MANUALE DI GESTIONE DOCUMENTALE

Sommario

1 PRINCIPI GENERALI

1.1 Il Manuale di gestione documentale

Il manuale di gestione documentale è uno strumento operativo che descrive il sistema di produzione e di gestione dei documenti (analogici e digitali), come previsto dalle Linee guida sulla formazione, gestione e conservazione dei documenti informatici di cui alla determinazione n. 371 del 17 maggio 2021 dell'Agenzia per l'Italia digitale (d'ora in poi Linee guida AgID), con la quale è stata modificata e integrata la precedente determinazione n. 407 del 9 settembre 2020.

Le Linee guida AgID hanno lo scopo di aggiornare le regole tecniche in base all'art. 71 del Codice dell'amministrazione digitale (CAD) sulla formazione, protocollazione, gestione e conservazione dei documenti informatici, incorporandole insieme alle circolari in materia in un'unica linea guida, addivenendo ad un "unicum" normativo che disciplini gli ambiti sopra citati, nel rispetto della disciplina in materia di beni culturali.

Nel dettaglio, il Manuale descrive le procedure e fornisce 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'Azienda Regionale di Coordinamento per la Salute (ARCS) secondo parametri di corretta registrazione di protocollo, smistamento, assegnazione, classificazione, fascicolatura, reperimento e conservazione dei documenti, nel rispetto della normativa vigente in materia di trasparenza degli atti amministrativi, di tutela della privacy e delle politiche di sicurezza.

Il Manuale è destinato alla più ampia diffusione interna ed esterna. Costituisce, infatti, sia una guida interna non solo per l'operatore di protocollo e per i responsabili dei procedimenti amministrativi, ma per tutti i dipendenti, sia un vademecum ai soggetti esterni che si relazionano con ARCS per comprendere e per collaborare nella gestione documentale stessa (ad es. utilizzando formati idonei per la formazione delle istanze, etc.).

1.2 Modalità di approvazione e aggiornamento

Il responsabile della gestione documentale, d'intesa con il responsabile della conservazione e il responsabile per la transizione digitale, acquisito il parere del responsabile della protezione dei dati personali, predispone il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione.

Il manuale deve essere aggiornato periodicamente effettuando il censimento delle attività/prassi in essere, la razionalizzazione delle stesse, l'individuazione e la definizione degli aspetti organizzativi e gestionali in termini di fasi, tempi e risorse umane impegnate nell'automazione dei flussi documentali nel rispetto della normativa.

Ogni evento suscettibile di incidere sull'operatività ed efficacia del manuale medesimo deve essere tempestivamente segnalato al responsabile della gestione documentale, al fine di prendere gli opportuni provvedimenti in ordine all'eventuale modifica e/o integrazione della procedura stessa.

1.3 Forme di pubblicità e divulgazione

La Pubblica Amministrazione è tenuta a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale.

Il presente Manuale è reso pubblico mediante la diffusione sul sito web istituzionale, come previsto dalla Linee guida AgID nella sezione "Amministrazione trasparente":

https://arcs.sanita.fvg.it/it/arcs/amministrazione-trasparente/disposizioni-generali/atti-generali/atti-amministrativi-generali/

Il Manuale deve, inoltre, essere capillarmente divulgato alle unità organizzative responsabili (UOR) dell'unica area organizzativa omogenea (AOO) dell'Azienda Regionale di Coordinamento per la Salute, al fine di consentire la corretta diffusione delle nozioni e delle procedure documentali.

1.4 Definizioni e acronimi

AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005 e ss.mm.ii.)
D.L.	Decreto-legge
D.Lgs.	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPO	*Data Privacy Officer*
DPR	Decreto del Presidente della Repubblica
GDPR	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
IPA	Indice delle Pubbliche Amministrazioni
PEC	Posta Elettronica Certificata
PEO	Posta Elettronica Ordinaria
RPD	Responsabile della protezione dei dati
RPCT	Responsabile per la prevenzione della corruzione e della trasparenza
RUP	Responsabile unico del procedimento
UOP	Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo
UOR	Unità Organizzativa Responsabile

Per quanto riguarda ulteriori definizioni dei termini e degli acronimi, che costituiscono la corretta interpretazione del dettato del presente manuale, si rimanda al Glossario dei termini e degli acronimi (allegato 1 alle Linee Guida AGID).

2 ASPETTI ORGANIZZATIVI

2.1 Area Organizzativa Omogenea (AOO)

Ai fini di una gestione documentale unitaria e coordinata, l'Amministrazione ha individuato una sola area organizzativa omogenea (AOO) denominata "Protocollo generale", composta dall'insieme di tutte le sue strutture ed in cui è istituito un unico servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

All'interno dell'AOO il sistema di protocollazione è unico e segue un modello distribuito: le procedure di registrazione in arrivo avvengono a cura di nuclei di protocollazione incardinati nell'ufficio di protocollo centrale (PEC primaria) e in altre strutture dell'Azienda (PEC secondarie); anche la protocollazione in uscita avviene a cura dei protocollisti abilitati nell'ambito delle diverse strutture dell'Azienda.

Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del Responsabile del servizio di gestione documentale e del Responsabile della Struttura di competenza della PEC secondaria.

Alla AOO ARCS fano capo anche le Unità organizzative responsabili (UOR) descritte nell'allegato 2.

Le UOR sono definite con riferimento all'organigramma e funzionigramma dell'Azienda disponibile al link: https://arcs.sanita.fvg.it/it/arcs/amministrazione-trasparente/organizzazione/articolazione-degli-uffici-copy/ e possono essere oggetto di modifiche e integrazioni per effetto degli interventi sulla struttura organizzativa. A ciascuna UOR è affidata una competenza omogenea nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari, attività e procedimenti amministrativi.

In relazione al modello di riferimento e alle strategie organizzative vengono anche valutate le responsabilità, i ruoli e i permessi applicativi per la gestione del flusso (registrazione dei documenti e assegnazione alle strutture competenti) e l'archiviazione della documentazione (creazione, alimentazione e ricerca dei fascicoli) tramite *GIFRA*.

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

Nella AOO precedentemente individuata è istituito un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi presso la SC Affari generali. Il servizio ha competenza sulla gestione dell'intera documentazione archivistica, ovunque trattata, distribuita o conservata dall'Azienda, ai fini della sua corretta registrazione, classificazione, conservazione, selezione e ordinamento; vigila sull'osservanza degli adempimenti previsti in ambito archivistico dalla normativa in materia di gestione documentale durante l'intero ciclo di vita dei documenti.

Alla guida del servizio è posto il Responsabile della gestione documentale. Le altre figure che concorrono ad assicurare un trattamento uniforme dei documenti, una puntuale applicazione delle disposizioni ed un periodico monitoraggio delle modalità d'uso degli strumenti di gestione documentale sono:

- il Responsabile della conservazione;
- il Responsabile per la transazione digitale;
- il Servizio Tecnologie informatiche;
- il Responsabile per la prevenzione della corruzione e della trasparenza;
- il Responsabile della protezione dei dati.

Tutti gli accessi al sistema di protocollo e gestione documentale sono nominativi e ciascun utente è autenticato da un sistema centralizzato; tutte le operazioni effettuate sono registrate con l'indicazione della persona, della data, dell'ora e della descrizione dell'operazione.

Tutti i dipendenti sono utenti del sistema di gestione documentale, con la possibilità di ricevere assegnazioni documentali sulle quali operare. Ciascun dirigente ha pieno controllo del flusso documentale del proprio ufficio e svolge attraverso il sistema di gestione documentale le funzioni di

direzione, coordinamento e controllo dell'attività degli uffici, comprensive dei poteri sostitutivi, ove previsti.

I dipendenti hanno l'obbligo di consultare almeno quotidianamente il sistema di gestione documentale, poiché attraverso di esso sono effettuate le comunicazioni, le notifiche e le assegnazioni dei procedimenti. Le registrazioni del sistema hanno carattere probatorio e sono consultabili in ogni momento dagli interessati.

2.3 Unicità del Protocollo informatico

La numerazione delle registrazioni di protocollo è unica, progressiva, corrisponde all'anno solare ed è composta da almeno sette numeri, tuttavia sono possibili registrazioni particolari (sezione "Documenti soggetti a Registrazione Particolare" del presente Manuale).

Ad ogni documento è dato un solo numero, che non può essere utilizzato per la registrazione di altri documenti anche se correlati allo stesso.

Il sistema informatico di gestione del protocollo è sincronizzato per il calcolo dell'ora con il server di gestione.

Il software utilizzato dall'ARCS per la gestione documentale è denominato GIFRA. Tutti gli accessi al sistema di protocollo e gestione docu- mentale sono nominativi e ciascun utente è autenticato da un sistema centralizzato; tutte le opera- zioni effettuate sono registrate con l'indicazione della persona, della data, dell'ora e della descrizione dell'operazione.

Tutti i dipendenti sono utenti del sistema di gestione documentale, con la possibilità di ricevere assegnazioni documentali sulle quali operare. Ciascun dirigente ha pieno controllo del flusso documentale del proprio ufficio e svolge attraverso il sistema di gestione documentale le funzioni di direzione, coordinamento e controllo dell'attività degli uffici, comprensive dei poteri sostitutivi, ove previsti.

2.4 Ruoli e responsabilità

Responsabile della gestione documentale

Il Responsabile della gestione documentale è funzionalmente nominato con atto del Direttore Generale. Al servizio è preposto un dirigente o un incaricato di funzione, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.

In ogni AOO si individuano uno o più vicari del Responsabile della gestione documentale, per i casi di vacanza, assenza o impedimento di quest'ultimo, con idonea preparazione e competenza nella materia in argomento.

È compito del Responsabile della gestione documentale:

- predisporre e mantenere aggiornato il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici, nel rispetto della normativa in materia di trattamento dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione, e d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali;
- definire e assicurare criteri uniformi di trattamento dei documenti e di classificazione e archiviazione;
- garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi, incluse le funzionalità di accesso e le attività di gestione degli archivi anche in relazione alla selezione e allo scarto;
- garantire che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
- garantire la corretta produzione e la conservazione del registro giornaliero di protocollo;
- autorizzare le operazioni di annullamento;
- verificare l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA;
- formare correttamente la documentazione che andrà a costituire il pacchetto di versamento (PdV) e assicurare la sua trasmissione al sistema di conservazione con i formati concordati con il conservatore e secondo le modalità operative descritte nel manuale di conservazione del sistema di conservazione;
- cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate nel più breve tempo possibile;
- prevede 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, in accordo con i Responsabili delle Strutture dell'Azienda.

Responsabile della conservazione

Il Responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

In particolare, il Responsabile della conservazione:

- definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un Conservatore, le attività suddette o alcune di esse, ad esclusione dell'ultima, potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al Responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in *outsourcing* dalle Pubbliche Amministrazioni.

Il nominativo ed i riferimenti del Responsabile della conservazione devono essere indicati nelle specifiche del contratto o della convenzione di servizio con il Conservatore, nel quale sono anche riportate le attività affidate al Responsabile del servizio di conservazione.

Responsabile per la transazione digitale

Il Codice dell'amministrazione digitale impone a tutte le Pubbliche amministrazioni di nominare un dirigente responsabile per la transizione digitale.

Al Responsabile competono tutte le attività operative finalizzate alla transizione e i conseguenti processi di riorganizzazione funzionali alla realizzazione di un'Amministrazione digitale e aperta; all'erogazione di servizi facilmente utilizzabili e di qualità; al raggiungimento di migliori standard di efficienza ed economicità. Il Responsabile ha poteri di impulso e coordinamento e deve assicurare il rispetto degli obblighi previsti dalla normativa vigente.

In particolare, il Responsabile della transazione digitale è:

- referente IPA (indice delle pubbliche amministrazioni) per l'ARCS, con il compito di tenere aggiornati i propri dati all'interno del portale ovvero di interagire con il Gestore IPA per l'inserimento e la modifica dei dati dell'Amministrazione, nonché per ogni altra questione riguardante la presenza dell'Amministrazione nell'IPA.

Servizio Tecnologie informatiche

È compito delle Tecnologie informatiche:

- abilitare gli addetti dell'amministrazione all'utilizzo del Protocollo informatico (GIFRA) secondo le funzioni standard di abilitazione (ad esempio consultazione, modifica, etc.) a seguito di richiesta del Responsabile della Struttura di afferenza
- configurazione degli elementi della struttura organizzativa dell'AOO ARCS (struttura GIFRA).

Il Responsabile per la prevenzione della corruzione e della trasparenza è il soggetto al quale può essere presentata l'istanza di accesso civico, qualora la stessa abbia ad oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013 (allegato 7).

Il RPCT, oltre a segnalare i casi di inadempimento o di adempimento parziale degli obblighi in materia di pubblicazione previsti dalla normativa vigente, si occupa delle richieste di riesame dei richiedenti ai quali sia stato negato totalmente o parzialmente l'accesso civico generalizzato, ovvero che non abbiano avuto alcuna risposta entro il termine stabilito.

Responsabile della protezione dei dati (RPD) o *Data Privacy Officer* (DPO)

Il Responsabile della protezione dei dati è il soggetto nominato con apposito decreto del Direttore generale e ha il compito di sorvegliare sull'osservanza della normativa in materia di protezione dei dati personali, ossia il Regolamento UE 679/2016 (di seguito, anche "GDPR") e il D.Lgs. 196/2003 (di seguito, anche "Codice privacy"), come modificato dal D.Lgs. 101/2018.

Il Responsabile della protezione dei dati deve essere coinvolto in tutte le questioni che riguardano la gestione e la protezione dei dati personali.

Sono compiti propri del DPO:

- informare e sensibilizzare il personale dell'Azienda riguardo agli obblighi derivanti dalla citata normativa;
- di concerto con il Responsabile del servizio protocollo individua i documenti che, in ragione della necessità di protezione dei dati/informazioni ivi contenuti, sono sottratti alla procedura di scansione ovvero soggetti a registrazione particolare.

Le nomine

Le nomine delle suddette figure di responsabilità sono elencate all'allegato 5.

2.5 Caselle di Posta Elettronica Certificata (PEC) e Posta Elettronica Ordinaria (PEO)

L'AOO è dotata di una casella di posta elettronica certificata primaria e due caselle di posta elettronica secondaria, per la corrispondenza, sia in ingresso che in uscita. Tali caselle costituiscono l'indirizzo virtuale della AOO.

Ad ogni casella di posta elettronica certificata, integrata nel sistema di protocollo, corrisponde un punto di protocollazione. La responsabilità della registrazione della corrispondenza è affidata al Responsabile della Struttura incaricata.

Gli indirizzi PEC sono pubblicati sull'Indice delle Pubbliche Amministrazioni (IPA)a cura del Responsabile della transazione digitale. L'amministrazione comunica, attraverso il suo referente, tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa, in modo da garantire l'affidabilità dell'indirizzo di posta elettronica. Con la stessa tempestività l'amministrazione comunica la soppressione, ovvero la creazione di una nuova PEC.

Per quanto non espressamente qui specificato si rimanda alla Policy ARCS per l'utilizzo delle risorse informatiche.

Indirizzi istituzionali, integrati con il sistema di gestione documentale (allegato 3):

PEC istituzionale primaria

- arcs@certsanita.fvg.it

PEC istituzionali secondarie

- ceur@certsanita.fvg.it
- sores@certsanita.fvg.it

3 IL DOCUMENTO

3.1 Documento informatico e analogico: definizione e disciplina giuridica

Il documento elettronico è qualsiasi contenuto in formato digitale, come un'email, un testo, una foto o una registrazione sonora, visiva o audiovisiva. (ad es. la scansione di un contratto).

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.

Secondo quanto disposto dall'articolo 3 del Regolamento "*electronic IDentification Authentication and Signature*" - Regolamento UE 910/2014 (d'ora in poi "Regolamento eIDAS"), per firma elettronica si devono intendere i dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.

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 (art. 2712 Codice civile, art. 23-quater CAD, art. 2713 Codice civile).

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 elettronica 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** o 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 di firma digitale 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 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.

Si precisa che tutti i contratti stipulati dall'Azienda Regionale di Coordinamento per la Salute, anche quando quest'ultima agisce *iure privatorum*, richiedono la forma scritta *ad substantiam*.

L'Azienda ha stabilito che i propri documenti siano predisposti secondo quanto descritto nel *Manuale di stile* dell'ARCS, che consente, attraverso un'immagine aziendale coerente e sistemica, una riconoscibilità istantanea, attraverso la pianificazione e l'adizione di un set coordinato di colori, modelli e schemi.

3.1.1 Firma Digitale

La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

La firma digitale è un'operazione con la quale si genera un codice crittografico che dimostra l'identità e l'integrità di un documento. In altre parole, la firma digitale permette di verificare che il documento:

- è stato firmato da una ben precisa persona
- successivamente, non ha subito modifiche

La Firma Digitale viene effettuata, di norma, mediante l'utilizzo della carta operatore, per cui si rimanda alla Policy ARCS per l'utilizzo delle risorse informatiche.

3.2 Redazione/Formazione del documento informatico

Il documento informatico è formato mediante una delle seguenti modalità:

a) 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;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico: 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;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico deve essere identificato in modo univoco e persistente. L'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento.

L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti. Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immodificabilità e l'integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza;
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS, valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento a un sistema di conservazione.

Nel caso di documento informatico formato secondo le sopracitate lettere c) e d) le caratteristiche di immodificabilità e di integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
- produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente a esso i relativi metadati di cui all'allegato 5 alle Linee guida.

La disponibilità e la riservatezza delle informazioni contenute nel documento informatico sono garantite attraverso l'adozione di specifiche politiche e procedure predeterminate dall'ARCS, in conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali.

L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'allegato 2 alle Linee guida.

3.2.1 Validazione temporale

Costituiscono validazione temporale:

- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata;
- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica;
- 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 a un minuto primo;
- 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.

3.2.2 Formati

Il formato del file è il mezzo con cui vengono rappresentati i documenti informatici oggetto di creazione, elaborazione, ricezione, condivisione e conservazione.

I documenti informatici devono essere prodotti con formati che garantiscano la loro leggibilità e la loro reperibilità e inalterabilità durante le fasi di accesso e conservazione, assicurando l'immutabilità nel tempo del loro contenuto e della loro struttura. Allo stesso modo, i formati adottati devono rispondere ai requisiti generali per l'interoperabilità.

A tal fine, l'ARCS impiega formati conformi a quanto stabilito nell'allegato n. 2 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici. In particolare, i documenti informatici dell'Azienda sono prodotti con l'ausilio di applicativi di videoscrittura o text editor preferibilmente nei formati PDF-A e XML che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

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.

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico.

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 § 3.2 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 identificati e trattati nel sistema di gestione informatica dei documenti e, ove necessario, soggetti a registrazione di protocollo, segnatura, fascicolatura e repertoriazione.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità descritte in precedenza per il documento informatico, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenuti nel sistema di gestione documentale.

Al documento amministrativo informatico vengono associati l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA, i metadati relativi alla classificazione ai sensi dell'articolo 56 del TUDA e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.

3.4 Redazione e formazione del documento ammnistrativo analogico

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

Nell'attività amministrativa, di norma il documento analogico è un documento formato su supporto analogico prodotto con strumenti analogici (ad esempio, documento scritto a mano) o con strumenti informatici (ad esempio, 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 terzo 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 autografa, conservato agli atti dell'Azienda, cioè nel fascicolo relativo al procedimento amministrativo o all'affare trattato.

In questi casi il documento va scansionato e acquisito all'interno del sistema di gestione documentale per la protocollazione informatica.

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 esempio, i verbali di una riunione o di un'assemblea).

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

3.6 Il documento amministrativo informatico costituito dal corpo della PEC istituzionale

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

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

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

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

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

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

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

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

Le *e-mail* inviate da una casella istituzionale dell'Azienda 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, 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, "tra uffici" (scambiati tra UOR).

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 è ricevuto e trasmesso per posta elettronica interna e di norma le comunicazioni non sono protocollate.

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale – PEC – accessibile esclusivamente dall'Ufficio Protocollo e le altre caselle PEC dell'Azienda accessibili all'Unità Organizzativa responsabile della protocollazione in arrivo integrate nel sistema documentale dell'ARCS.

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.

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 Linee guida AgID;
- sono formate nel rispetto delle Linee guida AgID 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.

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 auto-sufficiente né auto-esplicativa, ma deve sempre e necessariamente documentare sé 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.

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, etc.);
- garantire l'identificazione permanente delle relazioni tra gli oggetti informativi, ad es., indici di classificazione e fascicolatura;
- conservare le informazioni che supportano l'intellegibilità degli oggetti informativi, ad es., procedimento amministrativo cui il documento è connesso.

3.14.2 Metadati essenziali per la registrazione nel protocollo informatico

Gli elementi essenziali minimi sono i seguenti:

- identificativo;
- denominazione / codice unico che individua l'Ente;
- corrispondente (mittente/destinatari);
- oggetto;
- numero degli allegati e descrizione degli stessi;

- numero di protocollo;
- data di registrazione a protocollo;
- indicazione dell'Unità organizzativa responsabile (UOR);
- impronta che lega il documento digitale ai metadati sopra indicati.

4 FORMATO DEI DOCUMENTI

L'Azienda Regionale di Coordinamento per la Salute utilizza per la formazione e per la gestione dei documenti informatici tipologie di formato coerenti con quanto indicato nell'Allegato 2 delle *Linee guida* AgID e tali da garantire i principi di interoperabilità tra i sistemi di conservazione in base alla normativa vigente.

Il "formato" del file è il mezzo con cui vengono rappresentati i documenti informatici oggetto di creazione, elaborazione, ricezione, condivisione e conservazione.

La scelta del formato è stata effettuata considerando che essa deve garantire la leggibilità e la reperibilità del documento informatico nell'intero ciclo di vita dello stesso e, ove pertinente e tecnicamente possibile, l'interoperabilità tra sistemi differenti.

Per la natura stessa dell'argomento trattato, quanto individuato potrà essere periodicamente oggetto di aggiornamento sulla base dell'evoluzione tecnologica e dell'obsolescenza degli strumenti software disponibili oltre che degli standard internazionali in essere (formali o *de facto*).

Riguardo la scelta dei font da utilizzare, l'ente si avvale del *Manuale di stile*.

4.1 Eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi

Ogni eventuale ulteriore formato di file, viene ammesso esclusivamente a fini specifici e particolari, per un uso esclusivamente interno dell'ufficio o della persona che utilizza il software che lo genera.

4.2 Procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento

Le procedure per la valutazione periodica di interoperabilità dei formati e le procedure di riversamento sono demandate ai gestori incaricati della conservazione documentale.

5 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.

Per la gestione dei documenti, l'ARCS ha individuato un'unica Area Organizzativa Omogenea - AOO al cui interno il registro di protocollo è unico ed ha cadenza annuale: inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Il protocollo informatico assicura il tracciamento e la storicizzazione di ogni operazione, comprese le operazioni di annullamento, e la loro attribuzione all'operatore.

Ai sensi del punto 3.1.5 delle Linee guida AgID il sistema di protocollo informatico assicura che:

- le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista dall'art. 54 del TUDA;
- le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
- le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
- per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema storicizzi tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili, nel rispetto di quanto previsto dall'art. 54, comma 2 del TUDA.

5.1 Modalità di utilizzo della componente "sistema di protocollo informatico"

L'ARCS utilizza l'applicativo GIFRA – Gestione Integrata Flussi e Registrazione Atti, fornito da INSIEL, società ICT in house della Regione Friuli-Venezia Giulia.

Per la registrazione, trattazione e ricerca dei documenti all'interno di GIFRA sono presenti tre applicativi integrati denominati:

1) Protocollo:
    - consente la registrazione dei documenti in entrata ed uscita;
    - la creazione / modifica delle anagrafiche dei corrispondenti;
    - lo smistamento dei documenti alle UOR;

- la creazione dei fascicoli e l'inserimento dei documenti negli stessi contestualmente alla classificazione.

2) IterAtti

   Mette a disposizione funzionalità orientate alla gestione dei flussi documentali e permette di acquisire e visualizzare i documenti assegnati ad una UOR e ad un operatore, di predisporre nuovi atti, trasmetterli ad altri operatori per la trattazione nell'ambito dell'istruttoria, consente al responsabile del procedimento di firmare digitalmente i documenti, protocollarli, trasmetterli telematicamente e di gestire i fascicoli.

3) Visura

   Permette di visualizzare tutti i documenti di competenza della propria struttura già protocollati attraverso molteplici funzionalità di ricerca.

   La descrizione funzionale del protocollo informatico è costituita dal Manuale Utente, fornito dalla ditta produttrice del sistema, aggiornato alla release in uso.

5.2 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'Azienda, 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. Il registro dove sono annotati cronologicamente i documenti soggetti a registrazione particolare è detto "repertorio" e la numerazione di ciascun repertorio si rinnova ogni anno solare.

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'Azienda, 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 Responsabile della gestione documentale e a persone espressamente delegate.

L'inalterabilità e l'immodificabilità della registrazione di protocollo sono garantite dal sistema di gestione documentale.

In nessun caso gli operatori di protocollo sono autorizzati a riservare numeri di protocollo per documenti non ancora resi disponibili.

5.2.1 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 e costituito da almeno sette cifre numeriche, generato automaticamente dal sistema;
- data di registrazione, assegnata automaticamente dal sistema;
- 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;
- data e protocollo del documento ricevuto, se disponibili.

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

5.2.2 Elementi obbligatori modificabili

Gli elementi obbligatori modificabili sono:

- unità organizzativa responsabile del procedimento/affare/attività (UOR);
- responsabile del procedimento amministrativo (RPA);
- classificazione archivistica;
- fascicolo.

5.2.3 Elementi non obbligatori modificabili

Gli elementi non obbligatori modificabili sono:

- recapiti del mittente;
- collegamento ad altri documenti o fascicoli diversi da quello d'inserimento;
- tipologia di documento;
- durata della conservazione;
- altri tipi di annotazioni (ad esempio, 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).

Qualora l'oggetto di un documento pervenuto:

- includa diciture automatiche di risposta (ad es. RE:, I: FW:, FWD:, POSTA CERTIFICATA:, etc.): è consentito modificare l'oggetto del documento pervenuto eliminando le diciture automatiche di risposta;
- è totalmente mancante: è consentito inserire termini utili per la sua comprensione o per garantire il reperimento in fase di ricerca;
- è estremamente fuorviante rispetto all'effettivo contenuto del documento (ad es. da protocollare, gentili, etc.): è consentito modificare l'oggetto del documento pervenuto eliminando le diciture fuorvianti inserendo termini utili per la sua comprensione o per garantire il reperimento in fase di ricerca.

Nel caso in cui, inoltre, l'oggetto di un documento pervenuto applicativa non sia corretto nei contenuti o non contenga tutti i termini utili per la sua comprensione o per garantirne il reperimento in fase di ricerca, è consentito integrare/completare le informazioni pervenute inserendole nell'apposito campo suppletivo "oggetto protocollo".

5.2.4 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.

5.3 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.

5.3.1 Per il documento informatico

Le informazioni minime associate al documento informatico sono:

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

Oltre alle informazioni minime la segnatura include:

- 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 (si veda l'allegato 6 alle Linee guida), purché siano adottate idonee modalità di formazione dello stesso in formato PDF/A.

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. Attraverso le funzionalità previste dall'applicativo IterAtti, il sistema documentale appone le informazioni di registrazione in modo visibile sul documento sottoscritto attraverso un *layer*, che nel pannello di verifica della firma appare come annotazione o commento.

5.3.2 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;
- 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.

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

La segnatura su un documento cartaceo viene apposta mediante timbro meccanico che riporta gli elementi normalizzati della segnatura, trascritti dall'operatore di protocollo a penna all'interno degli spazi predisposti.

5.4 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 etc.), 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.

5.5 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.

La registrazione differita non si applica per i documenti informatici pervenuti via PEC, in quanto la PEC ha lo stesso valore giuridico della raccomandata A/R e quindi fa fede la data di invio della PEC allo stesso modo del timbro postale di invio della raccomandata A/R.

5.6 Termini per la registrazione di protocollo

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e comunque non oltre 24 ore lavorative dal ricevimento, nel caso di oggettive impossibilità.

5.7 La ricevuta di avvenuta registrazione

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

- il numero e la data di protocollo;
- l'indicazione della UOR 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.

5.7.1 Per il documento analogico

Gli addetti alle UOP non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione.

La semplice apposizione del timbro datario della UOP per la tenuta del protocollo sulla copia non ha alcun valore giuridico e non comporta alcuna responsabilità del personale della UOP in merito alla ricezione ed all'assegnazione del documento.

Quando il documento cartaceo è consegnato direttamente dal mittente, o da altra persona incaricata alla UOP, ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, la UOP che lo riceve è autorizzata a:

- fotocopiare gratuitamente la prima pagina del documento;
- apporre gli estremi della segnatura se contestualmente alla ricezione avviene anche la protocollazione;
- apporre sulla copia così realizzata il timbro dell'amministrazione, con la data e l'ora d'arrivo e la sigla dell'operatore.

Nel caso di corrispondenza pervenuta ad una UOR, questa deve consegnarla alla UOP allo scopo di ottenere una ricevuta valida.

5.8 Documenti esclusi dalla registrazione di protocollo

Sono esclusi dalla registrazione di protocollo i documenti di cui all'art. 53, comma 5, del TUDA, ovvero:

- le gazzette ufficiali;
- i bollettini ufficiali della pubblica amministrazione;
- i notiziari della pubblica amministrazione;
- le note di ricezione delle circolari;
- le note di ricezione di altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali;
- le riviste;
- i libri;
- i materiali pubblicitari;
- gli inviti a manifestazioni.
- tutti i documenti già soggetti a registrazione particolare dell'amministrazione.

5.9 Documenti soggetti a Registrazione Particolare

Nell'allegato 6 sono riportati i documenti esclusi dalla registrazione di protocollo generale e soggetti a registrazione particolare. Tale tipo di registrazione deve consentire comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertoriazione.

5.10 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.

Gli elementi memorizzati nel registro giornaliero di protocollo sono descritti nel manuale di conservazione (allegato 8) adottato dall'ente ed afferiscono alla classe documentale (allegato 9) denominata REGPROT.

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

5.11 Il registro di emergenza

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

Al termine dell'emergenza, il Responsabile della gestione documentale, chiude il registro e dà contestuale comunicazione della revoca dell'emergenza.

Il registro viene predisposto su postazioni di lavoro operanti fuori rete e, nel caso in cui il normale utilizzo del protocollo sia impedito dalla mancanza di energia elettrica, viene utilizzato un registro di emergenza in formato cartaceo.

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 (allegato 4).

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

Sul registro di emergenza devono essere riportati gli estremi del provvedimento di autorizzazione.

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.

Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite sul registro di protocollo generale. Al ripristino della funzionalità del sistema le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati.

Durante la fase di ripristino, a ciascun documento protocollato nel registro di emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, continuando la numerazione di protocollo raggiunta al momento di interruzione del servizio.

Il sistema provvede a mantenere stabilmente la correlazione tra il numero utilizzato in emergenza ed il numero di protocollo generale. 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.

Per la decorrenza dei termini del procedimento amministrativo si fa riferimento alla data in cui è stata effettuata la protocollazione sul registro di emergenza, in modo da assicurare la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

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

Il registro di emergenza è conservato con le stesse modalità del registro ufficiale.

6 FLUSSI DI LAVORAZIONE DEI DOCUMENTI

6.1 Descrizione della lavorazione del flusso documentale

Per la gestione dei documenti è adottato un modello organizzativo di tipo decentralizzato sia per la corrispondenza in entrata sia per la corrispondenza in uscita.

Nello specifico, l'Ufficio Protocollo svolge i compiti di UOP principale dell'Azienda per la corrispondenza in entrata, ovvero provvede alla protocollazione degli atti pervenuti attraverso la PEC istituzionale principale. Le altre UOP, invece, provvedono alla protocollazione in entrata della corrispondenza pervenuta alle PEC secondarie di propria competenza.

La corrispondenza in uscita viene protocollata e classificata dalla UOR competente per materia del documento. La scelta di un modello decentrato - riguardo alla protocollazione in uscita - risiede nell'esigenza di attribuire autonomia agli Uffici, anche in ragione della numerosità degli atti prodotti dal personale dell'Azienda nell'ambito delle proprie competenze, e trasmessi a soggetti esterni. Per la spedizione della documentazione cartacea ci si avvale dell'Ufficio Protocollo. In tal caso, la documentazione va predisposta a cura della UOR competente.

I documenti pervenuti vengono registrati nel protocollo informatico al dine di garantire:

- la registrazione di protocollo, cioè l'attività di memorizzazione dei dati necessari a conservare le informazioni per ogni documento ricevuto o spedito;
- la produzione della segnatura di protocollo, cioè l'apposizione o l'associazione dall'originale del documento, in forma permanente non modificabile, dei metadati riguardanti il documento stesso funzionali alla ricezione o spedizione.

l personale assegnato alle UOP provvede alla ricezione ed all'apertura della posta, nonché alla segnatura, classificazione ed assegnazione del documento alla UOR competente.

I documenti amministrativi in arrivo possono pervenire con diverse modalità:

- tramite posta elettronica ordinaria (*e-mail*);
- tramite posta elettronica certificata (PEC);
- tramite servizio postale o corriere;
- con consegna a mano;
- altri applicativi.

6.1.1 Documenti ricevuti in forma analogica

I documenti analogici che pervengono a mezzo posta sono sottoposti dal personale addetto ad una preliminare verifica in merito all'indirizzo, al destinatario sugli stessi apposti e alla pertinenza della consegna all'ARCS.

Il personale dell'UOP provvede alla scannerizzazione del documento, con acquisizione del relativo file nel sistema informatico, alla registrazione e all'assegnazione alla UOR di competenza, individuata in base al modello delle competenze. La busta si allega al documento per la parte relativa ai timbri postali.

Il processo di scansione si articolerà di massima nelle seguenti fasi:

- acquisizione delle immagini in modo che a ogni documento, anche composto da più fogli, corrisponda un unico file in un formato standard abilitato alla conservazione;

- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei.

Qualora i documenti facciano riferimenti a comunicazioni intercorse ricerca nel sistema informatico i precedenti e durante la registrazione istituisce un legame tra i documenti attraverso la funzione "Precedenti".

Durante la registrazione nel sistema informatico vanno inseriti i metadati identificativi del documento e si riporta sul documento analogico il numero di protocollo assegnato dal sistema.

È ammessa la consegna dei documenti da parte di una persona diversa dal sottoscrittore senza alcuna delega.

Su quanto accolto non viene effettuato alcun controllo di merito in relazione al procedimento amministrativo di riferimento, attività di competenza della UOR responsabile.

Alla corrispondenza non soggetta a protocollazione va apposto un timbro meccanico con l'intestazione "Azienda Regionale di Coordinamento per la Salute" con la data di ricezione.

I documenti ricevuti dall'Azienda in formato cartaceo, una volta concluse le operazioni di smistamento, registrazione e segnatura, vengono collocati nel casellario della posta in arrivo, ubicato presso l'Ufficio Protocollo, per la successiva consegna o successivo ritiro alla/dalla UOR di competenza.

6.1.2 Documenti ricevuti in forma digitale

La ricezione dei documenti informatici è assicurata tramite le caselle istituzionali (primaria e secondarie) di posta elettronica certificata (PEC) riservate a questa funzione, integrate con il sistema informatico ed accessibili solo da parte del personale preposto alla registrazione del protocollo.

L'addetto al protocollo visualizza l'elenco dei documenti pervenuti e li prende in carico uno alla volta in ordine di arrivo. Verifica, tramite lettura dei documenti, la pertinenza dell'invio all'ARCS. Nel caso in cui:

- dal contenuto si rileva che sono stati erroneamente ricevuti, senza registrare nel protocollo, si restituisce la comunicazione al mittente con una dicitura che evidenzi l'errato destinatario (ad es. "Messaggio pervenuto per errore – Non di competenza di quest'Azienda", "Messaggio non di competenza di ARCS, pregasi verificare il corretto destinatario", o similari);
- difetti la leggibilità della provenienza e/o dell'integrità dei documenti stessi, senza registrare nel protocollo, si risponde al mittente con dicitura che evidenzi i difetti di leggibilità (ad es. "Dalla comunicazione non si desume il mittente. Si chiede di specificare nome e

cognome/denominazione sociale", "Nella comunicazione non sono presenti allegati" - qualora si tratti di comunicazioni di "inoltro allegati", o similari);
- si individuino eventuali spam si procede alla loro eliminazione;

Qualora pervenga alla casella di posta ordinaria un documento di rilevanza giuridico-probatoria lo stesso viene inoltrato alla casella di PEC ai fini della registrazione. 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. La UOR che inoltra il documento alla PEC va inserita quale tramite.

L'operatore della UOP esegue la procedura di registrazione a protocollo e smista il documento alla UOR di pertinenza.

6.1.3 Assegnazione dei documenti

L'assegnazione dei documenti agli uffici è effettuata dall'Ufficio Protocollo, o dagli altri punti di protocollazione che abbiano ricevuto il documento, tramite il sistema di protocollo informatico GIFRA. L'individuazione della UOR cui compete la trattazione viene effettuata per competenza come indicato nel funzionigramma, sulla base di indicazioni fornite dalla Direzione strategica, dal Responsabile dei flussi documentali o suo delegato, dall'analisi dei precedenti già trattati.

I documenti ricevuti dall'AOO per via telematica sono assegnati alle UOR competenti contestualmente alle operazioni di registrazione e segnatura di protocollo. L'assegnazione può essere effettuata: per conoscenza o per competenza. I destinatari del documento per "competenza" e/o "per conoscenza" lo ricevono esclusivamente in formato digitale.

L'UOR competente ha notizia dell'assegnazione di detti documenti attraverso la consultazione quotidiana di GIFRA sezione IterAtti/Atti Pervenuti.

I termini per la definizione del procedimento amministrativo decorrono dalla data di ricezione del documento da parte dell'Amministrazione.

Il sistema informatico traccia tutte le operazioni effettuate dagli operatori, identificati con l'UOR di appartenenza, cognome e nome.

6.1.4 Modifica delle assegnazioni e rifiuto

La modifica di un'assegnazione dei documenti ricevuti dall'Azienda può essere richiesta dalle UOR, dalla Direzione strategica o dal Responsabile dei flussi documentali o suo delegato, via e-mail o contatto

telefonico, esplicitando la motivazione della variazione di assegnazione che può riguardare la modifica dell'ufficio primo destinatario, l'invio di copia per conoscenza ad altri uffici.

Tali modifiche vengono effettuate, previa autorizzazione del Responsabile dei flussi documentali o suo delegato, esclusivamente dall'UOP con registrazione del flusso di lavorazione ed immediato inoltro alla UOR competente.

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

Il rifiuto di un'assegnazione deve essere sempre motivato esplicitando la motivazione nelle note pubbliche, possibilmente, segnalando l'ufficio ritenuto competente.

Il Dirigente dell'Ufficio Protocollo - considerata l'annotazione - provvederà a riassegnare lo stesso documento individuando l'Ufficio competente in base agli atti organizzativi adottati dall'

Nel caso di documento originale analogico, si può procedere alla nuova assegnazione ad altra UOR solo dopo aver ricevuto nuovamente l'originale rigettato, la UOR destinataria lo deve pertanto restituire all'Ufficio Protocollo con l'annotazione "documento pervenuto per errore" o "non di competenza" indicando – ove possibile – l'ufficio idoneo alla trattazione. L'Ufficio Protocollo, previa verifica nel funzionigramma dell'Azienda, provvede alla correzione dei metadati nel sistema informatico e all'inoltro.

In caso di conflitto di competenza tra UOR, è la Direzione strategica o il Responsabile dei flussi documentali che determina lo smistamento definitivo.

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

6.1.5 Documenti inviati in forma analogica

I documenti cartacei da spedire sono presentati all'Ufficio Protocollo in busta chiusa completi della firma del Responsabile del procedimento, del numero di protocollo, della classificazione e del numero di fascicolo, nonché del destinatario e del luogo di destinazione. Se si tratta di una raccomandata con avviso di ricevimento la compilazione delle cartoline avviene a cura della UOR mittente.

Eventuali situazioni di urgenza che modifichino la procedura descritta devono essere valutate ed autorizzate dalla SC Affari Generali.

6.1.6 Documenti inviati in forma digitale

Il sistema organizzativo adottato dall'Azienda Regionale di Coordinamento per la Salute prevede che ogni UOR gestisca autonomamente la protocollazione e l'invio telematico dei documenti digitali, che può avvenire secondo due modalità:

- *modalità secondo la funzione "protocollazione"*: l'operatore di cancelleria inserisce i metadati del documento nel sistema informatico, associa il fascicolo di riferimento, effettua l'*upload* del file già firmato digitalmente dal responsabile del procedimento, esegue le operazioni di registrazione ed invia telematicamente il documento;
- *modalità secondo la funzione "IterAtti"*: l'istruttore della pratica tratta il documento informatico e lo predispone per la firma e l'invio, associandolo ad un fascicolo e valorizzando tutti i metadati necessari. Pone il documento nella cartella di firma digitale del responsabile che, con un'unica azione, firma digitalmente l'atto e dà input al sistema informatico di provvedere alla contestuale protocollazione ed invio telematico.

7 CASISTICHE E COMPORTAMENTI

7.1 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 dall'ente è di tipo "aperto" ed è integrata nel sistema di gestione documentale. Per questa ragione possono pervenire documenti informatici sia da PEC che da PEO – posta elettronica ordinaria.

Il documento informatico che perviene nella casella di PEC è 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.

La verifica della validità della firma digitale è a cura del RPA. Il documento ricevuto viene registrato a protocollo indipendentemente dalla presenza della firma digitale. Spetta al responsabile del procedimento valutare se accettare il documento informatico assegnato non sottoscritto o non conforme agli standard e se richiedere al mittente un nuovo invio.

L'ARCS ha attivato una casella primaria di PEC istituzionale per la AOO dell'Azienda e due caselle secondarie di posta elettronica certificata ritenute necessarie per le esigenze specifiche di alcune UOR.

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 presenza di file troppo pesanti provoca il mancato invio o la mancata ricezione. Pertanto:

- in partenza, prima di inviare via PEC documenti protocollati, verificare che essi non siano eccessivamente ed inutilmente pesanti e, nel caso, frazionare l'invio con allegati plurimi. È consigliabile chiedere al destinatario la dimensione massima gestita dal suo gestore di servizio al fine di evitare la mancata consegna del messaggio;
- in ricezione è necessario chiedere ai mittenti l'invio di documenti che non superino i 50MB di pesantezza.

7.2 PEO istituzionali

La casella di posta elettronica fa corredo degli strumenti a disposizione di ogni dipendente per il quale il Dirigente preposto reputi opportuno l'uso della rete. Con la posta elettronica interna si assegna al dipendente uno strumento di lavoro agile, snello ed operativo, che sia in grado di assicurare una comunicazione anche a carattere ufficiale, sostitutiva della comunicazione scritta tradizionale.

Di norma la casella di posta elettronica assegnata prevede il suo uso interno ed esterno.

Le caselle di posta elettronica, sia ad uso interno che esterno sono nominative, tali cioè da identificare inequivocabilmente il titolare.

Ove ritenuto opportuno, sono create caselle di posta elettronica che individuano particolari uffici o attività da utilizzare sotto il diretto controllo di un responsabile. Tali caselle sono condivise da più dipendenti della struttura, secondo quanto indicato dal relativo responsabile. Di norma tutte le caselle postali create possono essere utilizzate (invio e ricezione) anche all'esterno dell'Azienda: vanno pertanto seguite le linee guida dell'Azienda per quanto attinente a stile, tono e linguaggio utilizzato.

La dimensione massima di un messaggio di posta ordinaria accettabile dal gestore del servizio è di 20MB (comprende tutti gli allegati e il corpo del messaggio).

7.3 Documenti anonimi

Il comportamento di un operatore durante la fase di registrazione di un documento in arrivo deve essere improntato 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.

I documenti sottoscritti con firma illeggibile vengono registrati indicando nel mittente la dicitura "illeggibile".

7.4 Priorità nella registrazione dei documenti in arrivo

Indipendentemente dal mezzo telematico di trasmissione, è data priorità nella registrazione a protocollo all'ordine cronologico di arrivo, tuttavia viene posta particolare attenzione a:

- atti giudiziari notificati;
- documenti della Regione Friuli-Venezia Giulia e dei Ministeri, della Prefettura – Ufficio Territoriale del Governo, Questura, Tribunali;
- documenti di rilevanza finanziario-contabile (MEF, Corte dei conti, etc.);
- documenti inerenti a procedure ispettive.

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.).

7.5 Apertura delle buste

Tutte le buste vanno aperte a cura dell'Ufficio Protocollo.

Fanno eccezione e, pertanto, non devono essere aperte, le buste:

- riportanti le seguenti diciture: riservato, personale, confidenziale o espressioni equivalenti;
- ripostanti le seguenti diciture: offerta, gara d'appalto, non aprire o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara (ad esempio, il CIG);
- le buste indirizzata nominativamente al personale vanno aperte nella convinzione che nessun dipendente utilizzi l'Amministrazione come casella postale privata. Chiunque riceva, tramite corrispondenza privata, documenti concernenti affari o procedimenti amministrativi dell'Amministrazione è tenuto a farli prevenite tempestivamente alla registrazione a protocollo.

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, sono spillate assieme al documento e trasmesse alla UOR di competenza.

7.6 Protocollo riservato

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

- tipologie di documenti individuati dalla normativa vigente relativamente a categorie di dati personali;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- atti dei procedimenti amministrativi in relazione ai quali sussistano particolari esigenze di protezione della riservatezza di terzi, persone, gruppi, imprese ed associazioni e dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- documenti legati a vicende di persone o a fatti privati o particolari;
- documento che contenga dati sensibili, giudiziari o personali, come definiti dal Codice in materia di protezione dei dati personali;
- documenti inerenti procedimenti amministrativi di pertinenza della polizia giudiziaria, della gestione del sistema sanzionatorio, dei procedimenti disciplinari.

7.6.1 Procedura del protocollo riservato

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

La selezione del livello di "riservatezza" rende la protocollazione riservata e visibile ai soli utenti abilitati.

A protezione della riservatezza il documento analogico viene trasmesso direttamente al RPA in busta chiusa, sigillata e firmata sui lembi di chiusura. 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 riservato saranno gli organi monocratici a definirne l'utilizzo in collaborazione con il Responsabile della gestione documentale.

7.7 Annullamento di una registrazione

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

Solo il Responsabile della gestione documentale e le persone espressamente delegate sono autorizzati 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 "Registrazione annullata" o un segno in posizione sempre visibile.

Il documento analogico annullato riporta gli estremi dell'annullamento e viene conservato dalla UOR che ha richiesto l'annullamento.

La richiesta di annullamento, inviata a mezzo *e-mail* sarà associata alla registrazione di protocollo del documento annullato a cura Responsabile della gestione documentale o delle persone espressamente delegate.

Nella registrazione di protocollo appaiono in forma ben visibile, oltre agli elementi già indicati, anche la data, il numero di matricola 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, con l'eccezione del caso in cui sia errato proprio l'indirizzo PEC del destinatario.

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), che viene protocollato e inviato via PEC.

I documenti annullati devono essere inseriti nei rispettivi fascicoli o, nel caso di documento non inerente a specifico procedimento, in un fascicolo annuale.

8 FORMAZIONE DELLE AGGREGAZIONI DOCUMENTALI

8.1 L'aggregazione documentale: definizione e funzione

Le Linee guida AgID (Glossario, allegato 1) definiscono l'aggregazione documentale come un "Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente".

Al § 4.1, le Linee guida AgID offrono una esemplificazione delle tipologie: "le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/2000 42 e art. 44, comma 1-bis, CAD".

Infatti, sempre nel Glossario, il fascicolo informatico è definito come "Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento", mentre la serie è definita come un "Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica)".

8.2 Il fascicolo: definizione e funzione

Il fascicolo è l'unità di base dell'archivio corrente.

Ogni fascicolo contiene documenti che ineriscono a un medesimo affare, attività o procedimento e sono classificati in maniera omogenea. La classificazione viene apposta (o associata) in base al contenuto e secondo il grado divisionale attribuito dal titolario (o piano di classificazione), salvo alcune eccezioni, come il fascicolo di persona.

All'interno di ciascun fascicolo i documenti sono inseriti secondo l'ordine cronologico di registrazione (ordine di sedimentazione), in maniera tale che l'inserzione a fascicolo individui subito il documento più recente. L'ordine 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[1].

La corretta tenuta del fascicolo garantisce sia la sedimentazione sia 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.

[1] 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 riferito al procedimento amministrativo, affare o attività principale, da cui deriva.

8.3 Il fascicolo analogico: formazione, implementazione e gestione

Per ogni procedimento, affare e attività, l'Azienda ha l'obbligo di conservare in un fascicolo cartaceo gli atti, i documenti e i dati da chiunque formati su supporto analogico, ovvero 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 digitalmente nativi.

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

- data di apertura e di chiusura del fascicolo;
- oggetto del fascicolo;
- numero del fascicolo;
- nominativo del responsabile del procedimento;
- altre amministrazioni partecipanti;
- elenco dei documenti contenuti;
- indice di classificazione.

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.

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.

8.4 Il fascicolo informatico: formazione, implementazione e gestione

Per ogni procedimento, affare e attività, l'Ateneo ha l'obbligo di conservare in un fascicolo informatico gli atti, i documenti e i dati da chiunque formati su supporto informatico: 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 di documenti nativi cartacei.

Il fascicolo informatico reca le seguenti indicazioni come set minimo di metadati:

- 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 istruito dal responsabile del procedimento o da una persona incaricata all'interno del sistema di gestione documentale GIFRA 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, trattandosi di una stringa con valore informativo e non probatorio. Se il contenuto è costituito da 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 UOR 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.

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

8.5 Il fascicolo ibrido

Il fascicolo, inteso come unità logica, può conservare documenti creati 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.

Questa pratica non esenta dalla conservazione dell'originale cartaceo nel fascicolo di riferimento.

8.6 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 obbligatori 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 dèi documenti contenuti nel fascicolo che ne consentono la reperibilità;
- data di apertura (o istruzione) del fascicolo;
- data di chiusura del fascicolo.

8.7 Metadati del 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 ha cadenza annuale ed è generato e gestito in forma automatica dal sistema di gestione informatica dei documenti.

8.8 Registri e Repertori informatici

L'Ente forma i propri registri e repertori informatici mediante la 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.

Per repertorio si intende il registro informatico 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. Il complesso dei documenti registrati a repertorio per forma omogenea costituisce una serie archivistica (o aggregazione documentale).

Sono un esempio la registrazione di contratti, convenzioni, etc.

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

9 ARCHIVIAZIONE DEI DOCUMENTI

Ai sensi del Codice dei Beni Culturali e del Testo Unico, ARCS individua nell'Archivio una funzione essenziale per garantire la certezza, la semplificazione e la trasparenza dell'agire amministrativo, il reperimento di informazioni affidabili sotto il profilo giuridico, la tutela della memoria storica di ARCS e il diritto di tutti i cittadini all'accesso all'informazione.

La richiesta di consultazione può pervenire dall'interno dell'Amministrazione, oppure da utenti esterni all'Amministrazione, per scopi giuridico-amministrativi o per scopi storici.

L'archivio e i singoli documenti sono beni archivistici; obbediscono pertanto alle disposizioni legislative di cui all'art. 2 e all'art. 10, comma 2, del Codice dei Beni Culturali.

L'archivio è suddiviso funzionalmente in:

- archivio corrente;
- archivio di deposito;
- archivio storico.

Per archivio corrente s'intende il complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso d'istruttoria e di trattazione o comunque verso i quali sussista un interesse corrente.

Per archivio di deposito s'intende il complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione o comunque verso i quali sussista un interesse sporadico.

Per archivio storico s'intende il complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto alla conservazione perenne nella sezione separata d'archivio.

L'archivio (anche se suddiviso in archivio corrente, archivio di deposito e archivio storico) è unico.

10 GESTIONE DELL'ARCHIVIO CORRENTE

10.1 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.

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 viene trasferita la gestione dei fascicoli, ma non la responsabilità.

10.2 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; 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 § 8.3 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 (segnatura archivistica).

Laddove una pratica abbia 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 (UOR) per la parte di propria responsabilità e competenza nel trattamento dell'affare.

I documenti creati nel corso dell'attività d'ufficio sono soggetti a fascicolazione obbligatoria ai sensi del TUDA, 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 UOR costituenti l'Amministrazione.

Un'attività secondaria 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, 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.

10.3 Gli strumenti dell'archivio corrente

Il trattamento dell'intero sistema documentale dell'Ateneo 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.

10.4 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.

10.5 Titolario (piano di classificazione)

Il Titolario, inserito all'interno del sistema di gestione documentale, è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (titolo/classe/eventuale sottoclasse) stabilite sulla base delle funzioni dell'Azienda.

Tutti i documenti ricevuti o prodotti dagli uffici dell'Azienda, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al Titolario di classificazione. Tale operazione consente di organizzare logicamente i documenti prodotti, ricevuti e spediti dall'Azienda nell'esercizio delle sue funzioni e di guidarne la sedimentazione all'interno dell'archivio.

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 soggetto a revisione periodica, qualora ciò si renda necessario a seguito di modifiche di carattere normativo o in seguito a cambiamenti dell'organigramma dell'Ente. In questo caso, il Titolario è adottato 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.

L'aggiornamento del Titolario compete esclusivamente all'ufficio competente per materia, quando necessario e opportuno.

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

10.5.1 Classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze dell'Azienda.

Essa è eseguita in base al Titolario di classificazione.

10.6 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.

10.7 Repertori

Per repertorio si intende il registro in cui sono annotati con numerazione progressiva i documenti, uguali per forma e diversi per contenuto. Essi sono soggetti a registrazione particolare, cioè con l'assegnazione di una numerazione continua e progressiva. Sono un esempio la registrazione di decreti, contratti e convenzioni, deliberazioni, etc.

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

10.8 Selezione e scarto

Il massimario di scarto è uno strumento da utilizzare durante la fase di deposito dell'Archivio, come previsto dall'art. 68 del TUDA e con cui l'Azienda individua le disposizioni di massima e definisce i criteri

e le procedure attraverso i quali i documenti, non rivestendo interesse storico ai fini della conservazione permanente e avendo esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della Soprintendenza archivistica, ai sensi del D.Lgs. 22 gennaio 2004, n. 42, art. 21.

L'Azienda procede ad effettuare la selezione della documentazione da conservare perennemente e lo scarto degli atti per i quali sono venute meno le esigenze di conservazione; ciò allo scopo di conservare e garantire il corretto mantenimento e la funzionalità dell'archivio, nell'impossibilità pratica di conservare indiscriminatamente ogni documento.

Un documento si definisce scartabile quando ha perso totalmente la sua rilevanza giuridico-amministrativa e non ha assunto alcuna rilevanza storica.

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; 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.

Le operazioni di selezione e scarto sono effettuate, secondo la normativa vigente, sotto la vigilanza del Responsabile della gestione documentale o da persona da questi delegata.

Anche i documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di conservazione nel rispetto della normativa sui beni culturali.

A seguito dell'autorizzazione, il Responsabile della gestione documentale avvia il procedimento per il ritiro del materiale e l'eliminazione fisica dei documenti; la ditta affidataria effettua le operazioni di ritiro e macero della documentazione con rilascio di relativo verbale di esecuzione.

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

11 L'ARCHIVIO DI DEPOSITO

L'archivio di deposito è la fase intermedia del processo di tenuta dei documenti prodotti dall'Azienda 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 non consentono la 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 TUDA, 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.).

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.

12 LA CONSERVAZIONE

Il TUDA prevede all'art. 68 l'obbligo per i soggetti pubblici di dotarsi di un "piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni contenute in materia di tutela dei beni culturali e successive modificazioni ed integrazioni".

La conservazione è l'attività volta a proteggere e custodire nel tempo gli archivi di documenti e dati informatici.

12.1 Il Piano di conservazione

Il piano di conservazione è lo strumento con cui l'Amministrazione individua le disposizioni di massima e definisce i criteri e le procedure per la corretta esecuzione delle operazioni di selezione ai fini della conservazione e dello scarto documentale; infatti i documenti che non rivestono interesse storico ai fini della conservazione permanente e hanno esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della Soprintendenza archivistica del Friuli-Venezia Giulia.

Il piano di conservazione definisce pertanto i tempi di invio in conservazione e i tempi di scarto per ciascuna classe documentale.

12.1.1 Pacchetti di archiviazione destinati allo scarto

Nel caso di affidamento esterno del servizio di conservazione le modalità operative di selezione e scarto dei pacchetti di archiviazione sono concordate dal Titolare dell'oggetto di conservazione e dal Conservatore.

L'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione e trasmesso al responsabile della conservazione che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o suo delegato.

L'autorizzazione è rilasciata ai sensi della normativa vigente in materia di beni culturali.

Il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, procede alla distruzione dei pacchetti di archiviazione. Nel caso di affidamento esterno del servizio di conservazione, il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore affinché provveda alla distruzione dei pacchetti di archiviazione. L'operazione di scarto viene tracciata sul sistema mediante la produzione delle informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio. Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, il Titolare dell'oggetto di conservazione notifica l'esito della procedura di scarto agli organi preposti alla tutela.

12.1.2 Conservazione analogica

La persistenza di documentazione cartacea richiede l'attivazione di corrette procedure di conservazione, rispettose della vigente normativa.

La documentazione corrente è conservata a cura del responsabile del procedimento competente, fino al trasferimento in archivio di deposito.

Periodicamente ogni Direttore di struttura individua i fascicoli cartacei relativi ai procedimenti conclusi o, comunque, non più necessari allo svolgimento delle attività correnti, da trasferire all'archivio di deposito.

Possono essere trasferiti agli archivi di deposito solo documenti ordinati e raccolti in fascicoli; non possono essere portate in archivio di deposito carte sciolte o miscellanee.

Gli elenchi di trasferimento devono essere inviati dal Responsabile della gestione documentale per consentire di avere il quadro completo della situazione degli archivi.

Prima della sua trasmissione fisica all'archivio di deposito, il fascicolo analogico deve essere sottoposto a sfoltimento e condizionamento all'interno di un faldone. In particolare, il funzionario che ha creato il fascicolo e ne ha curato la gestione è tenuto ad effettuarne un accurato controllo per verificare che vi siano effettivamente inseriti tutti i documenti relativi alla pratica e che non vi siano materiali non pertinenti, fotocopie e doppioni. Devono, invece, essere conservati i documenti acquisiti al protocollo e quelli a carattere strumentale rilevanti ai fini della ricostruzione dell'istruttoria.

Gli adempimenti relativi alle operazioni di trasferimento sono di competenza dei Direttori di struttura.

La documentazione conservata negli archivi di deposito è consultabile dalle strutture dell'Azienda che abbiano necessità di esaminarla e di servirsene nello svolgimento delle proprie attività. Le richieste devono essere rivolte dai Responsabili di struttura direttamente al soggetto conservatore e per conoscenza al Responsabile della gestione documentale.

12.1.3 Conservazione digitale

Per la conservazione della documentazione digitale il Responsabile dei flussi documentali pone in essere azioni secondo criteri concordati con il Responsabile della conservazione digitale dell'Azienda.

12.2 Responsabile della conservazione

L'Azienda, quale soggetto "Titolare dell'oggetto della conservazione", assicura la conservazione dei propri documenti informatici tramite il sistema di conservazione messo a disposizione dalla Regione FVG, per il tramite di INSIEL S.p.A., ai sensi del combinato disposto dell'art. 34, comma 1-bis lett. b), e dell'art. 44, comma 1quater, del CAD, che attua il processo di conservazione per il tramite di INSIEL/Gestore del servizio di conservazione.

Il servizio di conservazione dei documenti analogici, invece, è stato affidato a Omniadoc spa quale gestore del servizio di conservazione.

Il Responsabile della conservazione cura l'aggiornamento periodico del manuale di conservazione in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti in collaborazione con il responsabile della gestione documentale.

Le responsabilità e i compiti del Responsabile della conservazione dell'Azienda, le modalità di interazione con il Responsabile del servizio di conservazione affidatario, sono formalizzate nel manuale di conservazione e negli atti di affidamento del servizio.

13 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[2].

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.

Affinché il processo di gestione informatica dei documenti possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento.

13.1 Sicurezza del sistema informatico

La sicurezza dei dati, delle informazioni e dei documenti informatici gestiti dall'Azienda è intrinsecamente garantita dall'applicazione informatica adottata per il sistema di gestione documentale che assicura che tutte le fasi del ciclo di vita del documento (formazione, gestione, trasmissione, interscambio, accesso e memorizzazione), inclusa la gestione delle copie di sicurezza (backup), siano gestite con criteri rigorosi. Tali criteri garantiscono la disponibilità, l'integrità e la riservatezza delle informazioni.

I dati, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento, vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, agendo secondo il principio di *privacy by default*.

Gli elaboratori sono protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615 quinquies del codice penale (virus) mediante idonei programmi antivirus, la cui efficacia e il cui aggiornamento sono verificati periodicamente.

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'Azienda/UOR siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme

[2] TUDA, art.1, lettera r.

alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

13.2 Il sistema di gestione documentale

Il sistema di gestione documentale è costituito dall'insieme delle tecnologie e da tutti i dispositivi e i programmi presenti presso le sedi dell'Azienda Regionale di Coordinamento per la Salute che permettono l'utilizzo del sistema.

In particolare, sono parte integrante dell'infrastruttura i cablaggi e gli apparati di rete presenti presso le sedi dell'Azienda e necessari per la connettività, i sistemi informatici e le componenti software sottese al sistema di autenticazione dell'Azienda e tutte le postazioni di lavoro utilizzate dagli utenti del sistema di gestione documentale.

Le misure di sicurezza fisica e logica specifiche e le procedure comportamentali adottate per la protezione dell'infrastruttura del sistema di gestione documentale, delle informazioni e dei dati sono riportate nei paragrafi seguenti.

13.3 Le postazioni di lavoro

Per l'utilizzo del sistema di gestione documentale è previsto il coerente utilizzo delle postazioni di lavoro, da tavolo o portatili, o gli strumenti comunque funzionalmente assimilabili e l'impiego 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;

13.4 Accesso ai dati e ai documenti informatici

Il sistema adottato dall'Azienda 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;
- 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.

13.5 Sicurezza dei documenti informatici

L'accesso al sistema di gestione documentale da parte di ciascun utente dell'Azienda è gestito centralmente ed è subordinato alla richiesta di abilitazione del Responsabile della UOR di appartenenza dell'utente medesimo.

Le identità digitali utilizzate per l'accesso al sistema di gestione documentale sono costituite da nome utente e password o demandati a sistemi di autenticazione alternativi (es. *loginfvg*).

Il sistema di gestione documentale rispetta le misure di sicurezza previste dal Regolamento UE 2016/679 GDPR – *General Data Protection Regulation* relativo alla protezione dei dati personali.

13.6 Profili di abilitazioni di accesso interno alle informazioni documentali

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 delle categorie particolari di dati.

L'accesso al sistema di gestione documentale, l'accessibilità e la riservatezza delle registrazioni, dei dati personali e delle categorie particolari di dati, sono garantite tramite l'assegnazione differenziata di profili di abilitazione, in rapporto alla UOR e ufficio di appartenenza, alle funzioni e al ruolo svolto dagli utenti.

13.7 Criteri e modalità per il rilascio delle abilitazioni di accesso

Le abilitazioni di accesso per ciascun utente devono essere inoltrate dai responsabili delle UOR tramite richiesta scritta (e-mail) al servizio Tecnologie informatiche, che autorizza la creazione o la modifica delle utenze di concerto con il richiedente.

A ciascun utente del sistema sono attribuiti diritti di visibilità diversificati in ragione dell'appartenenza a un determinato settore dell'organizzazione e delle specifiche funzioni derivanti dal ruolo e dai compiti assegnati.

I responsabili delle UOR sono tenuti a comunicare tempestivamente al servizio Tecnologie informatiche la cessazione delle utenze del personale non più assegnato a funzioni che richiedano l'abilitazione al sistema.

Il Servizio Risorse Umane provvede periodicamente a comunicare al servizio Tecnologie informatiche e al Responsabile della gestione documentale o suo delegato la cessazione dal servizio dei dipendenti ai fini di disabilitarne l'accesso.

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

Gli utenti a cui sono affidate le postazioni di lavoro dell'Azienda, sono soggetti a tutte le responsabilità dettate dalla normativa vigente e applicabile e da quanto previsto dalla Policy per il corretto utilizzo degli strumenti Informatici ed eventuali ulteriori Regolamenti in materia dell'Azienda.

14 MISURE DI SICUREZZA E DI PROTEZIONE DEI DATI PERSONALI

14.1 Applicazione del Regolamento UE 2016/679 - GDPR

L'Azienda Regionale di Coordinamento per la Salute in qualità di Titolare del trattamento tratta i dati personali secondo i principi di liceità, correttezza e trasparenza nel rispetto del Reg. UE 2016/679 e del D.Lgs. 196/2003, novellato dal D.Lgs. 101/2018.

Il Titolare del trattamento, ai sensi dell'art.37 del GDPR, ha nominato il Responsabile della Protezione dei Dati personali (RPD / DPO) i cui contatti sono pubblicati al seguente link:

https://arcs.sanita.fvg.it/it/arcs/policy-arcs-materia-protezione-dati-personali/trattamento-dei-dati/

In particolare, il RPD informa e fornisce consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono attività di trattamento connesse agli obblighi derivanti

dal GDPR, dalle disposizioni nazionali relative alla protezione dei dati, fungendo da punto di contatto con il Garante per la protezione dei dati personali.

14.2 Trattamento dei dati personali

Per trattamento di dati personali si intende qualsiasi operazione, o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o all'insieme di dati personali, anche se non registrati in una banca dati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'elaborazione, la selezione, il blocco, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione di dati personali.

I dati personali in possesso dell'Ente sono raccolti nelle forme previste dalla legge, vengono trattati nel rispetto degli obblighi di correttezza, liceità e trasparenza, con tutela della riservatezza e dei diritti degli interessati. Il conferimento dei dati richiesti nella modulistica predisposta, anche con accesso ai servizi on line al sito istituzionale dell'Ente, è necessario, ai sensi delle vigenti norme di legge e regolamentari in materia, e il loro mancato conferimento potrebbe pregiudicare l'accesso all'esercizio di diritti o di servizi erogati dall'Azienda.

La base giuridica del trattamento dei dati personali è costituita dall'adempimento di obblighi legali o dall'esecuzione di compiti di interesse pubblico o connesso all'esercizio di poteri pubblici di cui è investito l'Azienda.

Le finalità, cui sono destinati i trattamenti dei dati personali, rientrano in quelle previste dalle leggi e dai regolamenti, che regolano le funzioni e i compiti istituzionali dell'Azienda, in particolar modo, con riferimento al trattamento di categorie particolari di dati personali, le stesse si ricollegano alle funzioni esercitate in vista di un interesse pubblico rilevante previsto dal diritto dell'unione europea, da disposizioni di legge dell'ordinamento interno o dai regolamenti, nei casi previsti dalla legge, oltreché alle materie indicate nell'art. 2 sexies, comma 2, da lett. a alla lett. z e segg., del D. Lgs. 196/2003, novellato dal D.Lgs. n. 101 del 10 agosto 2018.

In relazione alle indicate finalità, il trattamento dei dati personali avviene mediante strumenti manuali e/o informatici con logiche di organizzazione ed elaborazione strettamente correlate alle finalità previste dalle norme, in modo da garantire la sicurezza, l'integrità, la disponibilità e la riservatezza dei dati stessi.

Ai fini di pubblico interesse il trattamento può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

Per le finalità indicate e il conseguimento degli scopi istituzionali dell'Azienda, dati personali possono essere comunicati ai soggetti esterni che trattano i dati per conto dell'Azienda opportunamente nominati Responsabili del trattamento, ex art. 28 GDPR (ad es., società di archiviazione, conservazione documentale, gestione di posta elettronica, etc.) e alle altre categorie di soggetti nei confronti dei quali le comunicazioni sono necessarie in quanto previste dalle norme di riferimento di ciascuna attività o obbligatorie, quali altri Enti e Organismi Pubblici e Istituzioni centrali e periferiche, Istituti previdenziali, assicurativi, del Servizio Sanitario Nazionale e Regionale, Istituzioni giurisdizionali, a meno che tali soggetti non siano già contitolari in virtù di specifici accordi.

L'interessato in qualsiasi momento può richiedere l'esercizio dei diritti di cui agli artt. 15, 16, 17, 18, 19, 20, 21 e 22 del Regolamento UE 2016/679. In particolare, se attuabile, ha il diritto di ottenere la conferma dell'esistenza o meno dei dati conferiti, verificarne le finalità del trattamento, i destinatari o le categorie di destinatari a cui i dati personali sono o saranno comunicati, il periodo di conservazione, ha il diritto di chiedere la rettifica, la cancellazione o la limitazione del trattamento, il diritto di proporre reclamo a un autorità di controllo, l'esistenza di un processo decisionale automatizzato e la logica utilizzata, il diritto all'oblio, alla portabilità e di sapere se sono trasmessi ad un Paese terzo.

Per l'esercizio dei propri diritti l'interessato può rivolgersi al responsabile per la protezione dei dati personali.

15 DISPOSIZIONI FINALI

Il presente manuale è operativo il primo giorno del mese successivo a quello della sua approvazione.

ALLEGATI

Allegato 1 – Riferimenti normativi

Allegato 2 – AOO e UOR

Allegato 3 – Elenco delle PEC

Allegato 4 - Registro di emergenza

Allegato 5 – Nomine responsabili della gestione documentale e della conservazione

Allegato 6 – Documenti soggetti a Registrazione Particolare

Allegato 7 – Regolamento in materia di accesso documentale e di accesso civico

Allegato 8 – Manuale di conservazione

Allegato 9 – Classi documentali