



AltaVita

ISTITUZIONI RIUNITE DI ASSISTENZA
IRA

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

(Approvato con Deliberazione del Consiglio di Amministrazione n. 39 del 12 luglio 2016)

1 Sommario

| | | |
|-------|--|----|
| 1. | PRINCIPI GENERALI | 5 |
| 1.1 | Premessa..... | 5 |
| 1.2 | Norme di riferimento..... | 5 |
| 1.3 | Registri di protocollo particolare..... | 6 |
| 1.4 | Area Organizzativa Omogenea | 6 |
| 1.5 | Strumenti per la gestione del protocollo informatico..... | 7 |
| 1.6 | Organizzazione dell'Istituto | 8 |
| 2 | PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI..... | 9 |
| 2.1 | Obiettivi del piano di sicurezza..... | 9 |
| 2.1.1 | Analisi dei rischi..... | 9 |
| 2.2 | Formazione dei documenti - Aspetti attinenti alla sicurezza..... | 10 |
| 2.3 | Componente logica della sicurezza..... | 11 |
| 2.4 | Componente infrastrutturale della sicurezza | 11 |
| 2.5 | Sistema di gestione della sicurezza | 12 |
| 2.6 | Conservazione - Aspetti della sicurezza..... | 14 |
| 2.7 | Monitoraggio e controllo..... | 14 |
| 3 | FORMAZIONE DEI DOCUMENTI | 15 |
| 4 | SOTTOSCRIZIONE E MARCATURA DEI DOCUMENTI INFORMATICI | 17 |
| 5 | FORMATO DEI DOCUMENTI DIGITALI..... | 18 |
| 5.1 | Classificazione dei formati..... | 19 |
| 5.2 | Strumenti per la visualizzazione | 21 |
| 5.3 | Metadati | 21 |
| 5.4 | Gestione e trattamento di documento informatico | 22 |
| 5.4.1 | Copie per immagine su supporto informatico di documenti analogici..... | 22 |
| 5.4.2 | Duplicati informatici di documenti informatici | 23 |
| 5.4.3 | Copie e estratti informatici di documenti informatici..... | 23 |
| 5.4.4 | Copie su supporto informatico di documenti amministrativi analogici..... | 23 |
| 5.4.5 | Modello ai attestazione di conformità | 24 |

| | | |
|-------|--|----|
| 6 | DESCRIZIONE DEL FLUSSO DOCUMENTALE..... | 25 |
| 6.1 | Modalità di ricezione dei documenti..... | 25 |
| 6.2 | Modalità di invio dei documenti verso l'esterno..... | 27 |
| 6.2.1 | Documenti Analogici..... | 27 |
| 6.2.2 | Documenti Informatici..... | 27 |
| 6.2.3 | Documenti interni..... | 28 |
| 7 | MODALITA' DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO..... | 29 |
| 7.1 | Registrazione dei documenti..... | 29 |
| 7.2 | Modalità di registrazione..... | 30 |
| 7.3 | Segnatura di protocollo..... | 30 |
| 7.4 | Documenti esclusi dalla registrazione..... | 31 |
| 7.5 | Documenti soggetti a registrazione particolare..... | 32 |
| 7.6 | Conservazione del registro giornaliero di protocollo..... | 33 |
| 7.6.1 | Metadati del registro di protocollo giornaliero..... | 34 |
| 7.6.2 | Sottoscrizione del registro di protocollo giornaliero..... | 34 |
| 8 | CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO..... | 35 |
| 8.1 | Documenti presentati in sede di gara di appalto..... | 35 |
| 8.2 | Lettere anonime o prive di firma..... | 35 |
| 8.3 | Documenti pervenuti per errore..... | 35 |
| 8.4 | Documenti in partenza con destinatari plurimi..... | 35 |
| 8.5 | Assegnazione dei documenti..... | 35 |
| 9 | ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO..... | 37 |
| 10 | REGISTRO DI EMERGENZA..... | 38 |
| 11 | DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO..... | 39 |
| 11.1 | Ricerca protocolli..... | 39 |
| 11.2 | Raggruppamento esipienti/argomenti..... | 40 |
| 11.3 | Gestione multipla inserimento protocolli..... | 40 |
| 11.4 | Creazione/modifica password d'accesso..... | 40 |

| | | |
|--------|--|----|
| 11.5 | Funzioni particolari..... | 41 |
| 11.6 | Gestione area organizzativa omogenea (AOO)..... | 41 |
| 11.7 | Protocollazione mail PEC..... | 41 |
| 11.8 | File..... | 41 |
| 11.9 | Log..... | 41 |
| 12 | SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE | 42 |
| 12.1 | Sistema di Classificazione..... | 42 |
| 12.2 | Fascicolo..... | 42 |
| 12.2.1 | Formazione dei fascicoli informatici..... | 43 |
| 12.2.2 | Sottofascicoli..... | 44 |
| 12.2.3 | Repertorio fascicoli..... | 44 |
| 12.3 | Il sistema archivio..... | 45 |
| 12.3.1 | Modalità per lo sfoltimento e versamento fascicoli dall'archivio corrente...46 | |
| 12.3.2 | Movimentazione dei fascicoli..... | 47 |
| 12.3.3 | Modello per il trasferimento atti dall'archivio corrente..... | 47 |
| 12.3.4 | Riordino archivio di deposito..... | 47 |
| 12.4 | Piano di conservazione..... | 48 |
| 13 | SISTEMA DI GESTIONE DEI PROCEDIMENTI AMMINISTRATIVI, MODULISTICA ON LINE | |
| | 49 | |
| 14 | DOCUMENTI DI NATURA SANITARIA..... | 49 |
| 15 | NORME TRANSITORIE E FINALI..... | 49 |

1. PRINCIPI GENERALI

1.1 Premessa

Il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 *“Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005”* , prevede l'adozione del Manuale di Gestione per tutte le amministrazioni di cui all'articolo 2, comma 2, del sopra citato D.Lgs. 7 marzo 2005, n. 82.

Il Manuale di Gestione, come previsto dall'art. 5, comma 1, del medesimo DPCM *“descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi”*.

Il presente Manuale di Gestione descrive il sistema di gestione documentale, definendo tutte le modalità di formazione, registrazione, classificazione, fascicolazione, archiviazione e conservazione dei documenti.

1.2 Norme di riferimento

- Legge 7 agosto 1990, n. 241 – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Circolare del 21 giugno 2001, n. AIPA/CR/31 - requisiti minimi di sicurezza dei sistemi operativi disponibili commercialmente;
- Decreto Legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale (CAD), nel seguito denominato 'Codice';
- Decreto del Ministero dell'economia e delle finanze 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 GU n. 59 del 12 marzo 2014 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71,

comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 GU n. 59 del 12 marzo 2014 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 GU n.8 del 12-1-2015- Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto legislativo n. 282 del 30 luglio 1999 - Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario.

1.3 Registri di protocollo particolare

L'Istituto ha adottato da sempre un unico sistema di protocollo generale per registrare un unico registro i documenti ricevuti e inviati.

Non sono ammessi nè autorizzabili modalità di registrazione diverse dal sistema di protocollo generale.

1.4 Area Organizzativa Omogenea

Per la gestione dei documenti l'amministrazione ha istituito un'unica Area Organizzativa Omogenea (AOO) dove è presente un unico servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. La AOO è stata istituita con Determinazione n. 457 del 9 ottobre 2015.

All'interno dell'Istituto il sistema di protocollazione è totalmente centralizzato, la gestione della corrispondenza, in ingresso e in uscita, è di competenza unicamente dell'Unità Organizzativa di registrazione di Protocollo presente presso il Settore Segreteria/Affari Generali.

L' Unità Organizzativa di registrazione di Protocollo svolge le seguenti attività:

- gestisce e coordina il sistema di protocollo informatico: registrazione, classificazione, assegnazione dei documenti, costituzione e repertoriatura dei fascicoli, autorizzazione per l'accesso alle funzioni della procedura, gestione del registro di emergenza, annullamento di registrazioni;

- gestisce l'archivio dell'Istituto (corrente, di deposito e storico), le procedure di versamento e scarto documentale e la consultazione e per quanto attiene all'archivio storico: la conservazione l'inventariazione, l'accesso e la valorizzazione.

Al Servizio per la gestione informatica del protocollo è preposto il Responsabile della gestione documentale, nominato con apposito atto dirigenziale, il quale ha i seguenti compiti:

- predisporre lo schema del manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del manuale sul sito istituzionale di AltaVita-IRA;
- abilitare gli utenti dell'AOO all'utilizzo del Servizio di Protocollo e definire per ciascuno di essi il tipo di funzioni disponibili;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta produzione e conservazione della copia del registro giornaliero di protocollo;
- garantire il ripristino del servizio in caso di indisponibilità del medesimo;
- 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;
- curare l'apertura, l'uso e la chiusura del registro di protocollo di emergenza.

1.5 Strumenti per la gestione del protocollo informatico

Il protocollo informatico è unico e sono di supporto i seguenti strumenti di gestione:

- Titolare di classificazione;
- Piano di formazione dei fascicoli;
- Organigramma;
- Piano di conservazione;
- Modelli verbali di versamento, copertina fascicoli;
- Modello protocollo di emergenza.

1.6 Organizzazione dell'Istituto

Sono indicate le Unità Organizzative Responsabili delle attività di registrazione di protocollo, di organizzazione e tenuta dei documenti all'interno dell' AOO.

| Unità Organizzativa | Attività |
|---|---|
| Protocollo Generale | Protocollazione in Entrata, Interni, Uscita |
| Area Direzione e Affari generali | Trattamento documenti assegnati |
| Area Tecnica - Patrimonio | Trattamento documenti assegnati |
| Area Finanziaria | Trattamento documenti assegnati |
| Area Risorse Umane | Trattamento documenti assegnati |
| Area Organizzazione e qualità | Trattamento documenti assegnati |
| Area Settore Economato – Provveditorato | Trattamento documenti assegnati |
| Area Sociale | Trattamento documenti assegnati |
| Area Socio-Sanitaria | Trattamento documenti assegnati |

2 PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

Vengono qui riportate le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali secondo il Dlgs 196/2003.

2.1 Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dall'AOO sono disponibili, integre e riservate e che nessun altro utente non autorizzato possa accedervi;
- i dati personali comuni, sensibili e/o giudiziari vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento;
- che il protocollo informatico e tutti i flussi ad esso associato, vengono gestiti secondo quanto richiesto dal Dlgs 196/2003.

Il perimetro di interesse del seguente piano è delimitato entro l'ambito definito dalle regole tecniche e precisamente:

- alla formazione;
- alla gestione;
- alla trasmissione;
- all'interscambio;
- all'accesso;
- alla conservazione dei documenti informatici.

2.1.1 Analisi dei rischi

Con riferimento agli adempimenti connessi alla gestione del protocollo informatico, il responsabile della sicurezza collabora con il responsabile dei sistemi informativi per assicurare la sicurezza dei documenti.

Le attività che discendono dall'applicazione della norma sono le seguenti:

- analisi dei rischi in relazione alla tipologia dei documenti;
- analisi dei rischi in relazione alla tipologia dei dati personali (D.lgs. 196/2003);
- misure di sicurezza da adottare di tipo organizzativo, procedurale e tecnico;
- formazione dei dipendenti;
- monitoraggio periodico del piano di sicurezza.

Il processo di analisi dei rischi disciplina le fasi di gestione della sicurezza e precisamente:

- identificazione del contesto da proteggere, classificazione delle risorse e informazioni da proteggere;
- identificazione e analisi delle minacce ;
- identificazione e analisi delle vulnerabilità e degli impatti;
- valutazione del rischio;
- identificazione delle misure per il trattamento del rischio;
- verifica e monitoraggio delle misure adottate.

Il "rischio" è la probabilità che una minaccia rivolta verso il sistema di gestione documentale, sfruttando le vulnerabilità del sistema, produca un danno ai documenti e dati anche personali trattati sia con strumentazione elettronica, sia senza strumentazione elettronica.

La "minaccia" è la capacità di un'azione o di un evento indesiderato di provocare un danno a fronte di una particolare vulnerabilità dell'infrastruttura considerata.

Una classificazione delle cause di minaccia è la seguente:

- cause naturali;
- cause umane associate al comportamento e all'attività delle persone che si possono distinguere in:
 - azioni involontarie o accidentali;
 - azioni volontarie.
- cause ambientali determinate dal concorso di comportamenti ed eventi fisici esterni;
- cause tecnologiche derivate dal cattivo funzionamento o errata configurazione di componenti hardware o software.

La vulnerabilità è il fattore di criticità – debolezza del sistema – rispetto ad una determinata minaccia che può provocare uno specifico danno o evento indesiderato.

2.2 Formazione dei documenti- Aspetti attinenti alla sicurezza

Il sistema operativo del client e del server che ospita i file utilizzati come deposito dei documenti è configurato in maniera da consentire:

- l'accesso esclusivamente tramite credenziali del protocollo informatico in modo che si possa accedere solo ai dati e documenti di specifica competenza;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso.

Il sistema di gestione informatica dei documenti che più avanti verrà descritto in modo dettagliato:

- 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 e anche della PEC indicata o indicata dall'AOO;
- consente il reperimento delle informazioni riguardanti i documenti registrati e del registro di protocollo;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy";
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

2.3 Componente logica della sicurezza

La componente logica verificata ed attuata per la gestione del protocollo informatico, garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura "a strati multipli di sicurezza" conforme alle best practices correnti.

Risulta comunque che sono stati adottati i requisiti previsti dalle buone regole di backup e disaster recovery e che vengono definite procedure sia semplici, come antivirus, etc, sia complesse, come sistemi di IPS e IDS.

2.4 Componente infrastrutturale della sicurezza

Presso l'Istituto sono presenti i seguenti impianti:

- antincendio;
- luci di emergenza;
- continuità elettrica;
- controllo degli accessi e dei varchi fisici;
- rilevazione dell'allagamento.

2.5 Sistema di gestione della sicurezza

Il sistema di gestione documentale è basato su sistema operativo della piattaforma 'server' conforme almeno alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni, ed assicura:

- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne la identificazione.

Il piano di sicurezza e le relative politiche di sicurezza riferite ai sistemi server, apparecchiature terminali e dispositivi di comunicazione della rete intranet, assicurano quanto segue:

- aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti;
- protezione contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici;
- applicazione di misure formali, anche con il ricorso di risorse esterne, per la gestione degli incidenti al fine di garantire il ripristino dell'accesso ai sistemi in caso di danneggiamento degli strumenti elettronici, in tempi certi;
- protezione contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale;
- gestione degli accessi amministrativi con archiviazione e rotazione periodica dei log di sistema, nonché la gestione formale autorizzativa e prepositiva degli addetti alla conduzione e alla manutenzione;
- protezione fisica relativamente all'accesso alle apparecchiature elettroniche del dispositivo 'sistema server' nonché rispetto a danni ambientali accidentali.

Nel seguito le misure di sicurezza generali adottate rispetto al sistema informatico di gestione dei flussi documentali e di protocollo informatico:

- a) protezione dei sistemi di accesso e conservazione delle informazioni mediante l'assegnazione ad ogni utente di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione granulare che consente ad ogni utente di accedere solo alle funzionalità del programma e ai documenti e dati relativi alla propria unità organizzativa e al proprio ruolo istituzionale;

- b) cambio delle password durante la fase di esercizio;
- c) piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristinare il sistema di gestione del protocollo informatico entro ventiquattro ore;
- d) conservazione, a cura del responsabile del sistema delle copie di sicurezza dei dati e dei documenti, in locali diversi da quelli in cui è installato il sistema di elaborazione di esercizio;
- e) gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne ed esterne qualificate;
- f) uso di codici identificativi per le registrazioni soggette a registrazione particolare (dati sensibili e giudiziari; dati o documenti sottratti all'accesso) in modo da renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- g) impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- h) archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità.

Al fine di ottemperare all'obbligo di comunicare al Garante entro 48 ore i casi di data breach, il responsabile del sistema documentale d'intesa con il responsabile dei sistemi informatici si impegna a comunicare tempestivamente:

- incidenti sulla sicurezza occorsi al proprio sistema di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza afferenti la fruibilità di dati oggetto di convenzione;
- ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;
- ogni modificazione tecnica od organizzativa del proprio dominio, che comporti l'impossibilità di garantire l'applicazione delle regole di sicurezza o la loro perdita di efficacia.

2.6 Conservazione - Aspetti della sicurezza

La conservazione digitale dei documenti individuati e/o obbligatori per legge è delegata a soggetto esterno accreditato AgID e in possesso di tutti i requisiti di sicurezza obbligatori per mantenere l'accreditamento.

Il trasferimento dei dati e dei documenti è sicuro e il processo è riservato, controllato e verificato.

In ogni caso sono adottate idonee misure organizzative, amministrative e tecniche per conservare gli archivi in conformità ai principi archivistici e al codice dei beni culturali e alle discipline generali per la conservazione dei dati sanitari.

2.7 Monitoraggio e controllo

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione attribuiti agli utenti che accedono e utilizzano il sistema di protocollo generale.

L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.

Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Il trasferimento dei documenti al sistema di conservazione è monitorato e verificato con frequenza giornaliera.

3 FORMAZIONE DEI DOCUMENTI

Il D.P.R. 28 dicembre 2000, n. 445 definisce il documento amministrativo come: “ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa. Inoltre il medesimo D.P.R. precisa che il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

All'interno di AltaVita-IRA i documenti vengono prodotti da ciascun ufficio secondo quanto previsto dalla normativa vigente nell'ambito di ogni specifica materia.

AltaVita-IRA, alla luce di quanto statuito dal DPCM 13 novembre 2014, che prevede la prossima produzione dei documenti esclusivamente in formato elettronico, con la completa digitalizzazione dei processi interni e dei flussi documentali, sta riorganizzando la propria attività amministrativa, con adeguamento anche del sistema informatico.

I documenti, pertanto, possono essere prodotti sia in formato analogico che digitale.

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

Il documento analogico si definisce “originale”, nella sua redazione definitiva, perfetta e autentica negli elementi sostanziali e formali in possesso di tutti i requisiti di garanzia e d'informazione del mittente e del destinatario, stampato su carta intestata e munito di firma autografa.

D'altro canto il documento informatico può essere formato secondo i seguenti modi:

- mediante strumenti informatici;
- acquisizione 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.

Ogni documento formato per essere inoltrato formalmente all'esterno o all'interno:

- deve trattare un unico argomento, indicato in maniera sintetica ma esaustiva nello spazio riservato all'oggetto;
- deve essere identificato univocamente da un solo numero di protocollo;
- può fare riferimento a più fascicoli.

Le firme di sottoscrizione, necessarie alla perfezione sotto il profilo giuridico del documento in uscita, devono essere apposte prima della sua protocollazione.

Il documento deve riportare le seguenti informazioni:

- la denominazione e il logo di AltaVita-IRA;
- l'indicazione completa dell'Area Organizzativa Omogenea e dell'Unità Organizzativa Responsabile che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione e i recapiti telefonici;
- la partita IVA dell'Istituto;
- la data (giorno, mese e anno);
- il numero di protocollo;
- il numero degli allegati, se presenti;
- l'oggetto;
- individuazione del destinatario del documento con relativo indirizzo (indicazione del nome e cognome se persona fisica, oppure della ragione sociale in caso di Enti e Ditte);
- firma digitale del Responsabile del Procedimento e/o del Responsabile del provvedimento finale, se trattasi di documento digitale;
- firma autografa del Responsabile del Procedimento Amministrativo e/o del Dirigente e/o del Segretario/Direttore Generale, se trattasi di documento cartaceo.

4 SOTTOSCRIZIONE E MARCATURA DEI DOCUMENTI INFORMATICI

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma elettronica/digitale, avvalendosi di un'autorità di certificazione iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'Agenzia per l'Italia Digitale.

I documenti informatici prodotti prima dell'apposizione della firma digitale vengono convertiti nel formato standard PDF/A.

Con l'apposizione della firma digitale qualsiasi file ha valenza giuridico-probatoria e soddisfa i requisiti di integrità, riservatezza e non ripudiabilità per l'invio all'esterno.

Per i casi in cui sia necessario la data certa si adottano una delle seguenti modalità:

- registrazione di protocollo;
- posta elettronica certificata;
- sistema di marcatura temporale, nei casi in cui non sia previsto l'utilizzo del sistema di protocollazione, tenuto conto che la PEC garantisce la data certa della trasmissione ma non degli eventuali allegati per i quali la disciplina preveda la garanzia del riferimento temporale.

5 FORMATO DEI DOCUMENTI DIGITALI

Si opera conformemente allo specifico allegato delle regole tecniche, aggiornando le procedure a fronte dell'aggiornamento delle stesse regole tecniche.

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato. Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.

In particolare, in una prima sommaria, e non esaustiva catalogazione, i più diffusi formati, secondo il loro specifico utilizzo si possono elencare come segue:

- Testi/documenti (DOC, HTML, PDF,...)
- Fogli di Calcolo (XLS, ...)
- Immagini (GIF, JPG, BMP, TIF, EPS, SVG, ...)
- Archiviazione e Compressione (ZIP, RAR, ...)
- Formati email (SMTP/MIME, ...)

Ai fini della formazione, gestione e conservazione, sono scelti formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita. Nella individuazione dei formati di documenti da presentare al sistema di conservazione si tiene conto delle seguenti caratteristiche:

| Caratteristica | Descrizione |
|------------------------|---|
| Apertura | Un formato è "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. |
| Sicurezza | La sicurezza di un formato dipende da due elementi il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno. |
| Portabilità | Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. |
| Funzionalità | Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico. |
| Supporto allo sviluppo | E' la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.). |

| | |
|------------|--|
| Diffusione | <p>La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici, Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.</p> <p>Inoltre nella scelta dei prodotti Altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.</p> |
|------------|--|

5.1 Classificazione dei formati

I formati di seguito indicati sono un primo elenco di quelli che sono usati nella gestione e idonei per la conservazione.

PDF - PDF/A

Il PDF (Portable Document Format) è un formato creato da Adobe e il documento PDF può essere firmato digitalmente in modalità nativa attraverso il formato ETSI PAdES.

| | |
|----------------|---|
| Sviluppato da | Adobe Systems - http://www.adobe.com/ |
| Estensione | .pdf |
| Tipo MIME | application/pdf |
| Formato aperto | Sì |
| Standard | ISO 32000-1 (PDF), ISO 19005 |

Il PDF/A è stato sviluppato con l'obiettivo di rendere possibile la conservazione documentale a lungo termine su supporti digitali. Caratteristiche principali di questa tipologia di file:

- assenza di collegamenti esterni,
- assenza di codici eseguibili quali javascript ecc.,
- assenza di contenuti crittografati.

Queste caratteristiche rendono il file indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo. Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.

TIFF

| | |
|-----------------|--|
| Sviluppato da | Aldus Corporation |
| Estensioni | .tif |
| Tipo MIME | image/tiff |
| Formato aperto | No |
| Ultime versioni | TIFF 6.0 del 1992 - TIFF Supplement 2 del 2002 |

Formato utilizzato per la conversione in digitale di documenti cartacei.

JPG

| | |
|----------------|----------------------------------|
| Sviluppato da | Joint Photographic Experts Group |
| Estensioni | .jpg, .jpeg |
| Tipo MIME | image/jpeg |
| Formato aperto | Sì |
| Standard | ISO/IEC 10918:1 |

Office -Open XML (OOXML)

| | |
|-----------------------|------------------------|
| Sviluppato da | Microsoft |
| Estensioni principali | .docx, .xlsx, .pptx |
| Formato aperto | Sì |
| Standard | ISO/IEC DIS 29500:2008 |

Comunemente abbreviato in OOXML, è un formato di file, sviluppato da Microsoft, e dispone di caratteristiche che lo rendono adatto alla conservazione nel lungo periodo.

Open Document Format

| | |
|----------------|---|
| Sviluppato da | OASIS - http://www.oasis-open.org/ |
| Estensioni | .ods, .odp, .odg, .odb |
| Tipo MIME | application/vnd.oasis.opendocument.text |
| Formato aperto | Sì |
| Derivato da | XML |

ODF (Open Document Format, spesso referenziato con il termine OpenDocument) è uno standard aperto, per la memorizzazione di documenti corrispondenti a testi, fogli elettronici, grafici e presentazioni.

XML

| | |
|----------------|----------------------------|
| Sviluppato da | W3C |
| Estensioni | .xml |
| Tipo MIME | application/xml - text/xml |
| Formato aperto | Sì |

TXT

Oltre a XML, per quanto concerne i formati non binari “in chiaro”, è utilizzato il formato TXT.

Formati Messaggi di posta elettronica

Ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, lo standard a cui fare riferimento è RFC 2822/MIME.

5.2 Strumenti per la visualizzazione

La tabella che segue riporta una prima e sommaria descrizione dei software disponibili per assicurare la lettura nel tempo dei documenti/oggetti digitali gestiti dal sistema di gestione documentale.

| Visualizzatore | Formato del file | Sistema operativo |
|------------------|---|-------------------|
| AdobeReader | PDF, PDF/A | Windows/Linux |
| TiffViewer | TIFF | Windows |
| JpegView | JPG | Windows |
| XmlReader | XML/TXT | Windows |
| OpenOffice | Open Document Format | Windows/Linux |
| Microsoft Viewer | Testi, calcolo, grafica (.docx, .xlsx, .pptx) | Windows |

5.3 Metadati

Per quanto riguarda i metadati descrittivi, amministrativi, gestionali che accompagnano il documento digitale si fa riferimento ai metadati indicati nelle regole tecniche del decreto e alla loro implementazione da parte del conservatore accreditato.

Particolarità riguarda il set di metadati dei documenti rilevanti ai fini delle disposizioni tributarie, di cui il DM 17 giugno 2014 Ministero Economia e Finanze il quale richiede che *siano consentite le funzioni di ricerca e di estrazione delle informazioni dagli archivi informatici in relazione almeno:*

- al cognome, al nome; alla denominazione, al codice fiscale, alla partita IVA, alla data o associazioni logiche di questi ultimi, laddove tali informazioni siano obbligatoriamente previste.

Ulteriori funzioni e chiavi di ricerca ed estrazione potranno essere stabilite in relazione alle diverse tipologie di documento con provvedimento delle competenti Agenzie fiscali.”

Le norme tecniche del decreto già forniscono una base di riferimento minima di metadati accompagnatori i documenti specificatamente per i documenti informatici, documenti amministrativi, fascicoli di documenti.

5.4 Gestione e trattamento di documento informatico

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

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

Il documento informatico assume la caratteristica di immodificabilità se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

Fermo restando che i documenti informatici sono in genere prodotti in origine con normali strumenti di produttività individuale o generati direttamente da applicazione informatica (vedi flusso fatture, bilancio, cedolini, ordinativi, interventi manutentivi, provvedimenti, altro), sono da considerare anche i documenti immagine prodotti in vari modi e le riproduzioni in copia o duplicazione di documenti digitali . Si distinguono i seguenti casi:

5.4.1 Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico di cui all'art. 22, commi 2 e 3, del Codice viene prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui e' tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

L'attestazione di conformità delle copie per immagine su supporto informatico di uno o più documenti analogici può essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico così prodotto é sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato. Nel successivo capitolo 5.4.5 è riportato il fac-simile della dichiarazione nella forma di documento separato. Il responsabile del sistema documentale provvede a individuare i

soggetti che sono autorizzati ad eseguire la procedura di attestazione e a dotarli dei dispositivi di sottoscrizione. Il riferimento temporale può essere applicato mediante protocollazione del documento di attestazione.

5.4.2 Duplicati informatici di documenti informatici

Il duplicato informatico di un documento informatico di cui all'art. 23-bis, comma 1, del Codice e' prodotto mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine. Il responsabile del sistema documentale d'accordo con il responsabile dei sistemi informativi provvede a formare gli utenti interessati sulle procedure adottate.

5.4.3 Copie e estratti informatici di documenti informatici

La copia e gli estratti informatici di un documento informatico di cui all'art. 23-bis, comma 2, del Codice sono prodotti attraverso l'utilizzo di uno dei formati idonei di cui al precedente capitolo 5.1, mediante processi e strumenti che assicurino la corrispondenza del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia.

L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico così prodotto è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato. L'istituto provvede a individuare i funzionari a ciò abilitati. Nel successivo capitolo 5.4.5 è riportato il fac-simile della dichiarazione nella forma di documento separato.

5.4.4 Copie su supporto informatico di documenti amministrativi analogici

L'attestazione di conformità, anche nel caso di uno o più documenti amministrativi informatici, effettuata per raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia, può essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia. Il documento informatico prodotto e' sottoscritto con firma digitale o con firma elettronica qualificata del funzionario delegato. Nel successivo capitolo 5.4.5 è riportato il fac-simile della dichiarazione nella forma di documento separato.

5.4.5 Modello ai attestazione di conformità

FAC-SIMILE DI DICHIARAZIONE DI CONFORMITÀ AGLI ORIGINALI ANALOGICI

Il sottoscritto nato a
..... il/...../....., nella sua funzione di pubblico
ufficiale incaricato con atto conservato presso questo Ente, preso atto delle
disposizioni di cui al D.P.R. 28 dicembre 2000 n. 445 e all'art. 23ter del D.
Lgs. 7 marzo 2005 n. 82, così come successivamente modificato,

DICHIARA LA CONFORMITÀ

delle copie su supporto informatico/per estratto/per immagine ai
corrispondenti originali su supporto analogico detenuti dall'Ente
presso :.....

| N. | Nome file (comprensivo di percorso completo) | Nome documento analogico (come approvato in delibera) |
|-----|--|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| ... | | |

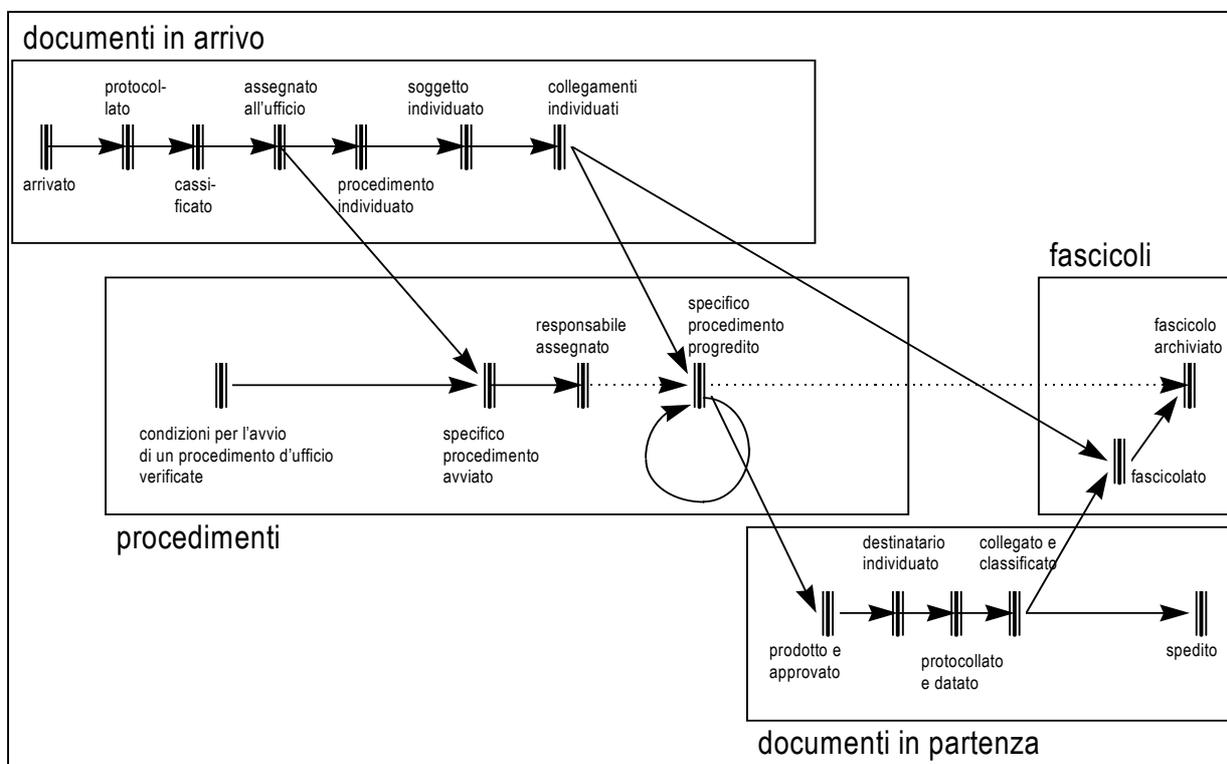
Luogo e data

Nome e cognome e ruolo del firmatario

Firmato digitalmente

6 DESCRIZIONE DEL FLUSSO DOCUMENTALE

Lo schema che segue sintetizza il flusso dei documenti in entrata e uscita dei documenti trattati dal sistema di gestione dei documenti, così come rappresentato nelle linee guida.



6.1 Modalità di ricezione dei documenti

Tutti i documenti pervenuti ad AltaVita-IRA sono registrati a protocollo, classificati, visti dal Segretario/Direttore Generale e assegnati all'Unità Organizzativa Responsabile di competenza, di norma, nella stessa giornata in cui sono pervenuti.

I documenti analogici in ingresso possono essere recapitati attraverso:

- Servizio Postale (corrispondenza ordinaria e servizi di recapito particolari). In tal caso l'Unità Organizzativa responsabile del Protocollo, procede con l'apertura della corrispondenza, con la protocollazione, la segnatura, la classificazione e alla successiva assegnazione dei documenti alle Unità Organizzative Responsabili. Successivamente i documenti protocollati congiuntamente ai documenti esclusi dalla registrazione vengono assegnati alle Unità Organizzative Responsabili;
- Fax: i documenti pervenuti tramite fax sono considerati analogici, ai sensi dell'art. 43, comma 6, del D.P.R. 445/200 soddisfano il requisito della forma scritta e alla loro trasmissione non deve seguire l'invio del documento in originale;

- *Brevi manu*: consegna diretta da parte del mittente oppure da persona delegata all'Ufficio Protocollo o presso le Unità Organizzative Responsabili, durante l'orario di apertura al pubblico degli Uffici. L'Ufficio procede con la registrazione, la segnatura, la classificazione e la scansione dei documenti, con relativo smistamento alle Unità Organizzative Responsabili. Su richiesta dell'interessato può essere rilasciata una ricevuta dell'avvenuta consegna del documento, mediante apposizione del timbro "protocollo in entrata" con l'indicazione della data di consegna nella fotocopia del documento medesimo, con la sigla dell'operatore.

I documenti informatici possono essere inviati mediante:

- caselle di posta elettronica istituzionale. La casella istituzionale di AltaVita-IRA è "segreteria generale@altavita.org". Le caselle di posta elettronica degli altri Settori sono pubblicate nel sito web istituzionale nella Sezione Amministrazione Trasparente – Organizzazione – Articolazione degli Uffici;
- posta elettronica certificata, l'indirizzo PEC di AltaVita-IRA è il seguente: "altavita@legalmail.it";
- Interoperabilità.

La ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti, che prevedono lo standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime accessorie. In fase di ricezione deve essere verificata l'autenticità, la provenienza e l'integrità dei documenti.

L'efficacia di un documento, inviato per posta elettronica, se non dotato di firma elettronica è analoga a quella di una lettera con mancata sottoscrizione, alla quale, ove sussista una necessità, è possibile l'attribuzione di una valenza giuridico-probatoria, inserendolo nella gestione documentale con il formato di origine, apponendo la dicitura "documento ricevuto via posta elettronica", per essere poi successivamente protocollato e assegnato.

Nel caso in cui il messaggio pervenga a una casella di posta elettronica non istituzionale, lo stesso deve essere inoltrato all'indirizzo di posta elettronica istituzionale.

In caso di invio, di un documento scansionato munito di firma autografa, deve esserne valutata la provenienza certa del documento e nel caso non sia verificabile verrà di volta in volta valutato il caso dal Responsabile del Procedimento.

I telegrammi sono soggetti a registrazione di protocollo in qualità di documenti senza firma.

6.2 Modalità di invio dei documenti verso l'esterno.

La trasmissione dei documenti all'esterno, dopo la registrazione a protocollo, viene svolta esclusivamente dall'UOP e può avvenire in uno dei seguenti modi:

6.2.1 Documenti Analogici

Si tratta in via generale di:

- Servizio Postale (corrispondenza ordinaria e servizi di recapito particolari);
- Fax;
- *Brevi manu*;
- documenti prodotti con sistemi di produttività individuale e per i quali è previsto l'uso su carta.

6.2.2 Documenti Informatici

Si tratta di documenti da inoltrare mediante:

- Posta Elettronica Certificata (PEC);
- Posta elettronica

I documenti informatici vengono inviati all'indirizzo di posta elettronica, dichiarato dai destinatari, abilitato alla ricezione della posta per via telematica.

Per la spedizione di tali documenti viene utilizzato il servizio di posta elettronica certificata, offerto da soggetto esterno che assicuri la consegna dei documenti attraverso il rilascio delle ricevute di ritorno elettroniche.

Nella fase transitoria di passaggio al sistema documentale interamente digitale, il documento può essere prodotto in formato analogico.

Se il documento è cartaceo deve essere redatto in due esemplari, di cui uno, dopo la registrazione a protocollo, viene trattenuto e conservato agli atti nel fascicolo di competenza. Qualora vi fossero molteplici destinatari in una lettera verranno inviate solo copie dell'unico originale.

Se la trasmissione del documento cartaceo avviene mediante canale digitale deve essere redatto un unico esemplare, che successivamente alla registrazione a protocollo, viene scansionato e acquisito nel sistema di protocollo e successivamente smistato.

Tutti i documenti da spedire, sia in formato digitale che analogico, sono inoltrati all'Unità Operativa responsabile del Protocollo, comprensivi di allegati, che ne curerà oltre che la protocollazione anche la spedizione, dopo aver eseguito tutte le verifiche di conformità a quanto stabilito nel presente manuale.

L'UOP provvede a tutti gli adempimenti relativi alla spedizione, compresa la compilazione delle ricevute di invio e di ritorno per le raccomandate, l'affrancatura e le distinte da consegnare all'Ufficio postale.

Sarà cura dell'Ufficio Protocollo recapitare la copia della lettera trattenuta all'Unità Organizzativa Responsabile per l'archiviazione nel fascicolo di competenza unitamente a tutte le ricevute di spedizione.

6.2.3 Documenti interni

La comunicazione interna ad AltaVita può avvenire per via formale oppure per via informale.

I documenti interni formali possono essere sia informatici che analogici e sono soggetti a registrazione di protocollo.

I documenti interni informali consistono nello scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione.

Tali comunicazioni sono trasmesse mediante posta elettronica interna e non vengono protocollate.

7 MODALITA' DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO.

I documenti ricevuti e spediti da AltaVita, ad eccezione dei documenti sotto specificati, sono soggetti a registrazione di protocollo.

Il registro di protocollo è unico ed è tenuto e conservato esclusivamente presso l'UOP della Segreteria Generale. La numerazione in esso contenuta inizia di anno in anno dal 1 gennaio e si chiude al 31 dicembre. Per ogni documento protocollato viene attribuito un solo numero di protocollo, composto da almeno sette cifre numeriche. Non è consentita la registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

Il registro di protocollo è un atto pubblico originario, che certifica l'effettivo ricevimento e l'effettiva spedizione di un documento in una certa data, indipendentemente dalla regolarità del documento stesso ed è opponibile ai terzi. Tale registro è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

E' facoltà di AltaVita stampare mensilmente il registro di protocollo per soli fini di consultazione

7.1 Registrazione dei documenti

Per ogni documento soggetto a protocollazione viene inserita apposita registrazione mediante il sistema di gestione del protocollo informatico, contenente dei dati obbligatori e delle informazioni accessorie. Gli elementi obbligatori sono:

- numero di Protocollo, composto di almeno sette cifre, è generato automaticamente dal sistema ed è imm modificabile;
- data di registrazione, generata automaticamente dal sistema;
- mittente per il documento in arrivo/destinatario per il documento in uscita;
- oggetto del documento;
- impronta;
- classificazione;
- UOR responsabile a cui il documento viene smistato.

Gli elementi facoltativi consistono in:

- collegamento del documento con un eventuale numero di protocollo precedente;
- modalità di trasmissione;
- numero di allegati e loro descrizione;
- copie per conoscenza;
- eventuali annotazioni.

La registrazione degli elementi obbligatori è rilevante sul piano giuridico probatorio, d'altro canto, la registrazione dei dati accessori rileva sul piano amministrativo, organizzativo e gestionale.

Qualsiasi variazione apportata successivamente dagli operatori di protocollo, comunque entro la mattinata successiva, viene tracciata e conservata con un criterio di storicizzazione, evidenziando data, ora e utente che ha effettuato la modifica.

7.2 Modalità di registrazione

L'UOP provvede alla registrazione dei documenti in entrata nel medesimo giorno di ricezione. I documenti devono essere registrati una sola volta, anche in caso di più destinatari il documento avrà un unico numero di protocollo.

Nel caso di temporanea, eccezionale e imprevista impossibilità a procedere alla registrazione nella medesima giornata di ricezione, e qualora dalla mancata registrazione possa venir meno in diritto di terzi, il Responsabile della Gestione Documentale, con apposito provvedimento, differisce i termini per la registrazione, individuando i documenti da ammettere, le cause e il termine entro il quale la registrazione deve comunque essere effettuata.

In ogni caso nei documenti oggetto di registrazione successiva, viene apposto il timbro con la data di effettiva ricezione.

7.3 Segnatura di protocollo

La segnatura di protocollo è l'apposizione, o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso, permettendone l'individuazione in maniera inequivocabile. Tale operazione è effettuata contemporaneamente alla registrazione di protocollo.

Le informazioni minime contenute nella segnatura di protocollo sono le seguenti:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;

- codice identificativo del registro;
- data e numero di protocollo del messaggio ricevuto o inviato;
- oggetto;
- mittente;
- il destinatario.

Nella segnatura di un documento protocollato in uscita possono essere specificate le seguenti informazioni:

- persona, ufficio destinatario,
- indice di classificazione;
- identificazione degli allegati;
- informazioni sul procedimento e sul trattamento.

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

In caso di documenti analogici la segnatura avviene mediante apposizione di un'etichetta sulla quale vengono riportate le seguenti informazioni:

- codice identificativo dell'Istituto;
- codice identificativo dell'Area Organizzativa Omogenea;
- data e numero di protocollo del documento.

L'operazione di acquisizione dell'immagine dei documenti analogici viene effettuata successivamente alla segnatura in modo da acquisire con l'operazione di scansione, come immagine, anche il "segno" sul documento.

7.4 Documenti esclusi dalla registrazione

Ai sensi di quanto previsto dall'art. 53, comma 5, del D.P.R. 445/2000 sono esclusi dalla registrazione i seguenti documenti:

- Gazzette Ufficiali, Bollettini Ufficiali P.A.;
- notiziari P.A.;
- giornali, Riviste, Libri e pubblicazioni su qualunque supporto;
- materiali pubblicitari;

- materiali statistici;
- atti preparatori interni;
- posta di carattere esclusivamente privato su cui appare la parola RISERVATA.

Le ricevute di ritorno, sulle quali precauzionalmente è stato riportato il numero del protocollo attribuito al documento di riferimento, non vengono protocollate bensì conservate unitamente al suddetto documento a cura dell'Unità Organizzativa Responsabile.

7.5 Documenti soggetti a registrazione particolare

Sono altresì esclusi dalla registrazione di protocollo i seguenti documenti soggetti a registrazione particolare su appositi registri:

- Determinazioni;
- Deliberazioni del Consiglio di Amministrazione;
- Delibere Presidenziali;
- Ordinanze del Presidente;
- Buoni d'ordine;
- Ordini di pagamento e di incasso;
- Fatture.

7.6 Conservazione del registro giornaliero di protocollo

Il registro di protocollo giornaliero viene sottoposto a conservazione seguendo accuratamente il flusso procedurale indicato nelle regole tecniche e precisamente come segue:



Tale registro è inviato al sistema di conservazione entro il giorno lavorativo successivo, garantendone l'immodificabilità del contenuto, ai sensi di quanto previsto dall'art. 7, comma 5, del DPCM 3 dicembre 2013.

L'utente carica sul Sistema documentale in cartelle organizzate i registri di protocollo giornalieri corredati di firme e log. In particolare sono prodotti i seguenti oggetti:

- File PROTOCOLLO.pdf/A del giorno richiesto con Impronta sha256 del protocollo e degli eventuali file allegati. Non vengono archiviati i files ma solo l'impronta sha256-hash degli stessi;
- File LOG.pdf/A del giorno richiesto: riporta le informazioni dei protocolli ed eventuali allegati in formato XML;
- File METADATI.xlm del giorno richiesto: riassume brevemente il contenuto dei documenti in modo da facilitarne l'identificazione.

Per ognuno di questi oggetti viene generata una entrata indice del pacchetto di versamento.

Un task schedulato dal lunedì al venerdì alle ore 12,00 inoltra al sistema di conservazione il pacchetto di versamento costituito con gli oggetti di cui sopra. A buon fine del processo, sul sistema documentale, l'indice e i documenti/registri correlati vengono segnati come "conservati".

7.6.1 Metadati del registro di protocollo giornaliero

I metadati da associare al Registro giornaliero di protocollo, comprensivi dei metadati minimi individuati per tutte le tipologie documentali, sono i seguenti:

1. Identificativo univoco e persistente
2. Data di chiusura (*data di creazione del registro*)
3. Soggetto produttore
4. Soggetto produttore 2 (Operatore che ha prodotto il Registro - Nome, Cognome, Codice fiscale)
5. Destinatario (Nome, Cognome, Codice fiscale se disponibile)
6. Impronta del documento informatico
7. Codice identificativo dell'amministrazione (*codice IPA*)
8. Denominazione dell'amministrazione
9. Codice identificativo dell'area organizzativa omogenea
10. Responsabile (*Responsabile della gestione documentale o Responsabile del servizio per la tenuta del protocollo informatico - Nome, Cognome, Codice fiscale*)
11. Oggetto (*descrizione della tipologia di registro; ad es. "Registro giornaliero di protocollo", "Registro giornaliero delle modifiche di protocollo", ecc.*)
12. Codice identificativo del registro
13. Numero progressivo del registro
14. Anno
15. Numero della prima registrazione effettuata sul registro
16. Numero dell'ultima registrazione effettuata sul registro
17. Data della prima registrazione effettuata sul registro
18. Data dell'ultima registrazione effettuata sul registro.

7.6.2 Sottoscrizione del registro di protocollo giornaliero

Il registro di protocollo viene generato in modo automatico attraverso l'estrazione dal sistema documentale di un insieme di dati, secondo una struttura predeterminata, per essere trasferito in forma statica nel sistema di conservazione, come indicato all'art. 3, comma 1, lettera d), del DPCM 13 novembre 2014.

Non si rende necessaria la sua sottoscrizione con firma digitale né ai fini di garantirne le caratteristiche di immodificabilità ed integrità né allo scopo di assicurarne la provenienza e l'autenticità, in quanto il registro di protocollo è comunque riferibile al pubblico ufficiale da cui è formato, cioè il responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo.

8 CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO

8.1 Documenti presentati in sede di gara di appalto

La corrispondenza che riporta l'indicazione "offerta" – "gara d'appalto" – "preventivo" o simili, o dal suo involucro è possibile evincere che si riferisce alla partecipazione a una gara, non viene aperta, ma viene timbrata dall'unità Operativa di Protocollo, registrata a protocollo e successivamente inoltrata all'Unità Organizzativa Responsabile che provvede alla sua custodia sino all'espletamento della gara.

Dopo l'apertura delle buste l'Unità Organizzativa Responsabile riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.

8.2 Lettere anonime o prive di firma

La lettera anonima giunta all'Unità Organizzativa di Protocollo, una volta aperta e attestata l'assenza di ogni riferimento al mittente, viene sottoposta all'attenzione del Segretario/Direttore Generale o persona delegata, il quale valuterà se sottoporla a protocollazione o meno. In caso affermativo sul campo mittente sarà apposta la dicitura "anonimo", in caso negativo la lettera verrà eliminata.

Nel caso di lettere prive di firma vanno protocollate con l'indicazione di "lettere prive di firma".

L'Unità Organizzativa Responsabile valuterà poi se il documento privo di firma debba ritenersi valido e come tale essere trattato all'interno di un procedimento amministrativo.

8.3 Documenti pervenuti per errore

I documenti pervenuti per errore non vengono protocollati e devono essere spediti immediatamente al destinatario con la dicitura "Erroneamente pervenuto ad AltaVita-IRA il".

8.4 Documenti in partenza con destinatari plurimi

In caso di documenti informatici da spedire a molteplici destinatari viene riportato il nominativo del primo nell'apposito campo e fornita l'indicazione di un allegato con gli altri destinatari.

8.5 Assegnazione dei documenti

Successivamente alla protocollazione i documenti vengono assegnati all'Unità Organizzativa Responsabile competente e al proprio Responsabile del Procedimento, che provvede alla presa in carico, assumendo la responsabilità del relativo procedimento amministrativo.

Il Servizio di Protocollo memorizza tutti i passaggi, conservando l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.

La traccia è rilevante anche ai fini di individuare i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

In caso di documento digitale l'assegnazione avviene attraverso i canali telematici al termine della registrazione di protocollo, di segnatura e di memorizzazione su supporti informatici in modo non modificabile.

Il Responsabile del Procedimento potrà visualizzare i documenti e la presa in carico avverrà automaticamente nella stessa data di assegnazione.

I destinatari del documento per "competenza" e/o per "conoscenza" lo ricevono esclusivamente in formato digitale.

In caso di documento cartaceo l'Unità Organizzativa di Protocollo acquisisce mediante scanner l'immagine del documento e successivamente invia il plico all'Unità Organizzativa Responsabile competente.

9 ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

Ai sensi dell'art. 54 del D.P.R. 445/2000 le informazioni non modificabili di cui all'articolo 53 lett.a), b), c), d), e) e f) sono annullabili, ma devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura.

La procedura per indicare l'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione.

L'indicazione dell'annullamento della registrazione va apposta anche sul documento, tramite barratura della segnatura, se cartaceo.

L'annullamento viene disposto dal Responsabile della Gestione Documentale che adotta le procedure previste dal citato DPR 445/2000.

Eventuali errori di digitazione dei dati immutabili che possono compromettere le funzioni di ricerca vengono valutati di volta in volta ed eventualmente corretti senza pregiudicare il contenuto giuridico dei medesimi.

10 REGISTRO DI EMERGENZA

In caso di impossibilità nell'utilizzo del protocollo informatico, i documenti verranno registrati su un supporto alternativo detto "Registro di emergenza" (allegato ___).

L'impossibilità deve sostanziarsi in una interruzione del servizio oltre le tre ore o che comunque pregiudichi la registrazione a protocollo in caso di scadenze inderogabili e prescrittive.

Il registro di emergenza si apre ogni anno al 1 gennaio e si chiude il 31 dicembre. Il Responsabile della Gestione Documentale annota a fine anno l'eventuale mancato utilizzo del medesimo registro.

Le registrazioni di protocollo possono avvenire mediante l'utilizzo del personale computer, se possibile, con la compilazione di modulo in formato excel, oppure, in caso di impossibilità mediante la trascrizione manuale in un modulo cartaceo.

I dati richiesti per le registrazioni sul registro di emergenza sono le medesime che devono essere trascritte nel sistema di protocollo informatico.

Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione sono associati anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

I documenti annotati ne registro e trasferiti nel protocollo generale riporteranno due numeri: uno derivante dal registro di emergenza, l'altro, attribuito dal protocollo generale.

La data da cui decorrono i termini per il procedimento amministrativo coincide con la data di registrazione nel registro di emergenza.

Il Responsabile della gestione documentale autorizza l'apertura del registro di emergenza, annotandone la data e l'ora, la causa di interruzione e, inoltre, in fase di chiusura deve apporre l'ora.

La segnatura di protocollo avviene apponendo un timbro sul documento con le informazioni ricavabili dal registro suddetto.

11 DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO

Di seguito viene descritta la soluzione per il protocollo informatico, comprensiva di fascicolazione e di classificazione dei documenti oggetto di protocollo ed è utile anche all'utente autorizzato alla protocollazione e alla fascicolazione e classificazione della pratica.

La schermata che appare aprendo il programma è quella di registrazione dei protocolli; questa scelta operativa evita qualche passaggio inutile in quanto le operazioni che vengono svolte solitamente nel programma sono quelle di registrazione e/o di ricerca. Premendo quindi il pulsante NUOVO si dà inizio alla registrazione; nella registrazione vengono proposte ANNO, DATA e NUMERO PROTOCOLLO (quest'ultimo solitamente è il numero progressivo dell'anno ed è conforme a quanto dettato dalla normativa). Per ogni nuova registrazione viene ovviamente identificato il TIPO, l'ARGOMENTO dove sono collegati i riferimenti di archivio e l'OGGETTO del protocollo. Il protocollo inoltre viene gestito con la possibilità di modificare i riferimenti di archivio.

Inoltre nella scelta del Mittente e/o del Destinatario è possibile avere :

ESIBENTE: attinge dalla tabella Esibenti specifica del programma Protocollo.

CLIENTE/FORNITORE: attinge dalle anagrafiche clienti/fornitori della Contabilità Economica/Finanziaria.

OSPITI: attinge dal fascicolo ospiti della Contabilità Ospiti / Contabilità Utenti / CSS.

PERSONE DI RIFERIMENTO: attinge dalle persone di riferimento della Contabilità Ospiti Contabilità Utenti / CSS.

DIPENDENTI: attinge dall'anagrafica dei dipendenti del software Stipendi/Presenze/Turni.

11.1 Ricerca protocolli

I parametri di ricerca dei protocolli registrati sono:

- DALLA DATA MOVIMENTO ... ALLA DATA MOVIMENTO...
- DAL NUMERO PROTOCOLLO ... AL NUMERO PROTOCOLLO ...
- TIPOLOGIA DI PROTOCOLLO
- DALLA DATA ALLA DATA DI RIFERIMENTO PER I PROTOCOLLI IN ARRIVO
- NUMERO DI RIFERIMENTO PER I PROTOCOLLI IN ARRIVO
- STATO PROTOCOLLO (Tutti – Stampati – Annullati)
- MITTENTE/I – DESTINATARIO/I – TUTTI

- ARGOMENTO/I – TUTTI
- UFFICIO/I – TUTTI
- PAROLA NELL'OGGETTO

11.2 Raggruppamento esibenti/argomenti

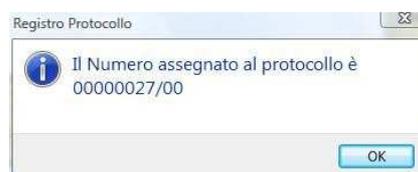
La funzione consente di raggruppare Esibenti e/o Argomenti per una razionalizzazione dei dati gestiti nel corso degli anni.

E' possibile scegliere l'operazione "RAGGRUPPA ESIBENTI" per ottenere l'elenco dei mittenti/destinatari, selezionare tramite flag le anagrafiche da raggruppare, selezionare il tipo di esibente e l'anagrafica desiderata ed infine premere il pulsante ELABORA. La nuova anagrafica sostituirà l'informazione nei protocolli già registrati e stampati di tutti gli anni.

Procedura analoga anche con l'opzione "RAGGRUPPA ARGOMENTI"; selezionare gli argomenti che si desiderano raggruppare e successivamente l'argomento che sostituirà nei protocolli già registrati quelli selezionati. In questo modo l'argomento prescelto sostituirà quelli selezionati in tutti i protocolli già registrati.

11.3 Gestione multipla inserimento protocolli

Il sistema consente l'inserimento multiplo contemporaneo dei dati nel registro protocollo. In automatico sarà il programma ad assegnare il numero di protocollo corretto nell'eventualità di registrazione multipla dei protocolli da parte di più operatori. L'operatore che si troverà in questa situazione sarà avvertito da un messaggio simile a quello riportato di seguito.



Il messaggio testimonia che il numero di protocollo assegnato in precedenza nella fase iniziale di registrazione è stato assegnato all'utente che per primo ha terminato e confermato l'operazione di inserimento; in questo caso al secondo utente, dopo aver confermato il suo inserimento, apparirà il messaggio.

11.4 Creazione/modifica password d'accesso

Gli utenti che hanno accesso al software "Protocollo Informatico" sono obbligatoriamente inseriti all'interno del sistema di autenticazione e autorizzazione che identificherà gli utenti

corrispondenti a persone fisiche (nome e cognome) e non sono accettati ad esempio utenti tipo "Ufficio Protocollo" o "Ufficio Amm.Vo".

11.5 Funzioni particolari

Tra gli utenti abilitati all'accesso nel Protocollo è identificato il Responsabile di Gestione (responsabile o dirigente interno alla Struttura) il quale potrà:

- **ANNULLARE** i protocolli registrati dai colleghi/collaboratori (tale informazione sarà registrata nel file LOG ed inviata in archiviazione digitale);
- **MODIFICARE** i protocolli registrati dai colleghi/collaboratori se NON ancora inviati in archiviazione digitale (tale informazione sarà registrata nel file LOG ed inviata in archiviazione digitale).

11.6 Gestione area organizzativa omogenea (AOO)

Il registro protocollo fa riferimento all'Area Organizzativa Omogenea (AOO) dell'Ente.

Nel caso in cui vi siano più AOO, ogn'una di esse gestirà una numerazione separata progressiva del proprio registro di protocollo.

11.7 Protocollo mail PEC

Come sopra descritto, le PEC vengono protocollate riportando nell'oggetto il contenuto descrittivo della mail ed allegando come file le notifiche/allegati che accompagnano la PEC. Con un unico numero di protocollo è quindi possibile gestire tutto il processo.

11.8 File

Tutti i files allegati vengono salvati all'interno di un database specifico creatosi in automatico; nel sistema di conservazione digitale del registro di protocollo informatico, vengono inviate solo le impronte digitali dei documenti allegati (sha256-hash) e non i fisici documenti.

11.9 Log

Ogni protocollo ha la sua videata di log in cui vengono memorizzate tutte le operazioni effettuate sul protocollo stesso indicando data/ora/utente/tipo di operazione (inserimento / modifica / annullamento / archiviazione).

12 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

L'art. 68 del D.P.R. 445/2000 prevede che ogni amministrazione debba dotarsi di un "*piano di conservazione*" degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti.

L'archivio e i singoli documenti sono inalienabili e, in quanto beni culturali, tutelati ai sensi e per gli effetti del "Codice dei Beni Culturali e del Paesaggio".

12.1 Sistema di Classificazione

Tutti i documenti registrati nel sistema di protocollo informatico devono essere classificati.

La classificazione è finalizzata alla corretta organizzazione dei documenti e dei fascicoli secondo un ordinamento logico riferito alle funzioni e alle attività dell'Istituto.

La classificazione si attua associando ai documenti dei codici numerici e caratterizza il sistema di fascicolazione dei documenti stessi.

Il Titolario di classificazione è organizzato in diversi livelli in particolare Titolo e Classe ed è attualmente dispiegato in otto Titoli come segue:

01 - Amministrazione

02 - Personale

03 - Ospiti

04 - Patrimonio

05 - Pratiche amministrative e contabili

06 - Massimario

10 - Archivi altri uffici

11 - Atti amministrativi

I fascicoli sono sempre costituiti sul livello inferiore del Titolario e numerati progressivamente per anno all'interno della classe stessa.

12.2 Fascicolo

Il fascicolo costituisce l'unità di base, indivisibile, di un archivio, mentre la busta, che contiene diversi fascicoli, si considera unità soltanto ai fini della conservazione materiale.

Talora il fascicolo comprende documenti relativi ad affari diversi, o a questioni di carattere generale.

Può essere articolato in sottofascicoli e inserti. Se l'archivio non è organizzato secondo criteri sistematici, è frequente trovare una pluralità di fascicoli miscelanei.

Il fascicolo rappresenta il raggruppamento organico dei documenti riferiti alla trattazione di uno stesso affare o procedimento amministrativo, che si costituisce nel corso dell'attività amministrativa, allo scopo di riunire, tutti i documenti utili allo svolgimento dell'attività.

Tutti i documenti registrati nel sistema di protocollo informatico devono essere fascicolati.

I fascicoli si identificano attraverso l'indice di classificazione (titolo e classe) e il numero di repertorio (numero e anno).

Per fascicolazione si intende l'operazione di inserimento del singolo documento nel relativo fascicolo, attraverso la registrazione nel sistema informatico del collegamento della registrazione di protocollo del singolo documento alla registrazione dei dati identificativi del fascicolo di destinazione.

I fascicoli possono essere distinti in varie categorie come segue:

- per affare
- per attività
- per procedimento amministrativo
- per persona fisica o persona giuridica

Un fascicolo è identificato nel sistema documentale e di archivio da una sua propria codifica costituita dall'indice di classificazione, dall'anno di costituzione e da un numero progressivo, oltre al suo oggetto e ad altri elementi che lo caratterizzino in modo inequivocabile.

Ad esempio i fascicoli per persona possono contenere tra i loro elementi identificativi un codice univoco associato alla persona di riferimento.

12.2.1 Formazione dei fascicoli informatici

Il Codice dell'Amministrazione Digitale impone che la pubblica amministrazione titolare del procedimento raccolga in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati.

Il fascicolo informatico reca l'indicazione:

- dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- delle altre amministrazioni partecipanti;
- del responsabile del procedimento;
- dell'oggetto del procedimento;
- dell'elenco dei documenti contenuti

Il sistema informatico di gestione dei documenti e del protocollo informatico consente la produzione di fascicoli e di inserire documenti correttamente protocollati e classificati in un fascicolo preesistente o di crearne uno nuovo. Parimenti consente di smistare un fascicolo tra una UOR e un'altra ovvero di trasferire la competenza di un fascicolo ad un'altra posizione organizzativa responsabile.

I metadati minimi associati ad ogni fascicolo informatico sono quelli indicati nell'allegato n. 5 del DPCM 3-12-2013 e il sistema di protocollo informatico viene adeguato a detta normativa entro i termini stabiliti dal decreto stesso.

Uno stesso documento può essere inserito in più fascicoli.

Il processo gestionale in obiettivo è il seguente:

- il documento entra nel sistema e viene protocollato
- il documento viene smistato alla UOR competente
- il documento produce l'apertura di un nuovo fascicolo oppure viene inserito in un fascicolo preesistente. Il documento può anche essere riferito a più fascicoli esistenti.

12.2.2 Sottofascicoli

Per particolari esigenze organizzative, è possibile creare sottofascicoli all'interno dei fascicoli principali. I sottofascicoli raggruppano quei documenti del fascicolo che si riferiscono ad aspetti particolari dell'oggetto del fascicolo stesso e che è necessario mantenere distinti. I sottofascicoli sono numerati progressivamente all'interno del fascicolo e sono aperti e gestiti in maniera analoga a quanto previsto per il fascicolo. Ad esempio il fascicolo del personale dipendente può contenere separati sottofascicoli organizzati secondo vari aspetti del rapporto contrattuale. La stessa dinamica può essere applicata al fascicolo 'Ospiti' per le tematiche specializzate relative alla gestione ma che si ritiene di mantenere aggregati (es: sottofascicolo amministrativo, psicologo, etc).

12.2.3 Repertorio fascicoli

Il repertorio dei fascicoli è l'elenco annuale, ordinato per progressione numerica, dei fascicoli formati all'interno di ciascuna classe del Titolario.

Sono presenti tanti repertori di fascicoli quante sono le classi previste dal Titolario di classificazione.

Il repertorio riporta, per ciascun fascicolo, almeno le seguenti informazioni:

- numero di repertorio;
- oggetto;

- UOR responsabile;
- elenco eventuali sottofascicoli;
- stato del fascicolo.

Il Responsabile del Servizio per la tenuta del Protocollo Informatico provvede annualmente, alla stampa del repertorio dei fascicoli dell'anno precedente e alla stampa degli aggiornamenti di quelli degli anni antecedenti. Il documento repertorio dei fascicoli costituisce a sua volta oggetto dell'archivio generale.

12.3 Il sistema archivio

L'Archivio raccoglie, ordina, conserva e rende consultabile, nel rispetto della vigente normativa, tutta documentazione prodotta dall'Istituto.

Il sistema archivio è unico all'interno della AOO e funzionalmente è strutturato in tre fasi:

- **Archivio corrente:** complesso di documenti relativi ad affari in corso;
- **Archivio di deposito:** complesso di documenti relativi ad affari conclusi;
- **Archivio storico:** complesso di documenti relativi ad affari conclusi da oltre 40 anni.

La documentazione che confluisce in Archivio di **deposito/storico** può essere conservata in sede diversa all'ubicazione della struttura.

La sezione corrente è, di norma, detenuta negli Uffici in quanto si tratta di documenti in corso di lavorazione, ovvero di documenti relativi ad affari o procedimenti non ancora conclusi.

La sezione corrente viene alimentata dalla corrispondenza ricevuta, inviata e/o interna formale relativa ad uno stesso affare conservata all'interno dei fascicoli.

La costituzione dei fascicoli, delle serie e dei repertori è funzione di base della gestione archivistica.

Periodicamente, e comunque almeno una volta all'anno si provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposita sezione di deposito dell'archivio generale costituito presso l'Istituto.

La regolare periodicità dell'operazione è fondamentale per garantire la qualità del materiale depositato.

Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.

Prima di effettuare il conferimento di cui sopra, si procede alla verifica:

- dell'effettiva conclusione ordinaria della pratica;
- dell'effettiva trascrizione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;
- di avvenuto scarto di eventuali copie e fotocopie di documentazione soggetti a scarto al fine di garantire la presenza di tutti e soli i documenti pertinenti alla pratica in oggetto;
- che il materiale così rimanente sia correttamente organizzato.

Ricevuti i fascicoli e controllato l'aggiornamento del rispettivo repertorio, il responsabile del protocollo redige un elenco di versamento, come disposto dal testo unico.

Copia di esso viene conservata dal Responsabile di cui sopra che ha versato la documentazione, anche allo scopo di ricercare pratiche "esaurite" .

Il fascicolo nell'archivio di deposito viene archiviato per materia con lo stesso ordine di classificazione dell'archivio corrente e per ordine cronologico.

Con la stessa metodologia vengono riversati nell'archivio di deposito anche gli altri repertori e le altre serie archivistiche presenti all'interno dell'Istituto.

I fascicoli del personale vanno trasferiti dall'archivio corrente all'archivio di deposito l'anno successivo a quello di cessazione dal servizio.

In relazione a quanto sopra è importante ribadire che le norme sono valide sia per i flussi di documenti cartacei che per quelli informatici.

Per questi ultimi, ci si riferisce al fascicolo elettronico, di repertorio elettronico, di versamento logico dell'archivio corrente in quello di deposito.

Quando saranno compiuti i progetti di dematerializzazione di determinati procedimenti da individuare, si provvederà a sottoporre ad aggiornamento la presente sezione del manuale per descrivere le modalità operative che dovranno essere seguite.

I documenti selezionati destinati alla sezione storica dell'archivio sono trasferiti contestualmente agli strumenti che ne garantiscono l'accesso secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali e di accesso ai dati normato dal decreto legislativo n. 196/2003.

12.3.1 Modalità per lo sfoltimento e versamento fascicoli dall'archivio corrente

Il Responsabile del procedimento amministrativo, trascorso un congruo periodo di tempo dalla cessazione degli affari che sta trattando, ed almeno una volta l'anno, provvede:

- allo sfoltimento dei fascicoli che si sono formati;
- alla redazione di un elenco degli stessi;

- ed al loro versamento presso l'archivio di deposito presso l'Unità organizzativa responsabile (UOR).

In nessun caso possono essere versati all'archivio di deposito fascicoli contenenti documenti i cui termini per la presentazione di ricorsi amministrativi o giudiziari non sono ancora scaduti.

12.3.2 Movimentazione dei fascicoli

L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito ad un ufficio della medesima UOR o di un'altra UOR deve avvenire solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.

Tale affidamento temporaneo avviene previa richiesta contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, la sua UOR o ufficio di appartenenza e la sua firma.

Un esemplare della richiesta viene conservato all'interno del fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio.

Tale movimentazione viene registrata in un apposito Registro di carico e scarico a cura del Responsabile dell'archivio. In esso sono riportati, oltre ai dati contenuti nella richiesta, anche la data di consegna/ invio e quella di restituzione, nonché delle eventuali note sullo stato della documentazione.

12.3.3 Modello per il trasferimento atti dall'archivio corrente

Ai fini del riversamento degli archivi correnti all'archivio di deposito, i fascicoli trasferiti sono elencati in apposite distinte in un modello con le seguenti caratteristiche generali:

| | |
|----------------------|---|
| Intestazione modello | Progressivo elenco / Anno di riferimento |
| | Elenco di versamento dei fascicoli chiusi dall'archivio corrente all'archivio di deposito |
| Colonne del Modulo | |
| Colonna prima | Numero Busta |
| Colonna seconda | Titolo della Busta – Titolo dei fascicoli contenuti – Classificazione dei fascicoli contenuti |
| Colonna terza | Anno di Inizio |
| Colonna quarta | Anno di Fine |
| Colonna quinta | Annotazioni |

12.3.4 Riordino archivio di deposito

L'operazione di riordino dell'archivio di deposito viene effettuata di norma con cadenza annuale e consiste nella valutazione della documentazione, organizzazione delle schede e creazione di elenchi di materiale omogeneo e nella sistemazione fisica del materiale

facendo riferimento al Titolario di archivio, con l'obiettivo di realizzare un inventario della documentazione conferita dalla sezione corrente dell'archivio a quello di deposito.

L'operazione si conclude con la sistemazione fisica del materiale inserendolo in contenitori che riportano l'indicazione del contenuto, la classificazione e la temporalità del contenuto.

Nell'ambito della sezione di deposito dell'Archivio viene effettuata la selezione e lo scarto degli atti che l'Istituto non ritiene più opportuno conservare ulteriormente. Un documento è ritenuto non conservabile quando ha perso rilevanza amministrativa e non assume contemporaneamente rilevanza storica.

L'Istituto non provvede allo scarto di documenti considerati "vitali" e cioè necessari a ricercare lo stato giuridico dell'ente stesso, la sua situazione legale e finanziaria, garantire i diritti dei dipendenti e degli ospiti, proteggere i suoi interessi.

Lo scarto dei documenti non viene effettuato per documenti per i quali sia prevista la conservazione permanente dei documenti in originale e relativamente ad eventuali loro copie, lo scarto non viene effettuato qualora le stesse contengano annotazioni amministrative o visti essenziali per ricostruire il procedimento nella sua correttezza.

12.4 Piano di conservazione

L'art. 68 del D.P.R. 445/2000 prevede che ogni amministrazione debba dotarsi di un "*piano di conservazione*" degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti.

L'eliminazione di taluni documenti deve essere preceduta dalla valutazione delle procedure di produzione documentaria, in modo che vengano assicurati la comprensione dell'attività dell'ente produttore e il mantenimento delle attestazioni di diritti.

L'adozione del piano di conservazione impegna l'Istituto agli adempimenti relativi alla procedura di scarto.

Detta procedura si sostanzia in un provvedimento adottato dall'amministrazione (determina dirigenziale) e nella acquisizione dell'autorizzazione da parte della Soprintendenza Archivistica competente per territorio.

E' da tener conto che il responsabile del servizio provvede a gestire lo scarto anche dei documenti posti in conservazione digitale a lungo termine. Il conservatore procederà allo scarto di parte o tutto il pacchetto di archiviazione previa la procedura di identificazione dei documenti/fascicoli da scartare, la puntuale loro elencazione e stampa, l'ottenimento da parte dell'istituto dell'autorizzazione prevista dalla legge, la comunicazione formale al conservatore di procedere con l'eliminazione e la ricostituzione eventuale dei pacchetti di

archiviazione residui. L'originale del verbale di avvenuta eliminazione viene conservato dall'Istituto e, per conoscenza, viene inviato alla Soprintendenza Archivistica territorialmente competente.

I documenti e gli atti in formato analogico sottoposti a procedura di scarto sono devoluti gratuitamente alle Organizzazioni previste. In caso di rifiuto o di impossibilità al trasferimento alle Organizzazioni previste, l'Istituto provvede in proprio all'eliminazione fisica della carta, individuando modalità di distruzione che garantiscano dalla diffusione illecita di documenti, con particolare riferimento a quelli riservati e tenendo presente il decreto legislativo n. 196/2003 'Codice in materia di protezione dei dati personali'.

L'originale del verbale di consegna e di avvenuta eliminazione viene conservato dall'Istituto e, per conoscenza, viene inviato alla Soprintendenza Archivistica territorialmente competente.

13 SISTEMA DI GESTIONE DEI PROCEDIMENTI AMMINISTRATIVI, MODULISTICA ON LINE

Nell'ambito delle azioni progettuali che l'Istituto intraprenderà per adempiere alla normativa che evoca trasformazioni verso il digitale di tutti i documenti e procedimenti e comunicazione con i soggetti esterni si procederà contestualmente ad aggiornare il sistema informatico di protocollo e gestione documentale.

14 DOCUMENTI DI NATURA SANITARIA

La gestione degli 'ospiti' comporta il trattamento di dati sociali e sanitari. Al momento la documentazione é trattata in modo cartaceo e le cartelle fascicoli sono gestiti e archiviati secondo le discipline specifiche. Il piano di conservazione integra dette tipologie documentarie.

15 NORME TRANSITORIE E FINALI

Le disposizioni del presente manuale si intendono modificate per effetto di modificazioni delle norme in materia di protocollo informatico, di documento informatico, di gestione degli archivi, delle norme di sicurezza e delle norme in materia di protezione dei dati personali.

Con l'entrata in vigore del presente manuale sono abrogate tutte le norme regolamentari interne all'Istituto/AOO con esso contrastanti.

Secondo il disposto del comma 3 dell'art. 5 del DPCM 3 dicembre 2013, il Manuale di gestione viene reso pubblico e portato a conoscenza anche mediante i piani di formazione interna al personale interessato.