.7.1 Protocolli 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.

I documenti Riservati sono accessibili solo al personale in possesso di adeguate autorizzazioni.

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

Un ferreo controllo nel rilascio delle credenziali di accesso, consente un adeguato livello di sicurezza ed accesso controllato.

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

Il responsabile della gestione documentale monitora periodicamente l'adeguatezza del sistema organizzativo e del software utilizzato per la registrazione di protocollo e gestione documentale. Particolare riguardo viene concesso agli aspetti della sicurezza e riservatezza.

I documenti potranno essere classificati come riservati se appartengono alle seguenti tipologie:

- Documenti relativi a vicende di persone o a fatti privati o particolari (dati sensibili, come definiti dalla D. lgs. 196/2003);
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati o procurare pregiudizio a terzi o al buon andamento dell'attività amministrativa (tipologie documentarie definite dalla Legge 241/1990, art. 24).

Tali documenti appartengono al cosiddetto protocollo riservato, costituito dalle registrazioni sul protocollo informatico unico dell'Ordine il cui accesso è consentito solamente alle persone autorizzate, in rapporto alle tipologie di procedimento amministrativo o alle tipologie documentarie dalle stesse trattate.

Le tipologie di documenti da registrare nel protocollo riservato saranno codificate all'interno del sistema di protocollo informatico a cura del responsabile del Servizio archivistico dell'Ordine, di concerto con il responsabile/direttore dell'Ordine. Le procedure adottate per la gestione dei documenti e dei procedimenti amministrativi ad accesso riservato, comprese la registrazione, la

segnatura, la classificazione e la fascicolazione, saranno le stesse adottate per gli altri documenti e procedimenti amministrativi. L'operatore che effettuerà la registrazione di protocollo di un documento attribuirà allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal sistema. Il sistema può associare il livello di riservatezza in relazione alla classe documentale assegnata al protocollo/documento.

In modo analogo, il RPA che effettuerà l'operazione di apertura di un nuovo fascicolo ne fisserà 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 sarà acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi fosse stato assegnato un livello di riservatezza minore od uguale. I documenti che invece avranno un livello di riservatezza superiore lo mantengono.

5.7.2 Documenti esclusi dalla registrazione di protocollo

Il DPR 445/2000 prevede che tutti i documenti in entrata e in uscita e tutti i documenti informatici siano registrati a protocollo, con alcune eccezioni. Tra le eccezioni troviamo i documenti soggetti a registrazione particolare di cui al precedente paragrafo 5.6.

Tali esclusioni devono comunque essere considerate come una facoltà, non un obbligo, anche in relazione a quanto riportato nel capitolo 5.6.

5.7.3 Annullamento delle registrazioni di protocollo

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

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

5.8 CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO

5.8.1 Lettere anonime

La lettera anonima proveniente tramite i canali postali, una volta aperta e attestata l'assenza di ogni riferimento al mittente, viene posta all'attenzione del Segretario/Direttore generale 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 (indicando nel campo mittente "anonimo") ovvero alla sua eliminazione.

5.8.2 Lettere prive di firma

Le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali. La funzione notarile del protocollo (cioè della registratura) è quella di attestare data e provenienza certa di un documento senza interferire su di esso.

È poi compito del responsabile/direttore dell'Ente valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

5.8.3 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".

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

5.8.4 Documenti inerenti a gare di appalto confezionati su supporti cartacei

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo" o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata alla UOR competente.

È compito della stessa UOR provvedere alla custodia delle buste o involti protocollati, con mezzi idonei, sino all'espletamento della gara stessa, salvo diverse indicazioni che devono essere fornite all'Ufficio protocollo.

Dopo l'apertura delle buste la UOR che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.

Per motivi organizzativi tutte le UOR sono tenute ad informare preventivamente il Responsabile del Servizio archivistico in merito alle scadenze di concorsi, gare, bandi di ogni genere.

5.8.5 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) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati sul protocollo generale e sono inseriti nel fascicolo relativo.

5.8.6 Documenti pervenuti per errore all'Ordine

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

5.8.7 Trattamento dei documenti con oggetto o smistamento plurimo

Ogni documento, anche se in più esemplari, deve essere individuato da un solo ed 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'ordine. 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 dagli altri destinatari. Qualora il documento sia già stato registrato si deve riportare la stessa segnatura anche sugli altri esemplari.

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, l'addetto alla registrazione deve individuare la classifica prevalente e smistare il documento acquisito a sistema alle UOR competenti.

Ogni documento in uscita deve obbligatoriamente trattare un solo oggetto (un solo argomento), deve necessariamente riferirsi ad un solo procedimento e quindi deve essere conservato in un unico fascicolo.

5.8.8 Documenti in partenza con più destinatari

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

Solo in casi eccezionali e qualora i destinatari siano in numero superiore a 10, si utilizza uno dei destinatari particolari, esempio: "ISCRITTI ALLA DATA DELL'INVIO" - Vedi elenco allegato alla registrazione". A discrezione del Responsabile del Protocollo nel caso in cui sia possibile potrà essere individuato un destinatario particolare anche per gruppi inferiori a 10.

Al fine di permettere una corretta protocollazione, nei casi di invio massivo di un documento ed utilizzo dei "destinatari particolari", Ufficio di protocollo procederà alla protocollazione del documento in modo da mantenere correlato il documento e la lista dei destinatari, associando al documento stesso un file contenente l'elenco dei destinatari.

5.9 Regole di smistamento e di assegnazione

L'operazione di smistamento consiste nell'assegnazione di un documento registrato alla UOR competente e al conseguente conferimento di responsabilità del relativo procedimento amministrativo.

Si adottano le modalità operative di seguito illustrate:

- Tutti i documenti analogici in entrata o in uscita registrati devono essere acquisiti in copia per immagine e associati alla registrazione di protocollo. Fanno eccezione i documenti che materialmente non possono essere sottoposti a scansione (a titolo meramente esemplificativo: volumi, registri, plichi, planimetrie di formato superiore all'A3, plastici, monete, ecc.). In questi casi si deve segnalare l'assenza degli allegati, nel campo "Note"
- Nel caso di documento analogico, l'originale sarà conservato nell'archivio generale dell'Ente;
- Nel caso di documenti informatici, l'originale sarà acquisito direttamente (salvo procedura di caricamento manuale) nel sistema di protocollo attraverso i canali previsti;
- Quotidianamente gli operatori e/o i responsabili verificano i documenti a loro assegnati;
- Il responsabile/direttore dell'Ente o qualsiasi altro soggetto dell'Ente in possesso delle adeguate autorizzazioni, visualizzano i documenti attraverso l'utilizzo del software di gestione documentale dell'Ente.
- Ogni soggetto provvede alla visione e alla gestione del documento assegnato e alla sua eventuale riassegnazione ad altro collega.

Dalla registrazione di protocollo, ai fini normativi e regolamentari, è possibile verificare i tempi di gestione ed i conseguenti riflessi sotto il profilo della responsabilità.

5.9.1 Procedure future non ancora implementate per lo smistamento e l'assegnazione

Si prevede in futuro di ampliare la gestione documentale con particolari funzioni di controllo dello stato della pratica/procedimento.

Tale sviluppo prevedrà l'uso di particolari work flow.

A titolo di esempio si prevede di poter disporre delle seguenti funzionalità:

- Il responsabile dell'UOR visualizza i documenti, attraverso l'utilizzo di IRIDEDOC
  - Visualizzare gli estremi del documento
  - Visualizzare il contenuto del documento
  - Individuare come assegnatario il RPA competente sulla materia oggetto dei documenti;
- Il RPA provvede alla visione e alla gestione del documento assegnato e mediante una delle seguenti azioni:
  - Riassegnazione: assegnazione ad altro ufficio o ad utenti del proprio ufficio
  - Rifiuto: restituzione del documento all'ufficio mittente in caso di errata assegnazione
  - Fascicolazione: inserimento nel fascicolo procedimentale.

Il sistema di gestione informatica dei documenti memorizzerà tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante definirà, ai fini normativi e regolamentari, i tempi e le modalità di gestione del flusso documentale ed i conseguenti riflessi sotto il profilo della responsabilità. La "presa in carico" dei documenti verrà registrata dal sistema in modo automatico e la data di ingresso dei documenti negli UOR di competenza coincide con la data di assegnazione degli stessi.

6 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

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

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

L'utilizzo del registro di emergenza deve essere autorizzato dal Responsabile del Servizio Archivistico (gestione documentale). In caso di assenza del responsabile del servizio provvede all'autorizzazione il vicario così 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 e dovrà essere successivamente salvato
2. Nel caso di impossibilità ad utilizzare i PC ci si avvarrà del modulo cartaceo di cui si allega fac simile 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 annotazioni ritenute rilevanti dal responsabile del protocollo informatico e della gestione documentale.

Prima di autorizzare l'avvio della procedura, il Responsabile del Servizio archivistico deve impostare e verificare la correttezza di data e ora sui rispettivi registri di emergenza. In caso di vicinanza alla data di fine anno solare, si tenga presente che ogni registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Il Responsabile del Servizio archivistico dovrà annotare nel protocollo informatico unico i periodi di attivazione del Registro di emergenza. Qualora nel corso dell'anno non si sia fatto ricorso al Registro di emergenza, deve annotarne anche il mancato uso.[4]

[4]L'annotazione avviene con la protocollazione di un documento che riporta le informazioni dei protocolli di emergenza. Si tratterà di un documento in Uscita con mittente l'Ente e destinatario lo stesso Ente.

Ogni documento è individuato dal numero assegnato nel Registro di emergenza, anno di registrazione, numero di protocollo nel formato stabilito; ad esempio: **RE01-2015-0000005.**
La segnatura del protocollo di emergenza deve essere apposta mediante timbro o altro dispositivo e riportare le informazioni desunte dal relativo registro.
Una volta ripristinata la piena funzionalità del sistema, il Responsabile del Servizio archivistico provvede alla chiusura dei registri di emergenza, annotando su ciascuno il numero di registrazioni effettuate e la data e ora di chiusura.
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.
L'utente adibito alla protocollazione, alla ripresa della piena funzionalità del sistema di protocollo informatico, provvede a riversare sul programma stesso tutte le registrazioni già eseguite sul registro di emergenza.
I documenti annotati nel registro di emergenza e trasferiti nel protocollo informatico unico recheranno, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo informatico unico. Al numero attribuito dal registro di emergenza si fa riferimento per l'avvio dei termini del procedimento amministrativo.

7 DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO

7.1 Descrizione funzionale ed operativa

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'amministrazione con particolare riferimento alle modalità di utilizzo nel contesto organizzativo dell'Ente.
La struttura modulare, che risponde ad esigenze di organizzazione e razionalizzazione delle componenti del sistema, è stata concepita per essere in grado di affrontare successive implementazioni, aggiornamenti o modifiche senza comprometterne l'impianto di base e le funzionalità già realizzate.
In relazione alla particolare struttura semplificata dell'Ordine (si veda cap. 1.1.1), il sistema consente di assegnare ogni documento ad un responsabile del procedimento (utente del sistema) e permette di ottenere la lista dei documenti a questo assegnati[5].
Ai sensi della normativa vigente sono disponibili funzioni per la produzione delle registrazioni di protocollo e relative ricerche, stampe, statistiche e reportistica anche ai fini del controllo di

[5] Mediante funzione di filtro in griglia.

gestione; funzioni per la produzione dei fascicoli informatici, dei relativi repertori (registri) e delle connesse funzionalità di ricerca.

Tutte le modalità funzionali ed operative sono descritte nella "guida utente" in linea del software di gestione documentale manuale adottato dall'Ente

7.1.1 Funzionalità future non ancora integrate

Anche se il sistema sembra per ora sufficiente alla gestione degli uffici, si prevede in futuro un maggiore sviluppo di tali funzionalità.

Ciò sarà possibile grazie a funzioni di amministrazione che consentono la gestione della struttura organizzativa (Organigramma), con i relativi ruoli operativi, definiti in base ai compiti assegnati agli utenti, ed a parallele funzioni di gestione delle scrivanie di lavoro virtuali a disposizione degli utenti.

Il sistema sarà integrato con tutti i canali di trasmissione informatica dei documenti previsti dall'Ente (posta elettronica, posta certificata, interoperabilità, fax server, istanze on-line), dai quali i documenti informatici vengono acquisiti a protocollo.

7.2 Abilitazioni di accesso

Gli utenti del servizio di protocollo e gestione documentale, in base agli uffici di appartenenza, ovvero in base alle rispettive competenze e ruoli, hanno autorizzazioni di accesso differenziate.

Ogni utente è quindi in possesso di:

- credenziale di accesso, costituita da:
  - **UserID**: parte Pubblica che permette l'identificazione dell'utente da parte del sistema;
  - **Password**: parte Privata o riservata di autenticazione;
- un insieme di autorizzazioni/abilitazioni di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

Le opzioni autorizzative sono un aspetto particolarmente delicato e nel contempo complesso che impongono una attenta analisi dei processi di lavoro al fine di garantire la necessaria appropriatezza del trattamento del dato.

Le abilitazioni possono essere assegnate per attribuire:

- La possibilità di accedere alle aree amministrative
- La possibilità di poter accedere a specifiche aree del sistema di gestione documentale
- La possibilità di poter accedere ai documenti di una classe documentale
- La possibilità di accedere al singolo documento

Al fine di garantire la corretta gestione della "catena della riservatezza", quando un utente non avesse accesso ad uno o ad un gruppo di documenti, questo implica che tale limitazione si estenda anche a tutti gli elenchi, griglie di ricerca e stampe che ne possano mostrare dettagli.
Nel caso il criterio di ricerca o la stampa includa tale documento, questo apparirà con i campi sensibili oscurati da "asterischi".
Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione degli uffici e del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'AOO, sono sottoposte a verifica, modifica, gestione e aggiornamento da parte del Responsabile della Gestione Documentale ovvero dal responsabile del Servizio Archivistico o delegate all'amministratore del sistema.
Come indicato dall'art. 61 del DPCM 445/2000, il sistema di gestione del protocollo informatico e gestione documentale adottato dall'Ente, tratta le abilitazioni al sistema in modo da permettere la distinzione tra abilitazione alla consultazione o abilitazione all'inserimento e modifica delle informazioni.
Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato, la cui password non è accessibile.
Le sessioni multiple con la stessa User ID sono proibite.

7.2.1 Ripristino delle credenziali private d'accesso

In caso di smarrimento della password l'utente contatta il Responsabile della Gestione Documentale ovvero il responsabile del Servizio Archivistico e fa richiesta di una nuova password per accedere al sistema di protocollo.

7.2.2 Effetti delle abilitazioni su Registro Giornaliero di Protocollo

La generazione del registro di protocollo giornaliero da parte di utente con limitazioni, può produrre un registro con dati oscurati (es. mittente, destinatario, oggetto, …). Tale registro potrebbe quindi non essere adatto al conferimento al conservatore.
Risulta importante che tale funzione sia svolta da utente in possesso di adeguate abilitazioni.

7.2.3 Catena della sicurezza del dato

I protocolli, ovvero i documenti trattati all'interno del sistema documentale e da classificare come riservati, possono ottenere[6] automaticamente tale condizione (in base alla configurazione del momento nel quale avviene l'operazione) in base all'appartenenza ad una classe documentale o alla scelta manuale dell'autore del protocollo che agisce sul singolo protocollo/documento

[6] Si intende ottenere per copia dalla configurazione fatta a livello di classe e disponibile al momento dell'assegnazione.

Fino a tale momento, eventuali documenti caricati nel sistema, ma non ancora protocollati, ovvero classificati o resi manualmente "riservati", sono a disposizione di tutti gli utenti abilitati a tale area del gestionale.

È quindi attuato dal responsabile della gestione documentale, un adeguato studio dei processi di lavoro e la stesura di adeguate procedure a cui gli utenti si dovranno attenere. Questo al fine di ridurre o eliminare ogni possibilità di perdita di riservatezza del dato nelle fasi di lavoro.

Sulla base di tale studio e valutate le diverse situazioni, il responsabile della gestione documentale può abilitare una particolare funzione del sistema di gestione documentale che limita la possibilità del trattamento del documento da protocollare al solo utente che ne ha fatto il caricamento nel sistema.

8 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

8.1 Protezione e conservazione degli archivi pubblici

8.1.1 Premessa

Ai sensi dell'art. 30 del D.lgs 42/2004, 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, 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 però tre fasi:

- **Archivio corrente**[7], composto dai documenti relativi ad affari in corso, conservati presso gli uffici (comprende fascicoli di persona fisica o giuridica);
- **Archivio di deposito**[8], composto dai documenti relativi ad affari cessati da meno di 40 anni conservati presso l'archivio di deposito presso l'Archivio generale dell'Ente, a determinate condizioni;

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

[8] 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)

- **Archivio storico**[9], composto dai documenti relativi ad affari cessati da più di 40 anni, selezionati per la conservazione permanente conservati presso l'Archivio generale dell'Ente, che funge da sezione separata.

Il presente capitolo riporta 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.

Il riferimento dell'Ente per l'attività di selezione è il *Piano di conservazione.*

Il titolario e il 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. Spetta ai vertici dell'amministrazione medesima adottare il titolario e il piano di conservazione con atti formali.

8.1.2 Misure di protezione e conservazione degli archivi pubblici

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

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

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

L'Ente adotta le misure previste dal D.Lgs 196/2003 a tutela delle informazioni, dei dati e dei documenti.

8.2 Titolario o piano di classificazione

8.2.1 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

[9] 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.

viene ricondotta la molteplicità dei documenti prodotti. Si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I° livello, II° livello, III° livello, etc.

L'Ente ha deciso di adottare un titolario a 2 livelli come suggerito dal gruppo di lavoro che ha seguito il "Progetto per la formulazione di proposte e modelli per la riorganizzazione dei comuni" consultabile dal sito DGA (Direzione generale degli archivi) al seguente indirizzo: http://www.archivi.beniculturali.it/index.php/cosa-facciamo/progetti-di-tutela/progetti-conclusi/item/551-archivi-dei-comuni

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 della funzione di governo dell'amministrazione ovvero dell'Ente.

Il titolario non è retroattivo: non si applica cioè, ai documenti protocollati prima della sua introduzione.

L'Ente Utilizza un Titolario di classificazione elaborato sulla base del documento prodotto dal Gruppo di Lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni e adeguato alle esigenze organizzative degli Ordini dei Medici Chirurghi e degli Odontoiatri da un gruppo di lavoro composto dalle segreterie di diverse province. Tale Titolario è adottato con Deliberazione n. 2 del 22 gennaio 2018 *(Allegato 11 Titolario di classificazione).*

Il titolario può essere aggiornato su proposta del Servizio archivistico e le eventuali modifiche e integrazioni entrano in vigore il 1° gennaio dell'anno seguente, previa informazione a tutti i soggetti abilitati all'operazione di classificazione dei documenti. Le modifiche, prima della loro ufficializzazione, sono approvate dal Consiglio Direttivo.

8.2.2 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, classe, al documento) è necessaria e preliminare all'attività di fascicolazione.

8.3 Fascicolazione

8.3.1 Fascicolazione dei documenti

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

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*" (definizione da bozza documento Agenzia delle Entrate *"Linee guida per la fascicolazione dei documenti elettronici" versione 1.0 20/01/2014*).

I documenti registrati e classificati nel sistema informatico (protocollati), indipendentemente dal supporto sul quale sono formati, possono essere riuniti in fascicoli.

Ogni documento, dopo la sua classificazione e protocollazione, viene se presente, inserito nel fascicolo di riferimento.

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

Il fascicolo viene sempre assegnato ad una voce del titolario, di norma viene aperto all'ultimo livello della struttura gerarchica del titolario. Il RPA (Responsabile del Procedimento Amministrativo) provvede anche all'archiviazione dei documenti all'interno del fascicolo.

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

Nel caso sussistano esigenze pratiche, il fascicolo può essere organizzato in sottofascicoli.

Ogni fascicolo è caratterizzato dai seguenti metadati:

- Anno
- Indice di classificazione, (cioè titolo, classe)
- Identificativo progressivo
- Oggetto del fascicolo
- Data di apertura del fascicolo
- Data di chiusura
- Nominativo del responsabile

8.3.2 Famiglie e tipologie di fascicolo

I fascicoli sono suddivisi in 2 famiglie:

1. Fascicoli inerenti persone fisiche o giuridiche
2. Fascicoli inerenti procedimenti

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

- Fascicoli relativi ad affari/attività
- Fascicoli relativi procedimenti amministrativi

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

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

8.3.2.1 Fascicoli relativi ad affari, attività o procedimenti amministrativi

I documenti sono archiviati all'interno di ciascun fascicolo, ed eventuale sotto 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. **La data di chiusura si riferisce alla data dell'ultimo documento prodotto.** Esso va archiviato rispettando l'ordine del repertorio, vale a dire il numeratore progressivo automatico generato nell'anno di apertura dal sistema di gestione documentale.

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

In caso di fascicolo cartaceo (analogico) o ibrido (analogico-digitale), sul raccoglitore analogico dei documenti vengono riportate le generalità del fascicolo generato informaticamente.

Al fine di rispettare i limiti imposti dalla normativa sulla PRIVACY, i dati riportati all'esterno del fascicolo analogico, al fine della sua identificazione e archiviazione, devono essere esclusivamente:

- Anno
- Identificativo progressivo
- Indice di classificazione, (cioè titolo, classe)
- Data di apertura del fascicolo
- Data di scadenza
- Data di chiusura
- AOO (e UOR)
- Nominativo del responsabile del procedimento/fascicolo

8.3.2.2 Fascicoli relativi a persone fisiche o giuridiche

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

L'apertura prevede la registrazione di alcune informazioni essenziali:

- Anno
- Identificativo progressivo
- Indice di classificazione, (cioè titolo, classe)
- Data di apertura del fascicolo
- Nominativo del responsabile del procedimento/fascicolo

I fascicoli delle persone fisiche e giuridiche costituiscono una serie archivistica autonoma.

8.3.2.3 Sotto fascicoli

Non esiste distinzione nella numerazione di fascicoli o sotto fascicoli. Questi ultimi risulteranno connessi al fascicolo padre da un semplice vincolo informatico.

8.3.3 Processo di assegnazione dei fascicoli

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

A seconda delle ipotesi, si procede come segue:

- Se il documento si ricollega ad 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 collegabile ad alcun fascicolo aperto, il soggetto preposto:
  - Esegue l'operazione di apertura del fascicolo
  - Collega la registrazione di protocollo del documento al nuovo fascicolo aperto

8.3.4 Repertorio (registro) 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)[10]

Lo strumento di gestione e organizzazione dei fascicoli è il Repertorio (registro) dei fascicoli, i cui elementi costitutivi 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

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

Regole aggiuntive:

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

- L'oggetto del fascicolo
- L'annotazione sullo stato del fascicolo, cioè se è aperto o chiuso
- Eventuali annotazioni

La numerazione dei fascicoli deriva sempre dalla gestione informatica. L'eventuale fascicolo "cartaceo" (analogico) che raccoglie i documenti cartacei (analogici), deve riportare in copertina il codice generato informaticamente (es. 2016-0000052).

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

8.4 Serie archivistiche e repertori

La serie archivistica[11] consiste in un raggruppamento di unità archivistiche (documenti, fascicoli, registri) riunite o per caratteristiche omogenee, quali la natura e la forma dei documenti, oppure in base alla materia trattata, all'affare, attività o al procedimento al quale afferiscono.

Fascicolo o sotto fascicoli costituiscono serie documentali distinte.

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

8.5 Registri gestiti al di fuori del sistema di protocollo

L'Ente gestisce altri registri non di protocollo, oltre a quello di protocollo informatico. A causa a volte della loro natura, a volte per semplici motivi storici, tali registri sono costituiti all'esterno della gestione informatizzata dei documenti e del protocollo informatico.

Tali registri sono:

- albo medici
- albo odontoiatri
- medici competenti
- 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 Commissione Medici e della Commissione Odontoiatri
- Verbali di altre Commissioni e gruppi di lavoro

[11] In un fascicolo la serie archivistica per documenti in esso contenuto, avviene progressiva per data inserimento nel fascicolo e calcolata alla chiusura del fascicolo stesso.

- Convenzioni e Protocolli d'intesa fra l'Ordine e altri Enti
- ….

L'Ente ha avviato 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.

8.6 Il fascicolo informatico, l'aggregazione documentale informatica e il fascicolo ibrido

L'Ente realizza il fascicolo informatico e l'aggregazione documentale informatica in maniera conforme ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico, secondo quanto stabilito dall'art. 41, c. 2 bis del D. Lgs n. 82/2005 e successive modifiche ed integrazioni.

La fascicolazione è un elemento fondamentale per attestare, in qualsiasi momento (nella fase corrente, di deposito o storica) quali documenti siano stati usati per portare a termine un determinato processo amministrativo e in che ordine siano stati prodotti o acquisiti dal responsabile del processo[12].

Il CAD definisce:

- **Il fascicolo informatico** come un'aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento;
- **L'aggregazione documentale informatica** come un'aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.

La formazione di un nuovo fascicolo informatico o di una nuova aggregazione avviene attraverso il sistema di gestione documentale che incrementa automaticamente il repertorio dei fascicoli attraverso la funzione di "apertura fascicolo".

L'insieme minimo dei metadati del fascicolo informatico e dell'aggregazione documentale informatica è il seguente[13]:

- Identificativo
- Amministrazione titolare
- Amministrazioni partecipanti
- Responsabile del procedimento

[12] Da *"ARCHIVISTICA" Teorie, Metodi,Pratiche*. A cura di Linda Giuva e Maria Guercio. Carocci editore.

[13] Come stabilito dall'art. 41, c. 2 bis del D. Lgs n. 82/2005

- Oggetto
- Documenti: elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità

Ci sono due registri dei fascicoli unici e pluriennali, uno per famiglia:

- Registro dei fascicoli personali e relativi sotto fascicoli
- Registro dei fascicoli NON personali e relativi sotto fascicoli

L'identificativo di ogni fascicolo, tenuto conto che la gestione avviene con strumenti informatici, è costituito dall'anno nel quale è generato il fascicolo, ed un progressivo all'interno dell'anno di appartenenza. Tale progressivo si stabilisce che venga generato in modo cronologico progressivo all'interno dell'anno solare.

Sia fascicoli che sotto fascicoli acquisiscono la numerazione progressiva in base alla loro creazione in modo progressivo e indifferenziato.

Ogni fascicolo può in più avere un "identificativo univoco informatico" generato al solo scopo di consentire un'efficiente e corretta gestione informatica. Tale identificativo è generato secondo le regole stabilite dal produttore del software e viene esposto nelle maschere o nelle stampe in base a scelte tecniche del produttore o dell'Ente.

Il software di gestione documentale e del protocollo informatico, per i fascicoli personali, identifica come "apertura del fascicolo" il momento in cui viene inserito il primo documento oppure viene creato il primo sotto fascicolo.

Esempio repertorio fascicoli 2015

Anno	**Numeratore**	**Data**	**Classe**	**Oggetto**	**Responsabile**	**Contenuto nel fascicolo** (se questo campo è valorizzato la riga si riferisce ad un sottofascicolo)
2015	00000001	03/01/2015	01.03	oggetto1	……	……
2015	00000002	08/01/2015	05.08	oggetto2	……	2015-0000001 oggetto1
2015	00000003	02/02/2015	03.11	oggetto3	……	……

Esempio repertorio fascicoli 2016

Anno	**Numeratore**	**Data**	**Classe**	**Oggetto**	**Responsabile**	**Contenuto nel fascicolo** (se questo campo è valorizzato la riga si riferisce ad un sottofascicolo)
2016	00000001	01/01/2016	08.01	……	……	……

2016	00000002	14/01/2016	05.08	……	……	2015-0000145 oggetto1
2016	00000003	06/02/2016	10.02	……	……	……

In alcuni casi, l'obbligo della produzione di documenti informatici previsto dal legislatore si riferisce solo a singole tipologie documentali e non all'intero procedimento. Questo comporta la formazione del fascicolo ibrido, ossia di un'unica unità archivistica originata da un affare/attività o da un procedimento amministrativo, composto da documenti formati su due supporti, quello cartaceo e quello informatico. La conservazione dei documenti del fascicolo ibrido è garantita secondo le diverse modalità previste in base alla natura del supporto.

L'Ente adotterà uno dei due supporti per l'archiviazione dell'intero fascicolo, seguendo criteri di economicità e di garanzia della conservazione, anche attraverso la produzione di copie conformi agli originali cartacei o informatici ai sensi del CAD.

8.7 Organizzazione, gestione e strumenti dell'archivio di deposito

8.7.1 Definizione delle responsabilità delle Unità organizzative

L'unica UOR dell'Ente, nomina un Responsabile che si occupa della gestione e conservazione dei propri Archivi di deposito. Tali responsabili hanno il compito di conservare la documentazione, garantirne l'accesso, registrare i movimenti del materiale documentario dato in consultazione, collaborare con il responsabile del Servizio archivistico nella selezione della documentazione per lo scarto ed il versamento all'archivio storico, quindi alla redazione di elenchi di scarto e di elenchi di versamento.

8.7.2 Il versamento dei fascicoli

Periodicamente e secondo un apposito piano di versamento concordato con il Responsabile dell'Archivio di deposito dell'Ente (di norma una volta all'anno), ogni singolo RPA (Responsabile del Procedimento Amministrativo) deve conferire al responsabile dell'Archivio di deposito i fascicoli relativi ad affari e procedimenti amministrativi conclusi o comunque non più necessari ad una trattazione corrente.

Tali fascicoli dovranno essere preventivamente sfoltiti, secondo le indicazioni fornite dal Servizio archivistico, a cura del RPA.

Per il versamento dei fascicoli cartacei ad oggi non è disponibile un modello cartaceo di versamento dall'archivio corrente all'archivio di deposito.

Le serie e i repertori delle deliberazioni di Giunta e Consiglio e i verbali delle sedute sono conservati per nove anni presso la Segreteria; trascorso tale termine vengono versati all'Archivio generale.

8.7.3 Strumenti per la gestione dell'archivio di deposito

Coerentemente con i consolidati principi della gestione archivistica, l'Ente utilizza i seguenti strumenti per la gestione dell'archivio di deposito:

- Elenco di consistenza, in cui sono riportati i fascicoli conservati presso l'archivio di deposito, suddivisi per titolo, classe e per anno di apertura (*Elenco di consistenza dei fascicoli archivio di deposito)*;
- Registro dei versamenti dei fascicoli dall'archivio corrente all'archivio di deposito e dall'archivio di deposito all'archivio storico (*Registro dei versamenti dei fascicoli*).

8.7.4 Selezione dei documenti per la conservazione/scarto: procedure e definizioni di responsabilità interne alle unità organizzative

Ogni triennio il Responsabile dell'archivio di deposito redige, sulla base del Piano di conservazione e sulla scorta delle indicazioni fornite dal Servizio archivistico dell'Ente *(Procedura per la selezione)*,un elenco della documentazione da versare all'Archivio storico (Archivio generale) (*Modello di elenco di versamento*) e un elenco del materiale che si propone di inviare allo scarto (*Modello di Elenco di scarto)*.

Ogni versamento dagli archivi di deposito delle UOR all'archivio storico (Archivio generale) deve essere identificato con un numero progressivo annuale, riportato dal Registro dei versamenti (*Registro dei versamenti e spostamenti)* .

In concomitanza con la redazione dell'Elenco di versamento, il RPA deve marcare le unità di condizionamento (buste o registri) contenenti il materiale da versare con apposite etichette, conformi al modello proposto (*Modello di etichetta per unità da versare*). Analoga marcatura con etichette deve essere effettuata per il versamento dagli archivi di deposito all'archivio storico (Archivio generale).

Il RPA deve inoltre marcare le unità di condizionamento contenenti il materiale da scartare con apposite etichette, conformi al materiale proposto (*Modello di Cartello per unità da scartare)*.

Il Responsabile del Servizio archivistico predispone per il Consiglio Direttivo la determinazione con l'elenco del materiale da scartare per l'autorizzazione e successivamente acquisisce la prescritta autorizzazione della Soprintendenza archivistica per il Veneto, ai sensi dell'art. 21, comma 1, lett. D), del D.lgs. 42/2004.

8.8 Organizzazione, gestione e strumenti dell'archivio storico

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

I documenti che costituiscono l'archivio storico (quelli relativi ad affari esauriti da oltre quarant'anni, giudicati degni di conservazione permanente) sono conservati presso l'Archivio generale che è parte integrante del Servizio archivistico. Essi devono essere ordinati ed inventariati.

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

La consultazione dell'archivio storico è gestita direttamente dal Servizio archivistico, mediante l'Archivio generale.

9 PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA

9.1 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 diritti entrambi costituzionalmente fondati.

Le specifiche procedure sono definite nei documenti di seguito indicati:

- Regolamento sull'attività e i procedimenti amministrativi
- Regolamento sul diritto di accesso dei cittadini agli atti e ai documenti amministrativi, approvato con Deliberazione del
- Regolamento per il trattamento dei dati sensibili e giudiziari da parte dell'Ordine, approvato con Deliberazione del Consiglio

In adempimento alla recente normativa in tema di trasparenza e accesso civico (Decreto legislativo n. 33 del 14 marzo 2013) l'Ordine 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'amministrazione.

Nelle forme previste dalla normativa pubblica (art. 10 del citato D. lgs. 33/2013) pubblica ed aggiorna annualmente il Programma triennale per la trasparenza e l'integrità ed il relativo stato di attuazione.

9.2 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'Ordine, 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'Ordine già citato, che può riguardare tutta la documentazione prodotta dall'Ordine 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 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, Allegato A2 del Codice in materia di protezione dei dati personali *(Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici)*.

10 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

10.1 Modalità di approvazione e aggiornamento del Manuale

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

Gli aggiornamenti potranno rendersi necessari a seguito di:

- Adeguamenti normativi che rendano superate le prassi definite nel Manuale
- Introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza
- Inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti

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

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

10.2 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'Ente mediante la pubblicazione sul proprio sito istituzionale.

Al fine di assicurarne adeguata conoscenza al personale dell'Ente il Manuale di gestione è pubblicato sulla rete Intranet dell'Ente e la sua conoscenza è inserita nei percorsi di formazione del personale in tema di gestione documentale.

11 Tabella dei delegati per la tenuta del protocollo informatico (cap. 1.5.1)

NOMINATIVO	DATA	FUNZIONE	RUOLO
BALBA Andrea		Impiegato	Delegato
MUSTATA Diana-Elena		Impiegata	Sostituto
PITTALUGA Simone		Impiegato	Sostituto

12 Il delegato per la conservazione (cap.1.5.2)

NOMINATIVO	DATA	FUNZIONE	RUOLO
BALBA Andrea		Impiegato	Delegato

13 Caselle di posta assegnazioni

Attualmente l'organizzazione dispone di 9 email, associate al dominio omceoge.org:

- protocollo@ su PC 01
- presidenza@ su PC 01
- direzione@ su PC 07
- segreteria@ su PC 05
- amministrazione@ su PC 06
- pubblico.genova@ su PC 02
- ufficioformazione@ su PC 04
- sat@ su PC 03
- sportelloenpam@ su PC 01

Oltre alle mail di cui sopra associate al dominio pec.omceo.it l'organizzazione dispone delle seguenti PEC fornite dall'associazione FNOMCeO:

- presidenza.ge@ su PC 01
- presidenza.cao.ge@ su PC 02
- direzione.ge@ su PC 07
- segreteria.ge@ su PC 05

E delle seguenti PEC fornite dell'organizzazione con dominio pec.omceoge.eu:

- ordinemedici@ su PC 01
- amministrazione@ su PC 06
- info@ su PC 07
- pubblico@ su PC 02
- ufficioformazione@ su PC 04

Tutte le email utilizzano il servizio di monitoraggio e controllo fornito da Sophos Endpoint.

14 Organigramma (cap. 1.4)

15 Tabella dei metadati e dei formati ammessi per ogni classe documentale

Si veda la scheda tecnica concordata con il conservatore per ogni classe documentale per la quale è previsto il conferimento in conservazione.