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

ORDINE DEI MEDICIDI TARANTO

VIA CRISPI, 107

74123 TARANTO

Area Organizzativa Omogenea: Protocollo OmceoTA

AZIONE	DATA	NOMINATIVO	FUNZIONE
Redazione	2024-2025	Dr.ssa Rosaria Velle	Resp Ufficio Gestione documentale e Uff Protocollo
Verifica	2025	Dr Sergio Prastaro	Segretario
Approvazione	2025	Consiglio direttivo	Organo di controllo

IL PRESENTE MANUALE È STATO APPROVATO E ADOTTATO CON DELIBERAZIONE N. 140 DEL 23.06.2025

INDICE

1 PRINCIPI GENERALI

1.1 Premessa

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

Il Manuale di gestione, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi".

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

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

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

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

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

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

Il registro di protocollo è atto di fede 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).

[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.

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 Taranto 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.

L'organizzazione degli uffici in considerazione della tipologia e della funzione svolta presenta esigenze di semplificazione della gestione documentale, che pertanto viene svolta in maniera coordinata e unitaria da un'unica AREA ORGANIZZATIVAOMOGENEA (AOO).

1.2 Ambito di applicazione e struttura del Manuale di Gestione

1.2.1 Ambito di applicazione

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

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

dei documenti.

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

1.2.2 Struttura del manuale

L'attuale manuale di gestione è organizzato in 9 capitoli ed include n.6 allegati.

1.3 Definizioni e norme di riferimento

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

- Decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- Decreto legislativo 7 marzo 2005 n. 82 - *Codice dell'Amministrazione Digitale*
- Decreto legislativo 26 agosto 2016, n.179 – *Modifiche e integrazioni al Codice dell'Amministrazione Digitale in materia di riorganizzazione delle amministrazioni pubbliche*.
- Decreto legislativo 22 gennaio 2004, n. 42 - *Codice dei beni culturali e del paesaggio*
- Decreto legislativo 30 giugno 2003, n. 196 - *Codice in materia di protezione dei dati personali*
- Legge 7 agosto 1990 n. 241 - *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*
- Legge 11 febbraio 2005, n. 15 - Modifiche ed integrazioni alla legge 7 agosto 1990, n. 241, concernenti norme generali sull'azione amministrativa
- Decreto del presidente del Consiglio dei Ministri 3 dicembre 2013 - *Regole tecnicheper il protocollo informatico*
- Decreto del presidente del Consiglio dei Ministri 3 dicembre 2013 - *Regole tecnichein materia di sistema di conservazione*

- Decreto del presidente del Consiglio dei Ministri 11 novembre 2014 - *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni*
- Decreto del presidente del Consiglio dei Ministri 22 febbraio 2013 - *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*
- Quaderno 21 CNIPA, febbraio 2006 - *Manuale di gestione del protocollo informatico, dei documenti e dell'archivio delle Pubbliche amministrazioni - Modello di riferimento*
- disposizioni integrative correttive al d.lgs. 26 agosto 2016, n. 179, del 13 dicembre 2017, n. 217 , concernente modifiche ed integrazioni al Codice dell'Amministrazione Digitale (CAD), di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche

Ai fini del presente manuale si intende per:

- "**Ente**", l'Ordine dei Medici Chirurghi e degli Odontoiatri della provincia di Taranto
- "**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 e integrazioni (aggiornato a dicembre 2017).

Di seguito si riportano gli acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea
- **MdG** - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi (il presente documento)
- **RPA** - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare
- **RSP** - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi
- **SGD** – Servizio gestione documentale
- **UOR** - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato

Per altre definizioni si faccia riferimento all'*Allegato 1 - Definizioni*

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

Ai fini della gestione unica e coordinata dei documenti l'Ente è costituito da un'unica Area organizzativa omogenea (AOO unica), formalmente definita con Deliberazione n. 99 del 24.04.2018

Sigla dell'AOO =Protocollo OMCeO TA Cod. AOO OMCEOTA

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.

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

A norma dell'art. 61 del DPR 445/2000, Il Consiglio direttivo ha istituito, con Deliberazione n. 100 del 24.04.2018, l'ufficio denominato "Servizio archivistico dell'Ordine dei Medici chirurghi e degli odontoiatri di Taranto, con il compito di gestire il protocollo informatico, i flussi documentali e gli archivi.

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

- **la gestione e il coordinamento del sistema di protocollo informatico** - registrazione, classificazione, assegnazione dei documenti, costituzione e repertoriazione dei fascicoli, autorizzazione per l'accesso alle funzioni della procedura, gestione del registro di emergenza, annullamento di registrazioni
- **la gestione e il coordinamento degli archivi** 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 per la tenuta del protocollo informatico a norma dell'art. 61, comma 2 del DPR 445/2000, in mancanza di una figura dirigenziale, è stata nominata quale RSP la dipendente dott.ssa VELLE Rosaria, in possesso di idonei requisiti professionali di informatica-tecnico-archivistica, acquisiti attraverso percorsi formativi adeguati in materia di digitalizzazione delle PA organizzati dalla FNOMCeO con la collaborazione dell'ANAI (Associazione Nazionale Archivistica Italiana) e nelle condizioni di poter assolvere all'incarico.

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

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

- predisporre lo schema del Manuale di gestione di cui all'art. 5 delle Regole tecniche per il protocollo
- curare la redazione e l'aggiornamento del Titolario, del Piano di fascicolazione e degli altri strumenti archivistici previsti

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

Sono inoltre compiti del Servizio:

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

1.5.1 Il delegato per la tenuta del protocollo informatico

E' in facoltà del Responsabile avvalersi della delega di funzioni a dipendenti dell'Ente in possesso dei necessari requisiti di competenza e professionalità.

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 archivistico e protocollo informatico.

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

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, dispone di un unico sistema di protocollo informatico e gestione documentale denominato Iride DOC prodotto da TECSIS srl

Il protocollo informatico unico è lo strumento attraverso il quale l'Ente garantisce l'effettiva ricezione e trasmissione dei documenti. Con la messa a regime di tale sistema è cessata di fatto la necessità di mantenere altri protocolli interni (protocolli di settore, servizio, ufficio, etc., protocolli multipli, 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 comprensivo del piano di fascicolazione e di conservazione (***Allegato 4- Titolario di classificazione***)
- Oggettario (***Allegato 5 - Oggettario***)
- Organigramma(***Allegato 6 - Organigramma***)

1.7 Misure per l'eliminazione di protocolli di settore

Il presente paragrafo riporta la pianificazione, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli diversi dal protocollo informatico.

Piano di attuazione:

in coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'Ente sono registrati all'interno di un unico registro di protocollo informatico. Pertanto, tutti i registri "particolari di protocollo" sono aboliti ed eliminati.

Al fine di eliminare i registri di protocollo diversi dal protocollo informatico sono svolte le seguenti attività:

- censimento preliminare e redazione di un elenco dei diversi registri di protocollo esistenti
- analisi e definizione degli interventi organizzativi, procedurali e tecnici da effettuare al fine di adottare il protocollo informatico, tenendo conto della realtà organizzativa dell'Ente della necessità di gestire la fase transitoria connessa con la definizione delle pratiche gestite con strumenti diversi dal protocollo informatico unico
- individuazione delle modalità e dei tempi di sostituzione
- attività di verifica periodica sulla corretta esecuzione del piano di attuazione.

1.8 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 del Regolamento Europeo 2016/679, circa la protezione dei dati personali, e del D.lgs. 196/2003 novellato dal D.lgs. 101/2018, e dalla circolare AgID del 18 aprile 2017 n. 2/201 che definisce le misure di sicurezza che ogni PA deve obbligatoriamente adottare entro il 31/12/2017.

2.1 Formazione dei documenti - aspetti di sicurezza

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

2.2 Gestione dei documenti informatici - aspetti di sicurezza

Il sistema di gestione informatica dei documenti:

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

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

2.2.1 Componente organizzativa della sicurezza

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 adeguate misure di sicurezza, la cui competenza è posta a carico di figure che sono appositamente individuate come prevista dalla normativa vigente.

Nell'ambito della sicurezza sono stati nominate le seguenti figure professionali:

- Amministratori di Sistema
- Responsabile Protezione Dati
- Responsabile Conservazione Sostitutiva

2.2.2 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
- rilevatori di allagamento
- 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.

2.2.3 Componente logica della sicurezza

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

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

- identificazione e autenticazione utente
- profilazione degli accessi (ACL - Access Control List)
- sistemi antivirus
- firma digitale (dove necessario)
- monitoraggio sessioni di lavoro
- disponibilità del software e dell'hardware
  - ridondanza dei sistemi di salvataggio
  - replica del salvataggio in Cloud (in area geografica diversa da quella dell'Ente)

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 l'*applicazione* utilizzata che presenta una architettura di tipo *client/server, con hardware localizzato nella sede*.

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

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

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

- interfaccia utente ⇔logica funzionale
- logica funzionale ⇔dati persistenti

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

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

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

- server applicativo
- DBMS + Repository file

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

All'interno del server applicativo 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 ***DatabaseManagement System*** (DBMS) è il software che permette la creazione, manipolazione einterrogazione di un DB. In Iride DOC 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'Ente e la necessità di distribuire le attività di protocollo e gestione documentale a tutti i dipendenti, rendono di fatto non necessaria la stratificazione di diversi livelli di autorizzazione fatta a livello di documenti. Quindi tutti i dipendenti abilitati alla protocollazione, hanno accesso a tutti i documenti gestiti dal sistema documentale. Per questo sono stati opportunamente edotti sulle responsabilità e formati in merito agli aspetti della sicurezza informatica. Sono gestiti livelli di autorizzazione differenziati per quegli utenti che 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'Ente in possesso delle adeguate credenziali amministrative
- per i tecnici informatici autorizzati, per le sole attività sistemistiche di amministrazione, aggiornamento e manutenzione delle componenti di sistema

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

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

2.2.4 Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitati su Iride Doc 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 Iride Doc

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.

2.2.5 Criteri di utilizzo degli strumenti tecnologici

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

Gli utenti interni, ciascuno nominato come Soggetto Autorizzato in base all'art.29 del R.E. 2016/679, nonché autorizzati ad utilizzare hardware e software di protocollo, operano nel rispetto del "Regolamento per l'utilizzo degli strumenti informatici e telematici dell'Ente", e che in riferimento alla sicurezza nell'utilizzo delle risorse tecnologiche, prevede i seguenti obblighi:

OBBLIGHI GENERALI

Riservatezza	1. Il Soggetto Autorizzato si impegna a mantenere il segreto professionale e l'assoluta riservatezza rispetto a tutte le informazioni apprese durante lo svolgimento dei compiti ad esso assegnati.
Rispetto delle norme GDPR e di sicurezza	2. Dovrà effettuare il trattamento dei dati nel rispetto della normativa vigente, delle misure di sicurezza adottate, e quelle che successivamente verranno indicate dall'Ente, in aggiornamento e/o in aggiunta, a quelle ivi previste.
Trattamento secondo finalità indicate e liceità	3. Dovrà svolgere il trattamento dei dati per le finalità e secondo le modalità stabilite dall'Ente, e successivamente trattarli in modo compatibile con tali finalità; comunque dovrà trattare i dati personali in modo lecito, corretto e trasparente nei confronti degli interessanti.
Non eccedenza	4. Dovrà trattare dati personali non oltre quanto necessario alle esigenze ed allo svolgimento delle proprie mansioni/attività lavorative nonché verificare che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
Minimizzazione ed esattezza	5. Dovrà verificare che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, oltre a verificare che i dati siano esatti e, se necessario, provvedere al loro aggiornamento.
Formazione	6. Dovrà partecipare agli interventi di formazione e aggiornamento sulla normativa in materia di trattamento dei dati personali che l'Ente fornisce attraverso le strutture, interne ed esterne, a ciò deputate.

Comunicazione	7. Dovrà comunicare dati personali esclusivamente ai soggetti interessati, salvo che non vi sia una esplicita richiesta dell'interessato stesso (delega scritta), oppure un obbligo legale, oppure la comunicazione sia necessaria per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.
Caso di incidente informatico e comunicazioni rilevanti	8. Dare immediata comunicazione al Responsabile Protezione Dati (DPO) nel caso constati o sospetti un incidente di sicurezza o situazioni e fatti rilevanti di particolare gravità, affinché vengano adottate tutte le misure precauzionali e/o riparatorie necessarie.
Collaborazione con il titolare del trattamento	9. La Persona Autorizzata dovrà fornire all'Ente, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo e per compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico.

OBBLIGHI INERENTI AL DEVICE AZIENDALE

Uso a soli fini lavorativi	10. Dovrà utilizzare gli strumenti aziendali (PC e Tablet) a scopo esclusivamente lavorativo e non personale; non sarà dunque possibile consultare internet e la posta elettronica a fini privati ovvero ascoltare o scaricare file audio o video, se non a fini prettamente lavorativi.
Divieto di copia	11. Non potrà estrarre copia di banche dati o di singoli dati personali o creare nuove ed autonome banche dati al di fuori di quanto necessario alle mansioni lavorative.
Password di accesso al Device aziendale	12. Dovrà accertarsi che gli strumenti aziendali in dotazione siano protetto da una password di accesso composta da almeno otto caratteri alfanumerici e non contenga riferimenti agevolmente riconducibili alla Persona Autorizzata.
Modifica della password al primo accesso e notifica di violazione	13. Se fornito, dovrà modificare il proprio codice d'accesso gli strumenti aziendali al primo utilizzo e, successivamente, ogni tre mesi; in caso di dubbi, anche minimi, sulla possibilità che la segretezza della password sia stata compromessa dovrà immediatamente procedere alla sostituzione della stessa e darne comunicazione all'Ente.
Divieto di comunicare la propria	14. Se fornito, non comunicare o rendere conoscibile a terzi il proprio codice di accesso e/o consentire a terzi di utilizzare gli strumenti aziendali e/o accedere ai software e ai dati per nessun motivo senza

password	previa autorizzazione del Titolare dell'Ente.
Divieto di salvataggio dei dati *in locale*	15. Salvare i dati esclusivamente nelle banche dati indicate e fornite dalla azienda, in ogni caso seguire le indicazioni degli Amministratori di Sistema circa le procedure di salvataggio dei dati personali.
Divieto di modifica di configurazioni preimpostate.	16. Non modificare le configurazioni preimpostate degli strumenti aziendali e/o scaricare ulteriori applicazioni o programmi senza previa espressa autorizzazione degli Amministratori di Sistema.
Diligenza nella custodia	17. Non dovrà lasciare incustodito o accessibile a terzi gli strumenti aziendali se non temporaneamente per esigenze operative ed in ogni caso devono essere protetti, specie durante le sessioni di trattamento dei dati, da accessi non autorizzati attraverso sistemi di autenticazione attivati automaticamente a seguito del loro prolungato inutilizzo (ad es. mediante screensaver).
Obbligo del rispetto delle misure di sicurezza	18. Il Soggetto Autorizzato è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione, perdita o modifica, anche accidentale, dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, già in atto o che, in futuro, venissero indicate dall'Ente.

OBBLIGHI INERENTI A DOCUMENTI CARTACEI

Copie di documenti cartacei	19. Con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, il Soggetto Autorizzato dovrà restituire gli stessi al termine delle operazioni affidate senza mantenerne copia; quando tali atti e i documenti contengano speciali categorie di dati personali e gli sono affidati per lo svolgimento dei relativi compiti, quest'ultimo deve controllare e custodire i medesimi atti e documenti fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e deve restituirli al termine delle operazioni affidate.
Archivio e diligenza nella custodia di documenti	20. Dovrà archiviare e custodire i documenti all'interno di armadi/mobili/cassetti muniti di serratura. Conservare le chiavi con diligenza e restituirle al responsabile delle stesse; non lasciare le chiavi nella serratura o comunque in un luogo facilmente accessibile al termine della giornata lavorativa. Chiudere a chiave l'archivio (armadio,

cartacei	cassetto ecc.) o l'ufficio durante la giornata, in caso di allontanamento dall'ufficio (es. in occasione di pausa, riunioni, ecc.), al fine di impedire l'accesso da parte di persone non autorizzate.
Distruzione di documenti cartacei	21. Prima di cestinare documenti cartacei contenenti eventuali dati personali, dovrà procedere alla loro distruzione, strappandoli o utilizzando un apposito distruggi documenti, al fine di renderli illeggibili.
Utilizzo di supporti di memorizzazione	22. Dovrà curare, in caso di utilizzo autorizzato di eventuali supporti di memorizzazione da parte del Titolare e/o del Delegato interno, che i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori.

2.3 Trasmissione e interscambio dei documenti informatici - aspetti di sicurezza

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

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

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

2.4 Accesso ai documenti informatici

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

2.5 Politiche di sicurezza adottate dall'Ente

Le politiche di sicurezza sono riportate nel Documento programmatico sulla sicurezza, oltre che nel Registro dei trattamenti dei dati personali, 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 dagli artt. 33 e 55 del Regolamento Europeo 2016/679 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, di cui sono titolari, secondo la procedura telematica all'indirizzo https://servizi.gpdp.it/databreach/s/ per la violazione di dati personali (data breach) come da provvedimento del Garante n. 209 del 27.05.2021.

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

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

2.6 Servizio archivistico (doc. analogici)

La sede dell'archivio dell'Ente è individuata nei locali al piano 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 e 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 si organizza per rendere disponibili per via telematica moduli e formulari.

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

I documenti, 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.

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 Taranto" nelle forme stabilite dall'amministrazione
   - Unità Organizzativa Responsabile con eventuale indicazione del servizio e dell'ufficio
   - 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 istituzionale di posta elettronica certificata

2. Individuazione e descrizione del documento:

   - Numero di protocollo
   - Data di protocollo (giorno, mese, anno)
   - Eventuale numero del registro (repertorio)
   - Indice di classificazione: titolo, classe
   - Identificativo dei fascicoli nei quali è inserito
   - Numero e descrizione degli allegati
   - Numero e data del documento cui si risponde
   - Oggetto del documento

3. Individuazione del destinatario del documento:

   - Cognome e nome (per le persone) Denominazione (per gli enti e le imprese) e il Codice Fiscale/P.I (se disponibile)

   A seconda dei casi:
   - Indirizzo completo: via/piazza, numero civico, CAP, città
   - Indirizzo informatico (Pec…)

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

   - **Cognome, nome e qualifica del Responsabile del Procedimento Amministrativo**
   - **Sottoscrizione (firma autografa o digitale)**

5. **Individuazione del Responsabile dell'istruttoria:**

   - **Sigla del responsabile**

3.3 Formazione dei documenti - aspetti operativi generali

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

Ogni documento 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
- è riconducibile almeno ad un fascicolo o ad un'aggregazione documentaria

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 diplomatistici 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 e originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

Il documento informatico viene formato mediante una delle seguenti modalità:

[2] In conformità alla legge 241/90

- 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 in 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, inclusivi dell'indice di classificazione

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

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

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

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.

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

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

- attraverso l'utilizzo di software rilasciati gratuitamente, secondo la normativa, da enti certificatori

oppure

- attraverso specifiche funzioni integrate nel software di protocollo/gestione documentale, nel rispetto della normativa vigente

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

3.5.1.1 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"[3], utilizzata in tutti i casi nei quali vi sia il trattamento automatico di grandi quantità di documenti, da ottenere quindi automaticamente e senza presidio.

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

- solo il RSP può attribuire potere di firma ad un utente del sistema
- solo il RSP 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.

[3] Fonte documenti Namirial

Iride DOC consente la firma remota automatica anche ad un singolo documento.

3.5.1.2 La validazione temporale

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

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

3.5.2 Tipologie di formato del documento informatico

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

FORMATO	ESTENSIONE	STANDARD DI RIFERIMENTO
PDF - PDF/A	.pdf	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
File grafici	.tif, .jpeg, .jpg, .bmp, .png	ISO 12639 ISO 12234 ISO/IEC 10918:1
Office Open XML (OOXML)	.docx, .xlsx, .pptx	ISO/IEC DIS 29500:2008
Open Document Format	.odt, .ods, .odp, .odg, .odb	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
XML	.xml Derivati da XML: .svg	ISO 8879 – SGML Specifiche W3C
TXT	.txt	/
Formati messaggi di posta elettronica	.eml	RFC 2822 - MIME RFC 1847 - S/MIME
File audio	.mp3	
File video	.avi .mpeg4	
File compressi	.zip, .rar	
Documento firmato con firma elettronicaCAdES	.p7m	

I file compressi o che contengono altri formati devono contenere esclusivamente file con formato incluso nella tabella di cui sopra.
La scelta dei formati è stata effettuata considerando che essa, come da previsione normativa, deve garantire la leggibilità e la reperibilità del documento informatico nell'intero ciclo di vita dello stesso

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

Nel caso pervengano documenti su formati diversi da quelli elencati:

- questi non saranno presi in considerazione dal servizio gestione documentale, il quale avrà cura di avvisare il soggetto produttore in modo da permettere un nuovo invio con formato tra quelli previsti;

3.5.3 Documenti contenenti collegamenti ipertestuali.

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

4 FLUSSI DI LAVORAZIONE DEI DOCUMENTI

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

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

- ricevuto
- inviato
- interno

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

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

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

4.1 Documenti in entrata

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

4.1.1 Ricevuti o prodotti su supporto analogico

I documenti ricevuti su supporto analogico possono essere recapitati attraverso:

- a mezzo posta convenzionale, corriere o telegramma: I documenti analogici ricevuti tramite il servizio postale presso la casella postale dell'Ente pervengono al Protocollo generale al più tardi entro le ore 17 di ogni giorno lavorativo. Il Protocollo generale provvede a separare i documenti esclusi dalla registrazione di protocollo ***(Allegato 7 - Documenti esclusi dalla registrazione di Protocollo)*** 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
- a mezzo posta raccomandata
- brevi manu: consegna diretta presso gli sportelli aperti al pubblico e/o del Protocollo generale aperto al pubblico durante l'orario di apertura. Gli operatori provvedono alla registrazione, segnatura e scansione dei documenti, con relativo smistamento 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"

4.1.2 Ricevuti o prodotti su supporto informatico

I documenti informatici possono essere recapitati/trasmessi tramite:

- posta elettronica convenzionale o certificata (la casella mail istituzionale dell'Ente segreteria@omceota.it casella PEC dell'Ente segreteria.ta@postecert.it pubblicate sul sito istituzionale www.omceota.it)
- su supporto rimovibile quale, ad esempio, cd rom, dvd, pen drive, consegnato direttamente al SGD o inviato per posta convenzionale o corriere

4.2 Documenti inviati

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

4.2.1 Inviati su supporto analogico

I documenti analogici sono trasmessi attraverso:

- Servizi postali
- Brevi manu
- Notifica

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

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

4.2.2 Inviati su supporto informatico

I documenti informatici sono trasmessi attraverso:

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

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

4.2.3 Documento Cartaceo inviato elettronicamente

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

4.2.4 Documento Digitale inviato elettronicamente

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

4.3 Documenti interni

I documenti interni sono redatti con strumenti informatici, protocollati e smistati esclusivamente ai destinatari interni per mezzo dell'applicativo di protocollo con la modalità "posta interna".

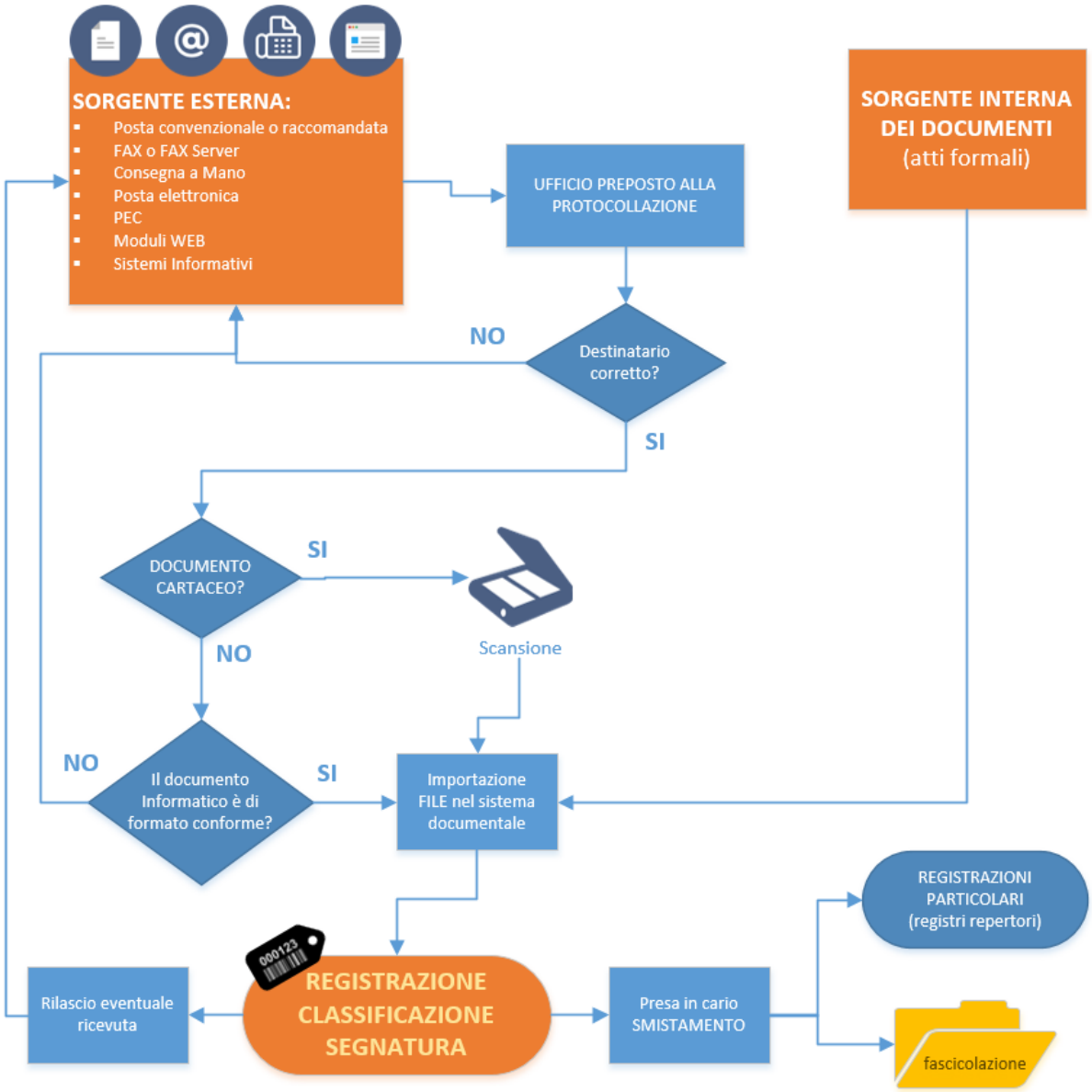
4.4 Descrizione del flusso di lavorazione dei documenti

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

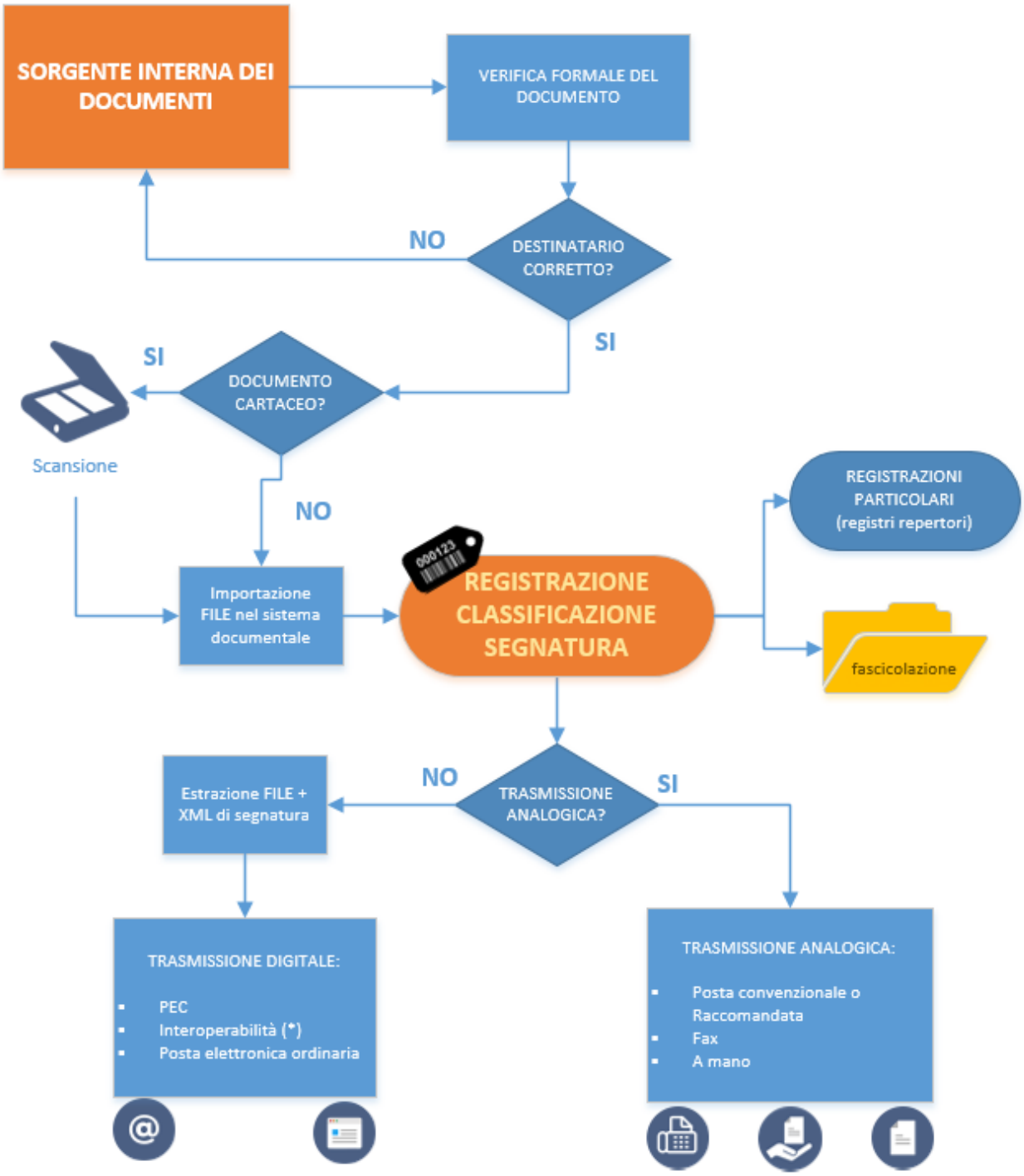
Essi si riferiscono ai documenti:

- ricevuti dall'Ente, dall'esterno o anche dall'interno
- inviati dall'Ente, all'esterno o anche all'interno

4.5 Flusso in entrata



4.6 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, con particolare riferimento a quei documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi, devono essere registrati sul protocollo informatico unico dell'Ente, con le modalità e le eccezioni di seguito illustrate.

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

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

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

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

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

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

5.2 Registro di protocollo

Il registro di protocollo[4], è un documento informatico prodotto e redatto secondo le modalità previste dalla vigente normativa.

[4]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

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

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

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

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

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

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

Il "registro di protocollo"[5] deve ricomprendere le informazioni minime richieste dall'art. 53, comma 1, del DPR 445/2000 e dalla Circolare AGID n. 60 del 2013.

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

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

Gli elementi non obbligatori, ma funzionali qualora disponibili sono:

- livello di riservatezza
- numero di protocollo del documento ricevuto
- data del documento ricevuto
- modalità di trasmissione
- numero degli allegati

Fonte: La natura giuridica e il valore probatorio del registro di protocollo di un ente pubblico. (www.StudioCataldi.it)

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

- numero raccomandata
- annotazioni

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

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

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

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

5.3 Modalità di registrazione di protocollo

Per registrazione di protocollo si intende l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. La registrazione si effettua di norma entro la giornata di arrivo o comunque entro 24 ore lavorative dal ricevimento o, se intercorrono dei giorni festivi o di chiusura programmata dell'Ente, nel primo giorno lavorativo utile. Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immodificabile. Contestualmente alla registrazione i documenti analogici vengono 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 RSP dell'Ente prende visione quotidianamente, tramite il sistema informatico, dei documenti pervenuti e procede alla loro fascicolazione o assegnazione.

5.4 La segnatura di protocollo

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

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

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

Ulteriori informazioni previste sono:

A. indicazione della UOR dell'Ente responsabile del documento prodotto.
B. identificazione degli allegati
C. anno
D. titolo
E. classe

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

Qualora il documento venga prodotto su formato analogico, al termine della registrazione, la segnatura viene apposta direttamente sul supporto cartaceo 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.

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 Documenti soggetti a registrazione particolare (Repertoriazione)

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

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

5.6 Procedure specifiche nella registrazione di protocollo

5.6.1 Protocollazione di documenti riservati

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

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

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

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

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

Il RSP 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.

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

In modo analogo, il RPA che effettua l'operazione di apertura di un nuovo fascicolo ne stabilisce anche il livello di riservatezza applicando, tramite le apposite funzioni, le autorizzazioni a livello di ruolo oppure di singolo utente.

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

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

5.6.2 Documenti esclusi dalla registrazione di protocollo

Il DPR 445/2000 prevede che tutti i documenti in entrata e in uscita e tutti i documenti informatici siano registrati a protocollo, con alcune eccezioni. Tra le eccezioni troviamo i documenti soggetti a registrazione particolare di cui al precedente paragrafo 5.5 e i documenti di cui all'allegato ***(Allegato 7 - Documenti esclusi dalla registrazione di Protocollo).***

5.6.3 Annullamento delle registrazioni di protocollo

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

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

5.7 Casi particolari di registrazioni di protocollo

5.7.1 Lettere anonime

La lettera anonima, una volta aperta e attestata l'assenza di ogni riferimento al mittente, viene posta all'attenzione del Segretario, 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.

5.7.2 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.

5.7.3 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.

5.7.4 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.

5.7.5 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 e sono inseriti nel fascicolo relativo.

5.7.6 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 Taranto il xx.xx.xxxx».

5.7.7 Trattamento dei documenti con oggetto o smistamento plurimo

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

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

5.7.8 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 può 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", l'Ufficio di protocollo procede 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 individuati con nome, cognome o Ragione Sociale.

5.7.9 Flussi documentali informatici

5.7.9.1 Flusso FNOMCeO-ENPAM

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

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

Il sistema si occupa poi di instradare i 2 File ai sistemi FNOMCeO o ENPAM.
La procedura dovrà essere revisionata in relazione delle nuove disposizioni in materia di trattamento dati (GDPR).

5.8 Regole di smistamento e di assegnazione

L'operazione di smistamento consiste nell'assegnazione di un documento registrato 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 è conservato nell'archivio generale dell'Ente;
- nel caso di documenti informatici, l'originale è acquisito direttamente (salvo procedura di caricamento manuale) nel sistema di protocollo attraverso i canali previsti;
- 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.

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 (***Allegato8: Modello del Registro di emergenza***).

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

L'utilizzo del registro di emergenza deve essere autorizzato dal Responsabile del Servizio per la tenuta del protocollo informatico. In caso di assenza del responsabile del servizio provvede all'autorizzazione il Segretario dell'Ordine ovvero dal Presidente e legale rappresentante 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 note ritenute rilevanti dal responsabile del protocollo informatico e della gestione documentale.

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

Il RSP 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.[6]

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 RSP 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.

[6] 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.

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 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

7.1 Protezione e conservazione degli archivi pubblici

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

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

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

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

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

- garantire la sicurezza e la conservazione del proprio archivio e procedere al suo ordinamento
- costituire uno, o più archivi di deposito nei quali trasferire annualmente i fascicoli relativi agli affari conclusi
- istituire una sezione separata d'archivio per i documenti relativi ad affari esauriti da più di 40 anni (archivio storico) e di redigerne l'inventario

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

- **Archivio corrente**[7],composto dai documenti relativi ad affari in corso, conservatipresso gli uffici (comprende fascicoli di persona fisica o giuridica)
- **Archivio di deposito**[8],composto dai documenti relativi ad affari cessati da meno di 40anni conservati presso l'archivio di deposito presso l'Archivio generale dell’Ente, a determinate condizioni
- **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 trattamento del sistema documentale dell’Ente implica la predisposizione di strumenti di gestione dell’archivio corrente che consentano un’efficace organizzazione e consultazione della documentazione, a prescindere dai supporti dei documenti

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

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

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

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

7.2 Titolario o piano di classificazione

7.2.1 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 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.

[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)

[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.

L'Ente utilizza un Titolario aggiornato, adottato con deliberazione n. 05 del 15.01.2018 (vedi ***Allegato 4 -Titolario di classificazione***) organizzato a 2 livelli suddiviso in titoli e classi. Il titolo (o la voce di I° livello) individua per lo più funzioni primarie e di organizzazione dell'Ente (macrofunzioni); le successive partizioni (classi) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

Titoli e classi sono nel numero prestabilito dal Titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del Consiglio Direttivo dell'Ente sentito il RSP.

Il Piano di classificazione o Titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'Ente, soggette a modifiche in forza delle leggi e dei regolamenti statali. L'aggiornamento del Titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RSP. La revisione viene proposta quando necessario ed opportuno.

Dopo ogni modifica del Titolario, il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche, le eventuali modifiche e integrazioni entrano in vigore il 1° gennaio dell'anno seguente. Il Titolario non è retroattivo: non si applica cioè, ai documenti protocollati prima della sua introduzione.

Il sistema di protocollazione garantisce la storicizzazione delle variazioni di Titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del Titolario vigente al momento della produzione degli stessi.

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

7.2.2 Classificazione dei documenti

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

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

7.3 Formazione del fascicolo

7.3.1 Il fascicolo

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

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

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

Qualora un documento dia luogo all'avvio di un 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 sotto fascicoli.

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

7.3.2 Famiglie e tipologie di fascicolo

I fascicoli sono suddivisi in 2 macro-categorie:

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

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

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

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

L'apertura prevede la registrazione di alcune informazioni essenziali:

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

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

- fascicoli relativi ad attività
- fascicoli relativi procedimenti amministrativi

I documenti sono archiviati all'interno di ciascun fascicolo, ed eventuale 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.**

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

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

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

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

7.3.3 Processo di assegnazione dei fascicoli

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

A seconda delle ipotesi, si procede come segue:

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

7.3.4 Repertorio dei fascicoli

Ogni Fascicolo ha un proprio "IDENTIFICATIVO", costituito da un codice che consente di identificare univocamente un'entità dal punto di vista amministrativo. Tale identificativo è strutturato conformemente a quanto indicato nella **CIRCOLARE AGID N. 60 DEL 23 GENNAIO 2013** (Pag. 71)[10]

[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).

Il repertorio dei fascicoli, ripartito per ciascun titolo del Titolario, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio quindi rispecchia quella del Titolario di classificazione e varia in concomitanza con l'aggiornamento di quest'ultimo. Mentre il Titolario rappresenta in astratto le funzioni e le competenze che l'Ente può esercitare, in base al proprio mandato istituzionale, il repertorio dei fascicoli rappresenta, in concreto, le attività svolte e i documenti prodotti in relazione a tali attività.

Gli elementi costitutivi del repertorio di fascicoli sono:

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

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

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

7.3.5 Il fascicolo personale dell'iscritto

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

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

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

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

Si distinguono due differenti sottofascicoli:

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

---

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.

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

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

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

7.4 Serie archivistiche e repertori

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

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

7.5 Tipologie di registri

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

- albo medici
- albo odontoiatri
- psicoterapeuti
- medicine complementari
- Registro unico fatture
- Registro cronologico mandati
- Registro cronologico reversali
- Inventario beni mobili ed immobili

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.

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

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

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

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

7.6.1 Piano di conservazione

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

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

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

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

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

7.6.2 Strumenti per la gestione dell'archivio di deposito

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

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

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

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

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

8 PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLARISERVATEZZA

8.1 Premessa

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

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

Le specifiche procedure sono definite nei documenti di seguito indicati:

- regolamento sul diritto di accesso dei cittadini agli atti e ai documenti amministrativi, approvato con Deliberazione n. 218 del 17.12.2018
- riguardo la riservatezza per tutte le attività svolte dall'Ordine si adottano i principi e le regole previste dal Regolamento Europeo 2016/679

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. Attraverso apposita sottosezione di Amministrazione trasparente è possibile consultare l'elenco dei procedimenti/provvedimenti amministrativi dell'Ordine dei Medici Chirurghi e degli Odontoiatri di Taranto.

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

8.2 Procedure di accesso ai documenti e di tutela della riservatezza

Merita chiarire preliminarmente alcuni principi e procedure che costituiscono un punto di riferimento per chi opera presso l'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 sono liberamente consultabili, ad eccezione:

- di quelli di carattere riservato relativi alla politica estera o interna dello Stato, che divengono consultabili 50 anni dopo la chiusura del fascicolo che li contiene
- di quelli contenenti dati sensibili, che diventano consultabili 40 anni dopo la chiusura del fascicolo che li contiene
- di quelli contenenti taluni dati sensibili (noti in gergo come "sensibilissimi"), idonei a rivelare lo stato di salute o la vita sessuale o i rapporti riservati di tipo familiare, che diventano consultabili 70 anni dopo la chiusura del fascicolo che li contiene.

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

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

9 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

9.1 Modalità di approvazione e aggiornamento del Manuale

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

Gli aggiornamenti potranno rendersi necessari a seguito di:

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

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

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

9.2 Pubblicità del presente Manuale

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

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