



MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DELL'ASP AMBITO 9 DI JESI

STATO DELLE REVISIONI

REV. N.	DESCRIZIONE REVISIONE	APPROVAZIONE	ENTRATA IN VIGORE	MODIFICHE APPORTATE
0	Prima emissione	Decisione del Direttore n. 91 del 19/03/2020	01/04/2020	
1	Revisione	Deliberazione del CdA n. 22 del 20/04/2023	20/04/2023	<ul style="list-style-type: none"> - Revisione Manuale; - Modifica Allegato 1 – AOO e Organigramma; - Modifica Allegato 2 – Procedimenti amministrativi ASP; - Inserimento Allegato 7 - Piano di organizzazione delle aggregazioni documentali e del Piano di conservazione.

SOMMARIO

1.	IL MANUALE DI GESTIONE	6
1.1.	Che cos'è, a cosa serve e a chi serve	6
1.2.	Modalità di redazione	6
1.3.	Forme di pubblicità e di divulgazione	6
1.4.	Quadro normativo di riferimento	7
2.	QUADRO ORGANIZZATIVO ISTITUZIONALE	8
2.1.	Area organizzativa omogenea e unità organizzative	8
2.2.	Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti	8
2.3.	Responsabile della gestione documentale	9
2.4.	Profili di abilitazioni di accesso interno ed esterno alle informazioni documentali	9
2.5.	Posta elettronica istituzionale	9
2.6.	PEC istituzionale	9
2.7.	Eliminazione dei registri di protocollo diversi dal protocollo informatico	10
2.8.	Responsabile della conservazione	10
3.	IL DOCUMENTO	12
3.1.	Documento informatico e analogico: definizione e disciplina giuridica	12
3.2.	Redazione/formazione del documento informatico	13
3.2.1.	Validazione temporale	14
3.2.2.	Formati	14
3.3.	Redazione/formazione del documento amministrativo informatico	15
3.4.	Redazione/formazione del documento amministrativo analogico	15
3.5.	Documenti redatti in originale su supporto analogico	16
3.6.	Il documento amministrativo informatico costituito dal corpo della PEC istituzionale	16
3.7.	Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale	17
3.8.	Distinzione dei documenti in base allo stato di trasmissione (arrivo, partenza, scambiati tra UO, scambiati tra AOO dello stesso ente, fax, PEC, e-mail)	17
3.9.	Duplicato del documento informatico e analogico	18
3.10.	Copia del documento informatico e analogico: nozione	18
3.11.	Copia informatica del documento amministrativo analogico	18
3.12.	Estratto informatico di documento amministrativo informatico	19
3.13.	Copia analogica di documento amministrativo informatico	19
3.14.	Metadati	20
3.14.1.	Obiettivi dei metadati archivistici	20
3.14.2.	Metadati essenziali per la registrazione nel protocollo informatico	20

4.	IL FASCICOLO	21
4.1.	Il fascicolo: definizione e funzione.....	21
4.2.	Il fascicolo analogico: formazione, implementazione e gestione	21
4.3.	Il fascicolo informatico: formazione, implementazione e gestione.....	22
4.4.	I fascicoli annuali ripetitivi	23
4.5.	Il fascicolo ibrido.....	23
4.6.	Metadati del fascicolo informatico	24
4.7.	Il repertorio dei fascicoli informatici.....	24
5.	LA GESTIONE DELL'ARCHIVIO CORRENTE	25
5.1.	Definizione.....	25
5.2.	Buone prassi per la gestione dell'archivio corrente	25
5.3.	Gli strumenti dell'archivio corrente.....	26
5.3.1.	Registro di protocollo	26
5.3.2.	Titolario (piano di classificazione).....	26
5.3.3.	Repertorio dei fascicoli	27
5.3.4.	Repertori.....	27
5.3.5.	Massimario di selezione o Piano di conservazione.....	27
5.4.	Spostamento di un archivio corrente analogico	28
6.	IL PROTOCOLLO INFORMATICO	29
6.1.	Registratura	29
6.1.1.	Elementi obbligatori immutabili (Registratura).....	29
6.1.2.	Elementi obbligatori modificabili.....	30
6.1.3.	Elementi non obbligatori modificabili.....	30
6.2.	Data e ora regolate sul UTC	30
6.3.	Segnatura.....	30
6.3.1.	Per il documento informatico	30
6.3.2.	Per il documento cartaceo (analogico)	31
6.4.	Modalità di produzione e di conservazione delle registrazioni	31
6.5.	La registrazione differita (o "protocollo differito").....	31
6.6.	Rilascio di ricevute attestanti la ricezione di documenti cartacei.....	32
6.7.	La ricevuta di avvenuta registrazione	32
6.7.1.	Per il documento cartaceo (analogico)	32
6.7.2.	Per il documento informatico	32
6.8.	Documenti esclusi dalla registrazione di protocollo	33
6.9.	Il registro giornaliero di protocollo	33
6.10.	Il registro di emergenza	34

7.	REGISTRI E REPERTORI INFORMATICI	35
7.1.	Repertorio - Nozione	35
7.2.	Repertori attivi.....	35
7.3.	Repertorio dei fascicoli	35
8.	FLUSSO DI LAVORAZIONE DEI DOCUMENTI	36
8.1.	Flusso del documento informatico in arrivo	36
8.2.	Ricezione dei documenti informatici tramite la casella di posta elettronica certificata (PEC) istituzionale	36
8.3.	Ricezione di documenti informatici nella casella di posta elettronica istituzionale	36
8.4.	Ricezione di documenti informatici su supporti rimovibili	37
8.5.	Ricezione link a documenti	37
8.6.	Priorità nella registrazione dei documenti informatici in arrivo	38
8.7.	Flusso del documento cartaceo (analogico)	38
8.8.	Apertura delle buste	38
8.8.1.	Conservazione ed eliminazione delle buste.....	39
8.9.	Priorità nella registrazione dei documenti analogici in arrivo	39
8.10.	Protocollo particolare	39
8.10.1.	Procedure del protocollo particolare.....	39
8.11.	Annullamento di una registrazione.....	39
8.12.	Corresponsabilità di un documento e di un fascicolo.....	40
8.13.	Documenti scambiati tra uffici non soggetti a registrazione di protocollo.....	41
8.14.	Casi di rigetto	41
8.15.	Flusso del documento informatico in partenza	41
8.16.	Flusso del documento informatico tra UO della stessa AOO.....	42
9.	CASISTICA E COMPORTAMENTI	43
9.1.	Gestione di concorsi e selezioni.....	43
9.2.	Denunce di infortuni	43
9.3.	Certificati di malattia	43
9.4.	Atti giudiziari	43
9.5.	Fatture elettroniche (Fattura PA)	44
9.6.	DURC on-line.....	45
9.7.	Gare e procedure negoziate gestite in modalità telematica	45
9.8.	Documenti informatici con oggetto multiplo	46
9.9.	Documenti pervenuti via PEC	46
9.10.	Gestione di più documenti diversi trasmessi via PEC o email.....	46
9.11.	Gestione di soli allegati pervenuti via PEC e di documenti costituiti dal solo corpo della PEC....	46
9.12.	Documenti pervenuti a mezzo <i>e- mail</i> semplice (non certificata)	47

9.13.	Gestione del secondo esemplare.....	47
9.14.	Documenti scambiati tra UO della stessa AOO.....	47
9.15.	Documenti anonimi	48
10.	DALL'ARCHIVIO CORRENTE ALL'ARCHIVIO DI DEPOSITO	49
10.1.	Archivio	49
10.2.	Archivio corrente, deposito, storico	49
10.3.	Trasferimento dei fascicoli cartacei nell'archivio storico.....	49
10.4.	Trasferimento dei fascicoli informatici	50
10.5.	Conservazione.....	50
11.	IL SISTEMA INFORMATICO E IL PIANO DI SICUREZZA	51
11.1.	Il modello organizzativo.....	51
11.2.	Il sistema di gestione documentale	51
11.3.	Accesso	51
11.3.1.	Accesso da parte degli utenti interni all'Amministrazione	51
11.3.2.	Gestione della riservatezza	52
11.4.	Sicurezza fisica dei documenti	52
11.5.	Sicurezza fisica del data center	52
11.6.	Rete dati.....	53
11.7.	Le postazioni di lavoro	53
11.8.	Le procedure comportamentali ai fini della protezione dei documenti	53

Allegato n. 1 – AOO e Organigramma

Allegato n. 2 – Procedimenti amministrativi ASP

Allegato n. 3 – Titolario di classificazione

Allegato n. 4 – Regole e modelli per l'attivazione del registro di emergenza

Allegato n. 5 – Raccomandazioni AURORA

Allegato n. 6 – Diagrammi di flusso dei documenti in arrivo, in partenza e interni

Allegato n. 7 – Piano di organizzazione delle aggregazioni documentali e Piano di conservazione dell'ASP
 AMBITO 9

1. IL MANUALE DI GESTIONE

1.1. Che cos'è, a cosa serve e a chi serve

Il manuale di gestione è uno strumento operativo che descrive il sistema di produzione e di gestione documenti (tradizionali e digitali), come previsto dall'art. 3 e dall'art. 5 del DPCM 3 dicembre 2013¹. Serve a indicare le procedure e a fornire le istruzioni per la corretta formazione, gestione, tenuta e conservazione della documentazione analogica e digitale. Esso descrive, altresì, le modalità di gestione dei flussi documentali e degli archivi, in modo tale da organizzare e governare la documentazione ricevuta, inviata o comunque prodotta dall'amministrazione secondo parametri di corretta registrazione di protocollo, smistamento, assegnazione, classificazione, fascicolatura, reperimento e conservazione dei documenti.

Il manuale di gestione costituisce una guida per l'operatore di protocollo e per il cittadino e per le imprese. Al primo, per porre in essere le corrette operazioni di gestione documentale, agli ultimi due per comprendere e per collaborare nella gestione documentale stessa (ad esempio utilizzando formati idonei per la formazione delle istanze, ecc.).

1.2. Modalità di redazione

La redazione del manuale di gestione deve temperare l'assolvimento dell'obbligo normativo e le esigenze concrete dell'Amministrazione (cfr. l'Appendice normativa descritta nell'allegato 1).

Per tale motivo è stato redatto previa verifica e analisi del modello organizzativo e dei procedimenti amministrativi (elencati nell'allegato 2).

Per la redazione di questo Manuale è stato utilizzato il modello di Manuale di Gestione dell'Università dell'Insubria, sviluppato nell'ambito del progetto *Procedamus* per gli atenei aderenti (www.procedamus.it).

1.3. Forme di pubblicità e di divulgazione

Il manuale di gestione è reso pubblico mediante la diffusione sul sito istituzionale, come previsto dal DPCM 3 dicembre 2013, art. 5, comma 3. Deve, inoltre, essere capillarmente divulgato alle unità organizzative dell'area organizzativa omogenea (AOO, di cui al § 2.1) dell'ENTE, al fine di consentire la corretta diffusione delle nozioni e delle procedure documentali e di consentire la necessaria collaborazione di cui al § 1.1.

È prevista, infine, un'attività di formazione continua e permanente in materia di gestione documentale per tutte le unità organizzative responsabili dell'Ente.

¹ Il legislatore ha approvato due DPCM 3 dicembre 2013, contenenti entrambi le regole tecniche previste dall'art. 71 del CAD (D.Lgs. 7 marzo 2005, n. 82) ed entrambi pubblicati nella Gazzetta ufficiale 12 marzo 2014, n. 59 – SO n. 20. Il primo contiene le *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*, mentre il secondo contiene le *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*. Se non diversamente indicato, in questo manuale si fa riferimento al secondo, citato semplicemente come DPCM 3 dicembre 2013.

1.4. Quadro normativo di riferimento

Di seguito sono riportate le disposizioni normative che disciplinano l'ambito tematico della gestione dei flussi documentali aggiornate al secondo semestre dell'anno 2019:

- DPR 28 dicembre 2000, n. 445, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- D.Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, come modificato dal D. Lgs. n. 101/2018 (regolamento Ue n. 679/2016);
- D.Lgs. 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
- D.Lgs. 7 marzo 2005, n. 82, Codice dell'Amministrazione digitale;
- DPCM 3 dicembre 2013, Regole tecniche per il protocollo informatico ai sensi degli art. 40 bis, 41, 47, 57 bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005, in particolare gli artt. 3 e 5;
- DPCM 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;
- DPCM 13 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.

Nel presente Manuale i rinvii alla normativa limiteranno al minimo la riproduzione dell'intera fonte legislativa.

2. QUADRO ORGANIZZATIVO ISTITUZIONALE

2.1. Area organizzativa omogenea e unità organizzative

L'area organizzativa omogenea (AOO) è l'insieme di funzioni e di strutture individuate dall'amministrazione cui sono assegnate funzioni omogenee. Essa, pertanto, presenta esigenze di gestione documentale in modo unitario e coordinato, ai sensi della normativa vigente.

L'unità organizzativa (UO) è, all'interno della AOO, un complesso organizzato di risorse umane e strumentali cui è stata affidata una competenza omogenea nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari, attività e procedimenti amministrativi.

L'ASP Ambito 9 ha una sola AOO e il suo organigramma, in cui sono dettagliate le UO, è descritto nell'allegato 1, come previsto dalla legge 7 agosto 1990, n. 241 (artt. 4-6), dal DPR 28 dicembre 2000, n. 445 e dal DPCM 3 dicembre 2013, art. 3, comma 1, lett. a).

L'AOO è descritta, unitamente alle altre informazioni richieste, nell'Indice delle Pubbliche Amministrazioni - IPA. È compito del Referente IPA dell'ente provvedere all'accreditamento, alla trasmissione delle informazioni richieste dalla legge e all'aggiornamento senza ritardo dei dati nel sito IPA.

Nell'allegato 1 sono dettagliate le informazioni della AOO e l'organigramma.

2.2. Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti

Presso l'Ente è istituita una UO Protocollo che si occupa della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi; inoltre, con deliberazione del Consiglio di Amministrazione n. 48 del 31/10/2019 sono stati individuati il Responsabile della gestione documentale e il rispettivo vicario, come previsto dal DPCM 3 dicembre 2013, art. 3, lett. b) e c).

In difetto di nomina espressa, il responsabile coincide con il Direttore dell'Ente.

L'UO Protocollo garantisce la corretta gestione, tenuta e tutela dei documenti, vigila sull'osservanza della corretta applicazione della normativa in materia di gestione documentale durante l'intero ciclo di vita dei documenti, oltre a ulteriori specifici compiti attribuiti dalla legge o dall'ordinamento interno dell'Ente.

In particolare il servizio cura:

- il livello di autorizzazione (*Acces Control List* - ACL) per l'accesso al sistema di gestione documentale – protocollo informatico - degli utenti secondo i profili distinti in ruoli abilitati alla mera consultazione, inserimento o modifica delle informazioni, sulla base delle richieste provenienti dai Responsabili delle UO. In tal caso il Responsabile di UO invierà richiesta con un messaggio all'indirizzo mail del responsabile della UO Protocollo, o attraverso apposito processo di gestione degli accessi (analogico o digitale);
- la correttezza delle operazioni di registrazione, segnatura, gestione dei documenti e dei flussi documentali;
- notifica l'eventuale indisponibilità del sistema e dà disposizioni per l'attivazione del registro di emergenza secondo quanto disposto al § 6.10;
- le autorizzazioni di annullamento e delle modifiche alle registrazioni di protocollo per l'AOO;
- l'adeguamento del sistema di gestione documentale alle eventuali modifiche dell'organigramma e funzionigramma dell'Ente.

2.3. Responsabile della gestione documentale

È compito del Responsabile della gestione documentale:

- definire e assicurare criteri uniformi di trattamento dei documenti e di classificazione e archiviazione;
- predisporre e mantenere aggiornato il manuale di gestione;
- predisporre, di concerto con il responsabile della conservazione, il responsabile dei sistemi informativi e con il responsabile del trattamento dei dati personali, il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici secondo quanto dettagliato al capitolo 11;
- produrre il pacchetto di versamento e assicurare il trasferimento del suo contenuto al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione.

Il Responsabile della gestione documentale è coadiuvato dal referente dei sistemi informatici e della sicurezza informatica e dal referente della protezione dei dati personali relativamente al sistema documentale come previsto dal D.Lgs. 7 marzo 2005, n. 82.

2.4. Profili di abilitazioni di accesso interno ed esterno alle informazioni documentali

Attraverso una *access control list* – ACL – il sistema di gestione documentale permette l'assegnazione differenziata dei profili di abilitazione, intervento, modifica e visualizzazione dei documenti di protocollo in rapporto alle funzioni e al ruolo svolto dagli utenti e garantisce la protezione dei dati personali e dei dati sensibili.

Il Responsabile della gestione documentale riceve dai responsabili delle UO, richiesta scritta (tramite e-mail, o apposito processo di gestione degli accessi) di abilitazione per ciascun utente, concordando, caso per caso, le tipologie di abilitazione.

2.5. Posta elettronica istituzionale

Tutti i dipendenti sono dotati di una casella di posta elettronica istituzionale nel formato n.cognome@comune.jesi.an.it.

2.6. PEC istituzionale

L'Ente si è dotato di due caselle di Posta Certificata (PEC) gestite dal servizio PostaRaffaello di Regione Marche, che opera in conformità alle regole tecniche e secondo quanto prescritto dal D.Lgs 82/2005 e dal DPR 68/2005. Le caratteristiche del servizio, le misure di sicurezza adottate, i livelli di servizio e le misure di protezione dei dati sono descritte dettagliatamente nel "Manuale Operativo" del servizio di posta certificata, codice documento: RMPC-MO-03 consultabile all'indirizzo:

<https://www.emarche.it/documents/manuale.operativo.emarche.pdf>

La casella PEC integrata con il sistema di gestione documentale è asp.ambitonove@emarche.it e le relative informazioni sono state registrate nel sito dell'Indice della Pubblica Amministrazione (IPA). Esiste un'altra casella di PEC denominata gare.asp.ambitonove@emarche.it dedicata alla gestione delle gare telematiche e gestita attraverso un apposito software di gestione e relativo portale. Tale casella è comunque integrata con il sistema di gestione documentale nel caso in cui alcune PEC arrivino direttamente a tale casella, senza che siano gestite dell'apposito software, e che debbano essere protocollate.

La casella di posta elettronica certificata integrata con il sistema di gestione documentale non deve mai essere utilizzata direttamente – senza passare dal sistema documentale - né attraverso un client di posta né attraverso un browser per effettuare l’invio o l’inoltro di messaggi e documenti.

Ogni messaggio inviato da una casella di posta certificata infatti produce per il mittente una serie di messaggi di ritorno che attestano l’avvenuta ricezione dei messaggi da parte degli attori coinvolti, sia alla sua eventuale registratura, annullo, ecc. che utilizzando direttamente la casella non possono essere ricongiunti e riconciliati con il documento inviato.

Al solo scopo di controllo dello stato della cartella e di risoluzione di problemi tecnici, è possibile accedere direttamente al contenuto delle PEC “emarche” tramite smart card di tipo CartaRaffaello emessa da Regione Marche, utilizzando il profilo dell’utente (o degli utenti) abilitati, collegandosi al sito <https://www.emarche.it/>.

Il computer deve essere configurato con i driver necessari per leggere la smart card CartaRaffaello, come da indicazioni tecniche contenute nel sito <http://www.regione.marche.it/Regione-Utile/Agenda-Digitale/Cittadinanza-digitale/Carta-Raffaello>.

La dimensione massima di un messaggio di posta certificata accettabile dal gestore del servizio è di 100MB (comprende tutti gli allegati e il corpo del messaggio), mentre il numero massimo di destinatari cui è possibile inviare messaggi di posta certificata è di 50.

E' garantito l'invio di messaggi di grandi dimensioni nel caso in cui il prodotto della dimensione del messaggio per il numero di destinatari diretti (to) di posta certificata, non superi i 100 MB (es. 10MB di messaggio per 10 destinatari). In caso contrario, il sistema non accetterà il messaggio notificando l'evento all'utente tramite il relativo messaggio di 'Avviso di non accettazione'. Prima di spedire un messaggio di dimensioni significative è sempre bene verificare di avere spazio sufficiente per ricevere correttamente tutte le ricevute di consegna. Se il messaggio viene inviato (in “TO (A)”) a molti destinatari di posta elettronica certificata e la dimensione del messaggio è significativa si deve considerare che ogni ricevuta di consegna ha in allegato tutto il messaggio inviato, a meno di disposizioni contrarie da parte del mittente.

In presenza di allegati e di molteplici destinatari può essere quindi necessario procedere con più invii.

2.7. Eliminazione dei registri di protocollo diversi dal protocollo informatico

Il registro di protocollo è unico nell’Ente. Sono cessati di fatto e di diritto tutti i cosiddetti protocolli interni (cioè di settore, di divisione, protocolli multipli, protocollo del telefax, etc.) o altri sistemi di registrazione dei documenti diversi dal protocollo unico. Qualsiasi registrazione eventualmente effettuata su registri non autorizzati è nulla di diritto e non può produrre alcun effetto giuridico-probatorio.

2.8. Responsabile della conservazione

Il sistema di conservazione opera secondo modelli organizzativi espliciti, definiti e distinti dal sistema di gestione documentale. Il Responsabile della conservazione, pertanto, può coincidere con il Responsabile della gestione documentale.

Qualora la conservazione sia svolta all’esterno dell’Ente, all’interno della struttura organizzativa è nominato un Responsabile della conservazione che fornisce le indicazioni utili alla definizione delle politiche del sistema di conservazione e alla predisposizione del manuale di conservazione.

Il Responsabile della conservazione opera d’intesa con il responsabile del trattamento dei dati personali e con il Responsabile della sicurezza, oltre che con il Responsabile della gestione documentale nel caso in cui non sia la stessa persona.

Con deliberazione del Consiglio di Amministrazione n. 48 del 31/10/2019 è stato nominato il Responsabile della conservazione, il quale coincide con il Responsabile della gestione documentale.

3. IL DOCUMENTO

3.1. Documento informatico e analogico: definizione e disciplina giuridica

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Il documento informatico è, quindi, un *file*, cioè una sequenza determinata di valori binari indifferente al supporto fisico su cui è memorizzata.

Il documento analogico è la rappresentazione non informatica, di atti, fatti o dati giuridicamente rilevanti. Qualsiasi documento non informatico (ad es., un documento cartaceo) è, dunque, un documento analogico.

A differenza del documento analogico, che si caratterizza per la pluralità di forme (scrittura privata, atto pubblico, scrittura privata autenticata) che sostanziano il diverso valore giuridico-probatorio, il documento informatico si caratterizza per la pluralità di firme elettroniche (con il valore di sottoscrizione, firma, sigla o visto), che caratterizzano e diversificano l'efficacia giuridico-probatoria del documento.

La firma elettronica non è, infatti, la rappresentazione informatica grafica della firma, ma un meccanismo di associazione di dati per l'imputazione di effetti giuridici in capo a un determinato soggetto che ne appare l'autore.

L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono valutabili in giudizio tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità. Il documento informatico assume la caratteristica di immodificabilità se prodotto 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.

Il documento informatico può essere sottoscritto con firma elettronica, avanzata, qualificata o digitale: il tipo di firma utilizzata differenzia il valore giuridico del documento, secondo le norme previste dalla legge.

Il documento informatico privo di sottoscrizione è una copia informatica, come tale forma piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime (2712 cc, 23 quater CAD, 2713 cc).

Il documento informatico sottoscritto con firma elettronica semplice è liberamente valutabile dal giudice sia per quanto riguarda l'efficacia giuridica che per l'efficacia probatoria tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Il documento informatico sottoscritto con firma avanzata, se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità, al pari di una scrittura privata, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta, se colui contro il quale è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta.

Il documento informatico sottoscritto con firma qualificata, se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta.

L'utilizzo del dispositivo si presume riconducibile al titolare, salvo che questi ne dia prova contraria.

Il documento informatico sottoscritto con firma digitale, se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta.

L'utilizzo del dispositivo si presume riconducibile al titolare, salvo che questi ne dia prova contraria.

L'associazione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata

sottoscrizione; tuttavia le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.

Se stipulate sotto forma di documento informatico, devono essere sottoscritte a pena di nullità, salvo i casi di firma autenticata, con firma elettronica qualificata o digitale le scritture private relative ai seguenti tipi di contratti:

- i contratti che trasferiscono la proprietà di beni immobili;
- i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta;
- i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti;
- i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione;
- gli atti di rinuncia ai diritti indicati dai numeri precedenti;
- i contratti di affrancazione del fondo enfiteutico;
- i contratti di anticresi;
- i contratti di locazione di beni immobili per una durata superiore a nove anni;
- i contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato;
- gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite dello Stato;
- gli atti di divisione di beni immobili e di altri diritti reali immobiliari;
- le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti.

Gli altri atti per cui la legge prevede obbligatoriamente la forma scritta soddisfano tale requisito se sottoscritti con firma elettronica avanzata, qualificata o digitale. Si precisa che tutti i contratti stipulati dalla Pubblica Amministrazione, anche quando quest'ultima agisce *iure privatorum*, richiedono la forma scritta *ad substantiam*.

3.2. Redazione/formazione del documento informatico

Il documento informatico è formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software: in tal caso il documento informatico assume le caratteristiche di immodificabilità e di integrità con la sottoscrizione con firma digitale/firma elettronica qualificata o con l'apposizione di una validazione temporale o con il trasferimento a soggetti terzi con PEC con ricevuta completa o con la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza o con il versamento ad un sistema di conservazione;
- 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: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili

all'utente: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione;

- 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: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei *log* di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

3.2.1. Validazione temporale

Costituiscono validazione temporale:

- i riferimenti temporali realizzati dai certificatori accreditati mediante marche temporali;
- i riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato secondo la scala di tempo UTC (IT) (INRIM) con una differenza non superiore ad un minuto primo;
- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata;
- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica.

3.2.2. Formati

L'Ente usa per la formazione e per la gestione dei documenti informatici le seguenti tipologie di formato coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico e tali da garantire i principi di interoperabilità tra i sistemi di conservazione in base alla normativa vigente.

La scelta del formato 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; pertanto nella scelta si è valutata l'apertura, la sicurezza, la portabilità, la funzionalità, il supporto allo sviluppo e la diffusione dello stesso.

Per tale motivo, sono utilizzati in via preferenziale i seguenti formati standard:

- Testo = Txt, Docx, Odt, Pdf/a;
- Immagini = Jpg, Tiff;
- XML;
- Formati e-mail = RFC 2822/MIME.

I file compressi (ZIP, ARJ, RAR, 7Z, ...) presenti nei messaggi di posta in arrivo devono essere decompressi e i singoli file inseriti nella sezione Allegati della maschera di protocollo a cura dell'UO Protocollo.

3.3. Redazione/formazione del documento amministrativo informatico

Il documento amministrativo è qualsiasi rappresentazione, comunque formata, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica.

Il documento amministrativo può assumere la forma di documento informatico o analogico.

Le amministrazioni pubbliche formano gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici, di cui al § 3.1 ovvero acquisendo le istanze, le dichiarazioni e le comunicazioni previste dalla legge. 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 duplicazioni e copie.

Il documento amministrativo informatico e le istanze, le dichiarazioni e le comunicazioni previste dalla legge sono soggette, ove necessario, a registrazione di protocollo, segnetura, fascicolatura e repertoriazione.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità oltre che nei modi di cui al § 3.2 anche con la registrazione nel registro di protocollo unico, nei repertori, negli albi, contenuti nel sistema di gestione documentale.

Il documento amministrativo informatico deve, di norma, contenere la denominazione dell'Ente e l'indicazione di:

- Data di sottoscrizione;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (indicare 0 zero se non presenti);
- Oggetto;
- Destinatario;
- Testo;
- Sottoscrizione;
- Elementi identificativi del responsabile del procedimento.

Il documento è sottoscritto prima di essere protocollato. Le informazioni relative alla classificazione atte a identificare il fascicolo di competenza, la data di sottoscrizione, il numero di allegati sono inserite prima della sottoscrizione del documento.

Di norma, la data di sottoscrizione e la data di protocollazione coincidono.

3.4. Redazione/formazione del documento amministrativo analogico

Per documento analogico si intende un documento formato utilizzando una grandezza fisica (ad esempio le tracce su carta, le immagini contenute nei film e le magnetizzazioni su nastro).

Nell'attività amministrativa, di norma il documento analogico è un documento formato su supporto analogico prodotto con strumenti analogici (ad es., documento scritto a mano) o con strumenti informatici (ad es., documento prodotto con un sistema di videoscrittura) e stampato su carta. L'originale analogico è il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali (sigillo, carta intestata, formulario amministrativo) e sostanziali, comprendente tutti gli elementi di garanzia e di informazione, del mittente e del destinatario e dotato di firma autografa.

I documenti analogici dotati di firma autografa aventi per destinatario un ente o un soggetto terzi, sono di norma redatti in due esemplari, un originale per il destinatario e una minuta da conservare agli atti nel fascicolo corrispondente.

Si definisce *minuta* l'esemplare del documento corredato di sigle, firma e sottoscrizione autografe, conservato agli atti dell'Ente, cioè nel fascicolo relativo al procedimento amministrativo o all'affare trattato.

Il documento amministrativo analogico in uscita è redatto su carta intestata e deve, di norma, contenere la denominazione dell'Ente e l'indicazione di

- UO;
- Data di sottoscrizione;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (indicare 0 zero se non presenti);
- Destinatario;
- Oggetto;
- Testo;
- Sottoscrizione;
- Elementi identificativi del responsabile del procedimento.

Il documento è sottoscritto prima di essere protocollato; di norma la data di sottoscrizione e la data di protocollazione coincidono.

3.5. Documenti redatti in originale su supporto analogico

Ai sensi del DPCM 21 marzo 2013, per particolari tipologie di documenti analogici originali unici, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato. Per documenti originali unici si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta (ad es., i verbali di una riunione o di un'assemblea).

Pertanto, tutti i documenti su cui vengono apposti manualmente dati di registrazione a protocollo, sigle e firma autografa (che non sono sottoscritti con firma elettronica, semplice, avanzata o digitale), sono documenti amministrativi analogici.

3.6. Il documento amministrativo informatico costituito dal corpo della PEC istituzionale

La posta elettronica certificata costituisce un mezzo di trasmissione che consente lo scambio di comunicazioni e documenti la cui trasmissione e ricezione sono giuridicamente rilevanti. Tale modalità di trasmissione dei documenti viene utilizzata nei casi in cui è necessario avere prova opponibile dell'invio e della consegna del messaggio di posta.

Il documento trasmesso/ricevuto con PEC ha lo stesso valore legale della raccomandata con avviso di ricevimento. In tal caso, l'avvenuta consegna del messaggio elettronico consente tra l'altro di ricorrere contro terzi.

La PEC, a differenza della posta elettronica semplice, ha le seguenti peculiarità:

- identificazione del mittente, se coincide con l'autore del documento;
- garanzia dell'integrità e della riservatezza dei messaggi;
- data certa di spedizione e consegna dei messaggi;
- ricevuta di avvenuta consegna o avviso di mancato recapito;
- tracciatura dei messaggi a cura del gestore.

Di norma, si dovrebbe usare la PEC per trasmettere e/o ricevere un documento informatico, ma può accadere che la comunicazione/istanza ricevuta sia costituita dal mero corpo della *e-mail*.

In questo caso si procede alla registrazione del messaggio in arrivo nel sistema di gestione documentale solo se il contenuto è rilevante al fine giuridico-probatorio.

3.7. Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale

L'e-mail costituisce un documento informatico sottoscritto con firma elettronica semplice, in quanto il mittente viene identificato inserendo il proprio *username* e la propria *password*.

Le *e-mail* inviate da una casella istituzionale dell'Azienda Servizi alla Persona ASP Ambito 9 sono considerate sottoscritte con firma elettronica semplice e sono soggette a protocollazione solo se il contenuto è rilevante al fine giuridico-probatorio. In questo caso si procede alla conversione dell'e-mail in formato pdf/a prima di provvedere alla sua registrazione. Trattandosi di un documento informatico nativo non si procederà alla stampa e apposizione tramite timbro della segnatura prima della registrazione di protocollo.

3.8. Distinzione dei documenti in base allo stato di trasmissione (arrivo, partenza, scambiati tra UO, scambiati tra AOO dello stesso ente, fax, PEC, e-mail)

I documenti, siano essi analogici o informatici, in base allo stato di trasmissione si distinguono in:

- documenti in arrivo;
- documenti in partenza;
- documenti interni (scambiati tra UO);

Per documenti in arrivo si intendono tutti i documenti di rilevanza giuridico-probatoria acquisiti dall'Amministrazione nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato.

Per documenti in partenza si intendono i documenti di rilevanza giuridico-probatoria prodotti dall'Amministrazione pubblica nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato ed anche ai propri dipendenti come persone fisiche e non nell'esercizio delle loro funzioni.

Per documenti interni o tra uffici si intendono i documenti scambiati tra le diverse Unità Organizzative. I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti dal personale nell'esercizio delle proprie funzioni al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi.

Per comunicazioni informali tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e di norma non sono protocollate.

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale – PEC – accessibile all'Unità Organizzativa che effettua la protocollazione in arrivo.

Il documento informatico trasmesso tramite casella di posta elettronica certificata – PEC - si intende spedito dal mittente se inviato al proprio gestore e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

3.9. Duplicato del documento informatico e analogico

Il duplicato del documento informatico è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto. I duplicati informatici hanno il medesimo valore giuridico del documento informatico da cui sono tratti se prodotti in conformità delle regole tecniche.

Il “duplicato informatico” è dunque un documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all’originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

Il duplicato di un documento analogico è la riproduzione di un documento analogico originale distrutto o smarrito che lo sostituisce a tutti gli effetti legali: esempio rilascio del certificato di laurea, della carta di identità etc.

3.10. Copia del documento informatico e analogico: nozione

La copia informatica di documento informatico è un documento informatico che, mediante processi e strumenti idonei, assicura la corrispondenza della copia alle informazioni del documento informatico di origine attraverso l’utilizzo di uno dei formati idonei ai sensi della normativa vigente. La copia informatica di documento informatico è, dunque, un documento informatico che muta il formato del documento originario o che muta il supporto del documento originario informatico (ad esempio il salvataggio di un file in un formato differente: da *.doc* a *.pdf*, oppure da *.doc* a *.ods*).

Le copie del documento informatico hanno la stessa efficacia probatoria dell’originale da cui sono tratte se la loro conformità è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta, fermo l’obbligo di conservazione dell’originale informatico.

La copia di un documento analogico è la trascrizione o riproduzione dell’originale. Si distingue in copia semplice, imitativa e conforme. La copia semplice è la pura trascrizione dell’originale senza riguardo agli elementi formali. La copia imitativa riproduce sia il contenuto che la forma (es. fotocopia). La copia conforme è la copia certificata come conforme all’originale da un pubblico ufficiale autorizzato ad eseguire tale attestazione nell’esercizio delle sue funzioni (copia “autentica”).

3.11. Copia informatica del documento amministrativo analogico

È possibile produrre la copia su supporto informatico di documenti amministrativi in origine su supporto analogico. La copia informatica ha il medesimo valore dell’originale analogico da cui è tratta se attestata conforme dal funzionario a ciò delegato nei modi stabiliti dalla legge. L’attestazione di conformità può essere inserita nel documento informatico contenente la copia informatica o può essere prodotta come documento separato contenente un riferimento temporale e l’impronta di ogni copia.

In entrambi i casi l’attestazione dev’essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come

documento informatico separato, questo deve contenere un riferimento temporale e l'impronta di ogni copia o estratto informatico oggetto dell'attestazione.

Per copia informatica di un documento analogico si intende:

- copia informatica del documento analogico, data dal documento informatico avente contenuto identico a quello del documento analogico da cui è tratto ma diverso come forma;
- copia per immagine su supporto informatico di documento analogico, avente contenuto e forma uguali all'originale.

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è 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.

Le copie informatiche di documenti analogici, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali hanno la medesima efficacia probatoria degli originali se a esse è apposta o associata, da parte di colui che le spedisce o le rilascia, una firma digitale o altra firma elettronica qualificata e dichiarazione di conformità:

- per "rilascio" si intende la consegna di un supporto fisico idoneo a ricevere la memorizzazione della rappresentazione corrispondente al documento analogico e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale;
- per "spedizione" si intende l'inoltro telematico del/dei file corrispondenti per il tramite di un sistema di posta elettronica o di altro sistema di comunicazione informatica e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale.

Le copie per immagine su supporto informatico di documenti originali formati su supporto analogico hanno la medesima efficacia probatoria degli originali, se:

- la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche;
- sono formate nel rispetto delle regole tecniche e se la loro conformità all'originale non è espressamente disconosciuta.

3.12. Estratto informatico di documento amministrativo informatico

La copia che riproduce solo una parte del contenuto del documento, viene definita "estratto". Gli estratti informatici devono essere prodotti in uno dei formati idonei definiti nel § 3.2.2.

L'estratto così formato, di uno o più documenti informatici, se sottoscritto con firma digitale o firma elettronica qualificata da chi effettua l'estratto hanno la stessa efficacia probatoria dell'originale, salvo che la conformità allo stesso non sia espressamente disconosciuta.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità può essere inserita nello stesso documento informatico contenente l'estratto, oppure prodotta come documento informatico separato; in entrambi i casi l'attestazione dev'essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l'impronta di ogni copia o estratto informatico oggetto dell'attestazione.

3.13. Copia analogica di documento amministrativo informatico

La copia analogica di documento amministrativo informatico è, di norma, la stampa cartacea.

La copia su supporto analogico di documento informatico, sottoscritto con firma elettronica avanzata, qualificata o digitale, per avere la stessa efficacia probatoria dell'originale da cui è tratta, deve essere certificata come conforme all'originale in tutte le sue componenti da un pubblico

ufficiale autorizzato a eseguire tale attestazione nell'esercizio delle sue funzioni (copia "autentica") salvo che la conformità allo stesso non sia espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

3.14. Metadati

La codifica dell'informazione digitale, a differenza di altre, non è mai né autosufficiente né auto-esplicativa, ma deve sempre e necessariamente documentare se stessa al livello minimo del singolo *atomo* di informazione, aggiungendo al dato/contenuto vero e proprio molte informazioni necessarie per la decodifica, l'identificazione, il recupero, l'accesso e l'uso². Nel contesto degli oggetti digitali il termine metadati può essere associato a tre categorie funzionali:

- *Descrittiva*: ha lo scopo di facilitare il recupero e l'identificazione dell'oggetto digitale;
- *Gestionale*: ha lo scopo di supportare la gestione dell'oggetto digitale all'interno di una collezione;
- *Strutturale*: ha lo scopo di collegare fra loro i componenti di oggetti informativi complessi.

3.14.1. Obiettivi dei metadati archivistici

Gli obiettivi dei metadati archivistici sono:

- garantire l'identificazione permanente dei singoli oggetti informativi, ad es.: identificativo univoco (numero di protocollo, data, autore, ecc.);
- garantire l'identificazione permanente delle relazioni tra gli oggetti informativi, ad es., indici di classificazione e fascicolatura;
- conservare le informazioni che supportano l'intellegibilità degli oggetti informativi, ad es., procedimento amministrativo cui il documento è connesso.

3.14.2. Metadati essenziali per la registrazione nel protocollo informatico

Gli elementi essenziali minimi sono i seguenti:

- Identificativo;
- denominazione/codice unico che individua l'Ente;
- corrispondente (mittente/destinatari);
- oggetto;
- numero degli allegati e descrizione degli stessi;
- numero di protocollo;
- data di registrazione a protocollo;
- indicazione dell'Unità organizzativa (UO);
- impronta che lega il documento digitale ai metadati sopra indicati.

² L'oggetto digitale (*data object*) in ambito Open Archive Information System è un «oggetto costituito da un insieme di sequenze di bit» e costituisce un oggetto informativo sempre e soltanto se in congiunzione con «le informazioni sulla sua rappresentazione».

4. IL FASCICOLO

4.1. Il fascicolo: definizione e funzione

Il fascicolo è l'unità di base dell'archivio corrente. Ogni fascicolo contiene documenti che ineriscono a uno stesso affare, attività o procedimento e sono classificati in maniera omogenea, in base al contenuto e secondo il grado divisionale attribuito dal titolare (o piano di classificazione), salvo alcune eccezioni, come il fascicolo di persona (e le rispettive tipologie, di personale, di studente, etc.) e il fascicolo di fabbricato.

All'interno di ciascun fascicolo i documenti sono inseriti secondo l'ordine cronologico di registrazione e la loro sedimentazione avviene in modo tale che si individui subito il documento più recente. L'ordine cronologico di sedimentazione è rispettato anche all'interno dei sottofascicoli, se istruiti. L'obbligo di fascicolatura dei documenti riguarda sia i documenti contraddistinti dalla segnatura di protocollo sia i documenti procedurali non registrati³.

La corretta tenuta del fascicolo garantisce sia la sedimentazione che l'esercizio del diritto di accesso. Si possono distinguere cinque tipologie di fascicolo:

- *Affare*: conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata. Per gli affari non esiste un termine per la conclusione previsto da norme;
- *Attività*: conserva i documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque previsto l'adozione di un provvedimento finale;
- *Procedimento amministrativo*: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un atto finale;
- *Persona fisica*: conserva i documenti relativi a diversi procedimenti amministrativi, distinti per affari o per attività, ma legati da un vincolo archivistico interno, relativo a una persona fisica determinata. La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'ente;
- *Persona giuridica*: conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica.

Il fascicolo può essere ulteriormente suddiviso in sottofascicoli e inserti. Queste suddivisioni sono identificate grazie a un'ulteriore sequenza numerica progressiva (detta anche "catena numerica"), gerarchicamente posta al di sotto del numero di fascicolo o del sottofascicolo.

Il sottofascicolo può essere chiuso prima del fascicolo, ma non viceversa, in quanto di norma trattasi di un subprocedimento o di un endoprocedimento stesso.

Le diverse tipologie di fascicoli formate da ASP durante lo svolgimento di procedimenti amministrativi ed attività diverse sono riportate nell'allegato 7 al presente Manuale di gestione documentale.

4.2. Il fascicolo analogico: formazione, implementazione e gestione

Per ogni procedimento, affare e attività, l'Ente ha l'obbligo di conservare in un fascicolo cartaceo gli atti, i documenti e i dati da chiunque formati su supporto analogico; cioè un documento nativo su supporto cartaceo deve essere conservato in originale su tale supporto all'interno dell'apposito

³ DPR n. 445/2000, art. 64 comma 4: «Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo».

fascicolo. Ovviamente un fascicolo analogico può contenere anche copie analogiche di documenti nativi digitalmente.

Ogni fascicolo deve essere contraddistinto dai seguenti elementi, atti a determinarne l'identificazione all'interno del sistema documentale:

- anno di apertura (o di istruzione);
- numero di fascicolo, cioè un numero sequenziale all'interno dell'ultimo grado divisionale, da 1 a n;
- l'oggetto del fascicolo, cioè una stringa di testo per descrivere compiutamente un affare, una pratica, un dossier, una cartella, una *papèla*, un procedimento amministrativo o più di questi insieme.

Per convenzione, il titolo va scritto in numeri romani, mentre gli altri gradi divisionali vanno scritti in cifre arabe (titolo I; classe 3; sottoclasse 5; categoria 2; sottocategoria 6). L'anno va separato dal titolo da un trattino (-); il titolo va separato dagli altri gradi divisionali da una barretta (/); gli altri gradi divisionali, invece, vanno separati dal numero del fascicolo da un punto (.); l'oggetto del fascicolo va scritto tra virgolette caporali (« »)⁴.

Esempio: 2016 - IX/1.6 «Costruzione della nuova sede degli uffici».

Il fascicolo raccoglie i documenti, creati e ricevuti, fino al termine della pratica. La chiusura della pratica comporta la chiusura del fascicolo. Il fascicolo può essere di durata annuale, oppure la durata può essere la stessa dell'affare a cui si riferisce. I fascicoli chiusi sono conservati presso l'Ufficio produttore per un limite minimo di un anno al fine di consentire l'eventuale reperimento dei documenti necessari allo svolgimento delle attività giornaliere.

Non si forniscono limiti massimi di giacenza dei fascicoli chiusi presso l'archivio corrente poiché i tempi possono risultare diversi a seconda della natura della pratica e dell'attività d'ufficio⁵.

In ogni caso, i responsabili di UO non devono mantenere i fascicoli di attività cessate non più consultati e che non hanno più alcuna utilità diretta presso gli uffici per evitare un eccessivo ingombro e una conseguente difficoltà nella gestione dei fascicoli aperti e attivi. Il trasferimento dei fascicoli chiusi dall'archivio corrente all'archivio di deposito avviene secondo le modalità presentate al § 10.

4.3. Il fascicolo informatico: formazione, implementazione e gestione

Per ogni procedimento, affare e attività, l'Ente ha l'obbligo di conservare in un fascicolo informatico gli atti, i documenti e i dati da chiunque formati su supporto informatico; cioè un documento nativo su supporto informatico deve essere conservato in originale su tale supporto all'interno dell'apposito fascicolo. Ovviamente un fascicolo informatico può contenere anche copie di qualunque tipo⁶ di documenti nativi cartacei.

Il fascicolo informatico reca le seguenti indicazioni:

- amministrazione titolare del procedimento;
- altre amministrazioni partecipanti;
- nominativo del responsabile del procedimento;
- oggetto del procedimento;
- elenco dei documenti contenuti;

⁴ G. Penzo Doria, *La linea dell'arco*, pp. 25 e 26.

⁵ A. Romiti, *L'archivio di deposito nelle Pubbliche amministrazioni*, Lucca, Civita, 2008, p. 49: "Il momento del trasferimento, indipendentemente dai limiti minimi, non può rispondere a regole rigide, in quanto si collega con l'interesse che l'ufficio produttore ha nel conservare le carte presso di sé; per il rispetto dei limiti massimi non vi è, d'altra parte, alcun obbligo normativo cogente dal quale possano provenire sollecitazioni a trasferire nel deposito tutte le pratiche concluse."

⁶ A proposito dei diversi tipi di copie di un documento si veda il capitolo 3.

- indice di classificazione (titolo, classe, etc.);
- numero del fascicolo, identificativo di una catena numerica relativamente alla classe e al titolo di riferimento dell'anno di creazione;
- data di apertura e di chiusura del fascicolo.

Il fascicolo informatico è creato dal responsabile del procedimento o da una persona incaricata all'interno del sistema di gestione documentale ed è visualizzabile con possibilità di intervento da parte degli utenti abilitati a operare sui documenti della UO responsabile.

Istruendo i fascicoli, è necessario evitare la frammentazione delle pratiche, l'accorpamento eccessivo di documenti all'interno della stessa unità, la tendenza a costituire fascicoli intestati ai destinatari invece che basati sull'analisi di processi e funzioni.

Se necessario, i fascicoli possono essere rinominati. Se il contenuto è costituito di documenti esclusivamente informatici questa attività è sufficiente; se è costituito da documenti informatici e documenti cartacei bisogna rinominare anche la camicia del fascicolo cartaceo.

Il fascicolo informatico in un sistema totalmente digitale garantisce la possibilità di essere direttamente consultato e alimentato dalle amministrazioni coinvolte nel procedimento. Le regole per l'istruzione, l'identificazione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale e alla disciplina della formazione, gestione, trasmissione e conservazione del documento informatico.

4.4. I fascicoli annuali ripetitivi

È possibile prevedere la possibilità di aprire automaticamente fascicoli annuali ripetitivi.

L'indicazione della UO e del RPA (Responsabile del procedimento amministrativo) concorrono all'identificazione del fascicolo e alla individuazione del responsabile. La UO e il RPA devono essere gli stessi di ciascun documento, del fascicolo e degli eventuali sottofascicoli. Ogni qualvolta cambia il RPA il fascicolo informatico deve essere immediatamente trasferito per competenza al nuovo responsabile del procedimento.

I fascicoli informatici saranno trasferiti in conservazione, mediante pacchetto di versamento, a cura del Responsabile della gestione documentale o dal suo vicario dopo la loro chiusura, nelle modalità previste dal Manuale di conservazione.

4.5. Il fascicolo ibrido

Il fascicolo, inteso come unità logica, può conservare documenti affissi su diverse tipologie di supporto. Tale problematica, particolarmente sentita negli odierni sistemi di gestione documentale, produce il cosiddetto *fascicolo ibrido*. Si tratta di un fascicolo composto da documenti formati su supporto cartaceo e su supporto informatico, e tale duplicità dà origine a due unità archivistiche fisiche di conservazione differenti.

L'unitarietà del fascicolo è comunque garantita dal sistema di classificazione mediante gli elementi identificativi del fascicolo (anno di istruzione, titolo/classe, numero del fascicolo, oggetto) e dal contenuto dei documenti. Il risultato è che un fascicolo di tale natura occuperà due luoghi distinti (un faldone e un *file system*) e questa caratteristica permane per tutta la vita del fascicolo, dal momento della sua istruzione al momento del trasferimento nell'archivio di deposito e, infine, per il versamento all'archivio storico. Tale peculiarità rende, ovviamente, più complessa la gestione del fascicolo e dei documenti che vi afferiscono: entrambi vanno gestiti correttamente rispettando le caratteristiche proprie del supporto su cui il documento è stato prodotto e deve essere conservato. Qualora si ravvisi l'utilità di avere tutti i documenti presenti in un fascicolo in un determinato formato, si suggerisce di privilegiare il fascicolo informatico e creare le opportune copie per immagine dei documenti nativi analogici; è possibile inserire all'interno del fascicolo, qualora lo si

ritenga necessario, anche documenti di carattere strumentale non soggetti a registrazione di protocollo, mediante la modalità denominata “non protocollato” prevista dal sistema di gestione informatica dei documenti.

Questa pratica non esenta dalla conservazione dell’originale cartaceo nel fascicolo di pertinenza.

4.6. Metadati del fascicolo informatico

I metadati sono un insieme di dati associati a un fascicolo informatico per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permettere la gestione nel tempo nel sistema di conservazione.

I metadati minimi del fascicolo informatico e della aggregazione documentale informatica rispettano la codifica di caratteri ISO-8859-1.

I metadati minimi del fascicolo informatico sono:

- identificativo univoco e persistente rappresentato da una sequenza di caratteri alfanumerici associata in modo univoco e permanente al fascicolo in modo da consentirne l’identificazione;
- AOO;
- UO responsabile del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- responsabile del procedimento: cognome e nome;
- eventuali amministrazioni partecipanti al procedimento;
- oggetto: metadato funzionale a riassumere brevemente il contenuto del fascicolo o comunque a chiarirne la natura;
- elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità;
- data di apertura del fascicolo;
- data di chiusura del fascicolo.

4.7. Il repertorio dei fascicoli informatici

Il repertorio dei fascicoli informatici è costituito da un elenco ordinato e aggiornato dei fascicoli istruiti all’interno di ciascuna classe e di ciascun titolo del titolario di classificazione adottato, riportante:

- anno e numero progressivo del fascicolo;
- classificazione nell’ambito del titolario adottato;
- oggetto dell’affare/procedimento/attività;
- UO responsabile dell’affare/procedimento/attività;
- nominativo del responsabile dell’affare/procedimento/attività;
- date di apertura e chiusura del fascicolo;
- numero dei documenti contenuti nel fascicolo;
- dati relativi alla movimentazione del fascicolo;
- stato: chiuso/aperto.

Il repertorio dei fascicoli informatici è unico per la AOO, ha cadenza annuale ed è generato e gestito in forma automatica dal sistema di gestione informatica dei documenti.

5. LA GESTIONE DELL'ARCHIVIO CORRENTE

5.1. Definizione

Per archivio corrente si intende il complesso dei documenti relativi ad affari, ad attività e a procedimenti amministrativi in corso di istruttoria e di trattazione o, comunque, verso i quali sussista un interesse non ancora esaurito.

L'organizzazione dell'archivio deve rispondere a criteri di efficienza ed efficacia al fine di garantire la certezza dell'attività giuridico amministrativa dell'Ente e la conservazione stabile della memoria nel tempo. L'archivio corrente è, quindi, il primo elemento gestionale per il corretto funzionamento del sistema documentale⁷.

Il responsabile del procedimento amministrativo è tenuto alla corretta gestione, conservazione e custodia dei documenti e dei fascicoli, siano essi di natura analogica, digitale o ibrida, relativi ai procedimenti di propria competenza; a esso è quindi affidata l'attuazione delle disposizioni contenute in questo manuale in merito al corretto funzionamento dell'archivio corrente di propria pertinenza.

La UO che crea il fascicolo mantiene la responsabilità amministrativa dei documenti creati durante la fase corrente e la fase di deposito; quindi, per la fase corrente e di deposito, viene garantito il libero accesso, da parte delle sole UO che hanno la titolarità dei documenti, attraverso il sistema di gestione documentale.

5.2. Buone prassi per la gestione dell'archivio corrente

Il responsabile del procedimento amministrativo, come si è detto sopra, è incaricato della corretta gestione dell'archivio corrente di sua pertinenza e ciò comporta in primo luogo la corretta creazione dei fascicoli e inserimento dei relativi documenti⁸; in secondo luogo il responsabile del procedimento è tenuto alla corretta gestione dei fascicoli stessi e tale incombenza varia a seconda del supporto con cui vengono creati.

I fascicoli analogici devono essere creati secondo le indicazioni fornite nei § 4.2 e successivamente conservati all'interno di appositi faldoni o cartelle nell'archivio corrente situato presso gli uffici di ciascuna UO. Il faldone, per consentire l'agevole e immediato reperimento dei fascicoli deve riportare sul dorso le seguenti informazioni:

- l'ufficio produttore;
- l'oggetto;
- gli estremi cronologici;
- gli estremi identificativi dei fascicoli contenuti (indice di classificazione e numero progressivo di repertorio).

Laddove una pratica avesse dimensioni tali da occupare singolarmente più di un faldone, questi andranno contrassegnati con le medesime indicazioni esterne e con una numerazione progressiva, a partire da 1, così da risultare immediata la comprensione del legame tra le unità di conservazione. I fascicoli restano collocati presso ogni singola UO per la parte di propria responsabilità e competenza nel trattamento dell'affare, sia come archivio corrente sia come archivio di deposito.

⁷ P. Carucci e M. Guercio *Manuale di archivistica*, Urbino, Carocci, 2009, p. 204: «Per gestione dell'archivio corrente si intende quindi la funzione di organizzazione e controllo generale e sistematico esercitata da un ente sulla propria documentazione corrente al fine di disporre del necessario supporto informativo-documentario per lo svolgimento efficiente della propria attività sia a fini interni che a fini giuridici e di trasparenza amministrativa». Questi principi di carattere generale sono funzionali all'adempimento delle disposizioni contenute nel DPR n. 445/2000 art. 65.

⁸ A proposito si veda il capitolo 6.

I documenti creati nel corso dell'attività d'ufficio sono soggetti a fascicolazione obbligatoria ai sensi del DPR 445/2000, art. 64, c. 4, indipendentemente dal supporto su cui sono creati. Inserire i documenti nell'apposito fascicolo permette la costituzione di un archivio organizzato essendo essi le unità logiche del sistema di gestione documentale e, di conseguenza, consente il facile e veloce reperimento dei documenti di un determinato procedimento permettendo il rispetto del principio di trasparenza e dell'istituto del diritto di accesso. La fascicolazione deve essere effettuata in maniera continuativa e sistematizzata da parte di tutte le unità organizzative costituenti l'Amministrazione.

Un'attività secondaria, ma molto utile da un punto di vista di gestione corrente delle unità di archivio, è lo sfoltimento dei fascicoli. Lo sfoltimento è l'operazione preliminare e propedeutica a una corretta conservazione documentale: al momento della chiusura del fascicolo, oppure prima del trasferimento dello stesso all'archivio di deposito, il carteggio di carattere transitorio e strumentale deve essere selezionato ed estratto dal fascicolo da parte dell'operatore incaricato del trattamento della pratica. Si tratta, cioè, di estrarre dal fascicolo le copie e i documenti che hanno appunto carattere strumentale e transitorio, utilizzati dall'operatore incaricato o dal responsabile del procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad es., appunti, promemoria, copie di normativa e documenti di carattere generale).

Questa operazione riguarda principalmente i fascicoli cartacei.

5.3. Gli strumenti dell'archivio corrente

Il trattamento dell'intero sistema documentale dell'Ente comporta la predisposizione di strumenti di gestione dell'archivio corrente che permettano un'efficiente organizzazione e consultazione della documentazione, a prescindere dai supporti dei documenti.

5.3.1. Registro di protocollo

Il registro di protocollo è lo strumento finalizzato all'identificazione univoca e certa dei documenti ricevuti e spediti mediante la registrazione di determinati elementi che caratterizzano ogni singolo documento. Il registro di protocollo svolge, quindi, una fondamentale funzione giuridico probatoria attestando l'esistenza di un determinato documento all'interno del sistema di gestione documentale e garantendone l'autenticità. Il registro di protocollo è un atto pubblico di fede privilegiata (si rimanda al cap. 6).

5.3.2. Titolario (piano di classificazione)

Il titolare è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (titolo/classe/eventuale sottoclasse) stabilite sulla base delle funzioni dell'ente. Ciascun documento, registrato in modalità arrivo, partenza, interno, anche non protocollato, è classificato in ordine alla corrispondenza tra il suo contenuto e la relativa voce attribuibile, desunta dal titolare e successivamente fascicolato.

La classificazione, necessaria e fondamentale, è prodromica all'inserzione di un documento all'interno di un determinato fascicolo. La relazione tra i documenti (vincolo archivistico) di un'unità archivistica è garantita dalla segnatura archivistica completa (anno di istruzione, classificazione, numero del fascicolo).

Il titolare è inserito nel sistema di gestione documentale. Può essere soggetto a revisione periodica, qualora ciò si renda necessario a seguito di modifiche di carattere normativo e/o statutario. In questo caso, essi sono adottati a partire dal 1° gennaio dell'anno successivo a quello di approvazione.

Il sistema di gestione documentale garantisce che le voci del titolario siano storicizzate, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della loro registrazione. Il titolario è sottoposto, altresì, all'approvazione della Direzione generale archivi del Ministero per i beni culturali e del turismo e comunicato alla Soprintendenza archivistica per la regione Marche.

Il titolario unico, valido per l'AOO dell'Ente, è descritto nell'allegato n. 3.

5.3.3. Repertorio dei fascicoli

I fascicoli istruiti durante lo svolgimento dell'attività amministrativa, sono annotati nel repertorio dei fascicoli. Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio rispecchia quella del titolario di classificazione e, di conseguenza, 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 alla propria missione istituzionale, il repertorio dei fascicoli rappresenta, in concreto, le attività svolte e i documenti prodotti in relazione a tali attività. Il repertorio dei fascicoli è costantemente aggiornato.

5.3.4. Repertori

I repertori formano serie omogenee di documenti uguali per forma e diversi per contenuto come previsto nell'allegato 7 al presente Manuale di gestione documentale (Piano di organizzazione delle aggregazioni documentali). Essi sono soggetti a registrazione particolare, cioè con l'assegnazione di una numerazione continua e progressiva per anno. Sono un esempio la registrazione di decisioni, contratti e convenzioni, deliberazioni, etc. e l'elenco dettagliato è indicato al §7.2.

5.3.5. Massimario di selezione o Piano di conservazione

Il Massimario di selezione o Piano di conservazione (allegato 7 al presente Manuale di gestione documentale) è uno strumento da utilizzare durante la fase di deposito dell'Archivio, come previsto dall'art. 68 del DPR 445/2000.

Il Massimario di selezione o Piano di conservazione è lo strumento con cui l'ente individua le disposizioni di massima e definisce i criteri e le procedure attraverso i quali i documenti, 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, ai sensi del D.lgs. 22 gennaio 2004, n. 42, art. 21.

Il Massimario di selezione o Piano di conservazione individua le tipologie documentali in rapporto ai procedimenti che le costituiscono e, a partire da tali tipologie, si applicano i criteri e le disposizioni atti ad individuare i termini di conservazione: distinzione oggetto ed atto esercitato sull'oggetto; inoltre, è uno strumento indirizzato sia alla conservazione che all'eliminazione, detto in altri termini il Massimario di selezione o Piano di conservazione consente la selezione che ha come conseguenze o la conservazione o la distruzione.

Del Massimario di selezione o Piano di conservazione è parte integrante il prontuario di scarto, nel quale sono menzionati i tempi di conservazione in relazione alle tipologie documentarie. Le operazioni di selezione, necessarie a garantire la corretta gestione e la conservazione del complesso documentale dell'ente, avvengono 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 (espresso in metri lineari o in chilogrammi, solo per i documenti analogici) e le motivazioni dell'eliminazione, corredata da disposizione

dirigenziale, è inviata alla Soprintendenza archivistica delle Marche nelle modalità concordate. L'attività è soggetta ad autorizzazione della Soprintendenza archivistica ai sensi del D.lgs. 42/2004 art. 21.

A seguito dell'autorizzazione, l'Ente avvia il procedimento per individuare il soggetto legittimato al ritiro del materiale e alla eliminazione fisica dei documenti; la ditta affidataria individuata effettua le operazioni di ritiro e macero della documentazione con rilascio di relativo verbale di esecuzione. Per i fascicoli informatici la proposta di scarto segue lo stesso iter per quanto riguarda l'autorizzazione della Soprintendenza e il Responsabile della gestione documentale invierà un documento informatico firmato digitalmente.

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

5.4. Spostamento di un archivio corrente analogico

Qualora una UO dovesse spostare la documentazione corrente, a seguito di mutamento della sede operativa o per altra ragione, dovrà darne informazione tempestiva al Responsabile della gestione documentale producendo un apposito elenco dei fascicoli soggetto di spostamento.

Inoltre, il Responsabile della Gestione Documentale o suo delegato provvederà a effettuare un sopralluogo per verificare l'idoneità degli spazi e la correttezza della collocazione del nuovo archivio, rimanendo in ogni caso a disposizione per eventuali chiarimenti o consigli sulle modalità di spostamento della documentazione. Lo spostamento dell'archivio corrente non necessita di alcuna autorizzazione preventiva da parte della Soprintendenza archivistica pertinente per territorio⁹.

⁹ D.Lgs 42/2004, art. 21, c. 3: «Lo spostamento degli archivi correnti dello Stato e degli enti ed istituti pubblici non è soggetto ad autorizzazione».

6. IL PROTOCOLLO INFORMATICO

Il registro di protocollo è un atto pubblico di fede privilegiata. Come tale, fa fede fino a querela di falso e, in particolare, circa la data e l'effettivo ricevimento o spedizione di un documento determinato, di qualsiasi forma e contenuto. Esso, dunque, è idoneo a produrre effetti giuridici tra le parti.

Il registro di protocollo ha cadenza annuale: inizia il 1° gennaio e termina il 31 dicembre di ogni anno ed è unico per tutta l'AOO.

6.1. Registratura

I documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi devono essere registrati a protocollo o a repertorio.

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'Ente, ossia i cui mittenti/destinatari sono esterni all'Ente, e anche tutti i documenti informatici, ad eccezione di quelli espressamente esclusi dalla normativa vigente (DPR 445/2000, art. 53, comma 5) e altri documenti informatici già soggetti a registrazione particolare.

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 48 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 immutabile.

La registrazione di protocollo per ogni documento è effettuata mediante la memorizzazione di elementi obbligatori immutabili, elementi obbligatori modificabili ed elementi non obbligatori e modificabili.

La registrazione degli elementi obbligatori immutabili del protocollo informatico non può essere modificata, integrata, cancellata ma soltanto annullata mediante un'apposita procedura in capo al Responsabile della gestione documentale e a persone espressamente delegate. L'immutabilità e l'immutabilità della registrazione di protocollo devono essere garantite dal sistema di gestione documentale.

6.1.1. Elementi obbligatori immutabili (Registratura)

Gli elementi obbligatori immutabili servono ad attribuire al documento data e provenienza certa attraverso la registrazione di determinate informazioni rilevanti sul piano giuridico-probatorio.

Essi sono:

- numero di protocollo progressivo e costituito da almeno sette cifre numeriche;
- data di registrazione;
- corrispondente, ovvero mittente per il documento in arrivo, destinatario per il documento in partenza;
- oggetto;
- impronta del documento informatico;
- numero degli allegati;
- descrizione degli allegati.

L'insieme di tali elementi è denominato *registratura*.

6.1.2. Elementi obbligatori modificabili

Gli elementi obbligatori modificabili sono:

- unità operativa responsabile del procedimento/affare/attività (UO);
- classificazione archivistica;
- fascicolo.

6.1.3. Elementi non obbligatori modificabili

Gli elementi non obbligatori modificabili sono:

- recapiti del mittente;
- collegamento ad altri documenti o a fascicoli diversi da quello d'inserimento;
- tipologia di documento;
- altri tipi di annotazioni (ad es., si può annotare l'arrivo in data successiva di un secondo esemplare dello stesso documento precedentemente ricevuto e protocollato, previa verifica della sua conformità al primo).

6.2. Data e ora regolate sul UTC

Il *server* del protocollo informatico è regolato sul tempo universale coordinato (UTC) e, in particolare, sulla scala di tempo nazionale italiana UTC (IT), secondo le indicazioni dell'Istituto nazionale di ricerca metrologica - INRiM.

6.3. Segnatura

La segnatura di protocollo consiste nell'apposizione o nell'associazione al documento in originale, in forma non modificabile e permanente, delle informazioni memorizzate nel registro di protocollo. Essa consente di individuare ciascun documento in modo univoco.

6.3.1. Per il documento informatico

Le informazioni minime da associare al documento informatico sono:

- codice identificativo dell'amministrazione;
- codice identificativo dell'AOO;
- codice identificativo del registro;
- numero di protocollo;
- data e ora di protocollo.

Oltre alle informazioni minime la segnatura deve prevedere:

- codice identificativo dell'ufficio a cui il documento è assegnato;
- ogni altra informazione utile o necessaria, già disponibile al momento della registrazione.

I dati relativi alla segnatura di protocollo di un documento trasmesso da una AOO sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML) 1.0, compatibile con un file DTD (Document Type Definition) (art. 18, DPCM 3 dicembre 2013).

L'Amministrazione ricevente può utilizzare le informazioni della segnatura per automatizzare le operazioni di registrazione di protocollo in arrivo del documento ricevuto.

6.3.2. Per il documento cartaceo (analogico)

Le informazioni da associare al documento analogico, desunte dal sistema di protocollo e gestione documentale, sono:

- l'identificazione in forma sintetica o estesa dell'amministrazione e dell'AOO individuata ai fini della registrazione e della gestione del documento;
- il numero progressivo di protocollo;
- la data di protocollo nel formato GGMMAAAA;
- la classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento;
- numero di fascicolo, se presente.

Gli elementi della segnatura devono essere presenti sia nei documenti prodotti da registrare in partenza, sia nei documenti scambiati tra le UO (protocollo tra uffici).

Sul documento analogico in arrivo va apposta un'etichetta adesiva, non modificabile e non staccabile, prodotta dal sistema di gestione informatica dei documenti con l'operazione di registrazione di protocollo, sulla quale sono riportati i dati appena elencati, sia in chiaro sia in codice a barre per facilitarne l'eventuale successivo processo di scansione batch.

Nel caso in cui non sia possibile apporre l'etichetta, vanno indicati a mano i dati della segnatura.

Nel caso di documenti analogici in partenza, se possibile va apposta l'etichetta, altrimenti i dati della segnatura vanno indicati a mano sul frontespizio.

6.4. Modalità di produzione e di conservazione delle registrazioni

Ogni registrazione di protocollo informatico produce un *record* nel sistema di gestione documentale che viene accodato in una base dati accessibile esclusivamente all'amministratore del sistema. Ogni operazione di inserimento e modifica viene registrata nello stesso database del sistema.

Nel sistema è possibile, per gli utenti abilitati, ottenere l'elenco delle modifiche effettuate su una data registrazione, permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione (smistamento, invio per conoscenza, restituzione, fascicolatura ecc.), ottenendo in dettaglio:

- nome dell'utente;
- data e ora;
- UO al quale l'utente ha avuto accesso per fare tale operazione;
- tipo di operazione (inserimento/modifica/visualizzazione/cancellazione);
- valore dei campi soggetti a modifica (valori originali e modificati).

Al fine di garantire l'immodificabilità delle registrazioni, il registro informatico di protocollo giornaliero viene trasmesso in conservazione entro la giornata lavorativa successiva. Ogni modifica a protocolli già registrati in date precedenti viene inserita nel registro di protocollo giornaliero della data di modifica.

6.5. La registrazione differita (o "protocollo differito")

È possibile effettuare la registrazione differita di protocollo nel caso di temporaneo, eccezionale e imprevisto carico di lavoro e qualora dalla mancata registrazione di un documento nell'ambito del sistema nel medesimo giorno lavorativo di ricezione, possa venire meno un diritto di terzi. La registrazione differita di protocollo informatico è possibile esclusivamente per i documenti in arrivo. Per "protocollo differito" si intende la registrazione di documenti in arrivo, autorizzata con comunicazione scritta (anche per email) del Responsabile della gestione documentale o da persona

espressamente delegata, in cui sono indicati nello specifico la data alla quale si differisce la registrazione del documento stesso e la causa che ne ha determinato il differimento.

In casi eccezionali, da motivare per iscritto, il Responsabile di Gestione Documentale può autorizzare la registrazione in tempi successivi, fissando comunque un limite massimo, e conferendo valore, nel caso di scadenze predeterminate, al timbro datario d'arrivo. Il Responsabile verifica pertanto che tale timbro sia sempre presente sui documenti, in modo da assicurare certezza circa l'effettiva data di consegna. Nei confronti dei terzi mittenti, ad esempio ai fini del decorso di termini legali, assume valore legale la data effettiva di consegna del documento, come risultante dalle segnature suddette. La registrazione differita non si applica per i documenti informatici pervenuti via PEC, in quanto la PEC ha lo stesso valore giuridico della raccomandata AR e quindi fa fede la data di invio della PEC allo stesso modo del timbro postale di invio della raccomandata AR.

6.6. Rilascio di ricevute attestanti la ricezione di documenti cartacei

Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'operatore che lo riceve è autorizzato a farlo, apponendo sulla medesima data di arrivo e sigla.

6.7. La ricevuta di avvenuta registrazione

La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo deve riportare i seguenti dati:

- il numero e la data di protocollo;
- l'indicazione dell'AOO che ha acquisito il documento;
- il mittente;
- l'oggetto;
- numero degli allegati se presenti;
- l'operatore di protocollo che ha effettuato la registrazione.

6.7.1. Per il documento cartaceo (analogico)

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è cura di chi effettua la protocollazione rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal sistema di gestione documentale o, se non è possibile effettuare la stampa, la fotocopia della prima pagina del documento con apposta l'etichetta che riporta i dati della segnature.

Nel caso in cui non sia possibile l'immediata protocollazione di un documento consegnato a mano (ad esempio per momentanea indisponibilità del sistema informatico), viene concordato l'invio telematico della ricevuta di protocollo all'indirizzo mail fornito da chi consegna il documento.

La ricevuta può essere altresì ritirata dall'interessato o da persona espressamente delegata nei giorni successivi.

6.7.2. Per il documento informatico

Qualora il documento informatico sia pervenuto tramite PEC, la ricevuta di protocollazione è rilasciata direttamente dal sistema di gestione documentale.

Se il documento informatico è pervenuto tramite *e-mail*, la ricevuta, se richiesta, sarà generata dal sistema (come per il documento analogico) in formato pdf o pdf/a e inviata via *e-mail* al mittente.

6.8. Documenti esclusi dalla registrazione di protocollo

Sono esclusi per legge dalla registrazione di protocollo¹⁰:

- le gazzette ufficiali;
- i bollettini ufficiali P.A.;
- i notiziari P.A.;
- le note di ricezione delle circolari;
- le note di ricezione di altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali;
- le riviste;
- i libri;
- i materiali pubblicitari;
- gli inviti a manifestazioni.

Sono esclusi su disposizione dell'Ente:

- le richieste di ferie, permessi (gestite da apposito flusso documentale);
- denunce di infortunio;
- certificati di malattia;
- comunicazioni presenze da parte di utenti a progetti in corso (es. tirocini di inclusione sociale);
- comunicazioni presenze da parte di dipendenti in strutture diverse da quella principale;
- documenti in partenza e in arrivo dal Comune di Jesi solo allo scopo di essere firmati dal Sindaco;
- le comunicazioni da parte di enti diversi di bandi di concorso;
- i DURC.

Sono inoltre esclusi dalla registrazione di protocollo i documenti già soggetti a registrazione particolare dell'Amministrazione, cioè quei documenti che per obbligo di legge sono registrati in repertori o registri diversi dal registro di protocollo generale.

I documenti esclusi dalla registrazione di protocollo devono comunque essere classificati per una corretta tenuta dell'archivio.

6.9. Il registro giornaliero di protocollo

Il registro giornaliero di protocollo è prodotto in maniera automatica dal software di gestione documentale entro il giorno lavorativo seguente, mediante la generazione o il raggruppamento delle informazioni registrate secondo una struttura logica predeterminata e memorizzato in forma statica, imm modificabile e integra.

Attualmente, in base allo stato dell'arte delle tecnologie e dei formati, è utilizzato sia il formato PDF sia il formato TXT (in cui sono specificate le modifiche e gli annullamenti di protocolli), a mente del DPCM 3 dicembre 2013, allegato 2.

Il registro giornaliero è trasmesso al Sistema di conservazione entro la giornata lavorativa successiva alla produzione.

¹⁰ DPR 28 dicembre 2000, n. 445, art. 53 comma 5.

6.10. Il registro di emergenza

Il Responsabile della gestione documentale autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su un registro di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica.

Le condizioni che si devono verificare per l'attivazione del registro di emergenza, le modalità di attivazione del registro stesso, i modelli per le registrazioni e per le autorizzazioni e le revoche delle stesse sono riportati nell'allegato 4 "Regole e modelli per l'attivazione e la gestione del registro di emergenza".

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le 24 ore, per cause di eccezionale gravità, il Responsabile della gestione documentale autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

Sul registro di emergenza devono essere riportati gli estremi del provvedimento di autorizzazione. Al termine dell'emergenza, il Responsabile della gestione documentale, chiude il registro e dà contestuale comunicazione della revoca dell'emergenza.

La sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.

Al ripristino delle funzionalità del sistema, si dovrà provvedere senza ritardo al recupero dei dati: a ciascun documento protocollato nel registro di emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza, utilizzando un'apposita funzione di ripristino.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo ordinario.

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo. In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

Il registro di emergenza si rinnova ogni anno solare: inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Il registro di emergenza è conservato con le stesse modalità del registro ufficiale come descritto al § 6.4.

7. REGISTRI E REPERTORI INFORMATICI

7.1. Repertorio - Nozione

Per repertorio si intende il registro in cui sono annotati con numerazione progressiva i documenti per i quali è prevista la registrazione particolare. I documenti sono comunque inseriti nel fascicolo archivistico di loro pertinenza per la loro minuta e in originale (o in copia conforme) nel repertorio. Il complesso dei documenti registrati a repertorio per forma omogenea costituisce una serie.

La numerazione di repertorio si rinnova ogni anno solare: inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

7.2. Repertori attivi

I repertori attivi sono i seguenti:

- Contratti e convenzioni (soggetti a registrazione in caso d'uso), compresi contratti di servizio e contratti di lavoro
- Deliberazioni del Consiglio di amministrazione
- Deliberazioni dell'Assemblea dei soci
- Deliberazioni del Comitato dei Sindaci
- Determinazioni del Direttore
- Registro informatico giornaliero di protocollo

7.3. Repertorio dei fascicoli

È il registro in cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno dei gradi divisionali del titolare.

8. FLUSSO DI LAVORAZIONE DEI DOCUMENTI

8.1. Flusso del documento informatico in arrivo

L'UO Protocollo dell'Ente registra in modo avalutativo i documenti che rivestono un valore giuridico-probatorio.

La documentazione da protocollare viene registrata, classificata e smistata alle UO competenti o che devono averne conoscenza. L'informativa della registrazione è resa immediatamente disponibile alla UO (per competenza o conoscenza) attraverso l'accumulo nella vaschetta del menu principale del sistema di gestione documentale. Il Responsabile della UO, a sua volta, può assegnare al documento (e di conseguenza al procedimento amministrativo cui si riferisce) il responsabile del procedimento interno al suo ufficio, oppure rifiutarlo e restituirlo alla UO Protocollo in caso di errore di smistamento.

I documenti amministrativi informatici in arrivo possono pervenire con diverse modalità:

- tramite posta elettronica certificata (PEC);
- tramite posta elettronica convenzionale (e-mail);
- su supporto rimovibile (Cd ROM, DVD, ecc.) con consegna diretta o trasmesso a mezzo servizio postale o corriere;
- da portali web;
- da altre banche dati.

8.2. Ricezione dei documenti informatici tramite la casella di posta elettronica certificata (PEC) istituzionale

La PEC è un vettore attraverso il quale è spedito/ricevuto un documento informatico che può essere allegato o incorporato nel corpo stesso. La PEC utilizzata nell'Ente è di tipo "chiuso" e incorporata nel sistema di gestione documentale. Per questa ragione, pervengono solo documenti informatici da PEC e non anche da posta elettronica semplice.

Il documento informatico che perviene nella casella di PEC va gestito, di norma, entro le 24 ore lavorative successive alla ricezione.

Deve essere chiaramente identificato il mittente (non sempre coincidente con il proprietario della PEC).

Una registrazione (sia in arrivo che in partenza via PEC), non permette di modificare i file informatici associati ad essa. Il sistema di gestione documentale genera tutte le ricevute previste dalla normativa in materia di posta elettronica certificata.

La verifica della validità della firma digitale è a cura del responsabile del procedimento amministrativo del documento.

Qualora il documento ricevuto non sia PDF o PDF/A (con o senza firma digitale) viene comunque registrato al protocollo. Spetta al responsabile del procedimento valutare se accettare il documento informatico assegnato non sottoscritto o non conforme agli standard e richiedere nuovamente il documento al mittente.

8.3. Ricezione di documenti informatici nella casella di posta elettronica istituzionale

L'*e-mail* è un mezzo di trasmissione che può anche costituire documento informatico se il messaggio è contenuto nel corpo della mail stessa.

Si possono avere i seguenti casi:

- documento che arriva alla casella di posta elettronica istituzionale dell'Ente come allegato alla e-mail: si apre l'allegato e, se non è già in formato pdf, con un *convertitore PDF*¹¹ si crea un file di formato PDF/A e lo si associa al sistema di gestione documentale procedendo alla registrazione in arrivo con le consuete modalità. Sarà cura del responsabile del procedimento della UO competente verificarne la provenienza e valutare se accettare o meno la firma elettronica leggera;
- documento che arriva alla casella di posta elettronica istituzionale dell'Ente costituito dal corpo della mail: si apre la mail e con un *convertitore PDF* si crea un file di formato PDF/A e lo si associa al sistema di gestione documentale procedendo alla registrazione in arrivo con le consuete modalità. Sarà cura del responsabile del procedimento della UO competente verificarne la provenienza e valutare se accettare o meno la firma elettronica leggera;
- documento che arriva alla casella di posta elettronica istituzionale di un dipendente dell'Ente (come allegato o corpo del testo). Il ricevente gira l'*e-mail con forward (inoltra)* corredata degli eventuali allegati alla casella di posta elettronica dell'addetto al protocollo in arrivo. L'operatore converte il file in PDF/A, registra nel protocollo informatico e associa il file con estensione PDF/A alla registrazione, insieme agli eventuali allegati;
- il documento via *e-mail* potrebbe anche non essere firmato (se è firmato digitalmente non serve fare nulla, perché l'autore del messaggio è già noto con sicurezza). È in capo al responsabile del procedimento verificare la provenienza del documento pervenuto via *e-mail* ed eventualmente chiedere al mittente un documento informatico firmato digitalmente e inviato via PEC. In questo caso sarà un nuovo protocollo e non un secondo esemplare, in quanto quest'ultimo è sottoscritto;
- nel caso di e-mail da cui non sia possibile desumere l'indicazione di nome e cognome il documento sarà trattato come Anonimo (cfr. § 9.15).

I documenti informatici così pervenuti saranno protocollati a cura dell'UO Protocollo, di norma, entro le 24 ore lavorative dal giorno di arrivo.

In ogni caso, se un dipendente riceve nella propria casella di posta fornita dall'Amministrazione documenti concernenti affari o procedimenti amministrativi dell'Amministrazione è tenuto a inoltrare tempestivamente il messaggio e-mail all'addetto alla protocollazione in arrivo della UO Protocollo.

8.4. Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono pervenire anche in modalità diverse dalla posta elettronica o dalla posta elettronica certificata e quindi su supporti diversi.

L'UO Protocollo verifica la leggibilità dei dati contenuti nel supporto informatico e provvede alla registrazione solo in caso di esito positivo. È cura della UO responsabile verificarne le caratteristiche e la provenienza certa.

I documenti informatici così pervenuti sono protocollati, di norma, entro le 48 ore lavorative successive dal giorno di arrivo.

8.5. Ricezione link a documenti

Se il documento informatico ricevuto contiene un link/collegamento ad un cloud, i file raggiungibili tramite questo collegamento devono essere allegati al protocollo, se le loro dimensioni non sono eccessive per i limiti tecnologici imposti dalla soluzione software. Se ci sono problemi di spazio di

¹¹ Con *convertitore PDF* si intende qualsiasi programma o funzione software che consente di creare file in formato pdf partendo da file di diverso formato.

memorizzazione e c'è più di un allegato si può procedere ad effettuare più di una registrazione, collegandole tra loro.

In caso di impossibilità di inserimento dell'allegato, si provvede comunque a registrare il documento in arrivo indicando nelle note che non è stato possibile l'inserimento del file, e si valuta caso per caso l'opportunità di acquisire o meno gli allegati con altri mezzi (ad esempio con stampa cartacea o altro supporto di memorizzazione come DVD) insieme al Responsabile del procedimento.

8.6. Priorità nella registrazione dei documenti informatici in arrivo

È data priorità ai documenti pervenuti con PEC in considerazione del fatto che il sistema rilascia automaticamente al mittente la ricevuta di avvenuta consegna del documento.

Indipendentemente dal mezzo telematico di arrivo, è data priorità nella registrazione a protocollo a:

- atti giudiziari notificati;
- documenti del Ministero;
- documenti di rilevanza finanziario-contabile (MEF – Corte dei Conti, etc.);
- corrispondenza relativa a minori;
- domande relative a bandi in scadenza.

Tale casistica è soltanto indicativa ed è suscettibile di variazione in concomitanza con altre priorità che si dovessero presentare (scadenze bandi di concorso, gare, etc.).

8.7. Flusso del documento cartaceo (analogico)

La corrispondenza cartacea (analogica) in arrivo perviene all'UO Protocollo dell'Ente secondo le seguenti modalità:

- posta pervenuta per il tramite di Poste italiane SpA (o di altri gestori autorizzati);
- posta pervenuta direttamente alle UO e da questa recapitata all'UO Protocollo;
- posta pervenuta direttamente alla Portineria della Casa di Riposo di Jesi e da questa recapitata all'UO Protocollo;
- posta recapitata personalmente, *brevi manu*.

Gli uffici ai quali pervengono gli originali analogici devono apporre sulla prima pagina l'apposito timbro "Posta in arrivo" con indicata la data corrente.

8.8. Apertura delle buste

Tutte le buste vanno aperte a cura dell'UO Protocollo. Fanno eccezione e pertanto non vanno aperte, le buste:

- riportanti le seguenti diciture: "offerta", "gara d'appalto" "non aprire" o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara (ad es. il CIG);
- riportanti le seguenti diciture: riservato, personale, confidenziale, spm/sgm (sue proprie mani/sue gentilissime mani), etc. o dalla cui confezione si evinca il carattere di corrispondenza privata (ad. es. busta particolare);
- le altre buste indirizzate nominativamente al personale vanno aperte nella convinzione che nessun dipendente utilizzi l'Amministrazione come fermoposta o casella postale privata. Chiunque riceva, tramite corrispondenza privata, documenti concernenti affari o procedimenti amministrativi dell'Amministrazione è tenuto a farli pervenire tempestivamente all'UO Protocollo;
- la corrispondenza indirizzata agli ospiti della Casa di Riposo – Residenza protetta di Jesi.

8.8.1. Conservazione ed eliminazione delle buste

Le buste pervenute tramite posta raccomandata, corriere o altra modalità per la quale si renda rilevante evidenziare il mezzo di trasmissione e il timbro postale (ad es., una fattura passiva proveniente da un fornitore estero arrivata in prossimità del termine di scadenza per il pagamento), sono spillate assieme al documento e trasmesse alla UO di competenza.

Tutte le altre buste verranno eliminate e non conservate.

8.9. Priorità nella registrazione dei documenti analogici in arrivo

Indipendente dal mezzo di trasmissione, è data priorità nella registrazione a protocollo a:

- documenti consegnati *brevi manu*: si protocolla subito e si rilascia la ricevuta di avvenuta protocollazione;
- atti giudiziari notificati;
- documenti del Ministero;
- documenti di rilevanza finanziario-contabile (MEF – Corte dei Conti, etc.);
- documenti relativi a procedimenti ispettivi;
- corrispondenza relativa a minori;
- domande relative a bandi in scadenza;
- documenti di trasmissione di assegni o altri valori di debito/credito.

Tale casistica è soltanto indicativa ed è suscettibile di variazione in concomitanza con altre priorità che si dovessero presentare (scadenze bandi di concorso, gare etc.).

Di norma si procede all'apertura e alla registrazione di protocollo nella stessa giornata di consegna e comunque, di norma, entro le 48 ore lavorative successive alla ricezione.

8.10. Protocollo particolare

Sono previste particolari forme di riservatezza e di accesso controllato al protocollo unico per:

- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- documenti legati a vicende di persone o a fatti privati e, in particolare, i documenti riportanti dati sensibili e dati giudiziari.

8.10.1. Procedure del protocollo particolare

Le tipologie di documenti da registrare nel protocollo particolare sono individuate dal Responsabile della gestione documentale, d'intesa con i responsabili delle UO. Ogni documento reca il proprio numero di protocollo, come per ogni altro protocollo, ma deve essere modificata la visibilità del documento in modo che possa essere accessibile solo alle persone autorizzate, in base alle indicazioni del Responsabile della Gestione documentale o persone espressamente delegate.

Per i documenti in arrivo analogici particolarmente voluminosi, viene fotoriprodotta la lettera accompagnatoria con l'apposizione della dicitura "I documenti integrali sono consultabili presso..." indicando la UO presso cui tale documento è archiviato.

8.11. Annullamento di una registrazione

È consentito l'annullamento di una registrazione di protocollo per motivate e verificate ragioni.

Solo il Responsabile della gestione documentale e le persone espressamente delegate sono autorizzate ad annullare la registrazione.

L'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo.

I motivi per i quali è richiesto l'annullamento possono essere:

- errore di inserimento delle informazioni registrate in forma immodificabile;
- duplicazione di un documento per errore;
- la motivazione per cui il documento è stato prodotto è venuta meno purché il documento non sia già stato diffuso.

L'utente deve richiedere l'annullamento tramite il sistema informatico di gestione documentale e deve specificare la motivazione di tale richiesta, che viene associata alla registrazione di protocollo del documento annullato. Nel caso in cui il documento da annullare sia sostituito da una nuova registrazione, negli estremi del provvedimento di autorizzazione all'annullamento si indica che "il documento è stato sostituito e correttamente registrato con protocollo n. ____ del ____".

La registrazione annullata resta visibile all'interno del sistema di gestione documentale e della sequenza numerica con la dicitura "Annullato".

Il documento analogico annullato riporta gli estremi dell'annullamento e viene conservato nell'archivio della UO di provenienza.

Se il documento analogico o informatico annullato costituisce una tipologia documentale soggetta a registrazione per la quale è prevista la conservazione perenne (ad es. un contratto), lo stesso sarà conservato nel proprio repertorio con la dicitura "annullato" assieme alla richiesta di annullamento. In tema di annullamento dei provvedimenti occorre far riferimento alle disposizioni di cui alla L. 241/1990 in merito agli strumenti di autotutela.

Nella registrazione di protocollo appaiono, oltre agli elementi già indicati, anche la data, il cognome e nome dell'operatore che ha effettuato l'annullamento.

Le informazioni relative al protocollo rimangono comunque memorizzate nel registro informatico per essere sottoposte alle elaborazioni previste dalla procedura, comprese le visualizzazioni e le stampe, nonché la data, l'ora, l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo.

Si può comunque procedere all'annullamento di un documento ricevuto con PEC sebbene il mittente abbia già la ricevuta di avvenuta consegna.

Non si annulla mai un documento informatico trasmesso con PEC in quanto il destinatario è già in possesso del documento stesso. Si può procedere con la redazione di un nuovo documento che annulla e sostituisce il precedente (in questo caso è necessario citare il riferimento del protocollo), va protocollato e nuovamente inviato via PEC.

8.12. Corresponsabilità di un documento e di un fascicolo

La corresponsabilità di un documento e/o di un fascicolo è la partecipazione al procedimento amministrativo di più UO della stessa AOO (corresponsabilità di servizi interna).

Nella corresponsabilità di servizi interna, pur essendo la responsabilità amministrativa tra più UO e di conseguenza tra più responsabili di procedimento, la responsabilità della tenuta dei documenti in originale (per quelli analogici), cioè del fascicolo, spetta esclusivamente alla UO che ha la competenza prevalente sul procedimento amministrativo e che chi ha protocollato ha inserito per prima nella registrazione e prima riportata nella registrazione di protocollo. Spetta pertanto alla prima UO indicata aprire il fascicolo e poi renderlo disponibile alle altre UO coinvolte nella corresponsabilità di servizi.

8.13. Documenti scambiati tra uffici non soggetti a registrazione di protocollo

- Richieste di fornitura di cancelleria;
- Richieste di acquisti/pagamenti con cassa economale;
- Richieste di pagamenti alla UO Contabile.

8.14. Casi di rigetto

Per rigetto si intende la segnalazione di una UO all'UO Protocollo della erronea assegnazione di competenza su un determinato documento ricevuto in smistamento. Pertanto il rigetto avviene solo per i documenti in arrivo.

Prima del rigetto la UO deve riportare nella registrazione una annotazione motivando e indicando la UO competente.

Il documento informatico ritorna così in carico all'UO Protocollo che potrà immediatamente inoltrarlo alla UO competente.

Nel caso di documento originale analogico, si può procedere alla nuova assegnazione ad altra UO solo dopo aver ricevuto nuovamente l'originale rigettato mediante il sistema di protocollo.

In caso di conflitto di competenze tra UO, è il Dirigente/Direttore su proposta del Responsabile della gestione documentale, che determina lo smistamento definitivo.

Nessun documento, analogico e/o informatico, deve rimanere in carico all'UO Protocollo, soprattutto se pervenuto con PEC.

8.15. Flusso del documento informatico in partenza

Il documento informatico prodotto deve essere redatto preferibilmente nel formato PDF/A o per casi particolari (cfr. Capitolo 9) secondo gli altri formati stabiliti in precedenza (cfr. § 3.2.2) e in base alla tipologia di documento informatico, deve avere i seguenti requisiti minimi di forma e contenuto per poter essere registrato al protocollo:

a) documento informatico formato attraverso l'acquisizione della copia per immagine su supporto informatico di un documento analogico (scansione del documento cartaceo):

- Logo dell'Ente
- Luogo e data completa (giorno, mese, anno) scritta per esteso;
- Indicazione dell'indirizzo PEC o e-mail del destinatario;
- Indicazione della UO Responsabile e del responsabile del procedimento;
- Numero degli allegati;
- Sottoscrizione autografa (nei casi previsti dalla normativa deve essere corredato da dichiarazione di conformità sottoscritta con firma digitale)

b) redazione tramite l'utilizzo di appositi strumenti software:

- Logo dell'Ente
- Luogo e data completa (giorno, mese, anno) scritta per esteso;
- Indicazione dell'indirizzo PEC o e-mail del destinatario;
- Indicazione della UO Responsabile e del responsabile del procedimento;
- Numero degli allegati;
- Firma digitale.

Può essere predisposto un flusso all'interno del sistema gestionale per i visti eventualmente richiesti all'interno dell'amministrazione prima della protocollazione del documento firmato digitalmente.

Il documento informatico protocollato può essere trasmesso a mezzo PEC o via *e-mail*.

8.16. Flusso del documento informatico tra UO della stessa AOO

Il documento tra uffici (o interno) è quello che una UO invia ad un'altra UO della stessa AOO.

Trattandosi di documenti endoprocedimentali, possono essere prodotti in PDF/A e la registrazione a protocollo costituisce firma elettronica avanzata.

9. CASISTICA E COMPORTAMENTI

9.1. Gestione di concorsi e selezioni

Se le istanze di partecipazione a concorsi e procedure di selezione sono inviate in formato cartaceo (analogico), tenuto conto che sono spesso corredate di allegati numerosi e, in alcuni casi, anche voluminosi, alla registrazione di protocollo può essere associata la sola scansione dell'istanza e non quella degli allegati. Sarà cura del servizio di registrazione indicare nel sistema di protocollo ciascun allegato ricevuto, inserendo una "Annotazione" immodificabile in cui si dà contezza del fatto che non si procede alla scansione, del tipo: "Non si procede alla scansione ... (ad es. delle pubblicazioni)". Le istanze devono essere protocollate direttamente dalla UO Protocollo e poi trasmesse alla UO competente.

Non è ammessa la consegna della domanda in busta sigillata: l'UO Protocollo apre il plico e registra le domande nella loro completezza, ferma restando la possibilità di non provvedere alla scansione degli allegati voluminosi.

Se le istanze di partecipazione a concorsi e procedure di selezione sono inviate in modalità telematica, a mezzo PEC, gli allegati saranno automaticamente associati alla registrazione.

9.2. Denunce di infortuni

Il datore di lavoro è tenuto a denunciare all'INAIL gli infortuni da cui siano colpiti i dipendenti prestatori d'opera, indipendentemente da ogni valutazione circa la ricorrenza degli estremi di legge per l'indennizzabilità.

Le denunce di infortunio sono inviate dall'Ente all'INAIL esclusivamente in modalità telematica accedendo al portale dell'INAIL con apposite credenziali rilasciate ai dipendenti incaricati. L'invio delle denunce tramite PEC è consentito solo in caso di malfunzionamento del sistema. Considerato che il sistema per l'invio telematico della denuncia prevede l'inserimento obbligatorio di dati ulteriori rispetto a quelli presenti sul certificato del pronto soccorso, è onere del lavoratore consegnare la dichiarazione di infortunio sul lavoro compilata in ogni sua parte. Il delegato alle denunce che ricevesse tale modulo compilato in modo incompleto dovrà chiederne tempestivamente l'integrazione all'infortunato. Il funzionario attesta la data certa e la piena conoscenza dell'infortunio sottoscrivendo e datando il documento. Questa procedura sostituisce il protocollo in arrivo del documento, quindi le denunce di infortunio sono una tipologia di documenti esclusa dalla registrazione di protocollo.

9.3. Certificati di malattia

I certificati di malattia sono acquisiti consultando la banca dati dell'INPS con apposite credenziali rilasciate ai dipendenti incaricati. Dopo averli visualizzati vengono inviati per e-mail al Comune di Jesi che si occupa della gestione delle presenze del personale. I certificati di malattia sono una tipologia di documenti esclusa dalla registrazione di protocollo.

9.4. Atti giudiziari

Ai fini dell'identificazione del corrispondente di atti e/o note inerenti a contenzioso, occorre tener presente la differenza tra la notifica (effettuata direttamente all'Amministrazione) e altri tipi di comunicazione.

La notifica avviene con la consegna dell'atto eseguita dall'ufficiale giudiziario, nelle mani proprie del destinatario o a soggetto rappresentante dell'amministrazione autorizzato a ricevere l'atto, o da

altro soggetto abilitato tramite servizio postale, a mezzo PEC o nelle altre modalità stabilite dalla legge.

Se l'atto è notificato a mano si considera come data di notifica quella indicata nella referta di notifica del documento; se è notificato con raccomandata si considera il giorno in cui si ritira la raccomandata.

Ai sensi dell'art. 149-bis cpc, la copia estratta dal documento originale deve essere firmata digitalmente dall'ufficiale giudiziario e, se non è fatto espresso divieto dalla legge, la notificazione può eseguirsi a mezzo posta elettronica certificata, anche previa estrazione di copia informatica del documento analogico. In questo caso, l'ufficiale giudiziario trasmette copia informatica dell'atto sottoscritta con firma digitale all'indirizzo di posta elettronica certificata del destinatario risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni. La notifica si intende perfezionata nel momento in cui il gestore rende disponibile il documento informatico nella casella di posta elettronica certificata del destinatario.

Per mittente si intende la parte istante, cioè il legale/avvocato delegato mediante procura alle liti che agisce in nome e per conto del soggetto interessato e che ha richiesto la notifica dell'atto. Anche un sindacato o un'associazione non riconosciuta, può essere mittente, nel caso in cui agisca in nome e per conto di un lavoratore in una controversia sindacale. Il mittente del documento non è l'organo giudiziario indicato generalmente sul frontespizio dell'atto (ad es. Tribunale, Corte di Appello), ma colui che ha richiesto la notificazione, generalmente il legale a cui il ricorrente/attore che ha conferito mediante mandato la procura alle liti (quindi il corrispondente apposto di norma sulla prima pagina dell'atto in alto a destra).

Diverse sono poi le comunicazioni (quali quelle consistenti in avvisi di deposito di note o di fissazione di udienza) che provengono direttamente dalla cancelleria dell'autorità giudiziaria (Tribunale, Corte di appello, ecc.) innanzi a cui pende il giudizio. In questi casi il mittente è sicuramente l'autorità giudiziaria medesima.

9.5. Fatture elettroniche (Fattura PA)

La fattura elettronica destinata alla pubblica amministrazione rispetta i requisiti di formato e contenuto prescritti dal Decreto Ministeriale 3 aprile 2013, n. 55 (e successive modifiche), e viene trasmessa e ricevuta attraverso il Sistema di interscambio (SdI).

È obbligatorio emettere fatture elettroniche nei confronti di tutte le amministrazioni pubbliche italiane (ciclo attivo e passivo).

Non si accettano più fatture cartacee emesse in data pari o successiva al 31 marzo 2015, salvo per i soggetti non tenuti a rispettare l'obbligo di fatturazione elettronica (es. fornitori esteri, persone fisiche o giuridiche senza partita IVA).

Le fatture cartacee che avrebbero dovuto essere emesse in formato elettronico vanno restituite al mittente utilizzando lo stesso canale di comunicazione, in piena simmetria delle forme.

Le fatture cartacee pervenute a mezzo PEC emesse a far data dal 31 marzo 2015 in poi devono essere annullate con la seguente motivazione: "Ai sensi della Legge 24 dicembre 2007, art. 1 commi 209-214, le fatture emesse nei confronti dell'ente in data pari o successiva al 31 marzo 2015 devono essere trasmesse in forma elettronica secondo il formato di cui all'allegato A "Formato della fattura elettronica" del Decreto Ministeriale 3 aprile 2013, n. 55". Il mittente riceverà la notifica di annullamento, comprensiva di motivazione, a mezzo PEC.

La fattura elettronica PA non è prevista per i fornitori non residenti in Italia. In tal caso la fattura andrà gestita come qualsiasi documento analogico: protocollata, assegnata e fascicolata.

La fattura elettronica perviene in formato XML via PEC, all'indirizzo dichiarato dall'Ente e registrati sull'indice IPA nel corrispondente servizio di fatturazione.

La fattura viene gestita direttamente dal sistema di gestione della contabilità, dove viene presa in carico per la verifica di correttezza e conformità. Sul sistema contabile si provvede alla registrazione della stessa sul registro delle fatture, entro 10 giorni dal ricevimento (DL 66/2014 art. 42).

La data di ricezione della PEC fa fede quale termine iniziale dei 15 giorni entro cui la fattura va accettata o rifiutata con motivazione (la mancata notifica di rifiuto entro 15 giorni equivale ad accettazione), nonché dei 30 (o 60, a seconda degli accordi con il fornitore) giorni previsti dalla legge decorsi i quali, in assenza di pagamento o contestazione, iniziano automaticamente a decorrere gli interessi moratori (D.Lgs. 192/2012, art. 1, comma 1, lett. d).

Le fatture elettroniche trasmesse dai fornitori alle PA (ciclo passivo), così come quelle emesse dall'Ente (ciclo attivo), sono obbligatoriamente conservate in modalità elettronica, secondo quanto espressamente disposto dalla legge¹², direttamente dal sistema di gestione della contabilità. Tale sistema, fornito dall'azienda CBA di Trento ed erogato in cloud come SaaS, è integrato con un sistema di conservazione a norma e accreditato AGID, fornito dall'azienda Savino Solution Srl.

9.6. DURC on-line

Ai sensi dell'art. 4 della Legge 78/2014, la verifica della regolarità contributiva avviene con modalità esclusivamente telematiche. In caso di Documento unico di regolarità contributiva (DURC) già disponibile, questi avrà durata pari a quanto indicato nel documento stesso, in caso di non disponibilità del documento il sistema ne comunicherà la data di disponibilità. Il documento così ottenuto avrà validità di 120 giorni dalla data di emissione.

Per i DURC richiesti, ma non immediatamente disponibili, occorre attendere la ricezione dell'avviso di disponibilità del documento che perviene a mezzo PEC. Tale PEC non dovrà essere protocollata, ma il protocollatore informerà la UO Contabile della disponibilità online di tale documento, via email ordinaria, e la PEC verrà impostata come completata.

A questo punto è possibile consultare il sistema del DURC on-line e procedere come per i DURC immediatamente disponibili.

9.7. Gare e procedure negoziate gestite in modalità telematica

All'interno dell'Ente, le gare sono svolte telematicamente attraverso due strumenti:

- il *Mercato Elettronico della P.A.* (MePA), ai sensi dell'art. 11 del D.P.R. 101/2002, per acquistare beni e servizi offerti dai fornitori abilitati presenti sui diversi cataloghi del sistema, con importo inferiore alla soglia comunitaria;
- il Portale GT-SUAM, gestito da Regione Marche e messo a disposizione in riuso, per importi uguali o superiori alla soglia comunitaria.

Al di fuori di tali piattaforme è anche possibile stipulare contratti in conseguenza all'adesione a Convenzioni o Accordi Quadro.

Tutti i documenti inerenti gare svolte mediante portale telematico (o pervenuti in modalità elettronica) devono essere soggetti a registrazione di protocollo.

Per quanto riguarda le offerte pervenute dagli operatori, queste vanno in ogni caso protocollate: la UO che si occupa della gestione della gara dovrà provvedere ad estrarre i documenti di gara dal portale ed effettuare la registrazione di protocollo.

Nel caso in cui si utilizzi un portale che permette l'accesso alle offerte solo dopo la data di chiusura del bando, le offerte saranno protocollate all'atto dell'apertura delle buste (quindi non il giorno dell'arrivo, perché non è noto). Nella registrazione di protocollo di tali offerte andrà indicata come data di arrivo la data di ricezione che appare all'interno del portale utilizzato (MEPA o GT-SUAM).

¹² DM MEF 17 giugno 2014.

Vanno protocollate anche le comunicazioni che intercorrono tra Ente e operatori e che riguardano lo svolgimento della gara stessa.

Si può derogare solo per comunicazioni inerenti richieste di sopralluogo e altre comunicazioni di servizio, su indicazione del Responsabile di procedimento della gara.

9.8. Documenti informatici con oggetto multiplo

Nel caso di documenti in arrivo che trattano più argomenti di competenza di UO diverse tra loro, concretando il caso del cosiddetto “oggetto multiplo”, il documento viene registrato redigendo l’oggetto in maniera esaustiva con tutte le informazioni necessarie a comprendere i vari argomenti. La classificazione del documento riguarderà l’argomento prevalente o comunque individuato come tale, poi smistato alla UO competente sullo stesso e anche alle altre UO competenti. Ciascuna UO corresponsabile dovrà gestire e fascicolare la propria copia informatica.

Nel caso di documento in partenza è compito della UO responsabile verificare che il documento prodotto tratti un solo argomento, chiaramente espresso nel campo “oggetto”.

9.9. Documenti pervenuti via PEC

La casella di PEC istituzionale dell’Ente è “chiusa” quindi può ricevere messaggi e documenti solo da altri vettori qualificati (altre caselle di PEC). In questo caso, al fine di rendere efficace la natura giuridico-probatoria del messaggio di PEC, si procede con la protocollazione, tranne nei casi citati al §6.8, in cui la PEC viene accantonata come conclusa (ma sempre rintracciabile nel sistema di gestione documentale).

La ricezione via PEC di un documento comprova il fatto che lo stesso ha raggiunto il destinatario.

In ogni caso sono soggetti a registrazione di protocollo:

- il messaggio;
- i file allegati.

Per quanto riguarda la corretta identificazione del mittente, bisogna tener presente che la PEC è solo un vettore, il mittente è colui che sottoscrive il documento allegato o, nel caso di testo nel corpo del messaggio (*body message*) senza allegato, colui che lo trasmette.

Nel caso in cui con uno stesso messaggio PEC pervengano documenti di firmatari diversi, senza alcun documento con funzione di lettera di trasmissione, è prodotta una registrazione distinta per documento, corredata di annotazioni esplicative. In alternativa è lasciato l’indirizzo così come pervenuto e nell’oggetto è scritto: “Trasmissione di documenti con firmatari diversi”. Oppure, se si evince che l’indirizzo PEC è riconducibile in modo certo a uno dei firmatari dei documenti trasmessi, si indica nell’oggetto: “Cognome Nome trasmette per sé e per ...”.

La regola generale da seguire, in base al principio di simmetria delle forme, è che a un documento pervenuto con PEC si risponde con un documento trasmesso con PEC, utilizzando lo stesso canale di comunicazione.

9.10. Gestione di più documenti diversi trasmessi via PEC o email

Se con un unico messaggio pervengono due o più documenti, si provvede alla registrazione dei singoli documenti e non del messaggio, quindi con tante registrazioni quanti sono i documenti pervenuti provvedendo ad inserire eventuali annotazioni di richiamo tra le registrazioni.

9.11. Gestione di soli allegati pervenuti via PEC e di documenti costituiti dal solo corpo della PEC

Qualora pervengano a mezzo PEC documenti identificabili come allegati e il documento principale si limita all'oggetto del messaggio, presentato dal protocollo informatico come oggetto nell'apposito campo in fase di registrazione, l'oggetto proposto rimane.

Il messaggio contenuto nel corpo della PEC deve considerarsi come documento sottoscritto e valido a tutti gli effetti di legge e, pertanto, va protocollato.

9.12. Documenti pervenuti a mezzo *e-mail* semplice (non certificata)

Se richiesto dal responsabile del procedimento o da suo delegato, si registrano a protocollo anche le *e-mail* semplici, limitatamente ai casi in cui il loro contenuto sia rilevante nell'ambito di un procedimento, valutando caso per caso. Per richiesta si intende l'inoltro della *e-mail* alla casella di posta elettronica istituzionale dell'operatore dell'UO Protocollo.

Le richieste di informazioni su orari di apertura e sul funzionamento di procedure (anche provenienti dall'estero) non sono soggette a registrazione di protocollo e ad esse si può rispondere a mezzo *e-mail* non protocollata. Invece lamentele, doglianze, comunicazioni di disservizi devono essere valutate caso per caso. Nei casi di particolare gravità e rilevanza, si procede alla registrazione a protocollo.

L'*e-mail* contenente dati o informazioni prodromiche alla formazione di un provvedimento amministrativo non sono soggette a registrazione di protocollo; sono, altresì, esclusi dalla registrazione a protocollo gli atti preparatori (bozze, proposte non ufficiali, etc.). Per i documenti registrati a protocollo e trasmessi a mezzo *e-mail* si valuta caso per caso.

9.13. Gestione del secondo esemplare

Per essere certi che si tratti di un secondo originale di un documento già protocollato, è necessario verificare l'esatta corrispondenza tra i due esemplari, inclusi gli allegati, in tutte le loro parti (firme, date, segnature di protocollo, ecc.). Per i documenti sottoscritti con firma elettronica è necessario verificare anche che la data e l'ora di firma coincidano.

Una volta appurata la perfetta identità tra i due documenti, si agirà diversamente nel trattamento a seconda della modalità di ricezione del secondo esemplare.

Se il secondo esemplare perviene in formato analogico, si appone su di esso la segnature di protocollo e l'indicazione "Secondo esemplare". Nella registrazione di protocollo si inserisce la "Annotazione" in modo immodificabile "Pervenuto secondo esemplare mediante raccomandata a/r" al fine di poter recuperare tutti gli esemplari pervenuti nel caso si debba, ad es., modificare la UO indicata nella segnature di protocollo.

Nel caso di arrivo mediante PEC o altro sistema informatico (*e-mail* semplice, ecc.) si annota sulla PEC la dicitura "Duplicata del protocollo n. ____ del ____" e si archivia tale PEC come "completata" (sempre rintracciabile nel sistema di gestione). Nella registrazione di protocollo del primo esemplare andrà invece inserita l'annotazione "Pervenuto secondo esemplare via PEC (o altro mezzo) in data ...".

9.14. Documenti scambiati tra UO della stessa AOO

Per documenti interni si intendono i documenti scambiati tra le diverse UO della medesima AOO.

I documenti informatici prodotti a seguito della protocollazione e scansione di documenti originali cartacei trasmessi tra le UO di ciascuna AOO sono inoltrati in formato digitale tramite il sistema di protocollo informatico, provvedendo anche all'inoltro dell'originale analogico alla UO Destinataria. Le comunicazioni informali tra uffici non sono soggette a registrazione di protocollo in base al principio di non aggravio del procedimento, ma a cura delle UO interessate possono essere acquisite nel sistema di protocollo come documento non protocollato.

9.15. Documenti anonimi

La *ratio* che deve governare il comportamento di un operatore durante la fase di registrazione di un documento in arrivo deve essere improntata all'avalutatività. In altre parole, l'operatore di protocollo deve attestare che un determinato documento, così come si è registrato, è pervenuto. Si tratta di una delicata competenza di tipo certificativo, attestante la certezza giuridica di data, forma e provenienza per ogni documento.

Le lettere anonime, pertanto, sono soggette a registrazione di protocollo.

Se il documento anonimo è pervenuto a mezzo PEC si lascia come mittente l'indirizzo PEC.

10. DALL'ARCHIVIO CORRENTE ALL'ARCHIVIO DI DEPOSITO

10.1. Archivio

L'archivio è costituito dal complesso documentario prodotto o acquisito da un ente nell'esercizio delle sue funzioni; in questa accezione si distingue in corrispondenza delle diverse fasi della gestione in archivio corrente, archivio di deposito e archivio storico.

I singoli documenti e l'Archivio dell'ASP, in quanto ente pubblico, ai sensi del D.lgs. 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, sono beni culturali (art. 10, comma 2, lettera b), sono assoggettati al regime proprio del demanio pubblico (art. 53, comma 1) e quindi sono inalienabili (art. 54, comma 1, lettera d). All'Archivio, considerato unitariamente come bene culturale dalla fase corrente a quella storica, si applicano le norme previste dal Codice, che sanzionano penalmente l'eventuale violazione dell'obbligo di conservare correttamente l'archivio nella sua integrità e organicità e di inventariare l'archivio storico, costituito dai documenti relativi agli affari esauriti da oltre 40 anni (art. 30, commi 1, 2 e 4 e art. 170, D.lgs. n. 42/2004). La Soprintendenza archivistica per le Marche svolge compiti di tutela e vigilanza sull'Archivio. Ai sensi del D.lgs. n. 42/2004 tutti gli interventi sugli archivi devono essere autorizzati dalla Soprintendenza.

10.2. Archivio corrente, deposito, storico

L'archivio corrente è costituito dagli affari/procedimenti in corso di trattazione e serie numerate e repertorate di atti o provvedimenti in corso di trattazione e serie numerate e repertorate di atti o provvedimenti. E' gestito direttamente dalle UO responsabili dei procedimenti che generano la documentazione archiviata, che ne sono responsabili.

L'archivio di deposito è costituito dagli affari/procedimenti la cui trattazione non è più corrente. Anche tale archivio è gestito direttamente dalle UO responsabili dei procedimenti che generano la documentazione archiviata, che ne sono responsabili.

L'archivio storico è costituito dagli affari/procedimenti, destinati alla conservazione permanente, conclusi da più di quaranta (40) anni, effettuate le operazioni di riordino e inventariazione. Non è ancora stato creato tale archivio vista la recente istituzione dell'Ente (2012).

10.3. Trasferimento dei fascicoli cartacei nell'archivio storico

Per il trasferimento viene predisposto a cura del responsabile del procedimento amministrativo l'elenco dei fascicoli trasferiti indicando, nell' intestazione l'ufficio di provenienza della documentazione, e per ogni unità trasferita la classificazione, il numero progressivo di repertorio del fascicolo, l'oggetto e gli estremi cronologici.

Con il versamento nell'archivio storico l'UO che si occupa dell'archivio dell'Ente acquisisce la piena titolarità dei documenti a esso affidati.

I fascicoli sono trasferiti rispettando l'ordine dei documenti all'interno dei fascicoli. Qualora i responsabili delle UO si trovassero nelle condizioni di dovere trasferire fascicoli o documenti prodotti e chiusi da molto tempo, oppure i cui responsabili non siano più in servizio, essi dovranno essere trasferiti nelle condizioni in cui si trovano, senza operare interventi sull'ordinamento degli stessi e redigendo l'elenco di consistenza.

Nei casi in cui ciò non sia possibile, i responsabili delle UO concorderanno le modalità opportune di trasferimento, caso per caso, con il Responsabile della gestione documentale. Prima del trasferimento i responsabili del procedimento amministrativo provvedono anche a verificare che i fascicoli risultino chiusi anche nel sistema informatico di gestione documentale.

Alla ricezione dei fascicoli il Responsabile della gestione documentale verifica la corrispondenza dell'elenco di consistenza con il verbale di trasferimento, sottoscritto insieme all'elenco anche dal responsabile del procedimento amministrativo al momento della consegna dei fascicoli.

La non corrispondenza, anche parziale, tra l'elenco di consistenza e il materiale documentale effettivamente versato è oggetto di dichiarazione a cura del Responsabile della gestione documentale e sarà informata la struttura versante con invito a provvedere entro 10 giorni alla regolarizzazione.

10.4. Trasferimento dei fascicoli informatici

Il Responsabile della gestione documentale provvede, almeno una volta all'anno, a generare e a trasmettere dei pacchetti di versamento al sistema di conservazione, secondo le regole che saranno previste nel manuale di conservazione, avvalendosi anche di processi di automazione disponibili nel sistema di gestione documentale.

10.5. Conservazione

Il Responsabile della gestione documentale attua tutte le iniziative finalizzate alla corretta conservazione della documentazione, sia in ambito analogico che digitale.

Per la conservazione della documentazione analogica, il Responsabile della gestione documentale verifica che nei depositi d'archivio siano rispettati i criteri che garantiscano la sicurezza della documentazione (ordinamento, sicurezza dei locali con sistemi antincendio e antintrusione, il controllo di temperatura e umidità relativa, prevenzione dall'intrusione di agenti patogeni, ordinaria manutenzione e pulizia, spolveratura periodica), in collaborazione con i servizi preposti alle attività tecniche. Il Responsabile della gestione documentale provvede anche ad attuare interventi di restauro, nei casi in cui si rendessero necessari.

Per la conservazione digitale il Responsabile della gestione documentale concorderà i criteri con il Responsabile della conservazione (art. 21, 29-31, D.lgs. 42/2004). Per l'Ente il conservatore è soggetto esterno, la Regione Marche.

11. IL SISTEMA INFORMATICO E IL PIANO DI SICUREZZA

Il sistema informatico è l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti. (DPR 445/2000, art.1, lettera r).

La gestione dei flussi documentali è un insieme di funzionalità che consentono di trattare e di organizzare la documentazione prodotta (in arrivo, in partenza e interna) dalle amministrazioni. Ogni AOO individua le misure di sicurezza da adottare secondo quanto stabilito dalle normative vigenti.

11.1. Il modello organizzativo

I servizi di *information and communication technology* per il supporto all'attività dell'Ente sono in parte gestiti autonomamente e in parte curati dal CED del Comune di Jesi, in virtù di un'apposita convenzione.

L'Ente provvede in autonomia all'acquisizione di dispositivi tecnologici (PC, stampanti, altro hardware) e dei software applicativi in uso specifico nell'Ente. Il Comune di Jesi mette a disposizione l'infrastruttura e i servizi di rete, nonché alcuni software utilizzati sia dall'ASP sia dal Comune.

Il CED del Comune di Jesi sovrintende al rispetto degli standard per la sicurezza nell'uso delle tecnologie.

11.2. Il sistema di gestione documentale

Nell'ambito della gestione documentale, l'Ente ha acquisito il software denominato Jlrìde, sviluppato dall'azienda Maggioli S.p.A.: il database e l'application server sono ospitati e gestiti dal CED del Comune di Jesi, come installazione parallela a quella di gestione documentale del Comune stesso.

La conduzione operativa del sistema è curata dal CED del Comune di Jesi, a cui sono demandati gli oneri di gestione e monitoraggio di tutte le componenti fisiche e logiche infrastrutturali, e dell'integrità delle basi di dati in conformità a quanto previsto dalla normativa vigente in materia di sicurezza e di protezione dei dati e di continuità operativa.

L'Ente ha in carico gli oneri per l'installazione iniziale e la manutenzione software ordinaria e straordinaria (compresi gli aggiornamenti periodici dell'applicativo sia per correzione di errori, sia per aggiornamenti normativi o tecnologici).

11.3. Accesso

11.3.1. Accesso da parte degli utenti interni all'Amministrazione

Il livello di autorizzazione all'utilizzo delle funzioni del sistema di gestione informatica dei documenti, distinte tra funzioni orientate alla consultazione dei dati e funzioni orientate all'inserimento e alla modifica delle informazioni, è attribuito dal Responsabile del gestione documentale per la tenuta del protocollo informatico di concerto con il responsabile del Servizio Informatica (art. 61, comma 3, DPR n. 445/2000).

Jlrìde è un'applicazione web il cui accesso è subordinato a un processo di autenticazione informatica con utente e password collegato all'autenticazione nel dominio Windows in Active Directory, in cui le password hanno una scadenza trimestrale e una complessità di livello medio/elevato.

L'accesso al sistema di gestione documentale da parte di soggetti esterni all'Ente non è consentito.

11.3.2. Gestione della riservatezza

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è associata una Access Control List (ACL) che consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso. Per default il sistema segue la logica dell'organizzazione, degli utenti, dei loro ruoli e delle abilitazioni all'utilizzo delle funzioni disponibili, nel senso che ciascun utente può svolgere solo le operazioni a cui è abilitato e accedere ai documenti che gli sono stati assegnati in modo diretto o indiretto (alla struttura di appartenenza e al suo ruolo, o agli uffici ad esso subordinati).

I documenti protetti da un'ACL non vengono mai visualizzati agli utenti non autorizzati, neanche a fronte di una ricerca globale nell'archivio o una ricerca full text. Il sistema filtra l'accesso non soltanto al contenuto del documento ma anche ai dati della registrazione.

Al fine di tutelare la riservatezza dei documenti, ai sensi del D. Lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", i certificati e gli atti trasmessi ad altre pubbliche amministrazioni contengono soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite (art. 16, comma 1, DPR n. 445/2000).

Nello svolgimento dei compiti è fatto divieto agli operatori di comunicare e/o di divulgare qualsivoglia dato sensibile e/o personale. Tale obbligo di riservatezza è esteso anche al periodo successivo alla scadenza dell'incarico, fino a quando le suddette informazioni non vengano divulgate a opera del Responsabile dell'Ente, oppure divengano di dominio pubblico.

Periodicamente, e comunque almeno annualmente, è verificata a cura del Responsabile della gestione documentale la sussistenza delle condizioni per il mantenimento dei profili di accesso.

11.4. Sicurezza fisica dei documenti

L'accesso in lettura e scrittura alle directory utilizzate come deposito dei documenti è effettuato solo dal processo server dell'applicativo di protocollo informatico, mai dalle stazioni di lavoro.

L'accesso a tali directory è permesso solo ad utenti amministratori.

Il Responsabile del Servizio informatico garantisce la puntuale esecuzione delle operazioni di backup dei dati e dei documenti da parte di personale appositamente autorizzato.

Ogni operazione di manutenzione o backup effettuata sul sistema è registrata su un file di log periodicamente controllato e archiviato.

Le copie di backup dei dati e dei documenti sono conservate, a cura del Responsabile del Servizio informatico, in locali sicuri e differenti.

11.5. Sicurezza fisica del data center

I sistemi server e gli apparati di rete sono ospitati in ambienti che presentano i seguenti livelli minimi di sicurezza fisica:

- locali dedicati esclusivamente a ospitare gli apparati server e i dispositivi di rete;
- sistema elettronico, di controllo e tracciatura degli accessi;
- sistema automatico di estinzione degli incendi;
- alimentazione elettrica protetta da dispositivi di stabilizzazione e continuità della tensione (UPS);
- impianto di climatizzazione automatico ridondato e opportunamente dimensionato in grado di mantenere una temperatura ambientale non superiore ai 25°.

I locali non devono

- essere soggetti ad allagamenti e devono disporre delle eventuali protezioni specifiche necessarie;

- ospitare apparecchiature pericolose o che aumentino il rischio di allagamenti, incendi o inagibilità dei locali stessi;
- essere utilizzati per stivare materiali infiammabili o essere utilizzati come deposito di materiale e attrezzature.

All'ingresso dell'edificio, a piano terra, è collocata la sede della Polizia Locale che effettua un presidio di controllo degli accessi.

Eventuali interventi di qualsiasi natura (anche non informatica) nei locali ospitanti gli apparati server e apparati di rete devono sempre avvenire in presenza di personale autorizzato.

11.6. Rete dati

L'utilizzo del sistema di gestione documentale è garantito dalla rete dati dell'Ente, collegata alla rete del Comune di Jesi. L'Ente è responsabile dei dispositivi collegati alla rete dell'Ente e utilizzati per l'accesso al sistema di gestione documentale e deve riferirsi all'amministratore della rete del Comune di Jesi per ogni violazione o sospetto di violazione della sicurezza informatica. Inoltre, opera secondo le direttive e le procedure stabilite dall'amministratore della rete, nel rispetto delle norme previste dall'Ente, garantendone altresì il rispetto, per quanto di propria competenza, da parte dell'utenza gestita e adottando tempestivamente i provvedimenti previsti.

11.7. Le postazioni di lavoro

La gestione e la manutenzione delle postazioni di lavoro per l'utilizzo del sistema di gestione documentale sono curate dal servizio di helpdesk del CED del Comune di Jesi.

L'Ente verifica il coerente utilizzo delle postazioni di lavoro, da tavolo o portatili, o gli strumenti comunque funzionalmente assimilabili e predispone la necessaria dotazione di dispositivi (*hardware*) e programmi (*software*) tali da consentire il corretto funzionamento e il mantenimento in condizioni di sicurezza ai fini del regolare svolgimento dell'attività lavorativa. Parte dei software (in particolare quelli necessari per la sicurezza come gli antivirus) sono gestiti e mantenuti dal servizio di helpdesk del CED.

Le postazioni di lavoro soddisfano i criteri minimi di sicurezza, in particolare:

- il sistema operativo è aggiornato e aggiornabile;
- gli applicativi installati e i loro componenti software aggiuntivi (ad es., *plug-in*) sono aggiornati e aggiornabili;
- sono dotate di un programma antivirus con funzionalità automatica di aggiornamento periodico;
- l'accesso al sistema operativo della postazione di lavoro è protetto da *password* di adeguata complessità, cambiata con cadenza regolare;
- salvo motivate e documentate eccezioni, sulle postazioni di lavoro non è permessa la connessione remota dall'esterno della Rete Dati dell'Ente (*RDP, SSH, VNC, ecc.*);
- la connessione da remoto alle postazioni di lavoro dall'interno della Rete Dati dell'Ente, ove attivata, viene effettuata esclusivamente mediante protocolli di comunicazione sicuri ed è consentita solo previo consenso dell'utente che in quel momento sta utilizzando l'elaboratore.

11.8. Le procedure comportamentali ai fini della protezione dei documenti

Le postazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà dall'Ente a vario titolo messi a disposizione del personale, sono uno strumento di lavoro

e il loro utilizzo è finalizzato allo svolgimento delle attività professionali e istituzionali dell'Ente. Ogni utente adotta comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza dei sistemi informativi.

In ogni caso, l'utilizzo delle risorse informatiche dell'Ente non deve pregiudicare il corretto adempimento della prestazione lavorativa, ostacolare le attività dell'Ente o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici.

Gli utenti a cui sono affidate le postazioni di lavoro dell'Ente, sono soggetti a tutte le responsabilità dettate dalla normativa vigente e applicabile. Si sottolineano le seguenti responsabilità:

- l'utente è responsabile per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui ha accesso; qualora sulle postazioni di lavoro siano memorizzati dati sensibili o giudiziari, il responsabile della postazione stessa deve attuare ulteriori misure di tutela di tali informazioni da accessi non autorizzati;
- l'utente è tenuto a segnalare immediatamente ai referenti informatici ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
- in caso di cessazione del rapporto di lavoro, l'utente deve restituire all'Ente qualsiasi risorsa informatica assegnata e mettere a disposizione ogni informazione di interesse istituzionale;
- Sulle postazioni di lavoro non è ammesso:
 - installare software tutelati ai sensi della convenzione sulla protezione delle opere letterarie e artistiche, nonché le banche dati che, per la scelta o per la disposizione del materiale, costituiscono una creazione intellettuale dell'autore, se non in possesso delle relative licenze d'uso;
 - installare modem per l'accesso da o verso l'esterno della rete dell'Ente, se non preventivamente autorizzati;
 - utilizzare dispositivi mobili quali punti di accesso da/all'esterno la rete dell'Ente, se non preventivamente autorizzati;
 - installare programmi non inerenti all'attività lavorativa e/o privi di licenze d'uso;
 - copiare dati la cui titolarità è dell'ASP Ambito 9 su dispositivi esterni personali.

Per adempiere al proprio dovere di diligenza e vigilanza nell'utilizzo dei beni e strumenti assegnati, il dipendente ha l'obbligo di impedire ad altri utilizzi indebiti della propria apparecchiatura informatica.

L'utente è tenuto a bloccare o a spegnere il *personal computer* in caso di sospensione o di termine dell'attività lavorativa, assicurandosi di evitarne l'utilizzo improprio da parte di terzi, mediante inserimento di apposite credenziali di accesso. Le stazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, messe a disposizione del personale, non devono essere lasciati incustoditi. Al termine dell'orario di servizio, i *computer* devono essere spenti prima di lasciare gli uffici. In caso di allontanamento temporaneo, l'utente deve attivare il salvaschermo con sblocco tramite *password*.

In linea generale è fortemente raccomandato di evitare la memorizzazione di dati sensibili o giudiziari su dispositivi mobili (palmari, *notebook*, *smartphone*, *penne USB*, dischi rigidi esterni, *memory card*, ecc.). Quando, per giustificati motivi, ciò si rendesse necessario, è necessario adottare idonee misure di protezione dei dati, come la crittografia o un controllo degli accessi.

Le credenziali di accesso (generalmente, *nome utente* e *password*) sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime.