AZIENDA DI SERVIZI ALLA PERSONA
Istituzioni Assistenziali Riunite di Pavia

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO

SOMMARIO

CAPITOLO 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 2013[1].

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 es., utilizzando formati idonei per la formazione delle istanze, ecc.)

1.2. Modalità di redazione

La redazione del manuale di gestione deve contemperare 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 delle procedure amministrative. In ASP le procedure e i processi più rilevanti sono state descritti nel provvedimento, descritto nell'allegato 1.

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 responsabili (UOR) delle aree organizzative omogenee (AOO, di cui al § 2.1) di ASP, al fine di consentire la corretta diffusione delle nozioni e delle procedure documentali.

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

---

[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.

CAPITOLO 2. QUADRO ORGANIZZATIVO ISTITUZIONALE

2.1. Area organizzativa omogenea e unità organizzativa responsabile

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 responsabile (UOR) 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.

ASP è organizzata nelle AOO e UOR descritte nell'allegato 3.

Le AOO e le UOR sono descritte, 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.

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

Presso l'AOO *Amministrazione Centrale* è istituito l'Archivio Generale di ASP con funzioni di servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, come previsto dal DPR 445/2000, art. 61.

All'Archivio Generale di ASP è attribuita la competenza di tenuta del sistema di gestione analogica e informatica dei documenti, dei flussi documentali e degli archivi, nonché il coordinamento degli adempimenti previsti dalla normativa vigente. Il responsabile dell'Archivio Generale è il Coordinatore della gestione documentale è , ai sensi del DPCM 3 dicembre 2013, art. 3.

Con DDG sono stati individuati il Coordinatore e i Responsabili della gestione documentale e i rispettivi vicari, come previsto dal DPCM 3 dicembre 2013, art. 3, lett. b) e c) e come descritto nell'allegato 4.

L'Archivio Generale di ASP 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 di ASP.

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 dal Responsabile AOO/UOR. In tal caso il Responsabile di AOO/UOR invierà richiesta al Coordinatore della gestione documentale scrivendo un messaggio all'indirizzo mail istituzionale dell'Archivio Generale;
- la correttezza delle operazioni di registrazione, segnatura, gestione dei documenti e dei flussi documentali;

- notifica ai Responsabili della gestione documentale di ciascuna AOO l'eventuale indisponibilità del sistema e dà loro disposizioni per l'attivazione del registro di emergenza secondo quanto disposto al § 6.9;
- le autorizzazioni di annullamento delle registrazioni di protocollo per l'AOO Amministrazione Centrale;
- l'adeguamento del sistema di gestione documentale alle eventuali modifiche dell'organigramma e funzionigramma di ASP.

2.3. Coordinatore della gestione documentale/Responsabile della gestione documentale

È compito del Coordinatore della gestione documentale e dei Responsabili della gestione documentale per le rispettive AOO di competenza:

- definire e assicurare criteri uniformi di trattamento dei documenti e di classificazione e archiviazione, nonché di comunicazione interna tra le AOO;
- 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 12;
- 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 Coordinatore della gestione documentale è coadiuvato dal referente dei sistemi informatici documentali 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 Coordinatore della gestione documentale riceve dai responsabili delle UO richiesta scritta (tramite e-mail) di abilitazione per ciascun utente, concordando, caso per caso, le tipologie di abilitazione. Il profilo di ogni utente è generato mediante la personalizzazione di modelli predefiniti che si elencano di seguito:

- Responsabile di AOO;
- Responsabile di UO;
- Responsabile della gestione documentale;
- Operatore Archivio Generale;
- Operatore di AOO;

- Direttore Generale; Legale Rappresentante

2.5. Posta elettronica istituzionale

Ogni AOO e ciascuna UO sono dotate della casella istituzionale di posta elettronica. La casella viene denominata in modo da rendere facilmente individuabile l'AOO/UO di riferimento.

Tutte le UO una casella di posta elettronica istituzionale.

L'utilizzo delle casella istituzionale di posta elettronica è regolamentato da linee guida descritte nell'allegato 5.

2.6. PEC istituzionale

ASP ha attivato la casella di PEC per il registro di protocollo, le caselle di posta elettronica certificata per la gestione della fatturazione elettronica e per le esigenze specifiche dei Dirigenti responsabili.

L'utilizzo delle PEC di ASP è regolato da linee guida cui all'allegato 6 il quale riporta elenco di tali caselle e loro modalità di utilizzo.

2.7. Piano di eliminazione dei registri di protocollo diversi dal protocollo informatico

Il registro di protocollo è unico per tutta ASP.

A far data dal 31 marzo 2014 sono cessati di fatto e di diritto tutti gli eventuali 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/Coordinatore della gestione documentale.

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 Coordinatore della gestione documentale nel caso in cui non sia la stessa persona.

Con DDG è stato nominato il Responsabile della conservazione, il quale coincide con il Coordinatore della gestione documentale.

CAPITOLO 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 rinunzia 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

ASP 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 i seguenti formati standard:

- Testo = Docx; Ods; Pdf/a;
- Calcolo= Xlsx; Odt;
- Immagini = Jpg, Tiff;

- Suoni = Mp3;
- Video = Avi:
- Eseguibili = Exe;
- XML;
- Archiviazione e compressione = Zip;

- Formati e-mail = RFC 2822/MIME.

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, segnatura, 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 per ciascuna Area organizzativa omogena (AOO), nei repertori, negli albi, contenuti nel sistema di gestione documentale.

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

- AOO/ UO;
- Data di sottoscrizione;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (indicare 0 *zero* se non presenti);
- Oggetto;
- Destinatario;
- Testo;
- Iniziali di redattore/responsabile;
- 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 es., 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 di ASP, 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'ASP e l'indicazione di

- AOO/ UO;
- Data;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (indicare 0 *zero* se non presenti);
- Oggetto;
- Destinatario;
- Testo;
- Sottoscrizione;
- Sigla eventuali istruttori;
- 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 di ASP 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 registratura. Trattandosi di un documento informatico nativo non si procederà alla stampa e apposizione tramite timbro della segnatura prima della registratura a protocollo.

3.8. Distinzione dei documenti in base allo stato di trasmissione (arrivo, partenza, scambiati tra UOR, 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 UOR);

N.B. I documenti scambiati tra AOO di ASP sono documento in arrivo e in partenza.

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 Responsabili (UOR) afferenti alla stessa Area Organizzativa Omogenea (AOO). 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.

Per documenti scambiati tra AOO dello stesso Ente si intendono documenti di preminente carattere giuridico probatorio sottoposti alla protocollazione in partenza per la AOO mittente, e alla protocollazione in arrivo per la AOO ricevente.

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale – PEC – accessibile all'Unità Organizzativa responsabile della 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.

3.10. Copia del documento informatico e analogico: nozione

La copia 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 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 es., 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'uso[2]. 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'ASP;
- corrispondente (mittente/destinatari);
- oggetto;
- numero degli allegati e descrizione degli stessi;
- numero di protocollo;
- data di registrazione a protocollo;
- indicazione dell'Unità organizzativa responsabile (UOR);
- 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».

CAPITOLO 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 titolario (o piano di classificazione), salvo alcune eccezioni, come il fascicolo di persona (e le rispettive tipologie, di personale, di ospite ricoverato, 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 registrati[3].

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.

[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».

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

4.2. Il fascicolo analogico: formazione, implementazione e gestione

Per ogni procedimento, affare e attività, l'ASP 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 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 con cadenza annuale;
- l'oggetto del fascicolo, cioè una stringa di testo per descrivere compiutamente un affare, una pratica, un dossier, una carpetta, una *pupèla*, 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: 2009 - 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. 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'ufficio[5].

In ogni caso, i responsabili di UOR 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 presentare al § 11.2.

[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.".

4.3. Il fascicolo informatico: formazione, implementazione e gestione

Per ogni procedimento, affare e attività, l'ASP 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 tipo[6] 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;
- 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 *Folium* ed è visualizzabile con possibilità di intervento da parte degli utenti abilitati a operare sui documenti della UOR 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 UOR e del RPA concorrono all'identificazione del fascicolo e alla individuazione del responsabile. La UOR 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.

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

I fascicoli informatici saranno trasferiti in conservazione, mediante pacchetto di versamento, a cura del Coordinatore/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 *Folium*. 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;
- UOR 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;
- UOR 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 ogni AOO, ha cadenza annuale ed è generato e gestito in forma automatica dal sistema di gestione informatica dei documenti.

4.8. Raccoglitore

Il raccoglitore non è un fascicolo, ma un contenitore che raggruppa documenti relativi a uno stesso argomento e afferenti a procedimenti diversi e quindi a fascicoli diversi, privi di una classificazione e una numerazione propria.

In buona sostanza, si tratta di un *dossier* a uso e consumo del responsabile del procedimento amministrativo per propria memoria e autodocumentazione, di norma, non destinato alla conservazione.

CAPITOLO 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 documentale[7].

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 UOR 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 UOR che hanno la titolarità dei documenti, attraverso il sistema di gestione documentale. Durante la fase di deposito all'Archivio Generale di ASP passa la gestione dei fascicoli, ma non la responsabilità. Nel caso di documenti cartacei, per la movimentazione dei fascicoli, viene effettuata una richiesta di accesso da parte della UOR.

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 documenti[8]; 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 nel § 4.2 e successivamente conservati all'interno di appositi faldoni o cartelle nell'archivio corrente situato presso gli uffici di ciascuna UOR. 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).

[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.

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 struttura (AOO/UOR) per la parte di propria responsabilità e competenza nel trattamento dell'affare, fino al momento del loro trasferimento nell'archivio di deposito. Il trasferimento è effettuato a cura del Coordinatore/Responsabile della gestione documentale o dal suo vicario secondo le modalità illustrate nel presente Manuale al § 11.2.

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 responsabile 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'ASP 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[8].

[8] Si veda anche il § 6 del presente Manuale.

5.3.2. Titolario (piano di classificazione)

Il titolario 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 titolario 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 titolario può essere corredato da un'appendice denominata *voci di indice*. Si tratta di un ulteriore strumento, strettamente correlato al titolario, che agevola le operazioni di classificazione. In esso sono presenti le possibili varianti lessicali, trattate e riportate in modo analitico, che possono essere incontrate nel contenuto del documento. Il titolario e, di conseguenza, il prontuario delle voci d'indice sono inseriti nel sistema di gestione documentale. Possono essere soggetti 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 Lombardia.

Il titolario unico, è descritto nell'allegato n. 7.

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. Essi sono soggetti a registrazione particolare, cioè con l'assegnazione di una numerazione continua e progressiva per anno. Sono un esempio la registrazione di decreti, contratti e convenzioni, deliberazioni, etc.[9].

[9] Si veda anche il § 7.1 del presente Manuale.

5.3.5. Massimario di selezione

Il massimario di selezione 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 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 e/o previa autorizzazione della Soprintendenza archivistica, ai sensi del D.Lgs. 22 gennaio 2004, n. 42, art. 21.

Il massimario 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 consente la selezione che ha come conseguenze o la conservazione o la distruzione.

Del massimario 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 della Lombardia 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'ASP 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 Coordinatore/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 UOR 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 e da questi al Coordinatore della gestione documentale, producendo un apposito elenco dei fascicoli soggetto di spostamento.

Inoltre, l'Archivio Generale di ASP 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 territorio[10].

[10] 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».

CAPITOLO 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'ASP.

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'ASP, ossia i cui destinatari sono esterni all'ente, e 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 24 ore lavorative dal ricevimento o, se intercorrono dei giorni festivi o di chiusura programmata dell'ASP, nel primo giorno lavorativo utile. Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immodificabile.

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

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

6.1.1. Elementi obbligatori immodificabili (Registratura)

Gli elementi obbligatori immodificabili 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;
- 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 organizzativa responsabile del procedimento/affare/attività (UOR);
- responsabile del procedimento amministrativo (RPA);
- 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;
- durata della conservazione;
- 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 di protocollo;
- anno solare di riferimento del registro di protocollo.

Oltre alle informazioni minime la segnatura deve prevedere:

- classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento;
- codice identificativo dell'ufficio a cui il documento è assegnato;

- ogni altra informazione utile o necessaria, già disponibile al momento della registrazione.

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

La firma digitale, infatti, produce un file, definito "busta crittografica", che racchiude al suo interno il documento originale, l'evidenza informatica della firma e la chiave per la verifica della stessa, che, a sua volta, è contenuta nel certificato emesso a nome del sottoscrittore.

Nel caso in cui si debba riportare sul documento annotazioni successive alla sottoscrizione (quali i dati della segnatura di protocollo), il documento dovrà essere predisposto per contenere dei campi testo ove sia possibile inserire delle informazioni successivamente alla firma senza invalidare la stessa in coerenza con quanto previsto dalle regole tecniche di cui al DPCM del 22 febbraio 2013.

6.3.2. Per il documento analogico

Le informazioni da associare al documento analogico, tramite timbro o altro sistema di identificazione del documento come stampa della segnatura, 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;
- la sigla della UOR/RPA o delle UOR/RPA a cui il documento è assegnato per competenza e responsabilità;
- le eventuali sigle della UOR/RPA o delle UOR/RPA in copia conoscenza.

Non si usa la conferenza di servizi.

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

6.3.3. Ragioni della scelta di un timbro meccanico

La segnatura su un documento cartaceo si appone mediante un timbro meccanico a inchiostro verde indelebile che riporta gli elementi normalizzati della registratura, trascritti dall'operatore di protocollo a penna blu all'interno degli spazi predisposti.

Vanno evitati dispositivi di segnatura meccanizzati (esempio etichettatrici, *printpen*, *barcode* e simili) per la scarsa maneggevolezza e per la frequente necessità di integrare la segnatura con trascrizioni e aggiunte, che possono essere soltanto manuali.

Più in dettaglio, l'etichetta adesiva ha una colla la cui composizione chimica (acida o basica) provoca il danneggiamento irreversibile del supporto cartaceo, con la perdita delle

informazioni. Col tempo, infatti, avviene il distacco dell'etichetta dal documento o un danneggiamento del documento (solitamente un foro).

La *printpen*, invece, obbliga l'operatore a intervenire per integrare gli scarni dati visto che questo strumento consente la contestuale segnatura della registrazione di norma solo per il codice struttura, data e numero di protocollo. Le informazioni di natura gestionale, titolo, classe, anno e numero del fascicolo, nonché le indicazioni di UOR, RPA e CC, non sono immediatamente consultabili in quanto non vengono riportate nella segnatura. Inoltre è poco immediata anche la lettura della data e del numero di protocollo. Nel caso del protocollo in arrivo differito la *printpen* non evidenzia le due date, cioè quella della registratura e quella del differimento, bensì solo la prima. I successivi interventi sul cambio di UOR e/o aggiunte di altre UOR, persone fisiche o organi, in copia conoscenza non si evincono mai dai dati stampati con la *printpen*. L'utilizzo di *barcode*, oltre agli inconvenienti già elencati, non è di immediata intelligibilità, e necessita sempre di un dispositivo di lettura.

L'uso di un timbro meccanico, pertanto, consente di raccogliere in forma sintetica gli estremi utili e necessari alla gestione del documento, anche grazie a una chiara e immediata lettura delle informazioni relative al documento.

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 inoltre su un file di log corredato da codici di controllo in grado di evidenziare eventuali tentativi di manipolazione. Da esso l'amministratore del sistema è in grado di 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;
- postazione di lavoro;
- tipo di operazione (inserimento/modifica/visualizzazione/cancellazione); valore dei campi soggetti a modifica.

Al fine di garantire l'immodificabilità delle registrazioni, il registro informatico di protocollo giornaliero viene trasmesso in conservazione entro la giornata lavorativa successiva.

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 provvedimento motivato 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.

Per i documenti ricevuti dall'Archivio Generale di ASP il differimento opera su iniziativa del Coordinatore della gestione documentale, o da suo delegato, che ne cura la registrazione differita corredata della motivazione.

Per i documenti ricevuti direttamente dalla UOR competente la registrazione differita avviene, per ogni AOO, su richiesta motivata della stessa UOR al Responsabile della gestione documentale o suo delegato, in cui è indicata anche la data di effettivo ricevimento.

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. 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 e descrizione degli allegati se presenti;
- l'operatore di protocollo che ha effettuato la registrazione.

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

6.6.2. 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 in formato pdf o pdf/a e inviata via *e-mail* al mittente.

6.7. Documenti esclusi dalla registrazione di protocollo

Sono esclusi per legge dalla registrazione di protocollo[11]:

- le gazzette ufficiali;
- i bollettini ufficiali P.A.;
- i notiziari P.A.;
- le note di ricezione delle circolari;

[11] DPR 28 dicembre 2000, n. 445, art. 53 comma 5.

- 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;
- Certificati Medici;
- Richieste ferie dipendenti;
- Richieste permessi retribuiti previsti dal CCN di Comparto.

Sono parimenti esclusi dalla registrazione di protocollo:

- i certificati medici dei dipendenti. Se pervenuti via PEC, essi sono registrati ma non protocollati.

Sono esclusi su disposizione dell'ASP:

- le richieste di ferie;
- le richieste di permessi retribuiti;
- le comunicazioni da parte di enti diversi di bandi di concorso (fatta eccezione dei bandi di mobilità di altri enti universitari o di bandi di consorzi interuniversitari che vengono pubblicati all'albo on line);
- i DURC.

6.8. 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, immodificabile e integra.

Attualmente, in base allo stato dell'arte delle tecnologie e dei formati, è utilizzato il formato XML, a mente del DPCM 3 dicembre 2013, allegato 2.

Gli elementi memorizzati del registro giornaliero sono i seguenti:

- Identificativo univoco e persistente, espresso in Codice IPA, AOO, anno, mese e giorno (8 cifre) (ad es., ipotizzando la denominazione del file inerente al registro giornaliero del 2 gennaio 2016, la stringa è la seguente: USInsUSInsAOO-00x-codice AOO-20160102.xml);
- Data di chiusura (data di creazione del registro);
- Impronta del documento informatico;
- Responsabile della gestione documentale (Nome, Cognome);
- Oggetto (descrizione della tipologia di registro; ad es., "Registro giornaliero di protocollo");
- Codice identificativo del registro:
- Numero progressivo del registro;
- Numero della prima registrazione effettuata sul registro;

- Numero dell'ultima registrazione effettuata sul registro;

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

6.9. Il registro di emergenza

Il registro di emergenza no né attivo presso ASP, ma nel caso fosse necessario, è opportuno attenersi a quanto segue.

Il Coordinatore della gestione documentale attiva il registro di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica, dandone immediata comunicazione.

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 Coordinatore 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.

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'area organizzativa omogenea.

Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema.

Durante la fase di ripristino, 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.

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.

Soluzioni analoghe sono adottate dal Responsabile della gestione documentale di ciascuna AOO, previa intesa, con il Coordinatore della gestione documentale. Al termine dell'emergenza, il Responsabile della gestione documentale, chiude il registro e dà contestuale comunicazione della revoca dell'emergenza.

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

CAPITOLO 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. Ogni repertorio è collegato a uno specifico registro di protocollo attivo per ogni area organizzativa omogenea dell'ASP.

7.2. Repertori attivi

L'elenco dei repertori attivi presso l'AOO Amministrazione Centrale di ASP è descritto nell'allegato 8.

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 titolario.

Nell'ASP è prodotto un repertorio dei fascicoli per ogni AOO collegato al rispettivo registro di protocollo.

CAPITOLO 8. FLUSSO DI LAVORAZIONE DEI DOCUMENTI

8.1. Flusso del documento informatico in arrivo

L'Archivio Generale di ASP registra in modo avalutativo i documenti che rivestono un valore giuridico-probatorio.

La documentazione da protocollare viene registrata, classificata e smistata alla UOR competente. Il Responsabile della UOR, a sua volta, assegna al documento (e di conseguenza al procedimento amministrativo cui si riferisce) il RPA. L'informativa della registrazione è resa immediatamente disponibile in due modalità:

- attraverso un messaggio *e-mail* che il sistema di gestione documentale invia automaticamente alla casella di posta elettronica indicata dal Responsabile della UOR;
- attraverso l'accumulo nella vaschetta del menu principale del sistema di gestione documentale.

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

- tramite posta elettronica convenzionale (e-mail);
- tramite posta elettronica certificata (PEC);

- su supporto rimovibile (Cd ROM, DVD, ecc.) con consegna diretta o trasmesso a mezzo servizio postale o corriere; □ da altre banche dati.

8.2. 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'Archivio Generale di ASP;
- documento allegato alla e-mail istituzionale: con *PDF creator*[12] si crea il PDF/a e lo si associa al sistema di gestione documentale procedendo alla registratura in arrivo con le consuete modalità. Sarà cura del RPA della UOR competente verificarne la provenienza e valutare se accettare o meno la firma elettronica leggera;
- documento costituito dal corpo della mail: con *PDF creator* si crea il PDF/a e lo si associa al sistema di gestione documentale procedendo alla registratura in arrivo con le consuete modalità. Sarà cura del RPA della UOR competente verificarne la provenienza e valutare se accettare o meno la firma elettronica leggera. I documenti informatici così pervenuti saranno protocollati a cura dell' Archivio Generale di ASP, di norma, entro le 24 ore lavorative dal giorno di arrivo;
- documento che arriva alla casella di posta elettronica istituzionale di una UOR diversa dall'Archivio Generale di ASP. La UOR ricevente gira l'*e-mail* con *forward* corredata degli eventuali allegati alla casella di posta elettronica istituzionale dell'Archivio Generale di ASP che converte il file in pdf/a, registra nel protocollo informatico e associa il file con estensione pdf/a, alla registrazione;
- il mittente è l'autore della *e-mail* e non la UOR che ha inoltrato il file all'Archivio Generale di ASP. 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);
- il documento via *e-mail* può non essere firmato e allora lo si dichiara nel campo immodificabile. Se è firmato digitalmente non serve alcuna descrizione. È in capo al RPA 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. I documenti informatici così pervenuti saranno protocollati a cura dell'Archivio Generale di ASP entro le 24 ore dal giorno di arrivo;

Analogamente 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 alla casella istituzionale dell'Archivio Generale di ASP.

[12] *Pdf creator* è un programma gratuito open source che consente di creare file in formato pdf utilizzando qualsiasi programma che abbia la funzione "Stampa".

8.3. 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 in ASP 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. Si identifica 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.

Per altri esempi si veda il Capitolo 9 - Casistica e comportamenti.

Se il documento informatico è privo di firma va evidenziato in un campo immodificabile con la dicitura *firma mancante*.

La verifica della validità della firma digitale è a cura del RPA 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 il documento al mittente.

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

I documenti informatici così pervenuti sono protocollati, di norma, entro le 24 ore lavorative successive dal giorno di arrivo.

8.4.1. Documenti informatici prodotti da banche dati dell'ASP o prodotti da banche dati di terzi

I documenti inseriti e convalidati da banche dati dell'ASP o prodotti da banche dati di terzi che arrivano nel sistema di gestione documentale possono essere trattati in due modi:

- essere gestiti in automatico dal sistema che li protocolla, attribuisce loro la classificazione, li inserisce nel fascicolo di pertinenza, li assegna alla UOR e al RPA di competenza;
- essere gestiti come bozze[13].

Ad esempio, ordini e fatture attive in formato Fattura PA destinati a pubbliche amministrazioni generati sul sistema di contabilità ONDA e trasferiti automaticamente al sistema di gestione documentale sono gestiti come bozze.

[13] In analogia a quanto avviene per i documenti ricevuti tramite PEC.

Prima di attivare una procedura automatica, il Coordinatore della gestione documentale, in collaborazione con il RPA e con il Responsabile dei sistemi informativi, dovrà stabilire le modalità del flusso e le condizioni per la protocollazione automatica che devono comprendere la valutazione della possibilità o meno di trattare adeguatamente dati sensibili.

Se il documento informatico pervenuto contiene dati sensibili, sarà registrato nella modalità di "riservato".

8.5. Priorità nella registrazione dei documenti informatici in arrivo

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

- atti giudiziari notificati;
- documenti del Ministero;
- documenti provenienti da Regione Lombardia
- Documenti provenienti da ATS o Enti di Vigilanza e Controllo preposti ad ASP
- documenti di rilevanza finanziario-contabile (MEF – Corte dei Conti, etc.);
- documenti ricevuti direttamente dalla segreteria del Direttore Generale;
- fatture passive pervenute al di fuori del Sistema di interscambio (es. le fatture in formato elettronico provenienti da fornitori esteri).

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

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.).

8.6. Flusso del documento analogico

La corrispondenza analogica in arrivo perviene all'Archivio Generale di ASP secondo le seguenti modalità:

- posta pervenuta per il tramite di Poste italiane spa e di altri gestori autorizzati;
- posta pervenuta direttamente alle UOR e da questa recapitata all'Archivio Generale di ASP
- posta recapita personalmente, *brevi manu*;
- posta ricevuta via telefax.

8.7. Apertura delle buste

Tutte le buste vanno aperte a cura dell'Archivio Generale di ASP. Fanno eccezione e pertanto non vanno aperte, le buste:

- 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);
- 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);

- 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'Archivio Generale di ASP.

8.7.1. 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 UOR.

Le altre buste sono conservate a parte in plichi quotidiani per 30 giorni. Trascorso tale termine sono eliminate senza formalità.

8.8. Priorità nella registrazione dei documenti analogici in arrivo

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

- atti giudiziari notificati;
- documenti del Ministero;
- documenti provenienti da Regione lombardia
- Documenti provenienti da ATS o Enti di Vigilanza e Controllo preposti ad ASP
- documenti di rilevanza finanziario-contabile (MEF – Corte dei Conti, etc.);
- documenti ricevuti direttamente dalla segreteria del Direttore Generale;
- fatture passive pervenute al di fuori del Sistema di interscambio (es. le fatture di fornitori esteri);
- documenti relativi a procedimenti ispettivi;
- documenti di trasmissione di assegni o altri valori di debito/credito;
- documenti consegnati *brevi manu*: si protocolla subito e si rilascia la ricevuta di avvenuta protocollazione.

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 24 ore lavorative successive alla ricezione.

Nel caso in cui non sia possibile l'immediata protocollazione di un documento consegnato a mano (ad es., per momentanea indisponibilità del sistema informatico), viene concordato l'invio telematico della ricevuta di protocollo all'indirizzo mail fornito da chi consegna il documento. In casi eccezionali, si rilascia la fotocopia del frontespizio del documento col timbro del protocollo.

Per la registratura dei documenti analogici rimane in uso il timbro meccanico Così pure tutti i timbri allora adottati quali:

- Protocollo differito al…….: per i documenti protocollati con motivato provvedimento che ammette il documento alla registrazione differita (ora per allora);

- Protocollo particolare n……..: per i documenti registrati nel protocollo particolare;
- Pervenuto al protocollo il ……..: per evidenziare che la data del documento è irritualmente antecedente rispetto alla data di protocollazione del documento. In questo caso non si tratta di protocollo differito, ma di un documento potenzialmente pervenuto con ritardo, fatto salvo anche l'errore materiale del mittente;
- Secondo esemplare: per evidenziare uno o più originali pervenuti in esemplare plurimo;
- Annullato il……..: per evidenziare l'annullamento di un documento.

8.9. Protocollo particolare

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

- *documenti di carattere politico e di indirizzo di competenza del Rettore o del Direttore Generale che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;*
- *documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;*
- *tipologie di documenti individuati dalla normativa vigente relativamente a dati sensibili i cd. sensibilissimi;*
- *documenti legati a vicende di persone o a fatti privati e, in particolare, i documenti riportanti dati sensibili e dati giudiziari.*

8.9.1. Procedure del protocollo particolare

Le tipologie di documenti da registrare nel protocollo particolare sono individuate dal Coordinatore della gestione documentale, in collaborazione con gli organi monocratici e d'intesa con i responsabili delle UOR.

Ogni documento reca un numero di protocollo e un numero di repertorio.

Per i documenti in arrivo analogici particolarmente voluminosi, viene fotoriprodotta la lettera accompagnatoria con l'apposizione della dicitura "I documenti integrali sono consultabili presso l'Archivio Generale di ASP".

8.10. L'archivio particolare

Il complesso dei documenti registrati col protocollo particolare costituisce l'archivio particolare, corredato da un repertorio interno al protocollo unico.

Per ragioni informative e di tenuta complessiva dell'archivio particolare, l'Archivio Generale di ASP conserva una fotocopia dei documenti analogici registrati. Per i documenti informatici non viene fatta alcuna stampa.

A protezione dei dati personali e sensibili, il documento analogico viene trasmesso direttamente al RPA in busta chiusa, sigillata e firmata sui lembi di chiusura. Al Rettore, al Direttore generale e agli altri eventuali destinatari in copia conoscenza viene inoltrata una copia del documento analogico sempre in busta chiusa, sigillata e firmata sui lembi di chiusura.

Per il documento informatico soggetto a registrazione di protocollo particolare saranno gli organi monocratici a definirne l'utilizzo in collaborazione col Coordinatore della gestione documentale.

Per le altre AOO dell'ASP, sarà il Responsabile della gestione documentale ad essere abilitato alla tenuta e gestione del protocollo particolare della AOO medesima.

8.11. Annullamento di una registrazione

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

Solo il Coordinatore 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 nel caso che dette informazioni non siano generate o assegnate automaticamente dal sistema;
- il documento registrato deve essere sostituito per rettifica del destinatario, dell'oggetto;
- la motivazione per cui il documento è stato prodotto è venuta meno purché il documento non sia già stato diffuso.

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 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 dall'Archivio Generale di ASP. La richiesta di annullamento, inviata a mezzo *e-mail* alla casella istituzionale dell'Archivio, sarà associata alla registrazione di protocollo del documento annullato a cura del Coordinatore della gestione documentale o dalle persone espressamente delegate.

In *Folium* i documenti annullati sono essere inseriti nei rispettivi fascicoli o, nel caso di documento non inerenti a specifici procedimenti, in un fascicolo annuale.

Se il documento analogico o informatico annullato costituisce una tipologia documentale soggetta a registrazione particolare (ad es., un contratto) per la quale è prevista la conservazione perenne, 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 in forma ben visibile, 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. In questo caso il mittente riceverà una notifica di annullamento del suo documento con la relativa motivazione.

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), è protocollato e 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 UOR della stessa AOO (corresponsabilità di servizi interna);
- più AOO dello stesso ente (corresponsabilità esterna di 1° livello);
- più AOO di enti diversi (corresponsabilità di servizi esterna di 2° livello).

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

La corresponsabilità di servizi esterna di 1° livello (tra più AOO dello stesso ente) e la corresponsabilità di servizi esterna di 2° livello (tra AOO di enti diversi) non sono utilizzate.

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

- Richieste di servizio di pulizie;
- Richieste di facchinaggio;
- Richieste di fornitura di cancelleria;
- Richiesta di piccole manutenzioni;
- Richiesta di sopralluoghi ai servizi tecnici;
- Richieste di sopralluoghi archivistici;
- Richiesta di fascicoli conservati nell'archivio di deposito per attività istituzionale;
- Richieste di accesso ai locali destinati all'archivio analogico;
- Trasmissione all'Archivio Generale di ASP dei repertori analogici per la conservazione illimitata.

8.14. Casi di rigetto

Per rigetto si intende la segnalazione di una UOR all'Archivio Generale di ASP 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 UOR deve riportare nella registrazione una annotazione motivando e indicando la UOR competente.

Il documento informatico ritorna così in carico all'Archivio Generale di ASP che potrà immediatamente inoltrarlo alla UOR competente.

I documenti possono comunque essere riassegnati direttamente nel caso di UOR appartenenti allo stesso Servizio.

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

In caso di conflitto di competenze tra UOR, è il Dirigente / Direttore su proposta del Coordinatore della gestione documentale, che determina lo smistamento definitivo. Sono ammessi solo due rigetti prima dell'assegnazione d'autorità.

Nessun documento, analogico e/o informatico, deve rimanere in carico all'Archivio Generale di ASP, 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) 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:

- sigillo;
- data completa (luogo, giorno, mese, anno) scritta per esteso;
- indicazione dell'indirizzo PEC o e-mail del destinatario; il nominativo del RPA;
- numero di protocollo;
- 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:

- sigillo;
- data completa (luogo, giorno, mese, anno) scritta per esteso;
- indicazione dell'indirizzo PEC o e-mail del destinatario;
- il nominativo del RPA;
- numero degli allegati;
- firma digitale.
- Il numero di protocollo può essere inserito solo nel caso si adottino particolari accorgimenti nella formazione del documento e si utilizzi il formato PAdES per la sottoscrizione 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 via *e-mail* e a mezzo PEC.

8.16. Flusso del documento informatico tra UOR della stessa AOO

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

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

8.17. Flusso del documento informatico tra AOO dell'ASP

Il flusso dei documenti informatici tra le AOO dell'ASP prevede la registrazione del protocollo in partenza per l'AOO mittente e la protocollazione in arrivo per la AOO destinataria.

L'interoperabilità è garantita mediante l'uso della PEC.

Il documento informatico perviene all'Archivio Generale di ASP nella casella "bozze o corrispondenza tra AOO" e viene redatto l'oggetto, classificato e assegnato alla UOR competente che provvederà alla fascicolatura.

8.18. Utilizzo delle firme elettroniche: firma elettronica semplice, firma elettronica avanzata, firma elettronica qualificata, firma digitale

Firma elettronica: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

Firma elettronica semplice: la cosiddetta "*firma debole*" intesa come l'insieme dei dati in forma elettronica, riconducibili all'autore (anche di tipo: *log identificativo*, *indirizzo mail*, ecc.), allegati o connessi ad atti o fatti giuridicamente rilevanti contenuti in un documento informatico, utilizzati come metodo di identificazione informatica.
Può essere utilizza per i documenti interni.

Firma elettronica avanzata: intesa come insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati. Le *annotazioni* sulle registrazioni del sistema di gestione documentale sono considerate firma elettronica avanzata e vengono utilizzate per l'attestazione di regolare esecuzione del servizio/fornitura e l'autorizzazione al pagamento delle fatture elettroniche.

Firma elettronica qualificata: una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. Ai sensi dell'art. 25, comma 3, del Regolamento del Parlamento e del Consiglio dell'Unione europea 23 luglio 2014, n. 910 corrisponde alla firma digitale italiana. Utilizzata per tutti i documenti per cui viene richiesto dalla normativa.

I contratti e le schede di Budget con l'ATS sono firmati con firma digitale in formato XAdES.

Le fatture elettroniche in formato PA (XML) destinate a pubbliche amministrazioni italiane, i contratti stipulati in forma pubblica amministrativa, i contratti stipulati mediante scrittura privata, i contratti stipulati (scambio di lettera commerciale) sulla piattaforma

Consip per il mercato elettronico della pubblica amministrazione (MePA), gli accordi tra pubbliche amministrazioni sono firmati con firma digitale in formato CAdES.

Nei casi in cui sia richiesto per norma di legge o opportuno inserire annotazioni successivamente alla sottoscrizione digitale è necessario utilizzare una firma digitale in formato PAdES).

CAPITOLO 9. CASISTICA E COMPORTAMENTI

9.1. Gestione delle gare d'appalto

9.1.1. Gare e procedure negoziate gestite in modalità analogica

Le buste sigillate riportanti le seguenti diciture: «offerta», «gara d'appalto» o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara d'appalto o a una procedura negoziata non vanno aperte e si registrano a protocollo per garantire la data certa di acquisizione.

La segnatura va apposta sulla busta. Inoltre, per le offerte consegnate nel giorno di scadenza, l'ufficio deputato alla ricezione apporrà sulla busta anche l'ora di consegna.

Se la registrazione avviene dopo l'ora fissata per la consegna o se la consegna avviene dopo la scadenza fissata dal bando di gara, a protocollo viene inserita anche una annotazione immodificabile del tipo: "documento pervenuto/consegnato alle ore hh.mm del giorno gg/mm/aaaa come risulta dall'indicazione riportata sulla busta che si digitalizza".

Nell'oggetto si riporta la descrizione della gara/offerta così come è riportata sulla busta, Gli uffici che indicono le procedure possono dare disposizione di apporre sulla busta una dicitura, ad es., "Non aprire: offerta per la procedura negoziata per la realizzazione di… - CIG: … - CUP: …".

9.1.2. Gare e procedure negoziate gestite in modalità telematica

I documenti inerenti alle gare svolte mediante portale telematico o pervenuti in modalità elettronica possono essere soggetti a registrazione di protocollo e comunque sono inseriti nel sistema di gestione documentale.

Qualora il portale non abbia possibilità di riversare i file della documentazione di gara o procedura negoziata nel sistema di gestione documentale, la UOR provvede a inserirli nelle rispettive registrazioni di protocollo o, in base alla natura del documento, come documenti non protocollati.

9.2. Gestione di concorsi e selezioni

Le domande di partecipazione a concorsi non sono di fatto protocollate.

Indipendentemente dalla modalità di arrivo in ASP (telematico o analogico), Si procede alla registrazione solo dell'elenco delle istanze di partecipazione redatto dall'Ufficio Personale.

9.3. 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).

Quando l'atto è notificato presso l'Avvocatura Distrettuale o Generale dello Stato, in quanto soggetto che assicura la difesa in giudizio dell'Amministrazione, l'Avvocatura stessa generalmente procede alla trasmissione dell'atto all'ASP, dandone informativa, quindi il mittente da indicare nella registrazione di protocollo è l'Avvocatura. In tal caso si tratta di una comunicazione, non di una notifica, il cui mittente da indicare nella registrazione di protocollo è appunto l'Avvocatura, come per tutte le comunicazioni dalla stessa provenienti.

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. Le comunicazioni che provengono dalla cancelleria dell'autorità giudiziaria arrivano tramite l'applicativo del processo civile telematico – PTC, sono conservate nella casella PEC, rilasciata dall'ordine professionale a cui è iscritto l'avvocato che ha in carico la pratica.

Si noti che nei procedimenti giuslavoristici (cause di lavoro) contestuale al ricorso introduttivo del giudizio si trova il pedissequo decreto di fissazione di udienza, in calce al ricorso stesso. In tal caso si è in presenza, contestuale di un atto di parte e di un atto prodotto dall'organo giurisdizionale.

9.4. Documenti informatici con oggetto multiplo

Nel caso di documenti in arrivo che trattano più argomenti di competenza di UOR 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 e smistato alla UOR competente sullo stesso.

Compatibilmente con la funzionalità del sistema di gestione documentale, ciascuna UOR corresponsabile potrà (dovrà) creare la propria copia informatica al fine di proseguire con la gestione e la fascicolatura. Nel caso di documento in partenza è compito della UOR responsabile verificare che il documento prodotto tratti un solo argomento, chiaramente espresso nel campo "oggetto".

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 che dovranno attendere l'emanazione di uno specifico decreto. In tal caso la fattura andrà gestita come qualsiasi documento analogico: protocollata, assegnata e fascicolata.

La fattura elettronica perviene in formato XML via PEC, agli indirizzi dichiarati dall'ente e registrati sull'indice IPA nel corrispondente servizio di fatturazione.

La fattura così pervenuta è automaticamente protocollata, assegnata alla UOR competente - che provvede alla classificazione e alla fascicolatura - e trasmessa al sistema di contabilità dove dovrà essere 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 protocollo 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 giorni previsti dalla legge decorsi i quali, in assenza di pagamento, iniziano automaticamente a decorrere gli interessi moratori (D.Lgs. 192/2012, art. 1, comma 1, lett. d).

Per inoltrare e ricevere le fatture elettroniche è stato integrato il sistema documentale con il sistema di contabilità. Nel sistema di protocollo sono utilizzati più indirizzi di posta elettronica certificata e più codici IPA specificamente destinati alla ricezione delle fatture elettroniche (Allegato 6).

La fatture elettroniche trasmesse dai fornitori alle PA (ciclo passivo), così come quelle emesse dall'ASP (ciclo attivo), sono obbligatoriamente conservate in modalità elettronica, secondo quanto espressamente disposto dalla legge[14].

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 le verifiche immediatamente disponibili on-line, si procede acquisendo l'immagine come documento non protocollato all'interno del sistema di gestione documentale.

Per i DURC richiesti, ma non immediatamente disponibili, occorre attendere la ricezione dell'avviso di disponibilità del documento che perviene a mezzo PEC. Anche questo avviso è acquisito come documento non protocollato. A questo punto è possibile consultare il sistema del DURC on-line e procedere come per i DURC immediatamente disponibili.

9.7. 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 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.

9.8. 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 sono stampati o salvati come file e inseriti nel fascicolo personale. I certificati di malattia sono una tipologia di documenti esclusa dalla registrazione di protocollo.

9.9. Documenti del portale degli acquisti della pubblica amministrazione

Gli strumenti messi a disposizione sulla piattaforma di *e-Procurement* gestito da Consip spa per conto del Ministero dell'economia e delle finanze sono:

[14] DM MEF 17 giugno 2014.

Il *Mercato Elettronico della P.A.* (MePA), ai sensi dell'art. 11 del D.P.R. 101/2002, mediante il quale le Pubbliche Amministrazioni possono acquistare beni e servizi offerti dai fornitori abilitati presenti sui diversi cataloghi del sistema, il cui importo deve essere inferiore alla soglia comunitaria.

Le *Convenzioni* contratti quadro stipulati da Consip ai sensi dell'art. 26 della Legge 488/99) nell'ambito dei quali i fornitori aggiudicatari di gare - esperite in modalità tradizionale o smaterializzata a seguito della pubblicazione di bandi - si impegnano ad accettare ordinativi di fornitura emessi dalle singole Amministrazioni che hanno effettuato l'abilitazione al sistema Acquisti in rete. Gli *Accordi quadro*, aggiudicati da Consip a più fornitori a seguito della pubblicazione di specifici Bandi, definiscono le clausole generali che, in un determinato periodo temporale, regolano i contratti da stipulare. Nell'ambito dell'Accordo quadro, le Amministrazioni che hanno effettuato l'abilitazione al sistema Acquisti in Rete, attraverso la contrattazione di "Appalti Specifici", provvedono poi a negoziare i singoli contratti, personalizzati sulla base delle proprie esigenze.

Si descrivono le procedure di acquisto d'uso più frequente:

- Affidamenti diretti MePA (Mercato Elettronico Pubblica Amministrazione)
- Adesioni Convenzioni
- Negoziazioni MePA (Mercato Elettronico Pubblica Amministrazione).

9.9.1. Affidamenti diretti sulla piattaforma MePA (OdA)

Nei casi previsti dalla normativa e dai regolamenti vigenti, si fa ricorso ad un ordine diretto, che consiste nel selezionare l'articolo di proprio interesse fra quelli presenti nel catalogo dei fornitori e di effettuare l'ordine di acquisto al fornitore che è in grado di fornire l'articolo al prezzo più conveniente per l'amministrazione.

Il processo può essere così brevemente schematizzato: il punto istruttore effettua una bozza dell'ordine attraverso la piattaforma e la invia al punto ordinante. Il punto ordinante, cioè la persona che dispone di potere di spesa e del dispositivo di firma digitale, controlla la bozza, genera attraverso la piattaforma il file pdf/a che costituisce il documento d'ordine, lo scarica localmente, lo firma digitalmente, lo registra nel sistema di protocollo e lo ricarica a sistema. La piattaforma MePA chiede il numero di protocollo come campo obbligatorio per procedere nella registrazione. Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l'emissione del corrispondente documento gestionale. Nel caso sia un documento di tipo "ordine", questo può essere trasmesso al sistema di gestione documentale dove si genera una bozza per la registratura a protocollo e la fascicolatura. Nel caso invece sia un documento di tipo "contratto" dal sistema contabile può essere richiamato il numero di protocollo assegnato all'ordine emesso sulla piattaforma MePA.

9.9.2. Adesioni – Convenzioni (OdA)

Quando l'articolo che si intende acquistare è presente in una delle convenzioni Consip attive, l'Amministrazione aderisce a tale convenzione ed effettua un ordine al fornitore che è vincitore della gara precedentemente espletata da Consip Spa.

Il processo può essere così brevemente schematizzato: il punto istruttore seleziona la convenzione, effettua una bozza dell'ordine attraverso la piattaforma e la invia al punto ordinante.

Il punto ordinante controlla la bozza, genera attraverso la piattaforma il file pdf/a che costituisce il documento d'ordine (Ordine di Acquisto OdA), lo scarica localmente, lo firma

digitalmente, lo registra nel sistema di protocollo e lo ricarica a sistema. La piattaforma MePA chiede il numero di protocollo per procedere nella registrazione. Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l'emissione del corrispondente documento gestionale. Nel caso sia un documento di tipo "ordine", questo può essere trasmesso al sistema di gestione documentale dove è generata una bozza per la registratura a protocollo e la fascicolatura. Nel caso invece sia un documento di tipo "contratto" dal sistema contabile può essere richiamato il numero di protocollo assegnato all'ordine emesso sulla piattaforma MePA.

9.9.3. Procedure negoziate (RdO) - MePA

Nei casi previsti dalla normativa e dai regolamenti vigenti, si fa ricorso ad un Richiesta di offerta (RdO), che consiste nell'espletamento di una gara telematica con gli strumenti offerti dalla piattaforma MePA. Si può fare inoltre ricorso alla Richiesta di offerta (RdO) per effettuare indagini di mercato finalizzate a una procedura di affidamento diretto.

Nell'esecuzione dell'iter che conduce alla creazione della RdO, è possibile allegare dei documenti prodotti dall'amministrazione, sia di carattere amministrativo che tecnico-economico, al fine di supportare i fornitori nella predisposizione dell'offerta. Esempi di tali documenti sono il disciplinare di gara, il capitolato tecnico, ecc.

Le buste arrivate sulla piattaforma MePA possono essere aperte solo alla scadenza della gara telematica con una seduta pubblica web.

Nel caso lo strumento dell'RdO sia utilizzato per una procedura negoziata i documenti di gara saranno salvati localmente dal punto ordinante e registrati sul sistema di gestione documentale come documenti non protocollati. Al momento della stipula del contratto con il fornitore aggiudicatario, si genera tramite la piattaforma il file pdf/a che costituisce il documento di stipula. Il punto ordinante salva il documento di stipula localmente, lo firma digitalmente lo registra nel sistema di protocollo e lo ricarica a sistema.

Nel caso lo strumento dell'RdO sia utilizzato per effettuare un'indagine di mercato ai fini di una procedura di affidamento diretto verranno salvati localmente dal punto ordinante solo i documenti relativi all'aggiudicatario.

9.10. Documenti pervenuti via PEC

Le caselle di PEC istituzionali ASP sono "chiuse" quindi possono ricevere messaggi e documenti solo da altri vettori qualificati (altre caselle di PEC). In questo caso, al fine di rendere efficace la natura giuridicoprobatoria del messaggio di PEC, si procede con la protocollazione o con la registrazione del documento come "non protocollato".

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 mondo 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.

Qualora il messaggio di posta elettronica pervenga a una casella di PEC dello stesso ente, ma diversa da quella competente, si annulla il documento in entrata e nella causale si indica l'AOO corretta e il relativo indirizzo PEC. Il mittente riceve il messaggio e ha quindi la possibilità di inoltrare il messaggio PEC alla casella corretta. Può capitare che il messaggio di notifica non possa raggiungere il mittente per problemi tecnici, quindi è bene, prima di procedere all'annullamento, salvare localmente il testo e gli allegati in modo da procedere all'invio della documentazione a mezzo *e-mail* alla UOR/AOO competente, precisando quanto avvenuto.

9.11. Gestione di due documenti diversi trasmessi via PEC

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 opportune annotazioni di richiamo tra le registrazioni.

9.12. 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 inalterato e si redige la seguente annotazione: «Considerato che nessuna [istanza /lettera di accompagnamento /altro] è pervenuta tramite questa PEC e che il documento allegato è (descrizione allegato/i), si deduce che la richiesta sia rappresentata da quanto descritto nel campo oggetto dal mittente. Si è pertanto proceduto con la protocollazione».

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

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

9.13.1. Rapporti con terzi esterni

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 associata all'Archivio Generale di ASP.

L'art. 65 comma 1 lettera c) del CAD recita: "Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica…" "…sono valide…" "… quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'art. 64, comma 2". L'insieme di queste disposizioni fornisce la possibilità di sostituire la firma

autografa su un modulo analogico con l'invio del modulo compilato da un indirizzo di posta elettronica istituzionale fornito dall'ente.

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.

9.13.2. Rapporti tra diverse AOO

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.

9.14. 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 segnatura 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 UOR indicata nella segnatura di protocollo.

Nel caso di arrivo mediante PEC o altro sistema informatico (*e-mail* semplice, ecc.) si effettua una registrazione come "Documento non protocollato", riportandovi tutti i dati già inseriti nella registrazione di protocollo del primo esemplare (oggetto, mittente, RPA, classificazione, fascicolo, etc.). Si inserisce, inoltre, la "Nota/Annotazione" in modo immodificabile del tipo "Il documento non è stato protocollato in quanto trattasi di secondo esemplare del documento già pervenuto e registrato col prot. n. 000 del gg/mm/aaaa". Nella registrazione di protocollo del primo esemplare andrà invece inserita l'annotazione "Pervenuto secondo esemplare via PEC (o altro mezzo) – vedi id. n. 000).

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.

9.16. Documenti scambiati tra UOR della stessa AOO

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

I documenti informatici prodotti a seguito della protocollazione e scansione di documenti originali cartacei trasmessi tra le UOR di ciascuna AOO sono inoltrati in formato digitale tramite il sistema di protocollo informatico senza procedere all'inoltro dell'originale analogico, che resta nella disponibilità della UOR mittente, che procederà alla sua gestione e fascicolatura.

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 UOR interessate possono essere acquisite nel sistema di protocollo come documento non protocollato.

CAPITOLO 10. ALBO ON-LINE

Si rinvia al Regolamento per l'Albo Pretorio on-line, descritto nell'allegato 9.

CAPITOLO 11. DALL'ARCHIVIO CORRENTE ALL'ARCHIVIO DI DEPOSITO

11.1. Archivio di deposito

L'archivio di deposito è la fase intermedia del processo di tenuta dei documenti prodotti dall'ASP nel corso della propria attività e si colloca temporalmente tra l'archivio corrente e l'archivio storico. Il suo carattere di transitorietà e l'introduzione dell'informatizzazione degli archivi ha condotto alla sottovalutazione di un momento gestionale che ha, prima di tutto, una dimensione logica e un'importanza funzionale rilevanti. L'archivio di deposito è il momento di decantazione dei documenti e delle informazioni relative, organizzati in fascicoli inerenti ad affari, ad attività e a procedimenti conclusi, per i quali non risulta più necessaria la trattazione corrente o verso i quali sussista solo un interesse sporadico.

Le attività che connotano questa fase d'archivio sono definite dal DPR 445/2000, artt. 67, 68 e 69, e riguardano l'obbligo della periodicità dei trasferimenti di documenti dall'archivio corrente, la conservazione ordinata delle unità archivistiche e la disponibilità dei mezzi di corredo per assicurare le funzioni di controllo e di ricerca del materiale (registri di protocollo, piani di classificazione repertori dei fascicoli, etc.)[15].

I documenti sono conservati con le modalità indicate dal Coordinatore della gestione documentale, rispettando l'organizzazione che essi avevano nell'archivio corrente.

La produzione e gestione informatica di dati e di documenti comporta una diversificazione delle procedure di gestione durante la fase di deposito determinata dalla peculiarità del supporto. Ciononostante non cambia il ruolo e la funzione concettuale svolta dall'archivio di deposito nella tenuta del sistema documentale. Si tratta, in ogni caso, di una fase di sedimentazione della documentazione, ossia di un periodo in cui i documenti esauriscono nel tempo le proprie funzioni rivelando la propria natura temporanea o permanente, a seconda del valore delle informazioni in essi contenute. I documenti nativi digitali sono caratterizzati dalla predeterminazione dei termini di conservazione. Ciò significa che la durata della vita di un documento è determinata nel momento stesso in cui il documento viene creato. Si tratta di una forma di impostazione della selezione a priori dei documenti, attività che avviene anche per i documenti analogici, ma che è messa in atto solo in un secondo momento, durante la fase di deposito.

L'archivio di deposito analogico è gestito e conservato a cura dell'Archivio Generale di ASP, che si occupa di organizzare i seguenti servizi e attività:

- Attività preliminari finalizzate alla creazione di locali d'archivio a norma:
    - Individuare, attrezzare adeguatamente e gestire i locali da destinare a deposito d'archivio (accesso limitato al solo personale qualificato, pulizia periodica etc.);
    - Individuare il responsabile del servizio.

- Attività ordinarie caratterizzanti la gestione dell'archivio di deposito:
    - Trasferimenti periodici dei documenti dagli uffici e acquisizione delle unità da parte dell'archivio di deposito: preparare annualmente il trasferimento

[15] P. Carucci, Maria Guercio, *Manuale di archivistica*, p. 217.

dei fascicoli relativi ad affari conclusi con la predisposizione di appositi elenchi di consistenza;

- Concentrazione ordinata dei documenti, mantenendo le aggregazioni (serie e fascicoli) create nella fase di formazione e procedere alla revisione degli elenchi di trasferimento: effettuare una schedatura sommaria delle unità trasferite in archivio attribuendo una numerazione univoca, continua e progressiva che determina la posizione logica e fisica delle unità nell'elenco di consistenza e nel locale d'archivio;
- Selezione della documentazione sulla base dei Massimari di selezione adottati dall'ASP;
- Campionatura di determinate tipologie documentali da non destinare integralmente alla conservazione a lungo termine;
- Scarto della documentazione;
- Riordinamento e ricostituzione delle serie originarie (rispetto del vincolo archivistico – Piano di fascicolazione – Titolario di classificazione – successione cronologica annuale, cioè le serie sono chiuse per anno); o Conservazione adeguata dei documenti: sostituzione delle unità di condizionamento laddove danneggiate o non adatte alla conservazione a medio o lungo termine, mantenimento delle condizioni ambientali ottimali etc.;
- Versamento della documentazione all'archivio storico: predisposizione degli elenchi di versamento e aggiornamento dell'elenco di consistenza;
- Servizio di ricerca documentale (recupero dei documenti/unità richieste – consultazione - creazione di copie semplici o conformi);
- Predisposizione di statistiche sia per le attività di trasferimento e versamento che di consultazione: consente un'adeguata programmazione degli spazi e ottimizzazione dei servizi;
- Elaborazione e aggiornamento del piano di conservazione degli archivi.

- Attività straordinaria - in caso di necessari interventi di recupero del pregresso:
  - Ricognizione, censimento o mappatura della documentazione presente nel locale adibito a deposito e della documentazione impropriamente conservata presso gli uffici produttori;
  - Messa in sicurezza del locale di deposito e spostamento di tutto ciò che non è documento;
  - Schedatura delle unità documentarie;

- Selezione della documentazione e redazione di:
  - Elenco di scarto, contenente la descrizione della documentazione da distruggere;
  - Elenco di versamento all'archivio storico, contenente la descrizione della documentazione da conservare senza limiti di tempo;
  - Elenco di consistenza dell'archivio di deposito, contenente la descrizione della documentazione rimasta dopo lo scarto ed il versamento in archivio storico, da conservare in archivio di deposito in attesa del suo versamento in archivio storico;

- Procedura di scarto.

11.2. Trasferimento dei fascicoli cartacei

Periodicamente e comunque almeno una volta all'anno, il RPA trasferisce, per la conservazione nell'archivio di deposito al Coordinatore della gestione documentale, i fascicoli relativi ad affari, attività e a procedimenti amministrativi conclusi e non più necessari a una trattazione corrente[16].

Per il trasferimento viene predisposto a cura del RPA 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.

Il trasferimento dei fascicoli comporta il passaggio della sola responsabilità gestionale all'Archivio Generale di ASP, mentre la titolarità amministrativa dei documenti rimane in capo alla UOR che ha creato i documenti; solo con il versamento nell'archivio storico l'Archivio Generale di ASP 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 UOR si trovassero nelle condizioni di dovere trasferire fascicoli o documenti prodotti e chiusi da molto tempo, oppure i cui RPA 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 UOR concorderanno le modalità opportune di trasferimento, caso per caso, con il Coordinatore della gestione documentale. Prima del trasferimento i RPA provvedono anche a verificare che i fascicoli risultino chiusi anche nel sistema informatico di gestione documentale.

Alla ricezione dei fascicoli il Coordinatore della gestione documentale verifica la corrispondenza dell'elenco di consistenza con il verbale di trasferimento, sottoscritto insieme all'elenco anche dal RPA 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 Coordinatore della gestione documentale e sarà informata la struttura versante con invito a provvedere entro 10 giorni alla regolarizzazione.

11.3. Trasferimento dei fascicoli informatici

Il Coordinatore 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. Per l'ASP il conservatore è soggetto esterno[17].

Qualora, per determinate tipologie di fascicoli o di documenti, si rendesse necessario predisporre l'attivazione della procedura di conservazione con tempistiche particolari, il

---

[16] DPR 445/2000, art. 67, c. 1: «Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione».

[17] In merito si veda il § 12.1.

RPA interessato deve darne tempestiva comunicazione al Coordinatore della gestione documentale, al fine di valutare congiuntamente con il Responsabile della conservazione e con il responsabile dei sistemi informativi le modalità più idonee per dare attuazione a tale esigenza.

A titolo di esempio, per tutti i documenti informatici a rilevanza fiscale occorre rispettare le tempistiche previste dal D.M 17 giugno 2014 quindi, nel caso in esame, delle fatture elettroniche attive e passive, inserite nel fascicolo della procedura di acquisto, si dovrà procedere al versamento anticipato in conservazione secondo le regole previste nel manuale di conservazione e gli specifici accordi di versamento stipulati con il soggetto esterno cui è affidato il processo di conservazione.

11.4. Trasferimento delle serie archivistiche

Le serie archivistiche (contratti, decreti, verbali, ecc.) sono trasferite all'archivio di deposito nella loro unitarietà, secondo un termine che può variare da serie a serie.

Le modalità di trasferimento sono le medesime previste per i fascicoli cartacei e informatici.

Se la serie archivistica è ibrida, cioè composta sia da documenti analogici che da documenti digitali, si procederà nel seguente modo:

- il repertorio digitale nel sistema di gestione documentale conterrà tutti i documenti informatici in formato nativo e la copia per immagine dei documenti analogici associata alla registratura;
- il repertorio analogico sarà composto dagli originali analogici dei documenti e dalla copia analogica conforme all'originale informatico dichiarata dal Responsabile del procedimento amministrativo;
- il documento originale deve essere fascicolato. Il documento è unico ma collocato sia nel repertorio che nel fascicolo. Analogamente per i documenti nativi analogici: due originali, uno a repertorio e il secondo nel fascicolo della pratica relativa o, in alternativa, copia conforme.

11.5. Ordinamento archivistico

L'ordinamento delle unità archivistiche nell'archivio di deposito avviene nel rispetto del principio di provenienza e dell'ordine originario. In particolare, per i fascicoli, l'ordine è quello stabilito dal repertorio dei fascicoli.

Il titolario di classificazione è parte integrante del presente Manuale ed è applicabile solo ai documenti prodotti/ricevuti dopo la sua adozione. Ciò significa che il piano di classificazione non ha mai efficacia retroattiva. I fascicoli prodotti in precedenza, quindi, vengono archiviati sulla base dei titolari/piani di classificazioni in vigore al momento della produzione dei documenti afferenti, specificatamente nell'anno di chiusura del fascicolo. L'ordinamento, infatti, comporta la ricostruzione delle serie originarie e si lavora per serie chiuse per anno considerando come data di riferimento la data di chiusura della pratica. Pertanto, il dato cronologico è fondamentale perché per ogni anno si ricostruiscono le serie di fascicoli sulla base della classificazione attribuita ai fascicoli e desumibile dal repertorio dei fascicoli. Se il fascicolo è pluriennale e il suo periodo di attività cade a cavallo di una modifica del titolario verrà inserito, in base alla sua classificazione, nella serie dell'ultimo

anno di vita della pratica, annotando la doppia classificazione di parte della documentazione causata dalla modificazione o aggiornamento del piano di classificazione.

Fascicoli e documenti analogici, prodotti senza l'applicazione di un titolario o piano di classificazione, sono ordinati dopo un'adeguata analisi degli stessi, al fine di un ordinamento secondo criteri condivisi e orientati a essere perduranti nel tempo. Gli interventi su questa documentazione vanno comunque valutati insieme alla Soprintendenza Archivistica della Lombardia.

11.6. Elenco di consistenza per l'archivio di deposito analogico

L'Archivio Generale di ASP produce un elenco in formato *xlsx* che riporta la schedatura sommaria delle unità trasferite dall'archivio corrente all'archivio di deposito. Alle unità trasferite è attribuita una numerazione univoca, continua e progressiva che determina la posizione logica e fisica delle unità nell'elenco di consistenza e nel locale d'archivio.

Il personale addetto all'archivio di deposito, ricevuti i fascicoli e le serie archivistiche, li dispone nei locali di deposito rispettando l'ordinamento archivistico loro proprio, provvedendo a integrare e aggiornare l'elenco di consistenza con i trasferimenti effettuati dagli uffici.

11.7. Servizio di ricerca documentale e movimentazione dei fascicoli (*record delivery*)

L'Archivio Generale di ASP è titolare e responsabile del servizio di ricerca documentale, effettuato su richiesta degli uffici dell'ASP o di altri soggetti autorizzati. Il servizio, ove necessario, viene effettuato con la collaborazione degli uffici produttori o interessati.

Il servizio è di norma erogato tramite comunicazione delle informazioni richieste o con la trasmissione di copia della documentazione pertinente. Solo ove richiesto o necessario si ricorre al prelievo dal deposito e alla trasmissione della documentazione originale.

È consentito il richiamo temporaneo di uno o più fascicoli, già trasferiti all'archivio di deposito, da parte della UOR produttrice o altra UOR autorizzata. È vietata l'estrazione di documenti in originale dal fascicolo, che va mantenuto nell'ordine di sedimentazione derivante dall'archivio corrente, rispettando il vincolo archivistico (cioè l'appartenenza di ogni documento alla rispettiva unità o sottounità archivistica).

Il richiamo di uno o più fascicoli è consentito per il tempo necessario alla UOR richiedente per l'esaurimento della pratica.

Un fascicolo chiuso e trasferito all'archivio di deposito non può essere riaperto se non dopo che il RPA si sia consultato con il Coordinatore della gestione documentale, al fine di valutare la correttezza di tale operazione o se invece sia opportuna la creazione di un nuovo fascicolo per il nuovo procedimento, indipendente dal fascicolo richiamato.

Il flusso della ricerca documentale deve essere esclusivamente digitale.

Il Coordinatore della gestione documentale (o suo delegato) tiene traccia delle richieste di prelievo dei fascicoli dall'archivio di deposito in un apposito registro di carico e scarico costituito da un documento informatico in formato *xlsx*. Il registro riporta, oltre ai dati identificativi del fascicolo, l'unità organizzativa richiedente, il nominativo del richiedente, la motivazione, la data della richiesta, la data di evasione della richiesta, la data della effettiva restituzione ed eventuali note sulla documentazione consegnata.

11.7.1. Come effettuare la richiesta di ricerca documentale

La procedura per la ricerca documentale è la seguente:

- Consultare l'elenco di consistenza dei documenti reperibile dalla piattaforma *elearning* (Archivio Generale di ASP).
- Il Responsabile della UOR invia una email di richiesta all'Archivio Generale di ASP all'indirizzo mail: protocollo.asp.pavia@pec.it, specificando: o gli estremi del documento, es. n° di protocollo se noto; o una breve descrizione dell'oggetto;
    - la motivazione della richiesta;
    - se la richiesta riguarda l'ottenimento di una copia o dell'originale del documento.
- Il responsabile della UOR riceve una mail di avviso quando l'unità di conservazione richiesta è disponibile presso l'Archivio Generale di ASP; decorsi 10 giorni senza che il richiedente abbia effettuato la consultazione dei documenti, l'unità viene rimandata in Archivio di deposito.
- La consultazione dei documenti richiesti avviene presso l'Archivio Generale di ASP e, nel caso venga individuato il documento di interesse, è possibile:
    - ottenere una fotocopia del documento; o disporre dell'originale per 30 giorni;

Entro 30 giorni, il Responsabile è tenuto alla restituzione del documento e l'Archivio Generale di ASP rilascerà copia della ricevuta di avvenuta restituzione.

11.8 Accesso civico agli atti secondo il D.Lvo 97/2016

Artt. 5, 5 bis, 5 ter D.Lgs 33/2103, come modificato dal D.Lgs 97/2016 - Accesso civico

Art. 5 (Accesso civico a dati e documenti) -

1. L'obbligo previsto dalla normativa vigente in capo alle Pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione.

2. Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del decreto 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti (dati sensibili e personali) secondo quanto previsto dall'articolo 5-bis.

3. L'esercizio del diritto di cui ai commi 1 e 2 non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente. L'istanza di accesso civico identifica i dati, le informazioni o i documenti richiesti e non richiede motivazione. L'istanza può essere trasmessa per via telematica secondo le modalità previste dal decreto legislativo 7 marzo 2005, n.82, e successive modificazioni, ed è presentata alternativamente ad uno dei seguenti uffici: a) all'Ufficio che detiene i dati, le informazioni o i documenti;

b) all'Ufficio relazioni con il pubblico;
c) ad altro Ufficio indicato dall'amministrazione nella sezione "Amministrazione trasparente" del sito istituzionale;

Per ASP Pavia, l'Ufficio individuato è l'Ufficio Relazioni con il Pubblico
Recapito telefonico: 0382/381362
mail: info@asppavia.it

d) al Responsabile della prevenzione della corruzione e della trasparenza, ove l'istanza abbia a oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del presente decreto 33/2013.

Per ASP Pavia, avv. Maurizio Niutta
Recapito telefonico: 0382/381319
mail: segreteria.direttoregenerale1@asppavia.it

4. Il rilascio di dati o documenti in formato elettronico o cartaceo è gratuito, salvo il rimborso del costo effettivamente sostenuto e documentato dall'amministrazione per la riproduzione su supporti materiali.

5 Fatti salvi i casi di pubblicazione obbligatoria, l'amministrazione cui è indirizzata la richiesta di accesso, se individua soggetti controinteressati, ai sensi dell'articolo 5-bis, comma 2, è tenuta a dare comunicazione agli stessi, mediante invio di copia con raccomandata con avviso di ricevimento, o per via telematica per coloro che abbiano consentito tale forma di comunicazione. Entro dieci giorni dalla ricezione della comunicazione, i controinteressati possono presentare una motivata opposizione, anche per via telematica, alla richiesta di accesso. A decorrere dalla comunicazione ai controinteressati, il termine di cui al comma 6 è sospeso fino all'eventuale opposizione dei controinteressati. Decorso tale termine, la pubblica amministrazione provvede sulla richiesta, accertata la ricezione della comunicazione.

6. Il procedimento di accesso civico deve concludersi con provvedimento espresso e motivato nel termine di trenta giorni dalla presentazione dell'istanza con la comunicazione al richiedente e agli eventuali controinteressati. In caso di accoglimento, l'amministrazione provvede a trasmettere tempestivamente al richiedente i dati o i documenti richiesti, ovvero, nel caso in cui l'istanza riguardi dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del presente decreto, a pubblicare sul sito i dati, le informazioni o i documenti richiesti e a comunicare al richiedente l'avvenuta pubblicazione dello stesso, indicandogli il relativo collegamento ipertestuale. In caso di accoglimento della richiesta di accesso civico nonostante l'opposizione del controinteressato, salvi i casi di comprovata indifferibilità, l'amministrazione ne dà comunicazione al controinteressato e provvede a trasmettere al richiedente i dati o i documenti richiesti non prima di quindici giorni dalla ricezione della stessa comunicazione da

parte del controinteressato. Il rifiuto, il differimento e la limitazione dell'accesso devono essere motivati con riferimento ai casi e ai limiti stabiliti dall'articolo 5-bis. Il responsabile della prevenzione della corruzione e della trasparenza può chiedere agli uffici della relativa amministrazione informazioni sull'esito delle istanze.

7. Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato al comma 6, il richiedente può presentare richiesta di riesame al responsabile della prevenzione della corruzione e della trasparenza, di cui all'articolo 43, che decide con provvedimento motivato, entro al termine di venti giorni. Se l'accesso è stato negato o differito a tutela degli interessi di cui all'articolo 5-bis, comma 2, lettera a), il suddetto responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del responsabile è sospeso, fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni. Avverso la decisione dell'amministrazione competente o, in caso di richiesta di riesame, avverso quella del responsabile della prevenzione della corruzione e della trasparenza, il richiedente può proporre ricorso al tribunale amministrativo regionale ai sensi dell'articolo 116 del Codice del processo amministrativo di cui al decreto legislativo 2 luglio 2010, n. 104.

8. Qualora si tratti di atti delle amministrazioni delle regioni o degli enti locali, il richiedente può altresì presentare ricorso al difensore civico competente per ambito territoriale, ove costituito. Qualora tale organo non sia stato istituito, la competenza è attribuita al difensore civico competente per I 'ambito territoriale immediatamente superiore. Il ricorso va altresì notificato all'amministrazione interessata. Il difensore civico si pronuncia entro trenta giorni dalla presentazione del ricorso. Se il difensore civico ritiene illegittimo il diniego o il differimento, ne informa il richiedente e lo comunica all'amministrazione competente. Se questa non conferma il diniego o il differimento entro trenta giorni dal ricevimento della comunicazione del difensore civico, I 'accesso è consentito. Qualora il richiedente l'accesso si sia rivolto al difensore civico, il termine di cui all'articolo 116, comma 1, del Codice del processo amministrativo decorre dalla data di ricevimento, da parte del richiedente, dell'esito della sua istanza al difensore civico. Se I 'accesso è stato negato o differito a tutela degli interessi di cui all'articolo 5-bis, comma 2, lettera a), il difensore civico provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per la pronuncia del Difensore è sospeso, fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni.

9. Nei casi di accoglimento della richiesta di accesso, il controinteressato può presentare richiesta di riesame ai sensi del comma 7 e presentare ricorso al difensore civico ai sensi del comma 8.

10. Nel caso in cui la richiesta di accesso civico riguardi dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del presente decreto, il responsabile della prevenzione della corruzione e della trasparenza ha l'obbligo di effettuare la segnalazione di cui all'articolo 43, comma 5.

11. Restano fermi gli obblighi di pubblicazione previsti dal Capo II, nonché le diverse forme

di accesso degli interessati previste dal Capo V della legge 7 agosto 1990, n.241.

Art.5-bis (Esclusioni e limiti all'accesso civico) -

1. L'accesso civico di cui all'articolo 5, comma 2, è rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno degli interessi pubblici inerenti a:
a) la sicurezza pubblica e l'ordine pubblico;
b) la sicurezza nazionale;
c) la difesa e le questioni militari;
d) le relazioni internazionali;
e) la politica e la stabilità finanziaria ed economica dello Stato;
f) la conduzione di indagini sui reati e il loro perseguimento;
g) il regolare svolgimento di attività ispettive.

2. L'accesso di cui all'articolo 5, comma 2, è altresì rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:
a) la protezione dei dati personali, in conformità con la disciplina legislativa in materia;
b) la libertà e la segretezza della corrispondenza;
c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

3. Il diritto di cui all'articolo 5, comma 2, è escluso nei casi di segreto di Stato e negli altri casi di divieti di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1, della legge n. 241 del 1990.

4. Restano fermi gli obblighi di pubblicazione previsti dalla normativa vigente. Se i limiti di cui ai commi 1 e 2 riguardano soltanto alcuni dati o alcune parti del documento richiesto, deve essere consentito l'accesso agli altri dati o alle altre parti.

5. I limiti di cui ai commi I e 2 si applicano unicamente per il periodo nel quale la protezione è giustificata in relazione alla natura del dato. L'accesso civico non può essere negato ove, per la tutela degli interessi di cui ai commi I e 2, sia sufficiente fare ricorso al potere di differimento.

6. Ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui al presente articolo, l'Autorità Nazionale anticorruzione, d'intesa con il Garante per la protezione dei dati personali e sentita la Conferenza Unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n.281, adotta linee guida recanti indicazioni operative.

Art. 5 ter (Accesso per fini scientifici ai dati elementari raccolti per finalità statistiche) -

1.Gli enti e uffici del Sistema statistico nazionale ai sensi del decreto legislativo 6 settembre 1989, n. 322, di seguito Sistan, possono consentire l'accesso per fini scientifici ai dati elementari, privi di ogni riferimento che permetta l'identificazione diretta delle unità statistiche, raccolti nell'ambito dr trattamenti statistici dr cui i medesimi soggetti siano titolari, a condizione che:
a) l'accesso sia richiesto da ricercatori appartenenti a università, enti di ricerca e istituzioni

pubbliche o private o loro strutture di ricerca, inseriti nell'elenco redatto dall'autorità statistica dell'Unione europea (Eurostat) o che risultino in possesso dei requisiti stabiliti ai sensi del comma 3, lettera a), a seguito di valutazione effettuata dal medesimo soggetto del Sistan che concede l'accesso e approvata dal Comitato di cui al medesimo comma 3;
b) sia sottoscritto, da parte di un soggetto abilitato a rappresentare l'ente richiedente, un impegno di riservatezza specificante le condizioni di utilizzo dei dati, gli obblighi dei ricercatori, i provvedimenti previsti in caso di violazione degli impegni assunti, nonché le misure adottate per tutelare la riservatezza dei dati;
c) sia presentata una proposta di ricerca e la stessa sia ritenuta adeguata, sulla base dei criteri di cui al comma 3, lettera b), dal medesimo soggetto del Sistan che concede l'accesso. Il progetto deve specificare lo scopo della ricerca, il motivo per il quale tale scopo non può essere conseguito senza l'utilizzo di dati elementari, i ricercatori che hanno accesso ai dati, i dati richiesti, i metodi di ricerca e i risultati che si intendono diffondere.
Alla proposta di ricerca sono allegate dichiarazioni di riservatezza sottoscritte singolarmente dai ricercatori che avranno accesso ai dati. E' fatto divieto di effettuare trattamenti diversi da quelli previsti nel progetto di ricerca, conservare i dati elementari oltre i termini di durata del progetto, comunicare i dati a terzi e diffonderli, pena l'applicazione della sanzione di cui all'art. 162, comma 2 bis del decreto legislativo 30 giugno 2003, n.196.

2.l dati elementari di cui al comma l, tenuto conto dei tipi di dati nonché dei rischi e delle conseguenze di una loro illecita divulgazione, sono messi a disposizione dei ricercatori sotto forma di file a cui sono stati applicati metodi di controllo al fine di non permettere l'identificazione dell'unità statistica. In caso di motivata richiesta, da cui emerga la necessità ai fini della ricerca e I 'impossibilità di soluzioni alternative, sono messi a disposizione file a cui non sono stati applicati tali metodi, purché l'utilizzo di questi ultimi avvenga all'interno di laboratori costituiti dal titolare dei trattamenti statistici cui afferiscono i dati, accessibili anche da remoto tramite laboratori organizzati e gestiti da soggetto ritenuto idoneo e a condizione che il rilascio dei risultati delle elaborazioni sia autorizzato dal responsabile del laboratorio stesso, che i risultati della ricerca non permettano il collegamento con le unità statistiche , nel rispetto delle norme in materia di segreto statistico e di protezione dei dati personali, o nell'ambito di progetti congiunti finalizzati anche al perseguimento di compiti istituzionali del titolare del trattamento statistico cui afferiscono i dati, sulla base di appositi protocolli di ricerca sottoscritti dai ricercatori che partecipano al progetto, nei quali siano richiamate le norme in materia di segreto statistico e di protezione dei dati personali.
Sentito il Garante per la protezione dei dati personali, il Comitato di indirizzo e coordinamento dell'informazione statistica (Comstat), con atto da emanarsi ai sensi dell'articolo 3, comma 6, del decreto del Presidente della Repubblica 7 settembre 2010, n. 166, avvalendosi del supporto dell'Istat, adotta le linee guida per I'attuazione della disciplina di cui al presente articolo. In particolare, il Comstat stabilisce:
a) i criteri per il riconoscimento degli enti di cui al comma l, lettera a), avuto riguardo agli scopi istituzionali perseguiti, all'attività svolta e all'organizzazione interna in relazione all'attività di ricerca, nonché alle misure adottate per garantire la sicurezza dei dati;
b) i criteri di ammissibilità dei progetti di ricerca avuto riguardo allo scopo della ricerca, alla necessità di disporre dei dati richiesti, ai risultati e benefici attesi e ai metodi impiegati per la loro analisi e diffusione;
c) le modalità di organizzazione e funzionamento dei laboratori fisici e virtuali di cui al comma2;

d) i criteri per l'accreditamento dei gestori dei laboratori virtuali, avuto riguardo agli scopi istituzionali, all'adeguatezza della struttura organizzativa e alle misure adottate per la gestione e la sicurezza dei dati ;
e) le conseguenze di eventuali violazioni degli impegni assunti dall'ente di ricerca e dai singoli ricercatori.

4. Nei siti istituzionali del Sistan e di ciascun soggetto del Sistan sono pubblicati gli elenchi degli enti di ricerca riconosciuti e dei file di dati elementari resi disponibili.

5. Il presente articolo si applica anche ai dati relativi a persone giuridiche, enti od associazioni.

Per ASP Pavia, l'Ufficio individuato è l'Ufficio Relazioni con il Pubblico
Recapito telefonico: 0382/381360
mail: info@asppavia.it

11.9. Conservazione

Il Coordinatore 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 Coordinatore 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 e ai servizi generali.

Il Coordinatore della gestione documentale provvede anche ad attuare interventi di restauro, nei casi in cui si rendessero necessari.

Per la conservazione digitale il Coordinatore della gestione documentale concorderà i criteri con il Responsabile della conservazione (art. 21, 29-31, D.Lgs. 42/2004).

CAPITOLO 12. IL SISTEMA INFORMATICO

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.

12.1. Il modello organizzativo

I servizi di *information and communication technology* per il supporto all'attività amministrativa e assistenziali di ASP sono curati dalla Direzione Generale di concerto con il referente de Sistemi Informativi aziendale .

Nel presente capitolo, il termine "conservazione" è utilizzato in luogo di "registrazione" dei dati su dispositivi di memorizzazione *on-line* e *near-line* o su supporti per il salvataggio dei dati in modalità *off-line*.

12.2. Sicurezza del sistema informatico

La sicurezza dei dati, delle informazioni e dei documenti informatici memorizzati (poi archiviati) nel sistema di gestione documentale è garantita dall'applicazione informatica adottata dall'ASP.

Il piano della sicurezza informatica relativo a formazione, gestione, trasmissione, interscambio, accesso, memorizzazione dei documenti informatici, ivi compresa la gestione delle copie di sicurezza nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico descritto nell'Allegato B del D.Lgs. 30 giugno 2003, n. 196 e successive modificazioni è predisposto e aggiornato annualmente dal Consorzio Cineca.

12.2.1. Il sistema di gestione documentale

Il sistema di gestione documentale è costituito dall'insieme delle tecnologie presenti presso il *data center* da tutti i dispositivi e i programmi presenti presso le sedi dell'ASP che permettono l'utilizzo del sistema.

12.2.2. Sicurezza fisica dei data center

Per le misure di sicurezza si rimandaal Documento Programmatico di Sicurezza redatto ogni anno entro il 31 Marzo, ai sensi del D.L.vo 193/03. In parte, sono anche di seguito descritte.

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;
- impianto antifurto con combinatore telefonico agganciato al servizio di vigilanza H24;
- 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.

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.

12.2.3. La manutenzione e la continuità operativa degli impianti elettrici

Gli impianti elettrici devono essere monitorati da sistemi automatici di allarme in grado di allertare i tecnici di manutenzione degli impianti elettrici in caso di anomalie e permetterne l'intervento entro il tempo di protezione garantito dai sistemi *UPS*.

12.2.4. Rete dati

L'utilizzo del sistema di gestione documentale è garantito dalla rete dati di ASP.

Il Centro Sistemi informativi e comunicazione, in qualità di amministratore della rete di ASP, assicura in modo esclusivo e tempestivo la gestione, il monitoraggio, l'aggiornamento e l'ampliamento della rete dati di ASP (cablaggio e parte attiva), sia sotto l'aspetto fisico che logico, fino alla presa utente compresa.

L'amministratore della rete di ASP registra – in appositi *file* di *log* – i dati relativi all'accesso alla rete e all'accesso ad internet o al traffico telematico in generale (escluso il contenuto della trasmissione dati). I dati registrati nei *file* di *log* sono raccolti, memorizzati e conservati in conformità alla normativa vigente. Le informazioni contenute nei *file* di *log* possono essere messe a disposizione dell'autorità giudiziaria, la quale può richiedere la non cancellazione e la conservazione per un periodo più lungo di quanto disposto dalla legge.

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

12.2.5. Le postazioni di lavoro

La gestione e la manutenzione delle postazioni di lavoro per l'utilizzo del sistema di gestione documentale è competenza esclusiva di ciascuna AOO. Le postazioni di lavoro degli utenti dell'Amministrazione Centrale sono gestite dal Centro Sistemi informativi e comunicazione.

Ogni AOO 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.

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;
- sono dotate di *firewall* locale impostato per consentire solo le connessioni instaurate dal client stesso e per i servizi legittimi (*client mode*);
- salvo motivate e documentate eccezioni, sulle postazioni di lavoro non è permessa la connessione remota dall'esterno della Rete Dati di ASP (*RDP*, *SSH*, *VNC*, ecc.);
- la connessione da remoto alle postazioni di lavoro dall'interno della Rete Dati dell'ASP, 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.

12.3. Sicurezza dei documenti informatici

L'accesso al sistema di gestione documentale di ogni utente di tutte le AOO dell'ASP è gestito centralmente ed è subordinato all'abilitazione a cura del Coordinatore della gestione documentale.

Le identità digitali utilizzate per l'accesso al sistema di gestione documentale sono costituite da *nome utente* e *password*. L'identificazione informatica dell'utente, cioè la validazione dell'identità digitale, è operata attraverso una infrastruttura di autenticazione centralizzata basata su *Microsoft Active Directory*.

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

Il sistema di gestione documentale rispetta le misure di sicurezza previste dagli artt. 31-36 e dal disciplinare tecnico di cui all'allegato B del D.Lgs. 30 giugno 2003, n. 196.

I dati sono resi disponibili e accessibili a chiunque ne abbia diritto; si individuano i soggetti preposti al trattamento dei dati:

- *Titolare del trattamento* – È il destinatario delle norme, ossia la persona fisica e/o giuridica, l'amministrazione pubblica o altro ente a cui compete decidere finalità, modalità del trattamento dei dati personali e gli strumenti utilizzati, compresa la sicurezza;
- *Responsabile del trattamento* – La persona fisica, giuridica, l'amministrazione pubblica o altro ente designato, facoltativamente, dal titolare a trattare i dati compreso il profilo relativo alla sicurezza:
  - i Direttori delle Direzioni Mediche di Presidio
  - il Direttore Generale per gli Uffici Amministrativi;
- *Responsabile esterno del trattamento*: in coerenza con il modello organizzativo adottato dall'ASP per la conduzione del Sistema di gestione documentale, alla ditta…….. è conferito il ruolo di Responsabile esterno del trattamento; in virtù di tale ruolo è …… che, per le attività di conduzione del sistema, gestione applicativa e assistenza, provvede alla nomina dell'amministratore di sistema, ne assolve i compiti e conseguenti adempimenti.
- *Incaricato del trattamento* – La persona fisica autorizzata a compiere operazioni di trattamento dati dal Titolare o dal Responsabile.

I Responsabili del trattamento designano, con provvedimento espresso, gli Incaricati del trattamento dei dati operanti all'interno della struttura di competenza.

Nello svolgimento dei compiti è fatto divieto agli Incaricati 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 Titolare, oppure divengano di dominio pubblico.

12.3.1. Accesso ai dati e ai documenti informatici

Il sistema adottato dall'ASP garantisce:

- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso ai documenti, alle informazioni e ai dati esclusivamente agli utenti abilitati;
- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;
- la registrazione delle attività svolte da ciascun utente anche rilevanti ai fini della sicurezza, in modo tale da garantirne l'identificazione;
- l'immodificabilità dei contenuti e, comunque, la loro tracciabilità.

Il controllo degli accessi è assicurato dall'utilizzo di credenziali di autenticazione con differenti profili di autorizzazione in relazione ai diversi ruoli di ciascun utente. I trattamenti associabili a ciascun profilo, preventivamente individuati dal Coordinatore della gestione documentale di concerto con i Responsabili del trattamento dei dati e i Responsabili della gestione documentale delle diverse AAO, sono in sintesi:

- *inserimento* dei dati per effettuare una registrazione;
- *modifica* dei dati di una registrazione;
- *annullamento* di una registrazione;
- *ricerca* di informazioni registrate ai fini della visualizzazione o consultazione; □ visualizzazione e consultazione;
- *download* dei documenti associati alla registrazione.

Periodicamente, e comunque almeno annualmente, è verificata a cura del Coordinatore della gestione documentale di concerto con i Responsabili delle strutture e i Responsabili della gestione documentale, la sussistenza delle condizioni per il mantenimento dei profili di autorizzazione per tutte le Aree Organizzative Omogenee. Per quanto riguarda la garanzia di immodificabilità dei contenuti si rimanda a quanto illustrato al § 6.8.

Quando l'accesso ai dati e agli strumenti informatici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni volte a individuare chiaramente le modalità con le quali il Titolare può assicurare la disponibilità di dati o di strumenti informatici in caso di prolungata assenza o di impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

In tal caso, la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'Incaricato dell'intervento effettuato.

Le stesse credenziali non possono essere assegnate a persone diverse, neppure in tempi diversi, quindi le credenziali sono strettamente personali.

Ciascun utente ha la possibilità di cambiare la propria *password* in qualsiasi momento ed è auspicabile che ciò avvenga nel caso in cui si presume che essa abbia perso il requisito della segretezza.

12.3.2. 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'ASP 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'ASP. 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 di ASP, non deve pregiudicare il corretto adempimento della prestazione lavorativa, ostacolare le attività dell'ASP o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici.

Gli utenti a cui sono affidate le postazioni di lavoro dell'ASP, 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 le misure idonee previste dall'Allegato B al D.Lgs. 30 giugno 2003, n. 196;
- 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'ASP qualsiasi risorsa informatica assegnata e mettere a disposizione ogni informazione di interesse istituzionale;

Sulle postazioni di lavoro non è ammesso:

- installare programmi per elaboratore 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'ASP, se non preventivamente autorizzati;
- utilizzare dispositivi mobili quali punti di accesso da/all'esterno la rete dell'ASP, se non preventivamente autorizzati;
- installare programmi non inerenti all'attività lavorativa e/o privi di licenze d'uso;
- copiare dati la cui titolarità è di ASP 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 fatto obbligo di adottare le misure idonee prescritte dal già citato allegato B al D.Lgs. 30 giugno 2003, n. 196.

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. Per la disciplina riguardante l'utilizzo delle credenziali, per la segretezza e per la protezione delle *password* è fatto riferimento espresso alle disposizioni contenute nel D.Lgs. 30 giugno 2003, n. 196, e, in particolare, agli artt. 4 comma 3 lett. d) e 34.

Allegato n. 1 – Riferimenti normativi

- Legge 7 agosto 1990, n. 241, *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*
- Decreto del Presidente della Repubblica 4 aprile 2002, n. 101, *Regolamento recante criteri e modalità per l'espletamento da parte delle amministrazioni pubbliche di procedure telematiche di acquisto per l'approvvigionamento di beni e servizi*
- Direttiva del Ministro per l'innovazione e le tecnologie 9 dicembre 2002, *Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali*
- Decreto legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*
- Legge 9 gennaio 2004, n. 4, *Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici*
- Decreto legislativo 22 gennaio 2004, n. 42, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*
- Decreto legislativo 7 marzo 2005, n. 82, *Codice dell'amministrazione digitale*
- Legge 24 dicembre 2007, n. 244, *Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008)*
- Decreto legge 29 novembre 2008, n. 185, *Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale*

- Legge 3 marzo 2009, n. 18 *Ratifica ed esecuzione della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, con Protocollo opzionale, fatta a New York il 13 dicembre 2006 e istituzione dell'Osservatorio nazionale sulla condizione delle persone con disabilità*
- Legge 18 giugno 2009, n. 69, *Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile*
- Decreto legislativo 27 ottobre 2009, n. 150, *Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*
- Deliberazione del Garante per la protezione dei dati personali 2 marzo 2011, n. 88, *Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web*
- Decreto Legge n. 9 febbraio 2012, n. 5 coordinato con la Legge di conversione 4 aprile 2012, n. 35*, Disposizione urgenti in materia di semplificazione e di sviluppo*
- Legge 17 dicembre 2012, n. 221*, Conversione in legge, con modificazioni, del Decreto Legge 18 ottobre 2012, n. 179 recante ulteriori misure urgenti per la crescita del Paese*
- Circolare dell'Agenzia per l'Italia Digitale – AIPA 23 gennaio 2013, n. 60 *Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni - Revisione della Circolare AIPA del 7 maggio 2001, n. 28 relativa agli standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati, ai sensi dell'art. 18, comma 2, del D.P.C.M. 31 ottobre 2000 di cui al D.P.R. 28 dicembre 2000, n. 445*
- DPCM 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*
- Circolare interpretativa del Ministero dell' Economia e Finanze numero 1/DF del 9 marzo 2015 *in tema di fatturazione elettronica*
- Circolare dell'Agenzia per l'Italia Digitale 29 marzo 2013, n. 61, *Disposizioni del Decreto legge n. 79 del 18 ottobre 2012 in tema di accessibilità dei siti web e servizi informatici. Obblighi delle pubbliche amministrazioni*
- Decreto del Ministro dell'Economia e delle Finanze 3 aprile 2013, n. 55, *Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244*
- DPCM 3 dicembre 2013, *Regole tecniche in materia di sistema di conservazione degli archivi digitali*
- DPCM 3 dicembre 2013, *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*
- Deliberazione del Garante per la protezione dei dati personali 15 maggio 2014, n. 243, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*
- Decreto del Ministro dell'Economia e delle Finanze 17 giugno 2014, *Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005*

- Regolamento del Parlamento e del Consiglio dell'Unione europea 23 luglio 2014, n. 910, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (eIDAS)*
- Decreto legge 24 aprile 2014, n. 66, *Misure urgenti per la competitività e la giustizia sociale*
- Legge 16 maggio 2014, n. 78, *Conversione in legge, con modificazioni, del decreto legge 20 marzo 2014, n. 34, recante disposizioni urgenti per favorire il rilancio dell'occupazione e per la semplificazione degli adempimenti a carico delle imprese*
- 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 ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*
- Decreto del Ministero del lavoro e delle politiche sociali 30 gennaio 2015, *Semplificazione in materia di documento unico di regolarità contributiva (DURC)*
- Deliberazione del Garante per la protezione dei dati personali 19 marzo 2015, n. 161, *Linee guida in materia di trattamento di dati personali per profilazione on line*
- Decreto legislativo 18 aprile 2016, n. 50 *Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture*
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*

Allegato n° 2 - Procedure e Processi Principali – Tabella riepilogativa

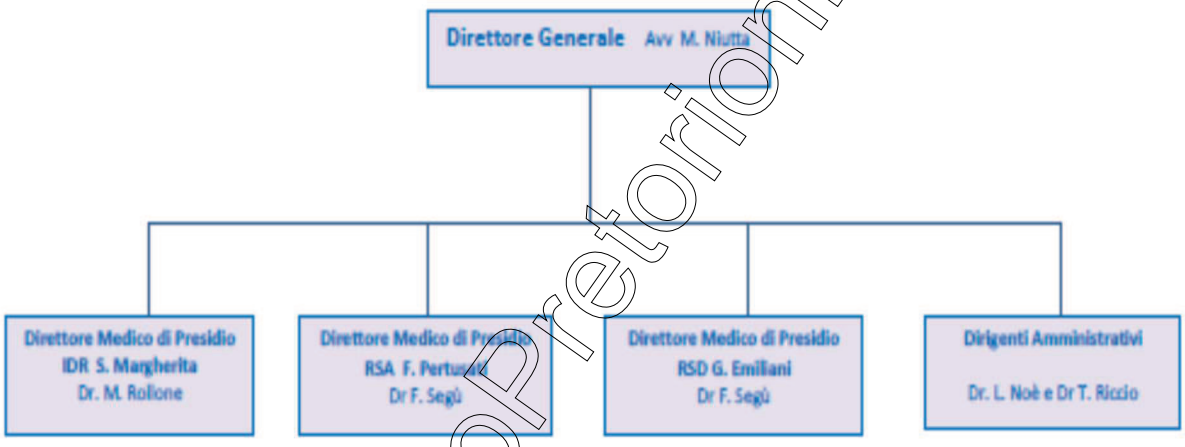
			Natura dato					
N° Identificativo	Finalità perseguita o attività svolta	Categorie di interessati	P	S	G	Ufficio e Responsabile	Altri incaricati	Strumenti utilizzati
1	Protocollazione, registrazione ed Archiviazione di tutte le pratiche trattate dall' ASP	Tutti i soggetti di tutte le categorie che si interfacciano per qualsiasi motivo con l'ASP.	x	x	x	Ufficio Protocollo /Archivio **Scarpa**	Maestri	2 PC in rete SW "Folium" e "Civilia"
2	Approvazione, smistamento, determinazioni relativamente a tutte le pratiche trattate dall'ASP. Strategia e Management	Tutti i soggetti di tutte le categorie che si interfacciano per qualsiasi motivo con l'ASP.	x	x	x	Direzione Generale e Segreteria **Niutta**	Bernuzzi	2 PC in rete SW "Folium" e "Civilia", Banche dati in rete
3	Gestione dati di natura economica e dati anagrafici di fornitori	Aziende ed enti esterni(fornitori)	x			U.O.F.C. **Riccio**	Di Maio, Tartarotti, Tavazzani, Ruzza	Software Gestionale "Onda"
4	Gestione dati personali e sensibili dei dipendenti	Tutto il personale dipendente	x	x		Stipendi **Rosa**	Rosa, Solerte, Alpeggiani, Finotti, Brugnoli, Reccagni, Viscomi	SW personalizzato "Syntecop" e "Gestione Personale" Biosistemi, vecchia e nuova versione
5	Gestione dati anagrafici per contratti	Aziende ed enti esterni(fornitori)	x			Contratti/Provvedi torato **Noè**	Bressani, Oltremonti	File singoli su file server non condivisi
6	Gestione dati personali e sensibili dei dipendenti	Tutto il personale dipendente	x	x		Personale **Rosa**	Solerte, Alpeggiani, Brugnoli Reccagni	SW "Gestione Personale" vecchia e nuova versione Biosistemi
7	Gestione dati tecnici	Aziende ed enti esterni(fornitori)	x			Tecnico **Ghilioni**	Beolchi, Montini, Albano.	File singoli su file server non condivisi
8	Gestione domande e ricovero RSA, IDR, CDI, Ambulatori, debito informativo e quindi Gestione dati personali e sensibili dei dipendenti. Attività connesse con il CUP.	Ospiti e possibili ospiti, tutto il personale dipendente e non	x	x		Statistica_Relazioni con il Pubblico - **Magnani**	Cavallotti, Graziano	Sw "SIESA" biosistemi Sw "SOSIAweb" SW "Gestione Personale" vecchia e nuova versione Biosistemi
9	Gestione dati sensibili di natura medica	Ospiti e dipendenti		x		Direzione Medica RSA **Segù**	Tolentino, Finotti, De Paoli, Corradini	File singoli su file server non condivisi, Sw "SIESA" biosistemi, SW "Gestione Personale" vecchia e nuova

								versione Biosistemi
10	Gestione dati sensibili di natura medica	Ospiti e dipendenti		x		Direzione Medica RSD **Segù**	Cavallotti T.,	"Gestione Personale" vecchia e nuova versione Biosistemi, dati in locale
11	Gestione dati per rette	Ospiti	x	x		Economato ASP **Pezza, Filippi Baccalini**	Pezza, Russino, Filippi, Baccalini,	Sw "Siesa" biosistemi
12	Gestione dati sensibili di natura medica	Ospiti e dipendenti		x		Direzione Medica IDR **Rollone**	Bocchi, Pellegrino	Domande di ricovero, cartelle cliniche.
13	Gestione pratiche inerenti al ricovero Gestione domande e ricovero IDR, CDI, Ambulatori, debito informativo	Ospiti e possibili ospiti	x	x		Spedalità SM **Rollone**	Simone, Bocchi, Reccagni, Brocchetta	Sw "Five" Debito Informativo, domande di ricovero
14	Centralino S. Margherita	Ospiti	x	x		Certificati di morte	Miranda, Fiammenghi, Aramini, Longhi	Elenco ospiti ricoverati
15	Centralino F. Pertusati	Ospiti	x	x		Elenco ospiti ricoverati	Ordali, Fusetto	Elenco ospiti ricoverati
16	Gestione dati salute e stato cognitivo utenti	Ospiti RSD		x		Animazione/ educazione **Cavallotti**,	Tutti animatori (elenco a parte)	File locali su PC non in rete. Solo il coordinatore ha 1 PC in rete
17	Gestione dati medici	Ospiti	x	x		**Attività sanitaria specifica**	Personale sanitario (medico ed infermieristico)	Documenti diversi in locale ed in rete
18	Gestione dati sui farmaci	Ospiti	x	x		**Farmacia Bellotti**	Naddeo	Sw "Magazzino Farmaci" biosistemi
19	Gestione dati di Geriatria, Endocrinologia e Diabetologia	Ospiti		x		**Attività sanitaria specifica**	Personale medico specializzato	Documenti diversi in locale ed in rete
20	Gestione prenotazioni ambulatoriali	Dati pazienti per le prenotazioni delle prenotazioni	x			**Prenotazioni ambulatoriali CUP**	Suardi, Bucci, Caselli, Pasolini	SW CUP Omnicom
21	Gestione di dati inerenti ai parametri bioumorali	Utenti esterni, ospiti, dipendenti		x		**Esecuzione esami di laboratorio**	Personale specializzato Bonora, Maggi,	Documenti diversi in locale

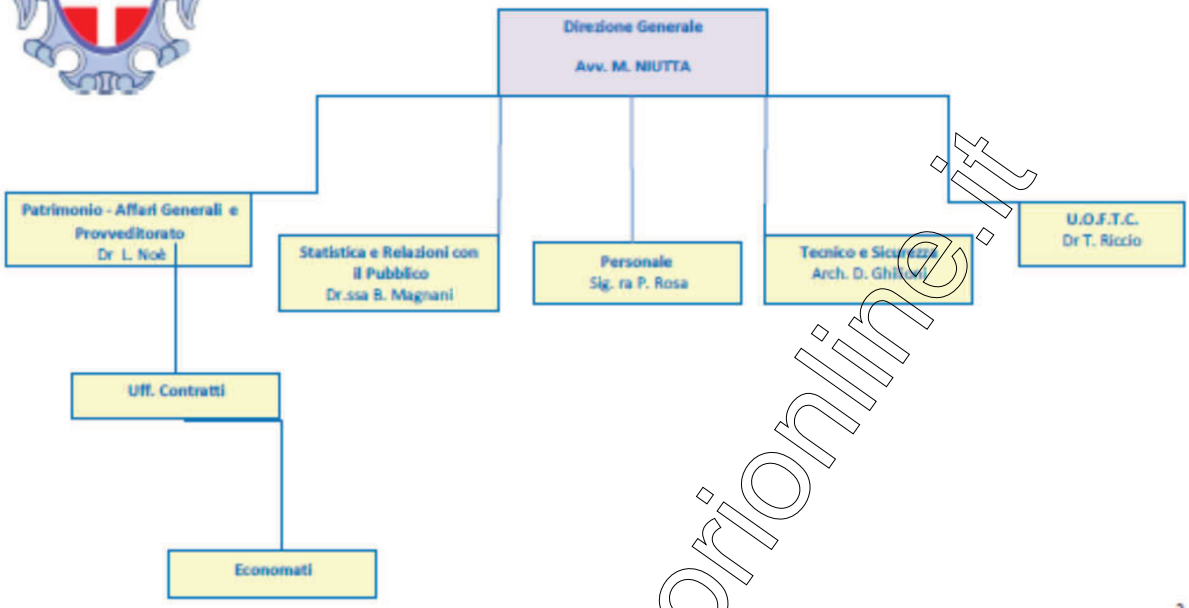
							Signorino, Picci	
22	Gestione dati Attività di palestra	Ospiti	x	x		**Serv. di Riabilitazione ASP Mazzacane**	Personale specializzato (FKT, elenco a parte)	Liste attesa fornito da Regione SW CUP

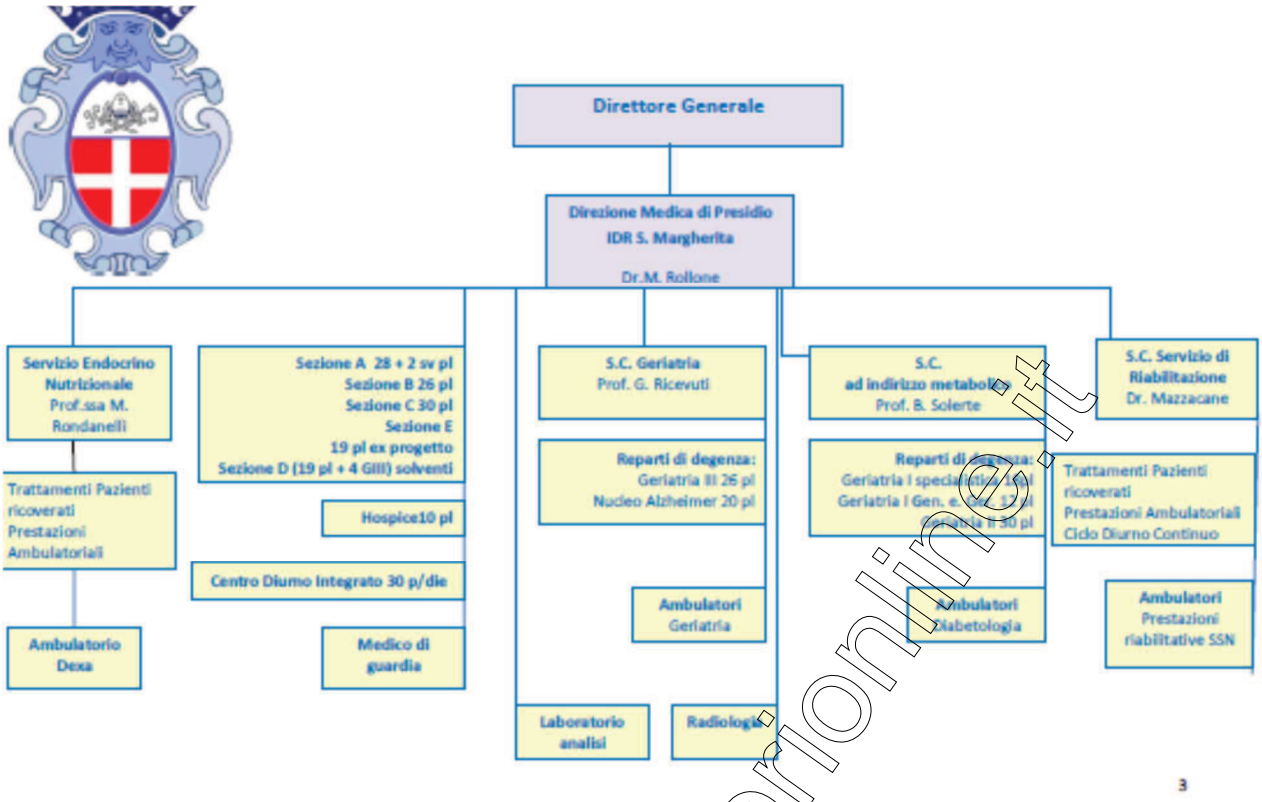
Per ciascuna attività svolta o finalità perseguita, ogni responsabile dovrà accuratamente redigere e decidere le procedure pertinenti

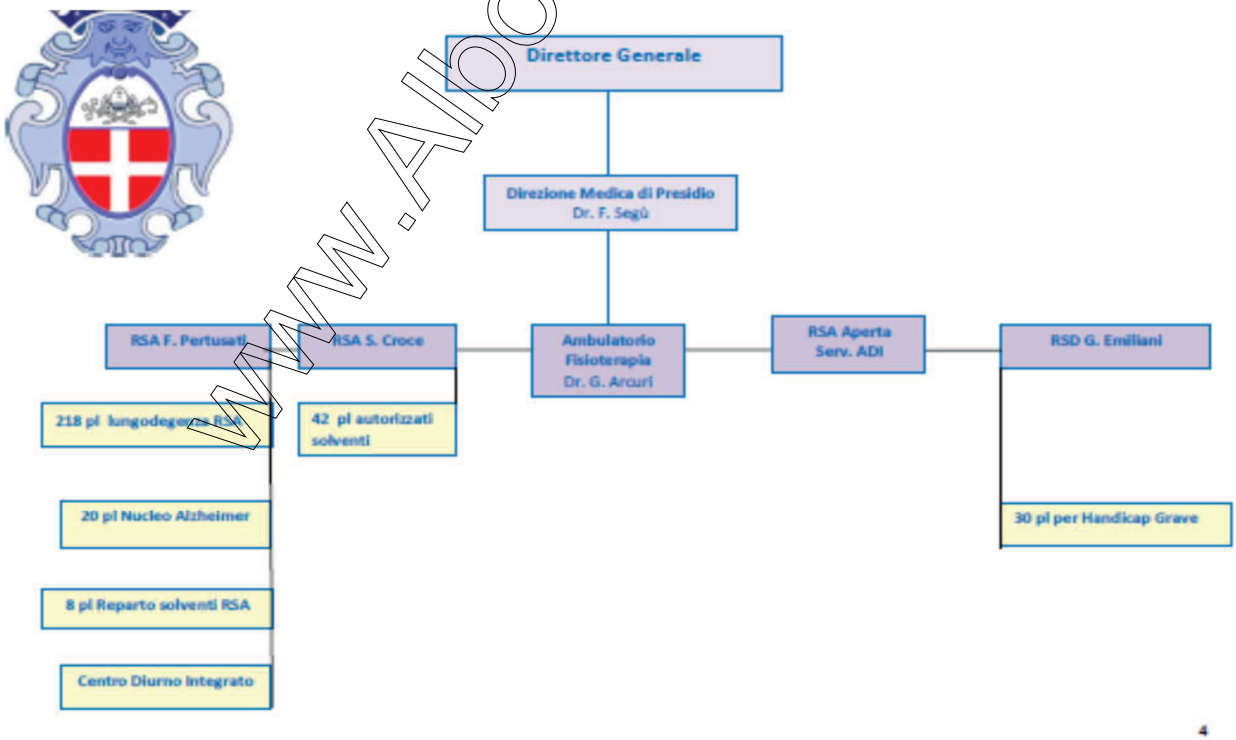
Allegato n. 3 – STRUTTURA ORGANIZZATIVA DI ASP
AOO – UOR



Area Amministrativa







Allegato n. 4 – Nomine coordinatore/responsabili della gestione documentale

RESPONSABILI E FIGURE DI RIFERIMENTO PER LA GESTIONE E LA CONSERVAZIONE DOCUMENTALE (DDG 1115/2015, allegato *infra*)

- Coordinatore della gestione documentale …….
- Coordinatore della gestione documentale vicario …… □ Responsabili e vicari della gestione documentale per AOO:

AOO	**Responsabile**	**Vicario**
Amministrazione Centrale	.	.
RSA F. Pertusati		
Centro Diurno F. Pertusati		
RSA S. Croce		

RSD G. Emiliani		
IDR Cure Intermedie S. Margherita UdO Geriatria Generale Geriatrica		
IDR Cure Intermedie S. Margherita UdO Geriatria di Mantenimento		
IDR Cure Intermedie S. Margherita UdO Geriatria Post specialistica		
IDR Cure Intermedie S. Margherita UdO reparto Solventi		
IDR Cure Intermedie S. Margherita UdO Hospice		
IDR Cure Intermedie S. Margherita UdO Ciclo diurno Continuo e trattamenti ambulatoriali		
IDR Cure Intermedie S. Margherita UdO Centro Diurno S. Margherita		
IDR UdO Servizio di Riabilitazione		
IDR S. Margherita UdO Ambulatori Geriatria e Gerontologia		
IDR S. Margherita UdO Ambulatori Geriatria e Gerontologia		
IDR S. Margherita UdO Ambulatori Diabetologia		
IDR S. Margherita UdO Ambulatori Endocrinologia		
IDR S. Margherita UdO Laboratorio di Analisi		
IDR S. Margherita UdO Servizio di Radiodiagnostica		

- Referente dei sistemi informatici documentali e della sicurezza informatica…….
- Referente della protezione dei dati personali relativamente al sistema documentale …….

Seguono gli atti di nomina…..

Allegato n. 5 – Linee guida per l'utilizzo del servizio di posta elettronica

1. Premessa

L'ASP fornisce una casella istituzionale di posta elettronica a tutti i responsabili responsabili di servizio. Nella definizione delle regole d'uso del servizio di posta elettronica e delle modalità di controllo ad essa connesse, l'ASP ritiene di grande importanza salvaguardare la libertà di espressione e di pensiero e garantire il diritto alla *privacy* dell'individuo.

2. Oggetto e finalità

1. Un indirizzo di posta elettronica codificato nel formato base *nome.cognome@asppavia.it* è assegnato alle persone afferenti alle seguenti categorie:
   - Dirigente a tempo determinato/indeterminato;

   I casi di omonimia sono risolti mediante apposizione di un suffisso numerico incrementale al termine della stringa *nome.cognome*.
   II
2. Un indirizzo di posta elettronica codificato nel formato base *Uff.ufficio@asppavia.it* è assegnato alle categorie di uffici e servizi.:

   I casi di omonimia sono risolti mediante apposizione di un suffisso numerico incrementale al termine della stringa *uff.ufficio*.
3. Un indirizzo di posta elettronica *pec* codificato nel formato base *nome.cognomepec@asppavia.it* è assegnato alle persone afferenti alle seguenti categorie:

   - Dirigente a tempo indeterminato amministativo
   - Dirigente medico con incarico di Direttore Medico;

3. Le comunicazioni ufficiali e istituzionali da parte dell'ASP sono inviate esclusivamente all'indirizzo di posta istituzionale di cui ai commi 1, 2 e 3 del presente articolo.
4. L'utilizzo degli indirizzi di cui ai commi 1, 2 e 3 del presente articolo costituisce "trattamento dei dati personali" e, pertanto, da conformarsi alle disposizioni del D.Lgs. 196/2003.

3. Accesso al servizio di posta elettronica

1. L'accesso al servizio di posta elettronica di ASP avviene mediante l'utilizzo delle credenziali associate alla propria identità digitale, costituite da *nome utente* e *password*.
2. Le caselle di posta elettronica di cui al punto 2.3 sono create come caselle con delega.
3. I soggetti titolari delle caselle di posta elettronica istituzionali sono responsabili del corretto utilizzo delle stesse.

4. Utilizzo della posta elettronica

1. Il servizio di posta elettronica è fornito in funzione dell'attività amministrativa e delle altre attività strumentali o correlate ai fini istituzionali di ASP.
2. È opportuno che ogni persona consulti regolarmente la propria casella istituzionale di posta elettronica.
3. Allo scopo di conseguire un più efficace impiego del servizio e nel contempo non sovraccaricare i relativi sistemi di sicurezza, è opportuno eliminare dalla casella istituzionale di posta elettronica i messaggi non necessari e i relativi allegati.
4. Non è consentito utilizzare la posta elettronica per diffondere, anche tramite collegamenti ipertestuali o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice eseguibile, ecc.), messaggi che contengano o rimandino a:
    - pubblicità non istituzionale, manifesta od occulta;
    - partecipazione a *forum* e/o dibattiti se non per motivi istituzionali, per diffondere notizie non veritiere o quanto altro che abbia contenuto offensivo e discriminatorio;
    - comunicazioni commerciali private;
    - materiale pornografico o che possa comportare una violazione della Legge 3 agosto 1998 n. 269, *Norme contro lo sfruttamento sessuale dei minori degli anni 18*;
    - materiale discriminante o lesivo in relazione a razza, sesso, religione;
    - materiale che violi la normativa in materia di protezione dei dati personali;
    - contenuti o materiali che violino i diritti d'autore di terzi;
    - materiale contenente codici dannosi (ad es., virus informatici; altri contenuti illegali; catene telematiche.
5. In caso di assenze programmate o prevedibili è opportuno che il personale dell'ASP attivi la funzione di risposta automatica per comunicare ai mittenti eventuali contatti alternativi.
6. In caso di assenza prolungata o improvvisa, è opportuno che il singolo dipendente si adoperi per consentire la corretta ricezione e gestione dei messaggi pertinenti all'attività istituzionale eventualmente recapitati nella propria casella di posta elettronica. Qualora tale accorgimento non sia posto in essere dal dipendente o, a tutela del buon andamento e dell'efficienza dell'attività istituzionale, si configuri la necessità di accedere ai messaggi giacenti nella casella di posta elettronica del dipendente, l'ASP si riserva la facoltà di attivare le misure tecniche atte a consentire al Responsabile della AOO/UOR di appartenenza del dipendente di accedere alla casella di posta attribuendo temporaneamente a quest'ultimo diritti di delega. Di tale attività deve essere redatto apposito verbale e deve essere informato l'utente interessato alla prima occasione utile.

5. Ciclo di vita della casella e conservazione dei messaggi

1. Il ciclo di vita delle caselle di posta elettronica è caratterizzato da tre fasi distinte:
    - *Attivazione*: la casella viene generata nel sistema di posta elettronica e viene attivata mediante assegnazione di una licenza d'uso;
    - *Disattivazione*: decorsi i tempi di validità del contratto di lavoro oppure cessata la carriera del dipendente, la casella di posta elettronica viene disattivata e non può più essere utilizzata dall'utente.

- *Cancellazione dei dati*: i messaggi contenuti nella casella sono cancellati definitivamente dal sistema di posta elettronica e non sono più recuperabili.

Personale di ASP

- *Attivazione*: contestuale alla creazione dell'identità digitale;
- *Disattivazione*: 12 mesi dopo la cessazione del contratto di lavoro/collaborazione/servizio;
- *Cancellazione dei dati*: 30 giorni dopo la disattivazione.

6. Monitoraggio e controlli

1. Per motivi tecnici e di sicurezza ed in particolare per prevenire malfunzionamenti, la ditta che ha in carico la gestione del server di posta elettronica effettua una registrazione delle componenti di traffico (*file* di *log*) riferiti alla posta elettronica.

7. Modalità di gestione degli incidenti

1. Nel caso dei seguenti eventi l'accesso ai servizi di posta elettronica può essere totalmente o parzialmente limitato dall'ASP, senza necessità di assenso da parte dell'utente e anche senza preavviso:
   - quando richiesto dalla legge e in conformità a essa;
   - in caso di comprovati motivi che facciano ritenere la violazione delle presenti regole e delle disposizioni di legge vigenti;
   - in casi eccezionali, quando richiesto, per esigenze operative critiche e improcrastinabili.

Allegato n. 6 – Linee guida per l'utilizzo delle caselle PEC e loro elenco

1. Premessa

Ai sensi del Codice dell'amministrazione digitale[18], ASP si è dotata di caselle di Posta Certificata – PEC sia ti tipologia connessa all'impiego del Sistema di Riferimento di Regione Lombardia SISS che ARUBA pec come al punto 2 di questo allegato. SISS e Aruba operano in conformità alle regole tecniche e secondo quanto prescritto dal D.Lgs 82/2005 e dal DPR 68/2005[19].

2. Elenco caselle posta elettronica certificata attivate

Nell'elenco che segue sono riportate le caselle di posta elettronica certificata attivate con l'indicazione di quali siano integrate nel sistema di gestione documentale e associate al registro di protocollo di ciascuna AOO, quali siano legate a funzioni di ricezione di fatture elettroniche e quali invece non siano integrate con il sistema di gestione documentale.

---

[18] Decreto Legislativo 82/2005 modificato e integrato dal Decreto Legislativo 235/2010 in vigore dal 1° gennaio 2006

[19] Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, *Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.*

Indirizzo istituzionale

- protocollo.asp.pavia@pec.it

integrata con il sistema di gestione documentale - Archivio Generale di ASP

- Collegata inoltre all'Ufficio_e FatturaPA (*ufficio centrale creato in automatico in Indice PA*)

Direzione Generale

- Maurizio.Niutta@pec.asppavia.it

Provveditorato

- Luigi.Noè@pec.asppavia.it

Ragioneria

- *Tiziano.Riccio@pec.asppavia.it*

Direzione Medica di Presidio S. Margherita

- *Marco.Rollone@pec.asppavia.it*

Direzione Medica di Presidio F. Pertusati e RSD G. Emiliani

- Filippo.Segù@pec.asppavia.it
-

8. Accesso al servizio - Caratteristiche generali

L'utilizzatore può accedere al servizio tramite *username* e *password* assegnate con apposito profilo di abilitazione al servizio di posta.

Per accedere alla casella di posta elettronica è possibile utilizzare il proprio *client* di posta elettronica,

9. Indicazioni comuni per tutte le caselle di posta certificata

Verificare l'identità del mittente e dei destinatari con i mezzi più idonei è una prassi consigliabile. A titolo di esempio si cita la possibilità di utilizzare la firma di sottoscrizione apposta su un allegato al messaggio per identificare il mittente. In nessun caso il nome della casella può costituire un indizio valido per identificare con sicurezza il titolare. Fermi restando gli obblighi normativi portare a conoscenza dei propri corrispondenti che si è in possesso di una casella di posta a valore legale, costituisce una garanzia anche per i destinatari.

Tutte le caselle di posta elettronica certificata devono avere l'archivio di sicurezza attivato sia per l'archiviazione dei messaggi inviati, sia per l'archiviazione di quelli in arrivo. L'archivio di sicurezza consente di archiviare automaticamente o selettivamente – mediante appositi criteri configurabili - la corrispondenza in ingresso ed in uscita in un archivio di *back-up* sicuro. I messaggi sono mantenuti

nell'archivio di sicurezza fino alla richiesta di cancellazione da parte dell'utente, indipendentemente dalla loro eliminazione o spostamento dalla casella. Questo permette di recuperare gli eventuali messaggi scaricati dalla casella sulla propria postazione di lavoro e successivamente persi.
L'archiviazione dei messaggi avviene dal momento in cui l'archivio è attivato. La funzione non è retroattiva e non è possibile archiviare manualmente i messaggi ricevuti prima dell'attivazione dell'archivio o non archiviati perché non corrispondenti agli eventuali criteri di archiviazione precedentemente impostati.
Per le istruzioni relative alla modalità per l'attivazione iniziale dell'archivio di sicurezza e per alla consultazione dei messaggi archiviati si faccia riferimento al "Manuale Operativo" del servizio.

È fortemente raccomandato dotare le postazioni di lavoro di un *antivirus* costantemente aggiornato per garantire maggiore sicurezza di quanto sia spedito e ricevuto. Infatti, se pure la casella è dotata di *antivirus* in grado di proteggere l'utente dai principali pericoli di infezione, non è possibile controllare automaticamente tutti i contenuti potenzialmente dannosi; in particolare si sottolinea che messaggi o *file* crittografati non possono essere sottoposti a controlli.

Rimane a cura dell'utente verificare costantemente l'aggiornamento della propria strumentazione rispetto ai criteri di sicurezza da adottare sia in termini di *antivirus* (per evitare di essere una fonte di contaminazione) sia in termini di sistemi operativi (utilizzando solo quelli che prevedono un costante aggiornamento di prevenzione alla contaminazione).

10. Caratteristiche tecniche e dimensioni

Numero massimo di destinatari cui è possibile inviare messaggi di posta certificata:

- numero massimo di destinatari diretti (to/a) 250
- numero massimo di destinatari totali (to/a e cc) 500

La dimensione massima di un messaggio di posta certificata accettabile dal gestore del servizio è di 50MB (comprende tutti gli allegati e il corpo del messaggio).

La dimensione massima complessiva degli allegati di cui è garantito l'invio per messaggi destinati a un singolo destinatario diretto (to) è di 37 MB. La dimensione di un messaggio con allegati varia inoltre in base al numero di destinatari dello stesso. Pertanto, nel caso di invio di messaggi a più destinatari al crescere del numero di destinatari il peso complessivo degli allegati deve diminuire per non superare il vincolo di 50 MB. Oltre questo limite il messaggio non può essere accettato dal gestore del servizio. In presenza di allegati e di molteplici destinatari può essere quindi necessario procedere con più invii.

11. Indicazioni specifiche per le caselle integrate con il sistema di gestione documentale

Le caselle di posta elettronica certificata integrate con il sistema di gestione documentale non devono mai essere utilizzate direttamente – senza passare dal sistema documentale - né attraverso un *client* di posta né attraverso un *browser* internet per effettuale 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.

12. Indicazioni specifiche per le caselle non integrate con il sistema di gestione documentale

Per un corretto utilizzo delle caselle di posta certificata si suggerisce all'operatore cui è affidato l'accesso alla casella PEC di una specifica UOR dell'ASP non integrata con il sistema di gestione documentale di consultare frequentemente la casella; infatti ogni messaggio ricevuto nella casella di posta elettronica certificata si intende pervenuto al titolare della casella stessa, anche quando non sia ancora stato letto. L'emissione della ricevuta di consegna al mittente non è legata al fatto che il destinatario apra il messaggio o meno ed è rilasciata comunque quando il messaggio è depositato in casella.

È bene gestire il contenuto della casella – anche cancellando i messaggi ricevuti e già gestiti - a condizione che sia stato attivato l'archivio di sicurezza. Ciò permette di evitare che lo spazio assegnato alla casella sia saturato e che i messaggi successivi vengano rifiutati.

Titolario di classificazione unico in vigore dal

Allegato n. 8 – Elenco repertori

Repertori dell'AOO Amministrazione centrale

- Albo on line
- Contratti di lavoro
- Contratti e convenzioni (soggetti a registrazione in caso d'uso)
- Contratti in forma pubblica amministrativa (Ufficiale rogante)
- Determine del Direttore Generale
- Deliberazioni del Consiglio di Indirizzo
- Libri contabili
- Protocollo particolare (partenza, tra uffici e arrivo)
- Rapporto di versamento
- Registro informatico giornaliero di protocollo
- Verbali del Consiglio di amministrazione

Repertori delle altre AOO

- Contratti e convenzioni (soggetti a registrazione in caso d'uso)
- Decreti
- Protocollo particolare (partenza e arrivo)
- Registro informatico giornaliero di protocollo
- Verbali Comitato tecnico scientifico
- Verbali ATS

Allegato n. 9 – Modalità di pubblicazione all'albo on line

Dal 1° gennaio 2015, in applicazione della normativa vigente, è attivo il repertorio dell'Albo on line, associato al protocollo dell'Amministrazione Centrale, unico per tutte le aree organizzative omogenee dell'ASP.
L'indirizzo dell'Albo on line è riportato sulla pagina iniziale del sito istituzionale di ASP e rimanda a una sezione dedicata.
Vanno pubblicati all'Albo on line i documenti previsti dall'ordinamento e quelli da cui possono nascere diritti, doveri, aspettative o interessi legittimi di terzi e dalla cui diffusione nei confronti di una indistinta pluralità di soggetti potenzialmente interessati dipende la loro efficacia.
La gestione dell'Albo on line è affidata all'ufficio di Statistica di ASP, mentre spettano al responsabile del procedimento amministrativo la verifica della regolarità tecnico amministrativa dell'atto, l'adozione di eventuali accorgimenti per la protezione dei dati personali e la definizione della durata della pubblicazione.
I documenti da pubblicare, redatti su carta intestata della struttura proponente e in formato pdf, dovranno essere inoltrati esclusivamente all'indirizzo e-mail uff.statistica_rp@asppavia.it entro le ore 13.00. I documenti pervenuti oltre tale orario saranno pubblicati il giorno lavorativo successivo.
L'e-mail di richiesta dovrà indicare la data di inizio della pubblicazione, la durata espressa in giorni e la data di termine della pubblicazione stessa.
La durata della pubblicazione è di quindici giorni consecutivi salvo diverse disposizioni legislative, regolamentari e provvedimentali. Nel caso in cui si richieda la pubblicazione per un periodo inferiore o superiore sarà necessario indicare la motivazione.