



Manuale di Gestione documentale Asl 7 Sulcis Iglesiente

Sc Affari Generali e Legali-
a cura del Responsabile della gestione
documentale

INDICE

Sezione I- Disposizioni Generali	
I.1 Premessa	pag.3
I.2 Scopo e ambito del documento	pag.4
I.3 Definizione dei termini e degli acronimi	pag 4
Sezione II Aspetti organizzativi	
II.1 Modello organizzativo adottato per la gestione dei documenti: l'AOO.	pag.9
II.2 Servizio per la tenuta del protocollo informatico, dei flussi e degli archivi.	pag 10
II.3 Il Responsabile per la Gestione Documentale	pag.10
II.4 La profilatura degli operatori dell'ufficio di protocollo	pag. 11
II.5 Gli altri Responsabili del Sistema di Gestione Documentale	pag 12
Sezione III – Il Sistema di Gestione Documentale	
III.1 Il S.G.D. – Definizione	pag.12
III.2 Tipologie di documento: il documento amministrativo analogico e digitale	pag.13
III.3 Sottoscrizione digitale dei documenti e verifica delle firme digitali	pag. 14
III.4 Formazione del documento informatico	pag. 14
III.5 Formati dei documenti informatici	pag. 16
III.6 Metadati dei documenti informatici	pag. 16
Sezione IV Il Protocollo Informatico	
IV.1 Il protocollo informatico- definizione, funzioni e oggetto	pag. 16
IV.2 La registrazione di protocollo	pag. 18
IV.3 Termini per la registrazione dei documenti e il protocollo differito	pag. 20
IV. 4 Segnatura di protocollo	pag. 21
IV .5 Registro di emergenza	pag. 22
Sezione V Casi particolari di registrazione di protocollo	
V.1.a Circolari e documenti con più destinatari	pag. 23
V.1.b Documenti su supporto cartaceo indirizzati nominalmente al personale dell'Amministrazione Lettere anonime e documenti non firmati	pag. 23
V.1.c Documenti informatici con certificato di firma scaduto o revocato	pag. 24
V.1.d Integrazioni documentarie	pag.24
V.1.e Allegati	pag.24
V.1.f Protocollazione di documenti digitali pervenuti erroneamente	pag.24
V.1.g Protocollazione dei documenti cartacei pervenuti erroneamente	pag. 25
Sezione VI Classificazione e fascicolazione dei documenti	pag.25
VI.1 Il Sistema di classificazione documentale	pag.25
VI.2 Il Piano di classificazione o Titolare	pag. 25
VI.3. Le aggregazioni documentali- Il Fascicolo informatico	pag. 26
VI.4 Formazione e identificazione dei fascicoli	pag. 27
VI.5 Piano di organizzazione delle aggregazioni documentali	pag. 28
VI.6 Gli strumenti dell'archivio corrente	pag.28
Sezione VII Flussi documentali	pag. 28

VII.1 I documenti provenienti dall'esterno	pag. 29
VII.2 Assegnazione dei documenti	pag. 30
VII.3 Modifica delle assegnazioni	pag.31
VII.4 I documenti inviati dalla AOO	pag. 31
Sezione VIII Piano di sicurezza	
VIII.1 Obiettivi	pag.32
VIII 2 Attività e competenze	pag. 33
VIII. 3 Formazione dei documenti – Aspetti attinenti alla sicurezza	pag. 35
VIII.4 Gestione dei documenti informatici	pag. 36
VIII.5 Trasmissione ed interscambio dei documenti informatici	pag. 36
VIII.5.1 Trasmissione ed interscambio dei documenti informatici all'esterno della AOO	pag. 37
VIII.5.2 Trasmissione ed interscambio dei documenti informatici all'interno della AOO	pag. 37
VIII. 6 Accesso ai documenti informatici	pag. 38
VIII. 6.1 Utenti esterni alla AOO- Altre AOO/Amministrazioni	pag. 39
VIII. 6.2 Utenti esterni alla AOO- Provati	pag. 39
VIII.7 Conservazione e memorizzazione dei documenti analogici, informatici e delle immagini digitali dei documenti cartacei	pag. 39
VIII.8 Conservazione dei documenti informatici	pag. 40
VIII.9 Trasferimento delle unità archivistiche negli archivi di deposito	pag. 40
VIII.10 Pacchetti di versamento	pag. 40
VIII.11 Selezione dei documenti	pag 41
IX Approvazione e aggiornamento del Manuale-Regole transitorie e finali	
IX .1 Modalità di approvazione e aggiornamento del Manuale	pag. 41
IX.2 Pubblicità del presente Manuale	pag.41

ALLEGATI :

All. 1- Registro di emergenza

All. 2 Atto di revoca autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza (art. 63 DPR445/2000) (Modello)

All.3 Titolare di classificazione

All. 4 Prontuario di selezione e scarto

All. 5 Regolamento di scarto e Piano di conservazione degli archivi
(Con Mod. A,B,C,D,E,F,G)

Principali riferimenti normativi

- RD 1163/1911, Regolamento per gli archivi di Stato;
- DPR 1409/1963, Norme relative all'ordinamento ed al personale degli archivi di Stato;
- DPR 854/1975, Attribuzioni del Ministero dell'interno in materia di documenti archivistici non ammessi alla libera consultabilità;
- Legge 241/1990, Nuove norme sul procedimento amministrativo;
- DPR 445/2000, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- DPR 37/2001, Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato;
- D.lgs 196/2003 recante il Codice in materia di protezione dei dati personali;
- D.lgs 42/2004, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
- D.lgs 82/2005, Codice dell'amministrazione digitale;
- D.lgs 33/2013, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- DPCM 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Reg. UE 910/2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013;
- RGPD 679/2016, 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;
- Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- AGiD - Linee guida sulla formazione, gestione e conservazione dei documenti informatici anno 2021
- D.lgs 101/2018 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679

SEZIONE I - DISPOSIZIONI GENERALI

I.1 Premessa

Il Manuale di Gestione Documentale è lo strumento operativo che descrive il sistema di produzione e di gestione dei documenti (analogici e digitali), come previsto dal combinato disposto delle Linee Guida Agid sulla formazione, gestione e conservazione dei documenti informatici del 10 settembre 2020 con il DPCM 3 dicembre 2013, Regole tecniche per il protocollo informatico ed il D.lgs 82/2005, Codice dell'Amministrazione Digitale.

L' Azienda Asl Sulcis Iglesiente è stata costituita il 1 Gennaio 2022, subentrando alla ATS, in esecuzione della Legge regione Sardegna n. 24 del 2022 che ha riconosciuto personalità giuridica pubblica alle Aziende sanitarie locali e ad ARES Sardegna, Azienda Regionale della Salute, la funzione di gestione unificata centralizzazione di alcuni servizi essenziali quale, per quanto qui interessa, il

Servizio Informativo.

Per il tramite di ARES Sardegna si è quindi provveduto ad attribuire alla Società informatica Accenture S.p.a, mandante dell' ATI aggiudicataria per ARES dei sistemi di gestione informatica, la gestione del Protocollo informatico e del Sistema di gestione documentale.

I.2 Scopo e ambito del documento

Il presente Manuale ha lo scopo di illustrare le modalità di formazione e gestione dei documenti informatici e di fornire le istruzioni il corretto funzionamento del servizio di protocollo informatico nonché le regole che sottendono alla corretta tenuta del patrimonio documentale. Esso descrive, altresì, le modalità di gestione dei flussi documentali e degli archivi, in modo tale da organizzare e governare la documentazione ricevuta, inviata o comunque prodotta dall'amministrazione secondo i parametri di corretta registrazione di protocollo, assegnazione, classificazione, fascicolatura, ricerca e conservazione dei documenti

Per quanto scritto in premessa le finalità del presente documento richiedono la stretta collaborazione del Servizio Informativo di ARES a partire dalla verifica ed attestazione della coerenza ed efficienza dell'impianto informatico con la normativa e l'organizzazione aziendale per arrivare al Manuale di Sicurezza informatico.

I.3 – Definizioni dei termini e degli acronimi

Per quanto riguarda la definizione dei termini e degli acronimi, funzionali alla corretta interpretazione del dettato del presente manuale, si riporta di seguito il Glossario allegato alle Linee Guida AGID (allegato n.1).

TERMINE	SIGNIFICATO
Accesso	Operazione che consente di prendere visione ed estrarre copia dei documenti informatici.
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico o nel sistema di gestione o conservazione.
Aggregazione documentale informatica	Aggregazione di documenti informatici o 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.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
Area Organizzativa Omogenea	Un insieme di funzioni e di strutture, individuate dall'amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n.445.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto, un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata.

	L'autenticità è valutata sulla base di precise evidenze.
Basi di dati	Collezione di dati registrati e correlati tra loro
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Chiave privata	L'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento in precedenza cifrato mediante la corrispondente chiave pubblica.
Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti da trasmettere al titolare delle predette chiavi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore
Comunità di riferimento	Gruppo ben individuato di utenti che dovrebbero essere in grado di comprendere un particolare insieme di informazioni
Conservatore	Soggetto, pubblico o privato, che svolge attività di conservazione dei documenti informatici.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti.
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da documento informatico cui è tratto
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato.
Digest	Vedi impronta crittografica
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa.
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD
Esibizione	Operazione che consente di visualizzare un documento conservato
Evidenza informatica	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS
Firma elettronica qualificata (firma digitale)	Vedi articolo 3 del Regolamento eIDAS
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali (art.1, co.1, lett.g) DPCM 22 febbraio 2013).

Identificativo Univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
Impronta crittografica	Sequenza di bit di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Manuale di Gestione per la Qualità e la Sicurezza delle Informazioni	Documento che descrive la struttura organizzativa (con la descrizione dei compiti e delle responsabilità delle funzioni), i criteri e le modalità connesse alla predisposizione ed all'attuazione del Sistema di gestione integrata per la Qualità e la Sicurezza delle Informazioni
Marca temporale	Una marca temporale è "il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo" art.1, co.1, lett.i) del DPCM 22 febbraio 2013. Nella pratica fornisce la prova con validità erga omnes della formazione di un documento in un momento certo o, comunque, della sua esistenza al momento della generazione della marca temporale. La marca temporale è un documento informatico rilasciato da un servizio di marcatura temporale generalmente gestito da un Certificatore. Nella marca sono contenute le seguenti informazioni: <input checked="" type="checkbox"/> - data e ora della creazione della marca temporale; - nome dell'emittente della marca temporale; <input checked="" type="checkbox"/> - impronta del documento cui la marca temporale fa riferimento.
Metadati	Dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura – così da permetterne la gestione nel tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Network Attached Storage (NAS)	Dispositivo collegato alla rete la cui funzione è quella di consentire agli utenti di accedere e condividere una memoria di massa costituita da uno o più dischi rigidi
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico
Pacchetto di Archiviazione (PdA)	Pacchetto informativo composto dalla trasformazione di uno o più Pacchetti di Versamento coerentemente con le modalità riportate nel manuale di conservazione
Pacchetto di Distribuzione (PdD)	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una richiesta
Pacchetto di File (file ackage)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono,

	collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente
Pacchetto di Versamento (PdV)	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti digitali da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
Piano della Sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano di Classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata
Piano di Conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Presa in Carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo di Conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui al capitolo 4.7 delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici.
Produttore dei PdV	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con Responsabile della Gestione Documentale
Produttore dell'Applicativo di Gestione Informatica dei Documenti	Persona fisica o giuridica che produce ed assiste il Sistema di gestione Informatica dei documenti.
Rapporto di Versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Responsabile della Conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
Responsabile del Servizio di Conservazione	Soggetto che coordina il processo di conservazione all'interno del conservatore accreditato, in possesso dei requisiti professionali individuati da AgID
Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi o Responsabile della gestione documentale	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	Soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AgID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al tempo universale coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono

	convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione
Scarto	Procedura con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico culturale
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica)
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi
Sistema di classificazione	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di Gestione Informatica dei Documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito delle amministrazioni pubbliche è il sistema di cui all'art. 52 del D.P.R. 28 dicembre 2000, n. 445.
Specificità di Contratto	Documento contenente i dettagli e le peculiarità di ogni singolo Canale Documentale tra cui: <ul style="list-style-type: none"> • i documenti da conservare per ogni Sistema di Classificazione e relative Aggregazioni Documentali; • i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa; • la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione; • la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni; • la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento
Supporto	Contenitore e/o l'oggetto materiale nel o sul quale sono memorizzate le informazioni (carta, film, nastro magnetico, supporti digitali).
Titolare	Persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica (art.1, co.1, lett. aa) del D.lgs n.82/2005 modificato dal D.lgs. n.33/2013
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Validazione temporale	Risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

SEZIONE II – ASPETTI ORGANIZZATIVI

II.1 – Modello organizzativo adottato per la gestione dei documenti: l'AOO

L'Azienda Socio Sanitaria n. 7 del Sulcis Iglesiente è strutturata in un'unica Area Organizzativa Omogenea (AOO) dove è istituito un Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. (art. 61 DPR 445/2000).

Nella AOO sono quindi ricomprese le Direzioni, le Unità Operative Complesse (UOC) le Unità Operative Semplici Dipartimentali (UOSD), le Unità Operative Semplici (UOS) e le unità/uffici non strutturati in prosieguo denominate tutte UOR

L'organigramma presente nell'applicativo di gestione documentale è stato definito sulla base delle funzioni espresse dalle varie strutture e secondo uno schema ad albero che pone a livello padre la Direzione Strategica - all'interno della quale sono incardinate la Direzione Generale, la Direzione Amministrativa, la Direzione Sanitaria – il Collegio Sindacale, il Collegio di Direzione, l'OIV; ai livelli sottostanti sono collocate le diverse UOC, UOSD UOS e gli uffici dipendenti dalle diverse aree e dipartimenti dell'Amministrazione.

L'AOO è dotata, a norma di legge, di una casella di posta elettronica certificata istituzionale protocollo@pec.aslsulcis.it per la corrispondenza. Tale casella costituisce il domicilio digitale della AOO da e verso l'esterno.

La casella di posta elettronica del protocollo garantisce la interoperabilità col sistema di protocollo

Le altre caselle di posta elettronica certificata (PEC) aventi dominio “.. @pec.aslsulcis.it” intestate ad alcune UOR aziendali non costituiscono domicilio digitale della AOO e non possiedono il requisito della interoperabilità pertanto la documentazione trasmessa/ricevuta a mezzo di tali canali che sia necessario acquisire al Protocollo, dovrà essere girata alla PEC del Protocollo.

L'AOO è accreditata con il codice E8GGUUN1 presso l'indice delle pubbliche amministrazioni (IPA), accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati. La struttura I.C.T. di ARES comunica tempestivamente all'IPA ogni modifica delle credenziali aziendali e la data in cui la modifica stessa è operativa, in modo da garantire l'affidabilità dell'indirizzo di posta elettronica e delle altre informazioni. Con la stessa tempestività l'Amministrazione comunica la soppressione o la creazione di una nuova AOO.

Le comunicazioni interne all'Azienda avvengono tramite l'utilizzo della casella di posta elettronica ordinaria (PEO) dei rispettivi uffici o servizi o dei singoli dipendenti, nel rispetto delle norme in materia di protezione dei dati personali, nonché previa informativa agli interessati circa il grado di riservatezza degli strumenti utilizzati.

La posta elettronica ordinaria viene utilizzata di norma per:

- convocare riunioni interne all'Ente;
- inviare comunicazioni di servizio o notizie dirette ai dipendenti in merito ad informazioni generali di organizzazione;
- diffondere circolari, ordini di servizio, copie di documenti.

Se una comunicazione viene protocollata come documento interno, viene trasmessa alle UOR destinatarie mediante il sistema di protocollo informatico.

Non possono essere inviate comunicazioni tra servizi della stessa Azienda utilizzando le caselle di Posta Elettronica Certificata.

Le UOR che hanno necessità di protocollare in ingresso, presso uno specifico punto di protocollo, una email che hanno ricevuto sulle proprie caselle di posta elettronica la inoltrano dal loro indirizzo email alla casella di posta ordinaria del protocollo protocollo@aslsulcis.it

All'interno della AOO il sistema di protocollo è pertanto unico e operativamente decentrato, ossia distribuito su più uffici diversamente abilitati, e precisamente:

- la registrazione dei documenti in arrivo è effettuata presso il Servizio Protocollo Generale (vedi paragrafo seguente);
- la registrazione dei documenti interni o in partenza è effettuata direttamente nelle UOR dal dipendente abilitato al protocollo informatico
-

II.2 – Servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi

Nella AOO è istituito il Servizio per la tenuta del protocollo informatico, gestione flussi documentali e degli archivi presso la SC Affari Generali e Legali così come previsto dall'Atto Aziendale approvato con delibera del Direttore Generale Asl Sulcis Iglesiente n. 213 del 16/05/2023 che gli attribuisce il macro-processo di "Gestione protocollo e segreteria e coordinamento attività amministrative della Direzione Generale".

L'Ufficio Protocollo Generale dell'Azienda è abilitato alla protocollazione di tutti i documenti in entrata pervenuti in formato digitale presso il domicilio digitale dell'Azienda e in formato cartaceo presso la sede di Carbonia, via Dalmazia n.83 (Sede Legale). Tutte le altre unità operative sono abilitate ai flussi di protocollo in uscita.

II.3 Il Responsabile della Gestione Documentale

Il Responsabile della SC Affari Generali e Legali in base all'Atto Aziendale assume il ruolo di Responsabile della Gestione documentale e, in mancanza di idonee figure anche quella di Responsabile della conservazione (la dualità dei ruoli essendo prevista dal par.4.5 lett. c) delle Linee guida AGID) e può, sotto la propria responsabilità, nominare un Vicario parimenti in possesso di idonee competenze giuridiche, per i casi di sua assenza o impedimento. del Responsabile (par. 3.1.2, lett. B. delle citate Linee guida).

Il Responsabile della Gestione documentale è incaricato di assicurare la formazione, la gestione, l'archiviazione e la corretta conservazione o eventuale eliminazione dei documenti informatici nel rispetto delle normative vigenti.

Oltre le specifiche competenze del servizio indicate nel successivo comma dalla lettera a) alla lettera f) spetta al Responsabile della Gestione documentale la stesura del Manuale di Gestione Documentale e la formazione del personale sull'uso degli strumenti documentali.

Il servizio cui è preposto il Responsabile della gestione documentale ha competenza sulla gestione dell'intera documentazione archivistica, ovunque trattata, distribuita o conservata dall'Amministrazione, 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.

Il Responsabile della gestione documentale svolge inoltre i seguenti compiti:

- a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni in base alle richieste dei Responsabili delle varie U.O della AOO. Le richieste di abilitazione vengono quindi trasmesse ai Responsabili informatici ARES per l'associazione tra utente e relativo profilo che ne delimita l'ambito di operatività;
- b) garantisce che le operazioni di registrazione e di segnatura di protocollo si volgano nel rispetto delle disposizioni del TUDA;
- c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53 del TUDA;
- d) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- e) conserva le copie di cui agli articoli 62 e 63 del TUDA, in luoghi sicuri differenti;
- f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 del TUDA e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69 del TUDA;
- g) autorizza le operazioni di annullamento di cui all'articolo 54 del TUDA;
- h) vigila sull'osservanza delle disposizioni del TUDA da parte del personale autorizzato e degli incaricati.

II.4 La profilatura degli operatori dell'ufficio di registrazione di protocollo

Il Responsabile della gestione documentale, su richiesta dei Direttori delle UO/Servizi, rilascia le autorizzazioni per le abilitazioni per l'utilizzo del protocollo generale aziendale (vedi par .II.3 lett. a) che successivamente vengono trasmesse ai Responsabili Informatici della procedura.

Il Sistema di gestione informatica prevede, infatti, livelli di accesso differenziati per quanto riguarda l'inserimento, la ricerca e la modifica di dati.

Ad ogni utente è associato un profilo che ne delimita gli ambiti di operatività all'interno della procedura informatica di protocollo.

Per ogni documento, all'atto della registrazione, il sistema di gestione documentale consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso, nel rispetto della normativa di trattamento e tutela dei dati personali.

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti. La password è strettamente personale e l'operatore è tenuto a conservare in modo da garantirne la segretezza.

Il sistema informatico adottato consente di gestire le abilitazioni assegnando ad ogni utente un login ed una password personali, in modo che sia sempre possibile risalire all'operatore che ha effettuato le registrazioni.

II.5 Gli altri Responsabili del Sistema di gestione documentale

Tutti i procedimenti amministrativi comportano la produzione, la tenuta e la conservazione di documentazione archivistica per cui ogni Dirigente preposto ad ogni struttura è responsabile della gestione documentaria in conformità alle disposizioni del presente regolamento.

Il Responsabile per la Transizione Digitale, o Responsabile per la sicurezza informatica, stante la centralizzazione dei sistemi informativi in Ares (vedi artt. 3 e ss L. R. 242020) è individuato da quest'ultima nell'espletamento delle sue funzioni istituzionali di supporto alle Aziende socio sanitarie Locali, scegliendo tra il suo personale dipendente.

Sono compiti propri Responsabile per la sicurezza informatica:

- abilitare gli addetti dell'amministrazione all'utilizzo del PdP (Prodotto di Protocollo Informatico) secondo le funzioni standard di abilitazione definite con il Responsabile della gestione documentale (ad esempio abilitazione alla sola consultazione ovvero anche alla modifica ecc) e autorizzate dallo stesso a seguito di richiesta del Responsabile della UOR;
- adozione e supervisione di tutte le soluzioni tecniche ed organizzative idonee a garantire la funzionalità e continuità operativa del sistema documentale;
- referente IPA (indice delle pubbliche amministrazioni) per ASL Sulcis Iglesiente;
- redigere e aggiornare, di concerto con DPO, la procedura per la composizione delle password e il blocco delle utenze;
- definire e aggiornare la procedura per il riutilizzo e la dismissione dei supporti rimovibili;
- monitorare la regolare produzione del registro giornaliero di protocollo e il conseguente invio al Sistema di Conservazione Sostitutiva, secondo quanto disposto dalle normative vigenti;
- fornisce supporto tecnico nei processi di formazione dei pacchetti di versamento (PdV) e di trasmissione al Sistema di conservazione;
- redigere il Piano per la sicurezza informatica al fine di garantire il rispetto delle misure di sicurezza ICT e della normativa sulla protezione dei dati personali;
- in generale compete al Responsabile per la sicurezza informatica affiancare il Responsabile della Gestione documentale per tutti gli aspetti strettamente tecnico-informatici e fungere da interfaccia con la Società appaltata per la fornitura del programma di Protocollo informatico e verificare la rispondenza di quest'ultimo ai requisiti strutturali previsti dalle Linee guida Agid sulla formazione, gestione e conservazione dei documenti informatici.

SEZIONE III-IL SISTEMA DI GESTIONE DOCUMENTALE

III.1 Il Sistema di gestione informatica dei documenti- Definizione

Il sistema di gestione informatica dei documenti comprende tutte quelle attività e strumenti per gestire l'intero ciclo di vita di un documento all'interno dell'Amministrazione, dalla sua creazione o acquisizione, fino alla sua archiviazione e conservazione a norma

Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per natura, finalità ed effetto giuridico e alle quali corrispondono prassi operative distinte e comunque tutte presidiate da specifiche procedure e sistemi informatici ed effettuate nel rispetto dei principi generali applicabili in materia di trattamento dei dati personali.

A norma dell'art 52 del D.P.R. 445/2000 "Testo Unico della Documentazione Amministrativa" il Sistema di gestione informatica dei documenti deve:

- a) garantire la sicurezza e l'integrità del sistema;
- b) garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
- c) fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
- d) consentire il reperimento delle informazioni riguardanti i documenti registrati;
- e) consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
- f) garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato

III.2 – Tipologie di documenti: il documento amministrativo analogico e digitale.

Per documento amministrativo si intende ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.

Sotto il profilo della sua formazione, il documento amministrativo, ricevuto, spedito o interno si distingue in:

- a) documento analogico
- b) documento informatico

Il documento analogico è formato su supporto fisico (tradizionalmente cartaceo) mediante strumenti non digitali, come la scrittura a mano o a macchina oppure mediante sistemi informatici (lettera scritta con Word) e successivamente stampato. In quest'ultimo caso, come originale si considera quello cartaceo -o analogico-, stampato su carta intestata e dotato di firma autografa.

Il documento informatico è "il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti "(art. 1 comma 1lett.p CAD).

I documenti prodotti dalla AOO Asl Sulcis Iglesiente, sia analogici che informatici, devono riportare le seguenti informazioni:

- a) logo e denominazione ufficiale dell'ASL Sulcis Iglesiente;
- b) l'Unità Organizzativa Responsabile (UOR) che ha prodotto il documento;
- c) indirizzo completo dell'ASL Sulcis Iglesiente (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, indirizzo istituzionale di posta elettronica, indirizzo istituzionale di posta elettronica certificata);
- d) data completa di produzione del documento (luogo, giorno, mese, anno)
- e) numero di protocollo;
- f) indice di classificazione;
- g) destinatario/destinatari del documento;
- h) oggetto del documento;
- i) numero degli allegati (se presenti);
- j) numero di collegamento/riferimento ad un eventuale precedente (se disponibile);
- k) indicazione del Responsabile del procedimento (Legge 7 agosto 1990, n. 241 e ss. mm. e ii.);

- l) indicazione del referente per la pratica;
- m) recapiti telefonici e indirizzo mail del Responsabile del procedimento/referente;
- n) sottoscrizione autografa o elettronico/digitale del Dirigente Responsabile (o del funzionario delegato).

III.3 Sottoscrizione digitale dei documenti e verifica delle firme digitali

Il documento è sottoscritto digitalmente prima di essere registrato.

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma digitale conforme alle disposizioni di legge che consente di attribuire pieno valore probatorio sino a querela di falso della provenienza del documento informatico dal suo sottoscrittore.

L'Azienda si avvale del servizio di firma digitale offerto dal sistema CNS di Infocamere assegnando personalmente al dipendente tessera e dispositivo di lettura

Il documento di origine deve essere preferibilmente in formato PDF e firmato all'interno dell'applicativo con una firma digitale in modalità PAdES.

Il sistema di gestione documentale permette la consultazione e la verifica della firma senza l'ausilio di software esterni.

La sequenza delle operazioni previste è la seguente:

- apertura della busta "virtuale" contenente il documento firmato;
- verifica della validità del certificato; questa attività è realizzata verificando on-line le Certificate Revocation List (CRL) con una periodicità predefinibile parametricamente nel sistema di protocollo
- verifica della firma (o delle firme multiple) con funzioni Java standard; in particolare, viene calcolata l'impronta del documento e verificata con quella contenuta nella busta "logica" - verifica dell'utilizzo, nell'apposizione della firma, di un certificato emesso da una Certification Authority (CA) presente nell'elenco pubblico dei certificatori accreditati e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle Certification Authority accreditate presso l'AOO;
- trasformazione del documento in uno dei formati standard previsto dalla normativa vigente in materia e attribuzione della segnatura di protocollo;
- inserimento nel sistema documentale del Sistema di Protocollo sia del documento originale firmato, sia del documento in chiaro;
- archiviazione delle componenti verificate e dei dati dei firmatari rilevati dal certificato in una tabella del database del Sistema di Protocollo per accelerare successive attività di verifica di altri documenti ricevuti.

Per i flussi di processo aventi rilevanza meramente interna la firma elettronica si basa su credenziali di accesso personali assegnate a ciascun dipendente che ne deve garantire la custodia e utilizzo secondo quanto previsto Codice di condotta aziendale e dal Modello organizzativo Privacy dell'Asl Sulcis Iglesiente.

III. 4 Formazione del documento informatico

La formazione del documento informatico può avvenire mediante una delle seguenti modalità:

- a) creazione diretta tramite software che producano documenti nei formati indicati nell'All.2 delle Linee guida AGID e nel rispetto delle regole di interoperatività ivi previste;
- b) acquisizione di documenti informatici per via telematica, o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) registrazione di transazioni informatiche: memorizzazione di dati provenienti da procedure automatizzate, come la compilazione di moduli online, form web o transazioni bancarie;
- d) generazione/raggruppamento automatico di dati: creazione di documenti attraverso sistemi gestionali o banche dati, raggruppando informazioni in modo automatico (es. report, fatture elettroniche).

La creazione diretta del documento di cui alla lettera a) richiede l'utilizzo dei formati che consentono di preservare l'integrità del contenuto del documento e la sua leggibilità e immodificabilità nel tempo. (Per l'elenco dei formati utilizzati nella Asl Sulcis Iglesiente vedi paragrafo successivo III.4). Ulteriore requisito per garantire al documento informatico la validità giuridica, oltre la l'immodificabilità e l'integrità, è la firma digitale (vedi par. II.3) o la sua memorizzazione nel sistema di gestione documentale

La seconda modalità di formazione del documento informatico di cui alla lett.b) è quella relativa al documento acquisito o "documento in ingresso"

Il documento in ingresso può essere un documento nativo informatico trasmesso via e-mail, PEC o su supporto informatico (quale, ad esempio, CD ROM, DVD, pen drive, etc) oppure un documento nativo analogico acquisito per copia dell'immagine attraverso scannerizzazione, mantenendo quindi la rappresentazione visiva dell'originale, o per copia digitale.

Il processo di scansione si articola 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;
- collegamento delle rispettive immagini alla registrazione di protocollo, mediante le funzioni: "File primario" e "Allegati".

Le operazioni di trasferimento e di registrazione nel Sistema di gestione documentale aziendale e nel sistema di conservazione garantiscono la fedeltà del documento acquisito rispetto a quello originale.

Al termine dell'operazione di registrazione e di classificazione del documento, i documenti acquisiti nell'AOO sono assegnati alla UOR di competenza che, nella persona del Responsabile o suo incaricato, ne individua il destinatario; questi provvederà, quindi alla presa in carico del documento nel Sistema Informatico e alle conseguenti operazioni di fascicolazione del documento, intese come corretto inserimento all'interno del fascicolo relativo al procedimento di afferenza del documento.

Nel caso di documento informatico formato secondo quanto previsto alle sopracitate lett. c) e d) le caratteristiche di immodificabilità e di integrità sono garantite dall'apposizione della firma digitale, dalla registrazione nei log di sistema dell'esito dell'operazione di formazione del documento

informatico e trasferimento dei dati nel sistema di conservazione.

III. 5 Formati dei documenti informatici

I documenti informatici creati dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma elettronico/digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione, al fine di garantire la loro **immodificabilità** durante le fasi di gestione e conservazione, l'**integrità** e **leggibilità** nel tempo del contenuto e della struttura.

L'ASL Sulcis Iglesiente utilizza per la formazione e per la gestione dei documenti informatici tipologie di formati coerenti con quanto indicato nell'allegato 2 delle LLGG AGID, tali da garantire i principi di interoperabilità tra i sistemi di conservazione in base alla normativa vigente.

L'elenco dei formati maggiormente utilizzati dalla ASL Sulcis Iglesiente comprende:

- Per i documenti amministrativi e sanitari (delibere, determine e referti clinici) PDF/A e PDF (.pdf);
- Per immagini diagnostiche e cliniche: DICOM (.dcm); JPEG (.jpg / .jpeg);
- Per documenti firmati digitalmente: P7M (.pdf.p7m / doc.p7m);PDF (Firma PAdES);
- Per messaggistica e comunicazioni: EML (.eml) e MSG (.msg);
- Per dati e reportistica: XML (.xml), TXT (.txt), CSV (.csv).

I formati dei file utilizzati potranno essere periodicamente oggetto di aggiornamento sulla base dell'evoluzione tecnologica e dell'obsolescenza degli strumenti software disponibili, oltre che degli standard internazionali in essere.

III.6 – Metadati dei documenti informatici

Al documento informatico è associato l'insieme minimo dei metadati, con riferimento all'allegato 5 delle Linee Guida AGID.

L'insieme minimo dei metadati è il seguente:

- identificativo univoco e persistente e/o numero di protocollo;
- data di chiusura e/o protocollazione;
- oggetto;
- soggetto produttore, identificazione/codice univoco che identifica l'ente;
- destinatario;
- classificazione del documento sulla base del Piano di classificazione adottato;
- numero allegati e descrizione;
- impronta digitale.

SEZIONE IV- IL PROTOCOLLO INFORMATICO

IV.1 Il Protocollo informatico: definizione, funzioni e oggetto

Il registro di protocollo è un atto pubblico di fede privilegiata, ossia prova sino a querela di falso la data e l'effettivo ricevimento o spedizione di un documento determinato, di qualsiasi forma e contenuto ed è quindi idoneo a produrre effetti giuridici tra le parti che decorrono dalla data attestata dal registro di protocollo.

Il Protocollo informatico Sisar è **unico** per tutta l'AOO Sulcis Iglesiente e sono pertanto inammissibili e considerati nulli di diritto, altri protocolli (di settore, di divisione, protocolli multipli, etc.) o altri sistemi di registrazione dei documenti diversi dal protocollo informatico.

La Numerazione di protocollo è unica e progressiva, corrisponde all'anno solare ed è composta di sette numeri. Ad ogni documento è dato solo un numero che non può essere utilizzato per la registrazione di altri documenti anche se correlati allo stesso.

I

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

Il protocollo informatico è uno strumento dell'archivio corrente che svolge oltre la suddetta funzione giuridico-probatoria, anche la funzione di gestione documentaria di conservazione e ricerca dei documenti e di monitoraggio dei flussi documentali.

Sono oggetto di registrazione obbligatoria:

- Tutte le istanze e le dichiarazioni sottoscritte con firma digitale, o sottoscritte e presentate allegando documento d'identità, o con identificazione dell'istante o dichiarante attraverso il Sistema Pubblico di Identità (SPID), Carta d'Identità Elettronica (CIE) o Carta Nazionale Servizi (CNS) o con App IO
Il mancato avvio del procedimento da parte del titolare dell'ufficio competente a seguito di istanza o dichiarazione inviata con le modalità di cui sopra, comporta responsabilità dirigenziale /disciplinare dello stesso (art 65/comma 1 ter CAD)
- tutte le comunicazioni che provengono da o sono inviate da domicili digitali eletti (IPA, INI-PEC, INAD);
- tutti i documenti ricevuti e spediti, indipendentemente dal supporto (cartaceo o informatico) e dal mezzo di trasmissione.

Sono esclusi dall'obbligo di protocollazione i documenti elencati dall'art 53, comma 5 del DPR 445/2000, ossia:

- gazzette ufficiali;
- bollettini ufficiali;
- notiziari della pubblica amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiali statistici;
- atti preparatori interni;
- giornali;
- Riviste;
- Libri;
- materiali pubblicitari;

- inviti a manifestazioni.
- e tutti i documenti già soggetti a registrazione particolare dell'amministrazione.

Sono esclusi dall'obbligo di registrazione al protocollo anche tutti i documenti informatici già soggetti a registrazione particolare, e precisamente:

- I documenti amministrativi soggetti a registrazione nel Repertorio Aziendale:
 - Contratti;
 - Convenzioni.
- I documenti amministrativi soggetti a registrazione nell'Albo Pretorio Aziendale
- I documenti contabili
 - Fatture con registrazione SDI (Sistema di Interscambio);
 - Ordini con registrazione NSO (Nodo Smistamento Ordini).
- Documentazione sanitaria
 - Documentazione clinica del paziente: cartelle cliniche (elettroniche e cartacee), verbali di pronto soccorso, lettere di dimissione e schede di dimissione ospedaliera (SDO);
 - Referti e prescrizioni: Referti di laboratorio, esami radiologici, tracciati diagnostici ed esiti di riscontri autoptici;
 - Registri dei reparti: Registri operatori, registri dei parti e casistiche dei singoli medici.
 - Flussi verso altre strutture: Richieste interne di esami verso altri reparti o presidi e schede di trasporto di campioni biologici;
 - Certificazioni mediche dei dipendenti: Certificati di malattia inviati telematicamente tramite i canali dedicati (es. INPS), gestiti direttamente dagli applicativi delle Risorse Umane.

IV.2 – La registrazione di protocollo

La prima attività di gestione documentale è la registrazione di protocollo con cui viene assegnato al documento, automaticamente e in forma permanente e non modificabile, la data certa, un numero progressivo, l'impronta digitale del documento e tutte le informazioni obbligatorie (nome mittente o destinatario e oggetto), che valgono a garantire la **tracciabilità** e l'**integrità** del documento

La registrazione di protocollo per ogni documento ricevuto o spedito dall'Azienda è effettuata mediante la memorizzazione delle seguenti informazioni:

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o il destinatario per i documenti spediti, registrati in forma non modificabile;
- Oggetto del documento, registrato in forma non modificabile;
- Data e protocollo del documento ricevuti (se disponibili);
- L'impronta del documento informatico, se trasmesso in via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

A garanzia della integrità e non modificabilità della registrazione di protocollo effettuate, questa vengono trasmesse al Sistema di conservazione attraverso un job automatico di sistema che si attiva ogni giorno dalle ore 19:00 alle ore 20:00 per produrre il registro giornaliero del giorno precedente, protocollarlo sul Registro apposito (RGP) e inviarlo ai servizi di conservazione Aruba

La registrazione degli elementi obbligatori del protocollo informatico non può quindi essere modificata, integrata, cancellata ma soltanto annullata mediante apposita procedura in capo al Responsabile della gestione documentale con il supporto del personale del Servizio SIAMM.

Gli elementi obbligatori della registrazione, che non possono essere oggetto di modifica, servono ad attribuire al documento data e provenienza certa attraverso la registrazione di determinate informazioni rilevanti sul piano giuridico-probatorio.

Essi sono:

- numero di protocollo progressivo e costituito da almeno sette cifre numeriche;
- data di registrazione;
- corrispondente, ovvero mittente per il documento in arrivo, destinatario per il documento in partenza;
- oggetto. Fatti salvi i vincoli di riservatezza epistolare, sono da evitare forme di oggettivazione troppo generica, in quanto la possibilità di identificare un documento fra altri di analogo argomento è strettamente legata alla significatività della descrizione dell'oggetto. A tutela dei dati personali, per il principio Privacy-by-default (art. 25 del Reg. UE 2016/679), si raccomanda di non riportare nell'oggetto esplicitamente categorie particolari di dati presenti sul documento, avendo sempre cura di non abbinare "Nome e Cognome" a categorie particolari di dati (Art. 9 del Regolamento UE 679/2016);
- impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile;
- numero degli allegati;
- descrizione degli allegati.

L'insieme di tali elementi è denominato registrazione.

Le uniche informazioni modificabili di una registrazione di protocollo sono:

- l'assegnazione interna all'amministrazione;
- la classificazione archivistica;
- Il fascicolo;
- Note;
- Collegamenti.

(per la procedura di modifica dell'assegnazione Vedi avanti paragrafo VII.3)

L'annullamento non può essere mai consentito, né autorizzato nei casi in cui:

a) il protocollo di cui si chiede l'annullamento sia pervenuto in entrata attraverso un canale digitale (PEC, mail istituzionali);

b) il protocollo di cui si chiede l'annullamento sia stato spedito in uscita con esito positivo attraverso uno o più canali digitali (PEC, mail istituzionali);

.

Le azioni di annullamento e di modifica delle registrazioni di protocollo vengono rimangono tracciate e visibili nel rispetto di quanto previsto dall'art. 54, comma 2 del TUDA

La necessità di modificare anche un solo campo tra quelli obbligatori della registrazione di protocollo, per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal Responsabile della gestione documentale o suo delegato.

In tale ipotesi la procedura riporta la dicitura "Registrazione annullata" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie.

Solo il Responsabile della gestione documentale, o suo vicario, è autorizzato a dare disposizioni di annullamento delle registrazioni di protocollo al Servizio Sistemi Informativi Amministrativi, che provvederà ad annullare la registrazione sul sistema informatico.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al Responsabile della gestione documentale.

Il registro riporta i motivi dell'annullamento e, se il documento è stato protocollato nuovamente, il nuovo numero di protocollo assegnato.

Analoga procedura di annullamento va eseguita quando, emerge che ad uno stesso documento in ingresso, ricevuto con mezzi di trasmissione diversi quali, ad esempio originale cartaceo, email, siano stati attribuiti più numeri di protocollo.

IV.3 – Termini per la registrazione dei documenti e il protocollo differito

La registrazione di protocollo si effettua di norma entro la giornata di arrivo del documento o comunque entro 24 ore lavorative dal suo ricevimento o, se intercorrono dei giorni festivi o di chiusura programmata, 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.

Nel caso di un imprevisto temporaneo o nel caso di eccezionale carico di lavoro che non permetta di evadere la corrispondenza ricevuta nella medesima giornata lavorativa (ad es. nel caso di un consistente numero di domande di partecipazione ad un concorso) e qualora dalla mancata registrazione a protocollo del documento nel medesimo giorno lavorativo di ricezione possa derivare un pregiudizio a diritti o legittime aspettative di terzi, i termini per la registrazione dei documenti vengono differiti con provvedimento motivato del Responsabile della gestione documentale o suo delegato

Nel provvedimento di differimento dei termini di registrazione di protocollo devono essere individuati i documenti da ammettere alla registrazione differita, le cause della stessa nonché il termine entro il quale la registrazione a protocollo deve comunque essere effettuata.

Possono essere ammessi alla procedura di protocollo differito soltanto i documenti in arrivo, distinti in tipologie omogenee da indicarsi nel provvedimento di 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 AR e quindi fa fede la data di invio della PEC allo stesso modo del timbro postale di invio della raccomandata AR.

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso viene prodotto automaticamente dal Sistema di Protocollo informatico e reso disponibile in formato PDF.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il Registro giornaliero di protocollo è inviato in conservazione. Tale operazione viene espletata automaticamente dal Sistema di protocollo.

IV.4 – Segnatura di protocollo

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.

La segnatura di protocollo apposta o associata al documento è effettuata contemporaneamente alla registrazione di protocollo o di altra registrazione cui esso è soggetto.

I requisiti necessari di ciascuna segnatura di protocollo sono:

- progressivo di protocollo (almeno 7 cifre numeriche, si rinnovano a ogni anno solare);
- data di protocollo;
- oggetto;
- ID dell'AOO;
- ID dell'ufficio cui il documento è assegnato o che lo ha prodotto;
- indice di classificazione (attribuire un indice al documento desunto da una struttura di voci che è il piano di classificazione);

Inoltre, possono essere aggiunti:

- persona o ufficio destinatari;
- classificazione e fascicolazione di competenza;
- identificazione degli allegati;
- informazioni sul procedimento e sul trattamento.

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione di una etichetta sulla quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- codice identificativo dell'amministrazione;

- codice identificativo dell'AOO;
- data e numero di protocollo del documento.

Nel caso in cui non sia possibile generare l'etichetta, l'operatore addetto all'Ufficio protocollo deve procedere comunque alla protocollazione mediante la segnatura del documento.

IV.5 – Registro di emergenza

Nelle situazioni di emergenza in cui per cause tecniche non sia possibile utilizzare il protocollo informatico, il documento deve essere registrato su un supporto cartaceo, denominato "Registro di emergenza".

L'attivazione del registro di emergenza è autorizzata dal Responsabile della gestione documentale e ne viene data immediata comunicazione agli uffici.

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

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

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

Qualora l'interruzione del funzionamento del Sistema di protocollo informatico si prolunghi per più di ventiquattro ore, il Responsabile della gestione documentale, ai sensi della normativa vigente, autorizza l'uso del Registro di emergenza per il periodo più lungo richiesto che comunque non può essere superiore ad una settimana.

In tali casi sul Registro di emergenza, oltre alle informazioni di cui sopra, vengono riportati gli estremi del provvedimento di autorizzazione.

Infine, quando viene ripristinata la piena funzionalità del sistema, il Responsabile della gestione documentale provvede alla chiusura del Registro di emergenza, annotando sullo stesso il numero delle registrazioni effettuate e la data e l'ora di ripristino della funzionalità del sistema

In sintesi la procedura è la seguente: (Vedi All. 1 e 2 del Manuale)

A) Attivazione del Registro di emergenza:

1. predisporre atto di attivazione del Registro di emergenza a firma del Responsabile della Gestione documentale;)
2. compilare il registro di emergenza [su supporto informatico; manuale (ALL 1)]
3. dare comunicazione agli uffici della attivazione del Registro di emergenza.

B) Al termine dell'emergenza si deve:

- revocare l'autorizzazione al protocollo di emergenza (ALL.2);
- inserire le registrazioni di emergenza nel protocollo informatico attivando l'apposita funzione;
- dare comunicazione alla struttura organizzativa dell'amministrazione della revoca dell'emergenza;
- conservare il registro di emergenza

Sezione V. – Casi particolari di Registrazioni di Protocollo

V.1.a – Circolari e documenti con più destinatari

Le circolari, le disposizioni generali e tutte le altre comunicazioni interne alla ASL SULCIS-IGLESIENTE che abbiano più destinatari si registrano con un solo numero di protocollo generale. Tutti i destinatari sono indicati in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo secondo le modalità previste dalla gestione anagrafica del sistema.

Al fine di garantire l'efficienza, l'efficacia e la tempestività dell'azione amministrativa laddove il numero di destinatari, comunque definiti, sia in numero maggiore di 20 l'operatore di protocollo potrà a seconda del caso:

- assegnare il documento nel sistema di protocollo secondo le normali procedure in uso;

- assegnare il documento nel sistema di protocollo alle sole macrostrutture di appartenenza (es. Dipartimenti) dei singoli destinatari che a loro volta provvederanno a recapitare con modalità telematica (assegnazione nel Sistema informatico o trasmissione a mezzo mail) il documento ai destinatari.

Laddove la comunicazione sia rivolta ad una pluralità indefinita di soggetti interni anche raggruppati per categorie (es. "a tutto il personale della ASL SULCIS-IGLESIENTE", "Al personale del Comparto" ecc.) l'operatore di protocollo potrà a seconda del caso:

- assegnare il documento nel sistema di protocollo alle macrostrutture di appartenenza dei singoli destinatari che a loro volta provvederanno a recapitare il documento ai destinatari con modalità telematica (assegnazione nel Sistema informatico o trasmissione a mezzo mail);

- trasmettere il documento protocollato alle mail dei destinatari (istituzionali ovvero altre mail espressamente indicate quale indirizzo di recapito) mediante sistemi di trasmissione massiva, riportando nel campo note associato al numero di protocollo acquisito l'avvenuta trasmissione a mezzo mail con indicazione della data e dell'ora di invio);

- pubblicare il documento in apposita sezione dedicata della INTRANET aziendale riportando nel campo note associato al numero di protocollo acquisito l'avvenuta pubblicazione con indicazione della sezione della Intranet e della data di pubblicazione.

V.1.b– Documenti su supporto cartaceo indirizzati nominalmente al personale dell'Amministrazione, lettere anonime e documenti non firmati

La corrispondenza indirizzata nominativamente a personale dell'Amministrazione è regolarmente aperta e registrata al protocollo, a meno che sulla busta non siano riportate le diciture "riservata", "personale", "riservata personale", "confidenziale" o simili o comunque dalla confezione si evinca il carattere di corrispondenza privata: in questi casi, la busta viene trasmessa chiusa al destinatario che, nel caso, ne richiede la protocollazione al più vicino ufficio abilitato alla registrazione di protocollo.

Le lettere anonime, devono essere protocollate e identificate come tali, con la dicitura “Mittente sconosciuto o anonimo” e “Documento non sottoscritto”. Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.

È compito delle UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall’ufficio assegnatario.

V.1.c – Documenti informatici con certificato di firma scaduto o revocato

Nel caso in cui l’Amministrazione riceva documenti informatici firmati digitalmente il cui certificato di firma risulta scaduto o revocato prima della sottoscrizione, questi verranno protocollati e inoltrati al responsabile del procedimento che farà opportuna comunicazione al mittente.

6.5 – Trasmissioni da piattaforme telematiche

L’Amministrazione è dotata di software gestionali collegati al sistema SISaR Protocollo in grado di acquisire automaticamente il documento e procedere con la registrazione di protocollo, nell’ambito di procedimenti riguardanti specifiche attività.

V.1.d– Integrazioni documentarie

L’addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.

Tale verifica spetta al RPA che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l’indirizzo al quale inviarli.

I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOR sul protocollo generale e inseriti nel fascicolo relativo.

V.1.e – Allegati

Tutti gli allegati devono essere inseriti nel sistema di protocollo, unitamente ai documenti a cui afferiscono, per la registrazione e trattamento secondo la procedura indicata nel presente manuale.

Nel caso in cui una PEC contenga allegati illeggibili che non permettono l’identificazione del UOR di competenza, la PEC dovrà essere restituita al mittente segnalando la problematica e richiedendo un nuovo invio per la registrazione.

V.1.f – Protocollazione di documenti digitali pervenuti erroneamente

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all’AOO non competente, l’addetto al protocollo, previa autorizzazione del responsabile della gestione documentale, provvede a protocollare il documento in uscita indicando nell’oggetto "protocollato per errore" e rispedisce il messaggio al mittente.

Nel caso in cui, nonostante le attente verifiche, non sia possibile per gli addetti al protocollo riconoscere un documento non di competenza dell’AOO, sarà cura del servizio ricevente procedere a protocollare il documento in uscita e rispedirlo al mittente.

V.1.g– Protocollo di documenti cartacei pervenuti erroneamente

Nel caso in cui, nonostante i controlli preventivi, sia protocollato un documento cartaceo erroneamente inviato all'Azienda, l'addetto al protocollo, previa autorizzazione del Responsabile della gestione documentale, provvede a protocollare il documento in uscita, indicando nell'oggetto "protocollato per errore"; il documento oggetto della rettifica viene restituito al mittente con la dicitura "protocollato per errore". Nel caso in cui, nonostante le attente verifiche non sia possibile per gli addetti al protocollo riconoscere un documento non di competenza dell'AOO, sarà cura del servizio ricevente procedere a protocollare il documento in uscita e rispedirlo al mittente.

SEZIONE VI – CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

VI.1 – Il sistema di classificazione documentale

Tutti i documenti ricevuti, spediti o interni all'Azienda al momento della registrazione nel protocollo informatico e contestualmente alla stessa devono essere classificati dall'operatore di protocollo.

Nel caso di documenti in arrivo la classificazione è effettuata dagli utenti autorizzati alla registrazione in entrata e la stessa può essere rettificata dalle strutture/uffici qualora la classificazione assegnata al documento in fase di registrazione sia ritenuta non corretta.

Il programma di protocollo informatico non permette la registrazione in uscita di documenti non classificati.

La classificazione è un'attività obbligatoria nel sistema di gestione informatica dei documenti dell'AOO e si applica, ai sensi della normativa vigente, a tutti i documenti prodotti e acquisiti dalla stessa, siano essi sottoposti o meno alla registrazione di protocollo ai sensi degli artt. 56 e 64 comma 4 del TUDA (D.P.R. 4445/2000)

Le operazioni di classificazione documentale consentono di ordinare i documenti secondo criteri logici e funzionali rendendone più agevole il recupero e la gestione

Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti.

La classificazione è quindi funzionale a:

- costruire l'archivio corrente dell'Azienda;
- costituire la base logica dei fascicoli (vedi Paragrafo seguente).

VI.2 – Il Piano di classificazione o Titolare

Il Piano di Classificazione o Titolare è lo strumento che consente di classificare logicamente i documenti prodotti, ricevuti e spediti dall'Amministrazione e di guidarne la sedimentazione, poiché le voci che lo compongono costituiscono le partizioni astratte e articolate in cui inserire la documentazione.

Il Piano di Classificazione o Titolare è strutturato in una gerarchia ad albero che comprende

l'insieme delle voci logiche stabilite sulla base delle funzioni dell'ente, gerarchicamente strutturate e articolate in gradi divisionali che procedono dal generale al particolare: titolo, (= rami di macro attività svolte dall'Azienda) classe (= tipologia di documenti) ed eventuale sottoclasse. (materia oggetto del documento) (Vedi Allegato 4)

Il Piano di classificazione è inserito all'interno del sistema di gestione documentale e può essere oggetto di revisione in seguito a modifiche di carattere normativo o statutario. Il Responsabile della gestione documentale verifica periodicamente la rispondenza del Piano di classificazione ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento

VI.3– Le aggregazioni documentali – Il fascicolo informatico.

L'Azienda documenta la propria attività tramite funzioni del sistema di gestione informatica dei documenti finalizzate alla produzione, alla gestione e all'uso delle aggregazioni documentali informatiche, corredate da opportuni metadati.

All'interno dell'AOO i flussi documentali vengono gestiti mediante fascicoli informatici predisposti secondo il Piano di classificazione e il relativo Piano di organizzazione delle aggregazioni documentali (o Piano di fascicolazione), anche con riferimento a fascicoli non afferenti a procedimenti.

Ogni documento registrato – in arrivo, in partenza o interno – è quindi classificato e successivamente inserito in una delle aggregazioni documentali (fascicoli) aperte in corrispondenza di ogni voce del Titolare: pertanto una corretta classificazione è necessaria per organizzare correttamente i documenti all'interno dei fascicoli.

All'interno di ciascun fascicolo i documenti sono inseriti secondo l'ordine cronologico di registrazione e la loro sedimentazione avviene in maniera tale che venga immediatamente individuato il documento più recente

Il fascicolo è l'unità di base dell'archivio corrente e contiene documenti classificati in maniera omogenea in base al contenuto, in quanto concorrono allo stesso affare, attività o procedimento.

Ai sensi della normativa vigente, l'obbligo di fascicolazione dei documenti riguarda sia i documenti contraddistinti dalla segnatura di protocollo sia i documenti procedurali non registrati.

Si distinguono differenti tipologie di fascicolo:

- Fascicolo per affare: raccoglie i documenti relativi a una competenza non oggetto di procedura o procedimento amministrativo; per gli affari non esiste un termine di conclusione previsto da norme;
- Fascicolo per procedimento amministrativo: conserva i documenti relativi ad azioni amministrative omogenee intraprese dall'ente e destinate a concludersi con un provvedimento finale;
- Fascicolo per attività: conserva i documenti, generalmente predefiniti, prodotti nell'ambito di una procedura prestabilita (con tempi certi, con contenuto tipico, per attività che possono reiterarsi nel tempo) che non porta all'adozione di un provvedimento amministrativo finale;
- Fascicolo di persona: conserva tutti i documenti afferenti a diversi procedimenti amministrativi, affari o attività, ma relativi a una determinata persona fisica o giuridica; la chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'ente.

È compito del Responsabile del procedimento amministrativo o dell'affare (RPA) assicurare la corretta gestione e conservazione dei documenti relativi ai procedimenti di propria competenza; pertanto, è affidata a tali responsabili l'attuazione delle disposizioni inerenti al corretto funzionamento dell'archivio corrente di propria competenza, inclusa la corretta creazione e tenuta dei fascicoli, in particolare:

- per ogni procedimento, affare o attività vige l'obbligo per l'Amministrazione di conservare in un fascicolo informatico gli atti, i documenti e i dati da chiunque formati su supporto informatico;
- gli atti, i documenti e i dati da chiunque formati su supporto analogico, invece, devono essere obbligatoriamente conservati in un fascicolo cartaceo, salvo i casi in cui l'originale cartaceo è scartato in seguito alla creazione di una copia conforme informatica.

In presenza di documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un unico affare o procedimento amministrativo, l'Amministrazione dà vita ad un fascicolo ibrido che dà origine a due unità archivistiche di conservazione differenti; l'unitarietà del fascicolo è garantita dal sistema mediante l'indice di classificazione e il numero di repertorio che dovrà essere identico su entrambe le unità archivistiche.

In presenza di documenti cartacei da inserire in fascicoli informatici, dovrà essere prodotta copia per immagine degli stessi secondo la normativa vigente.

L'originale cartaceo sarà conservato presso l'ufficio competente fino al trasferimento all'archivio di deposito.

VI.4–Formazione e identificazione dei fascicoli

L'organizzazione dei fascicoli digitali di ogni UOR è definita dal responsabile del procedimento; l'apertura del nuovo fascicolo è effettuata materialmente dall'operatore di protocollo abilitato. La formazione di un nuovo fascicolo avviene attraverso l'operazione di apertura regolata dal manuale operativo del sistema, che prevede la registrazione sul repertorio/elenco dei fascicoli o nel sistema informatico delle seguenti informazioni:

- categoria e classe del titolare;
- numero del fascicolo (dato in automatico dal sistema);
- oggetto del fascicolo;
- data di apertura;
- Tipologia di fascicolo;
- Ufficio responsabile.

Il sistema di protocollo informatico aggiorna automaticamente il repertorio/elenco dei fascicoli.

Il responsabile del procedimento o i singoli operatori verificano, consultando l'elenco dei fascicoli attivi del protocollo informatico, se il documento si colloca nell'ambito di un fascicolo già aperto, oppure se dà avvio ad un nuovo procedimento; nel primo caso, l'utente ha cura di indicare all'interno dell'applicativo di protocollo i dati del fascicolo nel quale il documento deve essere inserito, se invece dà avvio a un nuovo affare, il responsabile del procedimento, o l'operatore a cui il documento è assegnato, provvede ad aprire un nuovo fascicolo inserendo le informazioni sopra indicate. I documenti prodotti dall'ente sono fascicolati dall'utente che esegue le operazioni di registrazione di protocollo.

I fascicoli dell'archivio corrente sono formati a cura dei responsabili di procedimento e conservati, fino al trasferimento nell'archivio di deposito.

VI.5 Piano di organizzazione delle aggregazioni documentali

Il Piano di organizzazione delle aggregazioni documentali o Piano di fascicolazione è quello strumento che elenca le tipologie di fascicoli in cui organizzare la documentazione per ogni voce del Piano di classificazione/Titolario. I fascicoli aperti nel corso dello svolgimento dell'attività amministrativa sono poi registrati all'interno del repertorio dei fascicoli, strumento che ne consente la gestione e il reperimento.

Se il Piano di classificazione si pone come la rappresentazione astratta delle funzioni e delle competenze dell'ente, il repertorio dei fascicoli – costantemente aggiornato – è la rappresentazione concreta delle attività effettivamente svolte e dei documenti prodotti durante lo svolgimento di tali attività.

Il Piano di organizzazione delle aggregazioni documentali è integrato all'interno del Prontuario di selezione e scarto dell'Ente (Allegato 4) e, come quest'ultimo, è soggetto a verifica e aggiornamento periodico.

VI.6 – Gli strumenti dell'archivio corrente

L'archivio corrente è il complesso dei documenti relativi ad affari, attività o procedimenti amministrativi in corso di istruttoria o verso i quali sussista un interesse non ancora esaurito.

Il trattamento dell'intero sistema documentale comporta la predisposizione di strumenti di gestione dell'archivio corrente che permettano un'efficiente organizzazione e consultazione della documentazione, al fine di garantire la certezza dell'attività giuridico-amministrativa e la conservazione stabile della memoria nel tempo.

In particolare, ai sensi della normativa vigente, le Pubbliche Amministrazioni elaborano strumenti archivistici di supporto alle fasi di:

- classificazione dei documenti;
- aggregazione dei documenti in fascicoli o serie;
- valutazione e selezione dei documenti destinati allo scarto o alla conservazione.

SEZIONE VII – FLUSSI DOCUMENTALI

I flussi documentali comprendono i documenti ricevuti dalla AOO dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno alla AOO e i documenti inviati dalla AOO, all'esterno o anche all'interno della AOO in modo formale.

Le comunicazioni informali tra uffici, lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione, sono ricevute e trasmesse per posta elettronica ordinaria interna e non interessa il sistema di protocollo.

Durante la fase transitoria di migrazione all'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere in formato analogico.

VII.1 - I Documenti provenienti dall'esterno

I documenti che transitano attraverso il servizio postale (pubblico o privato), indirizzati a tutta l'amministrazione, sono consegnati quotidianamente all'Ufficio protocollo che si fa carico di selezionare e smistare la corrispondenza.

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.

Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.

Il personale abilitato al sistema informatico di protocollo controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale PEC e verifica se sono da protocollare.

Nel caso in cui il documento informatico venisse ricevuto su una casella di posta elettronica ordinaria (PEO) il ricevente dovrà inviare al mittente un messaggio con l'indicazione della casella di posta corretta. Il messaggio comunque ricevuto, previa verifica dei presupposti richiesti, viene gestito secondo le procedure previste per il documento digitale.

Se il ricevente, lo ritiene opportuno può procedere alla protocollazione della Email; se il ricevente appartiene ad una UOR in cui non è attivo il Sistema informatico di protocollo, dovrà rivolgersi al punto di protocollazione ad esso più prossimo che procederà alla protocollazione.

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica. Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà di acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a sua disposizione. Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

I documenti cartacei ricevuti a mezzo posta convenzionale o consegnati a mano presso un punto "fisico" di protocollazione vengono da questo direttamente gestiti. I documenti pervenuti a mezzo posta o ritirati dagli uffici postali sono consegnati al Servizio protocollo

Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti. Se la busta è indirizzata ad altra amministrazione, ancora chiusa deve essere restituita al servizio postale che provvede ad inoltrarla all'indirizzo corretto.

Le buste o contenitori o pacchi non contenenti documentazione amministrativa dovranno essere ritirati esclusivamente dal servizio ordinante. Nel caso in cui tale materiale dovesse pervenire agli uffici di protocollo generale gli operatori non potranno ritirarli e verranno restituiti al vettore per la restituzione al mittente.

Quando la corrispondenza non rientra nelle categorie indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.

La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta e, di norma, contestualmente protocollata. La busta si allega al documento per la parte relativa ai timbri postali

Nel caso in cui pervengano su una casella di posta istituzionale PEC o in una casella di posta tradizionale (non PEC), messaggi dal cui contenuto si rileva che gli stessi sono stati erroneamente trasmessi alla AOO (es. messaggi destinati ad altri Enti/soggetti destinatari diversi da ASL Sulcis Iglesiente), l'operatore trasmette un messaggio al mittente, con la dicitura "Si restituisce in quanto messaggio pervenuto per errore - non di competenza della ASL Sulcis Iglesiente". Tale messaggio, se ricevuto tramite la PEC in interoperabilità deve essere trasmesso attraverso la funzione "eccezione".

In entrambi i casi, se conosciuto, si può inserire nella comunicazione l'indirizzo pec corretto dell'Amministrazione destinataria

VII.2 - Assegnazione dei documenti

L'assegnazione dei documenti agli uffici è effettuata dal Servizio Protocollo, o dagli altri punti di protocollazione che abbiano ricevuto il documento, tramite il sistema di protocollo informatico SISaR, sulla base dell'organigramma dell'AOO e consiste nell'operazione di attribuire, direttamente dai punti di protocollazione in entrata, il documento protocollato all'UOR e contestualmente il materiale documentario allegato.

L'UOR ha notizia dell'assegnazione dei documenti attraverso la consultazione quotidiana della lista lavoro documenti. All'assegnazione del documento tramite sistema di protocollo da parte dell'ufficio protocollo non segue mai comunicazione mail se non per situazioni particolari di urgenza precedentemente concordate con il responsabile della gestione documentale.

Il responsabile dell'UOR è in grado di visualizzare i documenti, attraverso le funzionalità del Sistema informatico e, in base alle abilitazioni possedute, potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare la modalità di trasmissione del documento;
- visualizzare la PEC, se ricevuto con questa modalità tramite il sistema di interoperabilità;

L'assegnazione può essere effettuata: per conoscenza o per competenza.

All'assegnazione per competenza segue la presa in carico del documento da parte dell'UOR per il tramite degli operatori di protocollo delegati; in questa sede viene eseguita la classificazione del documento secondo le voci del Titolare e l'inserimento del documento nel fascicolo di competenza preesistente o eventualmente in un nuovo fascicolo.

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

I destinatari del documento per "competenza" e/o "per conoscenza" lo ricevono esclusivamente in formato digitale; nel primo caso devono effettuare l'operazione di "presa in carico" e procedere alla fascicolazione del documento. La "presa in carico" dei documenti informatici viene registrata dal sistema di protocollo in modo automatico e la data di ingresso dei documenti nelle UOR

competenti coincide con la data di assegnazione degli stessi

Nel caso possono di assegnazione per conoscenza si deve effettuare esclusivamente l'operazione di "visto".

Nel caso di assegnazione di copie informatiche di documenti analogici l'originale cartaceo viene tenuto presso l'Ufficio Protocollo e messo a disposizione del Servizio destinatario che provvederà a ritirarlo entro 15 giorni dalla data di protocollazione. . Le modalità di trasmissione/ritiro degli atti giudiziari alla/dalla SC Affari Legali vengono concordate direttamente col Direttore della struttura.

L'UOR competente, potrà visualizzare i documenti mediante la funzione "lista lavoro" del sistema di protocollo ed effettuare le medesime operazioni effettuate nel caso di documento pervenuto in formato digitale.

VII.3 – Modifica delle assegnazioni

La registrazione a protocollo sulla procedura informatica risulta in "carico" ad un determinato ufficio. Nel caso in cui l'assegnazione risulti non completa o errata, l'UOR assegnataria può:

- aggiungere ulteriori destinatari utilizzando la funzionalità copie presente nel Sistema di Protocollo;
- utilizzare la funzionalità "smista" per trasmettere il documento al servizio competente, se di sua conoscenza, oppure all'ufficio protocollo che provvederà alla sua riassegnazione; ad ogni passaggio è possibile sempre utilizzare lo spazio "note" per eventuali comunicazioni.

Il sistema di protocollo tiene traccia dei passaggi di cui sopra, memorizzando per ciascuno di essi l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. (Vedi Par. IV.2).

VII.4 I documenti inviati dalla AOO

I documenti inviati dalla AOO consistono nel flusso dei documenti in uscita formati dal personale degli uffici dell'Amministrazione nell'esercizio delle proprie funzioni, destinato ad essere trasmesso ad altra Amministrazione o ad altri soggetti privati, ovvero ad altro ufficio della stessa AOO.

Durante la fase transitoria di migrazione all'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere in formato analogico.

Ogni UOR è autorizzata a svolgere attività di registrazione di protocollo per la corrispondenza in uscita qualora la stessa sia a firma del responsabile della UOR o del responsabile del procedimento amministrativo; pertanto tutti i documenti originali da spedire, siano essi digitali o analogici, sono direttamente protocollati dalle UOR.

Nel caso in cui una UOR si trovi nella impossibilità temporanea di procedere alla protocollazione di un documento in uscita può rivolgersi all'Ufficio di protocollo che provvederà ad inserire come mittente l'UOR richiedente e come destinatario quello indicato nel documento (esterno/interno).

L'UOR mittente potrà verificare l'avvenuta protocollazione e visionare il documento utilizzando la

funzione “lista lavoro” sulla propria scrivania di protocollo.

La spedizione dei documenti digitali avviene all'interno del sistema informatico di gestione dei documenti con le procedure adottate dal manuale operativo dello stesso, dopo essere stati classificati, fascicolati e protocollati e comunque secondo i seguenti criteri generali:

- i documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, abilitato alla ricezione della posta per via elettronica, tramite casella di posta elettronica certificata;
- per la spedizione l'Azienda si avvale di una casella di posta elettronica certificata e dei servizi di autenticazione e marcatura (art.27, comma 3, DPR n.445/00);
- gli uffici provvedono:
 - ad effettuare l'invio elettronico utilizzando il Sistema di Protocollo informatico se abilitato all'invio delle pec in uscita, oppure utilizzando direttamente la PEC;
 - a verificare l'avvenuto recapito dei documenti spediti per via elettronica.

Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dall'art.49 del CAD

I documenti cartacei da spedire sono trasmessi all'ufficio spedizioni in busta chiusa completi della firma autografa del responsabile del procedimento, del numero di protocollo, della classificazione e del numero di fascicolo. Le buste devono essere accompagnate da un elenco con l'indicazione, per ciascuna lettera, del numero di protocollo, del destinatario e del luogo di destinazione. Nel caso di spedizione che utilizzi documenti di accompagnamento (raccomandate, ecc.), questi devono essere compilati a cura dell'ufficio produttore.

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

Copia del documento cartaceo spedito è archiviata nel fascicolo informatico al momento della protocollazione, mediante la funzione di inserimento degli allegati nel Sistema di protocollo informatico SISaR; allo stesso modo le ricevute delle raccomandate, le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo fascicolo a cura delle UOR.

Le UOR curano anche l'archiviazione delle ricevute di ritorno delle raccomandate. Queste ultime, sulle quali, precauzionalmente, è stato trascritto sia il numero di protocollo attribuito al documento a cui esse si riferiscono, sia l'UOR mittente, sono inizialmente raccolte dal Servizio Spedizioni e successivamente consegnate alle UOR medesime.

SEZIONE VIII – PIANO DI SICUREZZA

Il presente capitolo riporta, per le ragioni indicate nella premessa a questo Manuale, quanto indicato da ARES in merito alle misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

VIII.1 – Obiettivi

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'amministrazione/AOO/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 alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

VIII.2 – Attività e competenze

Considerata la complessità e la pluralità di competenze necessarie in funzione della organizzazione propria della AOO nonché delle misure e delle politiche di sicurezza necessarie per stabilire adeguati livelli di sicurezza proporzionati al 'valore' dei dati/documenti trattati, le funzioni/responsabilità inerenti la sicurezza del sistema di protocollo, sono assicurate attraverso l'azione coordinata, diretta e responsabile delle diverse figure coinvolte nella gestione del "servizio protocollo".

In particolare il Responsabile della gestione documentale, -il DPO e il SIAMM concorrono congiuntamente ad elaborare e definire:

- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui alla normativa vigente, in caso di trattamento di dati personali;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza a livello di accessi;
- i piani specifici di formazione degli addetti;
- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le misure tecniche e organizzative necessarie per assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni.

Compete altresì al SIAMM su richiesta del Responsabile della gestione documentale:

- l'assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- eventuali reset delle password durante la fase di esercizio;
- creazione e chiusura scrivanie e utenze di Protocollo;
- attivazione delle postazioni per la gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate per l'uso del protocollo di emergenza;
- verifica che l'accesso sia consentito soltanto al personale autorizzato per motivi di servizio;
- stabilire e controllare la selettività degli accessi a livello di protezione locale.

Il piano di sicurezza, si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e deve tenere conto ed integrarsi a tutte le disposizioni in materia previste dal DPO.

Il Piano della Sicurezza Informatica è:

- adeguato al rischio in materia di protezione dei dati personali ai sensi dell'art.32 del Regolamento UE 679/2016;

- contiene la descrizione da adottarsi in caso di violazione dei dati personali ai sensi degli art.33-34 del Regolamento UE 679/2016;
- è redatto nell'ambito del piano generale della sicurezza, in coerenza con quanto previsto dal vigente Piano Triennale per l'Informatica nella Pubblica Amministrazione.

Al fornitore del servizio sono demandate le seguenti attività:

- archiviazione giornaliera su nastro, dei backup del database e file system, con conservazione dei nastri come da specifiche di progetto (30 giorni solari);
- archiviazione giornaliera, in formato .pdf, delle copie del registro di protocollo;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie dei dati su nastro e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi lato server.

Il controllo degli accessi fisici ai locali protetti è regolato secondo i seguenti principi:

- ogni persona che accede alle risorse della sede in locali protetti è identificata in modo certo con sistemi di autenticazione forte;
- gli accessi alla sede sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;
- il personale della sede ha l'obbligo di utilizzare il badge sia in ingresso che in uscita dalla sede stessa.

Le misure di sicurezza fisica hanno un'architettura multilivello così articolata:

- a livello di edificio, attengono alla sicurezza perimetrale e sono atte a controllare l'accesso alla sede in cui sono ospitate risorse umane e strumentali;
- a livello di centro di servizio, sono destinate a controllare l'accesso ai locali del centro;
- a livello di locale, sono finalizzate a controllare l'accesso ai locali interni alla sede. Il controllo degli accessi fisici alle risorse della sede dell'amministrazione è regolato secondo i principi stabiliti dall'Area "Funzionamento" Sezione Logistica e sicurezza.

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente, nell'ambito del sistema di protocollo, è stata realizzata attraverso l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico:

- riservatezza dei dati;
- integrità dei dati;
- integrità del flusso dei messaggi;
- la ridondanza dei sistemi di esercizio.

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

L'architettura realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione degli addetti della AOO e degli operatori dell'erogatore del sistema di protocollo, con le seguenti caratteristiche:

- unico login server per la gestione dei diritti di accesso ai servizi applicativi;

- unico sistema di repository delle credenziali di accesso degli utenti;
- unico database delle anagrafiche contenente tutti i profili di utenza.

Presso il centro servizi del fornitore sono disponibili i seguenti impianti:

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

Il centro servizi è posto all'interno di un edificio adibito ad uffici, le sue condizioni ambientali per quanto riguarda polvere, temperatura, umidità, vibrazioni meccaniche, interferenze elettriche e radiazioni elettromagnetiche e livelli di inquinamento chimico e biologico, sono tali da non richiedere misure specifiche di prevenzione oltre quelle già adottate per le sedi di uffici di civile impiego.

Gli impianti e le considerazioni precedenti valgono anche per la componente infrastrutturale della sicurezza aziendale. In particolare:

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

L'accesso dall'esterno da parte di persone non autorizzate non è consentito in base all'architettura stessa del servizio.

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad esempio: dati, transazioni), presenti o transitate sul sistema di protocollo, che occorre mantenere, sia dal punto di vista regolamentare, sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema di protocollo, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite dalle registrazioni dell'applicativo Protocollo.

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:

- l'accesso alle registrazioni è limitato, esclusivamente, ai sistemisti o agli operatori di sicurezza addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- le registrazioni del modulo sono elaborate tramite procedure automatiche dal sistema di autenticazione e di autorizzazione;
- i log di sistema sono accessibili esclusivamente ai sistemisti autorizzati l'operazione di scrittura delle registrazioni del Protocollo è effettuata direttamente dagli applicativi;
- le registrazioni sono soggette a copia giornaliera su disco e a salvataggio su nastro;
- il periodo di conservazione del nastro è conforme alle specifiche di progetto.

VIII.3 – Formazione dei documenti – Aspetti attinenti alla sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO. I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF.

I documenti informatici redatti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (preferibilmente PDF/a), come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

VIII.4 – Gestione dei documenti informatici

Il sistema di protocollo informatico è conforme alle specifiche previste dalla normativa vigente. Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in maniera da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

VIII.5 – Trasmissione e interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con

strumenti informatici non possono prendere/duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'AOO, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata, allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dalla normativa vigente.

Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

VIII.5.1 – Trasmissione e interscambio dei documenti informatici all'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal Codice dell'Amministrazione Digitale.

VIII.5.2 – Trasmissione e interscambio dei documenti informatici all'interno della AOO.

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle già indicate.

Gli uffici organizzativi di riferimento (UOR) dell'AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica istituzionali o mediante le assegnazioni nel sistema di protocollo informatico, in attuazione di quanto previsto dalla Direttiva del Ministro per l'innovazione e le tecnologie del 18 novembre 2005 concernente l'impiego della posta elettronica nelle pubbliche amministrazioni.

VIII.6 – Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso, pubblica (UserID) e privata (Password) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva. La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Le regole per la composizione delle password e il blocco delle utenze valgono sia per gli amministratori dell'AOO che per gli utenti e sono disciplinate da opportuna procedura redatta e aggiornata dai sistemi informativi aziendali.

Il sistema di protocollo fruito dall'AOO:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente, o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una Access Control List (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

Considerato che il sistema di protocollo segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati alla sua UOR, o ad una UOR ad essa subordinata. Questo sistema garantisce la riservatezza dei documenti trasmessi in quanto visibili esclusivamente alle UOR competenti.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca cosiddetta "full text".

Nel caso in cui fossero necessari livelli differenti di riservatezza per particolari tipologie di documenti trattati, tali esigenze dovranno essere adeguatamente motivate e portate all'attenzione del responsabile della gestione documentale.

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal SIAMM previa formale richiesta del Responsabile della struttura di assegnazione.

Nel caso in cui la richiesta evidenzia la presenza di elementi di profilazione in contrasto con le disposizioni organizzative vigenti il SIAMM potrà sottoporre la valutazione preventiva alla profilazione al Responsabile della Gestione Documentale.

Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione

alla cancellazione e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti principi operativi:

- gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta esplicita dell'amministratore dell'AOO o per errori di inserimento);
- la credenziale privata degli utenti e dell'amministratore AOO transita in chiaro al momento della comunicazione della "one time password" e crittografata al momento del log-in.

VIII.6.1 – Utenti esterni alla AOO – Altre AOO/Amministrazioni.

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO/Amministrazioni avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui agli art. 72 e ss del d.lgs 7 marzo 2005 n. 82.

Le AOO che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzano funzioni di accesso per ottenere le seguenti informazioni:

- numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
- identificazione del l'UOR di appartenenza del RPA.

VIII.6.2 – Utenti esterni alla AOO – Privati.

L'accesso ai documenti è disciplinato dal Regolamento sul diritto di accesso documentale e civico.

Come previsto dal D.Lgs. n.33/2013, così come modificato dal D.Lgs. n.97/2016, è garantito a tutti i cittadini, mediante l'istituzione dell'accesso civico, la libera consultazione di tutti gli atti dell'Ente per i quali è disposta la pubblicazione obbligatoria.

Sul sito istituzionale è consultabile, pertanto, l'apposita sezione denominata "Amministrazione Trasparente" a cui il cittadino ha libero accesso e nella quale sono disponibili informazioni integre e conformi all'originale, pubblicate in formato di tipo aperto.

Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.

VIII.7 – Conservazione e memorizzazione dei documenti analogici, informatici e delle rappresentazioni digitali dei documenti cartacei

Il servizio per la gestione dei flussi documentali e degli archivi elabora ed aggiorna il 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. Dei documenti prelevati dagli archivi deve essere tenuta traccia del movimento effettuato e della richiesta di prelevamento.

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

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo, e conservati nell'archivio informatico a cura del Responsabile della Conservazione.

Le rappresentazioni digitali dei documenti originali su supporto cartaceo, acquisite con l'ausilio dello scanner, sono memorizzate nel sistema, in modo non modificabile, al termine del processo di registrazione.

VIII.8 – Conservazione dei documenti informatici

Il Responsabile della Conservazione documentale provvede, in collaborazione con il Responsabile della Gestione Documentale e con il supporto della tecnologia disponibile, a conservare i documenti informatici, e a controllare periodicamente a campione la leggibilità dei documenti stessi.

Il Responsabile della Conservazione documentale individua il Conservatore Digitale esterno certificato AGID, che effettuerà tutte le operazioni previste dalla normativa vigente ai fini della conservazione a norma.

Il sistema di conservazione deve inoltre fornire la documentazione del software di gestione e conservazione, del sistema di sicurezza, delle responsabilità per tutte le fasi di gestione del sistema documentario e delle operazioni di conservazione dei documenti.

Il manuale di gestione e i relativi aggiornamenti devono essere conservati integralmente e perennemente nell'archivio dell'ente.

VIII.9 – Trasferimento delle unità archivistiche negli archivi di deposito

La documentazione analogica corrente è conservata a cura del responsabile del procedimento fino al trasferimento nell'archivio di deposito.

All'inizio di ogni anno solare il responsabile della UOR, verificata l'effettiva conclusione ordinaria della pratica, provvede all'estrazione dall'archivio corrente cartaceo della documentazione che non si ritiene più necessario trattenere presso lo stesso e predispone l'elenco dettagliato dei fascicoli per il trasferimento della documentazione all'archivio di deposito competente per territorio, effettuando previamente la verifica della possibilità di scarto di eventuali atti secondo quanto stabilito nel Regolamento e prontuario di selezione e scarto per gli archivi.

I fascicoli informatici, mediante specifiche funzionalità di sistema, vengono trasferiti nel sistema di conservazione adottato.

VIII.10 – Pacchetti di versamento

Il Responsabile della Gestione Documentale assicura la trasmissione del contenuto del pacchetto di versamento al sistema di conservazione secondo le modalità operative definite nel Manuale di conservazione del conservatore.

Il Responsabile della conservazione dell'ente genera il rapporto di versamento relativo ad uno o più pacchetti di versamento e una o più impronte relative all'intero contenuto del pacchetto, secondo le modalità descritte nel Manuale di conservazione.

VIII.11 – Selezione dei documenti

Periodicamente, in base al Prontuario di selezione e scarto (allegato 4), viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale, secondo le regole previste dal Regolamento di selezione e scarto vigente, con l'invio della proposta alla competente Soprintendenza Archivistica.

IX – APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI

IX.1 – Modalità di approvazione e aggiornamento del manuale

L'Amministrazione adotta il presente "Manuale di gestione documentale" su proposta del responsabile della gestione documentale.

Il presente manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.

IX.2 – Pubblicità del presente manuale

Il presente manuale è disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento sul sito istituzionale della Asl Sulcis Iglesiente amministrazione

Inoltre copia del presente manuale è inviata ai direttori delle UOR.