SOLUZIONI PER IL SISTEMA ECONOMICO S.P.A.

MANUALE DI GESTIONE DOCUMENTALE

ver 1.7

17/09/2019

PRESENTAZIONE

Il Codice dell'Amministrazione Digitale, di seguito CAD, è stato istituito con il decreto legislativo 7 marzo 2005, n.82, successivamente modificato e integrato, dapprima con il decreto legislativo 22 agosto 2016 n.179 e poi con il decreto legislativo 13 dicembre 2017 n.217. Il CAD riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese.

Ai sensi dell'articolo 2, comma 2, del CAD, il codice si applica alle pubbliche amministrazioni vere e proprie, elencate all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n.165, ai gestori di servizi pubblici e alle società il cui capitale è controllato da una amministrazione pubblica, fattispecie nella quale ricade SOSE.

Peraltro, non tutti gli articoli del CAD e della normativa da esso derivata si applicano alle società a controllo pubblico, ma solo alle pubbliche amministrazioni.

In particolare, SOSE, non essendo una pubblica amministrazione in senso stretto, non ha l'obbligo di rispettare le Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del CAD, come definite nel DPCM del 3 dicembre 2013.

Tuttavia, in attesa di chiarimenti da parte dell'ente competente, la SOSE ha deciso ugualmente di seguire le regole tecniche per il protocollo informatico e provvedere alla nomina di un responsabile per la gestione documentale.

Il presente documento costituisce, pertanto, il Manuale della Gestione Documentale previsto, da ultimo, dall'articolo 3, comma 1, lettera c) del DPCM del 3 dicembre 2013 con il contenuto indicato dall'articolo 5 del medesimo DPCM.

Sotto il profilo applicativo, SOSE si è dotata di un protocollo informatico unico, coerentemente a quanto disciplinato dall'articolo 3, comma 1, lettera e), del citato DPCM.

Con l'entrata in funzione del protocollo e con l'avvio del sistema di digitalizzazione dei documenti, viene adottato un titolario di classificazione, predisposto con lo scopo di organizzare in maniera omogenea i documenti che si riferiscono a medesimi procedimenti secondo una logica di processo.

Sotto il profilo organizzativo, il titolario di classificazione, riportato in ***ALLEGATO 1,*** è pertanto il frutto delle attività di analisi e di classificazione dei documenti condotte con le Unità e aree organizzative di SOSE.

Il presente manuale, ad eccezione di alcuni allegati contenenti informazioni confidenziali e/o di interesse esclusivamente interno alla SOSE, è pubblicato sul sito internet istituzionale di SOSE sotto la sezione "Società trasparente / Altri contenuti".

INDICE

SEZIONE 1 – GENERALITÀ E ATTI PRELIMINARI

- PRINCIPI GENERALI
- METODOLOGIA PER LA STESURA DEL MANUALE DI GESTIONE
- ELIMINAZIONE DEI REGISTRI DIVERSI DAL REGISTRO DI PROTOCOLLO INFORMATICO

1. PRINCIPI GENERALI

1.1. Premessa

Obiettivo del presente **Manuale di Gestione Documentale** (d'ora in avanti indicato anche come MGD) è:

- descrivere il sistema di gestione, anche ai fini della conservazione, dei documenti informatici coerentemente a quanto stabilito dalla normativa e dalle direttive impartite presso SOSE – Soluzioni per il Sistema Economico S.p.A. (di seguito SOSE), in termini *di supporto* all'espletamento delle attività degli utenti del sistema, nei loro diversi ruoli all'interno dell'organigramma, in quanto una corretta ed efficace gestione dei documenti aziendali rappresenta un obiettivo comune a tutti gli utenti;
- realizzare le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno di SOSE, attraverso il corretto funzionamento del protocollo informatico, ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa;
- disciplinare le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo o interesse.
- favorire, tra gli altri elementi, la *digital transformation* nell'ottica di una maggiore efficienza dei processi associata a un incremento di produttività e al miglioramento dei processi decisionali.

In ottemperanza a quanto stabilito dalle direttive e dalle norme di seguito richiamate, le regole e le procedure riportate sul MGD sono state definite a conclusione delle attività preliminari di rilevazione, analisi e disegno dei processi interni di SOSE connesse con la gestione dei documenti, la migrazione dei documenti in ingresso dal supporto cartaceo al supporto informatico, l'introduzione di un sistema di classificazione e di un piano di conservazione.

Il MGD, a eccezione di alcuni allegati contenenti informazioni confidenziali e/o di interesse esclusivamente interno alla società, è pubblicato sul sito internet istituzionale di SOSE nella sezione "Società trasparente/Altri contenuti".

1.2. Ambito di applicazione del Manuale

Il presente manuale di gestione documentale (MGD), definito per l'unica AOO di SOSE attivata nel sistema documentale acquisito è adottato ai sensi dell'art. 3, comma 1, lettera d) del DPCM 03.12.2013 concernente le "Regole tecniche per il protocollo informatico".

Il MGD è redatto a cura del Responsabile della gestione documentale (RGD), che ne propone lo schema, e potrà essere aggiornato ogni qualvolta se ne ravvisi la necessità / opportunità, al ricorrere delle condizioni previste.Il MGD descrive le attività di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti, oltre alla gestione dei flussi documentali di SOSE.

Il protocollo fa fede, anche con effetto giuridico, dell'effettiva spedizione e del ricevimento di un documento.

1.3. Acronimi, definizioni e norme di riferimento

Di seguito si riportano gli acronimi utilizzati più frequentemente:

- **MGD -** Manuale di Gestione Documentale nonché del protocollo informatico, dei documenti e degli archivi - strumento che descrive il sistema

di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico DPCM 3 dicembre 2013 e successive modificazioni e integrazioni.

- **iPA –** indice delle Pubbliche Amministrazioni
- **AOO** - Area Organizzativa Omogenea, ovvero un insieme di UOR che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei flussi documentali
- **UOR -** Unità Organizzativa Responsabile - uno o più uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato
- **UU –** Ufficio Utente – un ufficio o una struttura organizzativa minima dell'AOO che utilizza i servizi messi a disposizione dal protocollo informatico; ovvero il soggetto, destinatario o emittente del documento
- **RP –** Responsabile del Procedimento - il dipendente che, con riferimento a uno specifico affare di volta in volta individuato, ha la responsabilità dell'esecuzione degli adempimenti relativi al procedimento
- **RGD** - Responsabile della Gestione Documentale, la figura professionale preposta al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi
- **RPI** – Responsabile della gestione del Protocollo Informatico
- **PPI** – Prodotto di Protocollo Informatico
- **UOP** – Unità Operativa Protocollante – rappresenta una struttura o una risorsa abilitata alla protocollazione e alla gestione dei flussi documentali, per la propria o più UOR
- **PDF** – *Portable Document Format*, formato di file basato su un linguaggio di descrizione di pagina sviluppato da Adobe Systems.

I termini più frequentemente utilizzati nel presente Manuale e le relative definizioni sono riportati nell'***ALLEGATO 2***.

1.4. Il sistema di Gestione Documentale

1.4.1. Unica Area Organizzativa Omogenea

Il presente MGD è focalizzato sull'elemento minimo auto consistente, previsto dalle norme, in termini di sistema archivistico e di gestione documentale, cioè l'Area Organizzativa Omogenea – AOO. Un'AOO è definita come un insieme di UOR che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei flussi documentali.

SOSE – Soluzioni per il Sistema Economico S.p.A. costituisce e istituisce un'unica AOO.

Tale scelta organizzativa consente diversi vantaggi:

- omogeneità e unitarietà di organizzazione dei flussi di documenti giuridicamente rilevanti;
- indipendenza da eventuali riorganizzazioni aziendali;
- uniformità e standardizzazione della classificazione dei documenti;
- riduzione della ridondanza;
- regolamentazione dell'iter documentale;
- riduzione dei costi di gestione.

.

All'interno della AOO di SOSE il sistema di protocollazione è unico e centralizzato, in entrata e in uscita, indipendentemente dalla dimensione e dall'organizzazione o dalla quantità di documentazione trattata.

Per questi motivi saranno unici:

- il presente Manuale di Gestione;
- la direttiva che descrive le operazioni e le procedure archivistiche, i relativi strumenti e i responsabili.

1.4.2. Descrizione del sistema informatico

Il sistema informatico a supporto del "**Sistema di gestione documentale e protocollo informatico**" (in breve SD) è costituito dall'insieme dei "Servizi Documentali" implementati e gestiti dalla UO.

1.4.3. Il Responsabile della Gestione Documentale

SOSE, ha conferito, con l'ordine di servizio n. 12/2019 del 20 giugno 2019, al dott. Emanuele Schirru il ruolo di responsabile del "Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi" (Responsabile della gestione documentale).

Al Responsabile, sulla base dei criteri stabiliti dal DPCM 3 dicembre 2013, spetta il compito di:

- predisporre lo schema del Manuale di Gestione Documentale di cui all'art. 5 del suddetto DPCM, con la descrizione dei criteri e delle modalità di revisione del medesimo;
- curare la pubblicazione del Manuale sul sito istituzionale di SOSE;
- proporre i tempi, le modalità e le misure organizzative e tecniche, di cui all'art. 3, comma 1, lettera e) del suddetto DPCM, finalizzate alla eliminazione di qualsiasi eventuale protocollo diverso dal protocollo informatico;
- predisporre, d'intesa con il Responsabile dei sistemi informativi e il Responsabile per la sicurezza informatica, nonché con il supporto del Responsabile della protezione dei dati personali, il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;
- abilitare, per il tramite del delegato alla gestione del PPI, gli addetti all'utilizzo del PPI e definire per ciascuno di esso il tipo di profilazione;
- vigilare sull'osservanza delle previsioni normative vigenti da parte del personale autorizzato all'utilizzo del PPI;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard previsti dalla normativa vigente;
- custodire le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri;

- garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, le attività di gestione degli archivi;
- autorizzare le eventuali operazioni di annullamento della registrazione di protocollo;
- aprire e chiudere il registro di emergenza del protocollo.

Inoltre, ai fini delle attività istituzionali, il RGD deve assistere la funzione di audit per tutte le operazioni di controllo interno relative ai flussi documentali, alla tenuta del protocollo informatico e alle procedure di conservazione.

Per i casi di vacanza, assenza o impedimento il Responsabile si avvale della facoltà di poter delegare le proprie funzioni nominando uno o più delegati per l'espletamento delle seguenti attività:

- gestione del prodotto di protocollo informatico (PPI) e la tenuta del protocollo informatico sul registro ufficiale e di emergenza;
- gestione dei flussi documentali verso il sistema di conservazione e per le procedure di conservazione;
- produzione e custodia delle copie di salvataggio delle informazioni contenute nel sistema di protocollo.

1.4.4. Sicurezza del Sistema di Gestione documentale

Il Piano della Sicurezza informatica relativo alla formazione, gestione, trasmissione, interscambio e archiviazione elettronica dei documenti, in quanto parte del più ampio Piano di Sicurezza Informatica, viene predisposto ed aggiornato periodicamente dalla società, sulla base delle evoluzioni del sistema stesso.
Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dalla AOO siano resi disponibili, integri e riservati;
- i dati personali 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.

1.4.5. Conservazione delle copie di riserva

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, al termine della giornata lavorativa, il contenuto del registro informatico di protocollo viene inviato in conservazione.

1.4.6. Tutela dei dati personali

SOSE in quanto titolare del trattamento di dati personali con riferimento alle attività di gestione del protocollo e dei flussi documentali ha ottemperato al dettato del Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (c.d. "GDPR"), sia mediante l'adozione di atti formali, aventi rilevanza interna ed esterna, sia attraverso l'implementazione di misure tecnico-organizzative di carattere sostanziale.

In relazione agli adempimenti interni, gli addetti autorizzati / abilitati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri devono

attenersi alle specifiche istruzioni impartite con lettera d'incarico dal titolare e/o dal responsabile interno di riferimento.

Per quanto concerne gli adempimenti esterni, l'AOO pone in essere opportune misure per garantire che i documenti trasmessi all'esterno della propria organizzazione contengano solo eccezionalmente, là dove sia strettamente necessario tenuto conto delle finalità per le quali vengono acquisite e/o comunicate, informazioni relative a stati, fatti e qualità personali, strettamente necessarie per il perseguimento delle finalità.

1.1. Sottoscrizione e scambio di documenti informatici

1.1.1. Sottoscrizione di documenti informatici

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.

SOSE si avvale dei servizi di un'autorità di certificazione accreditata, iscritta nell'elenco pubblico dei certificatori accreditati gestito dall'Agid.

I documenti informatici prodotti da SOSE, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con **firma digitale**, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità.

1.1.2. Strumenti informatici di scambio

Gli strumenti informatici di scambio e gli standard di composizione dei messaggi consentono di garantire sia l'interoperabilità, sia i requisiti minimi di sicurezza di seguito richiamati:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno dell'AOO;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

1.1.3. Firma digitale

La firma digitale rappresenta lo strumento che consente di sottoscrivere documenti in formato digitale, di qualunque tipo, compresa la copia giornaliera del registro di protocollo e di riversamento, con valenza giuridico-probatoria.

Per l'espletamento delle attività istituzionali SOSE fornisce i certificati firma digitale ai soggetti tenuti alla sottoscrizione di atti a rilevanza giuridica esterna.

La disponibilità della firma digitale non modifica i flussi documentali e le modalità di lavorazione del protocollo informatico e, come prescritto dalla normativa vigente, i messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità.

La firma digitale è assegnata alle figure professionali in base alle specifiche lavorative e alle procure attribuite. Il formato di firma utilizzato è di norma quello CAdES (generazione file con estensione .p7m).

1.1.4. Verifica delle firme digitali

Il prodotto di protocollo informatico (PPI) prevede funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati.

La funzionalità però permette solo di visualizzare le informazioni complete sulla firma e sul certificato, ma non si collega alle liste della Certification Authority per effettuare il controllo sulla validità della firma.

La sequenza delle operazioni automatiche prevede:

- apertura della busta "virtuale" contenente il documento firmato;
- verifica della validità del certificato;
- verifica della firma (o delle firme multiple).

La busta "virtuale" è costruita secondo la standard *PKCS#7* e contiene il documento, la firma digitale e il certificato rilasciato dall'autorità di certificazione unitamente alla chiave pubblica del sottoscrittore del documento. Il PPI è in grado di supportare la trasformazione del documento in uno dei formati standard previsto dalla normativa vigente in materia (PDF o XML o TIFF) ed effettuare la segnatura di protocollo.

1.2. Caselle di posta elettronica

1.2.1. Posta elettronica certificata (PEC)

SOSE utilizza, ai sensi del CAD, la PEC quale sistema di comunicazione in grado di attestare, a ogni effetto di legge ai fini dell'opponibilità ai terzi, attraverso la produzione da parte del sistema di ricevute, l'invio e l'avvenuta consegna dei messaggi di posta elettronica.

L'utilizzo della PEC consente di:

- inviare elettronicamente il messaggio;
- conoscere e provare la data e l'ora di trasmissione (UTC);
- garantire e dimostrare l'avvenuta consegna all'indirizzo di posta elettronica del destinatario risultante da pubblici registri;
- interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti ad altre Società o Amministrazioni Pubbliche.

Il PPI provvede automaticamente a classificare e collegare i messaggi di ritorno in invio/segnatura, accettazione, consegna, conferma protocollazione. Nel caso in cui venga annullata la registrazione di protocollo del documento inviato telematicamente tramite PEC, il PPI provvede a inviare sia al mittente che al destinatario dello stesso la ricevuta di annullamento protocollazione.

La trasmissione di un documento informatico tramite PEC è equiparato, ai sensi dell'art. 48 del CAD, all'invio di una raccomandata con ricevuta di ritorno e/o ad una notifica a mezzo del servizio postale.

L'AOO si è dotata di una casella di PEC istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata nell'iPA e denominata info@pec.sose.it . Tale casella costituisce l'indirizzo virtuale dell'AOO. SOSE si è dotata di altre PEC riferite a particolari applicazioni o servizi per una corretta gestione dei messaggi e delle relative ricevute.

Sono attive, inoltre, altre caselle di PEC create esclusivamente per flussi documentali specifici:

- acquisti@pec.sose.it : per la gestione degli approvvigionamenti.

1.2.2. Posta elettronica ordinaria

L'AOO è dotata di una casella di posta elettronica istituzionale info@sose.it di tipo ordinario destinata a ricevere messaggi di posta elettronica contenenti documenti ed eventuali allegati che possono, se del caso, essere destinati alla protocollazione.

SOSE è inoltre dotata di caselle funzionali di posta elettronica in ragione delle proprie strutture organizzative e/o dei processi governati da SOSE stessa, il cui accesso è consentito di norma al personale assegnato alla struttura/processo di riferimento.

Le caselle di posta elettronica funzionali sono:

- protocollo@sose.it : utilizzata per le comunicazioni del progetto fabbisogni standard.

1.3. Sistema di classificazione dei documenti

Al momento di avvio dell'attività operativa del protocollo informatico è stato adottato un unico titolario di classificazione per l'archivio centrale unico di SOSE.

Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base dei processi dell'AOO, consentendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti.

La definizione del sistema di classificazione è stata effettuata prima dell'avvio del sistema di protocollo informatico.

1.4. Formazione

Nell'ambito dei propri piani formativi, SOSE, con riferimento alle attività proprie del sistema di protocollo informatico, di gestione dei documenti e degli archivi, anche con riferimento agli aspetti che concernono la tutela dei dati personali, adotta annualmente un piano di formazione.

1.5. Accreditamento dell'AOO all'iPA

SOSE, nell'ambito degli adempimenti previsti, si è accreditata presso l'indice delle pubbliche amministrazioni (iPA), tenuto e reso pubblico dalla medesima, fornendo le informazioni che individuano SOSE come unica AOO.

SOSE comunica tempestivamente all'iPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa viene resa operativa, in modo da garantire l'affidabilità dell'indirizzo istituzionale di posta elettronica certificata.

2. METODOLOGIA ADOTTATA PER LA STESURA DEL MANUALE DI GESTIONE

Il presente Manuale è stato predisposto:

- coerentemente a tutte le norme e le regole emanate in materia di gestione del protocollo informatico, della gestione documentale, delle misure di sicurezza adottate e di protezione dei dati personali;
- sulla base delle esperienze maturate da SOSE e dalle sue risorse professionali impiegate nella gestione documentale;
- nello spirito di fornire indicazioni e direttive all'interno di SOSE.

Il Manuale predisposto per l'AOO:

- descrive le modalità operative di protocollazione, gestione, conservazione e accesso ai documenti amministrativi, affinché ogni operatore possa trovare nel manuale le istruzioni necessarie per svolgere correttamente, per qualsiasi tipo di documento, le operazioni di registrazione (o non registrazione), fascicolazione e archiviazione;
- definisce, con riferimento alle attività di protocollazione, compiti e responsabilità del personale all'interno dell'AOO;
- fornisce le istruzioni per il corretto e sicuro funzionamento e accesso al servizio;
- è reso pubblico secondo le modalità previste dalle norme vigenti.

3. ELIMINAZIONE DEI REGISTRI DI PROTOCOLLO DIVERSI DAL REGISTRO UFFICIALE DI PROTOCOLLO INFORMATICO E DEI DOCUMENTI CARTACEI

Con la pubblicazione del presente Manuale, e con l'avvio del protocollo unico e del sistema di gestione informatica dei documenti, si intendono sostituiti tutti gli attuali protocolli interni e relativi registri (protocolli di Direzione, di unità, di area, del fax, ecc.) o altri sistemi di registrazione dei documenti diversi dal protocollo unico. Tutti i documenti inviati e ricevuti dall'AOO vengono, pertanto, registrati all'interno del registro unico ufficiale di protocollazione informatica ad opera del personale addetto al servizio.

Il Responsabile della Gestione Documentale (RGD), può effettuare controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della catena documentale, sulla validità dei criteri di classificazione utilizzati in sede di applicazione del registro unico informatico di protocollo.

SEZIONE 2 – LA FORMAZIONE DEI DOCUMENTI

IL DOCUMENTO AMMINISTRATIVO

Per documento amministrativo s'intende (*ex* art. 22 L. 241/1990) ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualsiasi altra specie, del contenuto di atti, anche interni, prodotti o utilizzati ai fini dell'attività amministrativa.
Ai sensi del DPCM 13 novembre 2014, con Documento Amministrativo Informatico (DAI) si identifica ogni documento, nell'accezione sopra indicata, formato e gestito con strumenti informatici dalle pubbliche amministrazioni o dalle società a controllo pubblico, nonché i relativi contenuti; tale documento costituisce fonte di informazione primaria e originale da cui è possibile estrarre, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge. Infine, oltre alla naturale associazione determinata dal termine documento, risultano da includere nei DAI (cfr. sito AgID "Cosa si intende per Documento Amministrativo Informatico") anche:

- le registrazioni informatiche delle informazioni risultanti da transazioni o processi informatici;
- i dati derivanti da moduli o formulari presentati tramite strumenti telematici;
- le comunicazioni, istanze e dichiarazioni che pervengono o sono inviate dalla casella PEC (pubblicata sull'iPA) della pubblica amministrazione o della società pubblica;
- i dati e le informazioni scambiate tra pubbliche amministrazioni e società pubbliche.

2.1 Tipologia dei documenti

Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è così classificabile:

- documento in entrata;
- documento in uscita;
- documento tra uffici (interno formale o interno informale).

Il documento amministrativo come oggetto di scambio, in termini tecnologici è così classificabile:

- documento informatico;
- documento analogico.

Secondo quanto previsto dall'art. 40 del D.lgs. n.82/2005: "*Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71*".

2.1.1. Documenti in entrata

Per documenti "in entrata" s'intendono i documenti giuridicamente rilevanti acquisiti dall'AOO con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

Un documento informatico può essere recapitato:

1. a mezzo posta elettronica ordinaria o certificata, o a mezzo web;
2. su supporto rimovibile quale, ad esempio, *cd rom, dvd, pen drive, ecc.*, consegnato direttamente alle UOR o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per fax o telegramma;
4. con consegna diretta da parte dell'interessato, o tramite una persona dallo stesso delegata, alle UOR.

A fronte delle tipologie descritte ne esiste una terza, denominata "ibrida", composta da un documento analogico (lettera di accompagnamento) e da un documento digitale generalmente trasmesso su supporto rimovibile.

I documenti in entrata all'AOO vengono protocollati, ed eventualmente classificati e fascicolati, dalle UOP e assegnati, esclusivamente in formato elettronico, alla UOR/UU di competenza. La UOR/UU di competenza, se la UOP non è in grado, può provvedere autonomamente alla classificazione ed eventuale fascicolazione.

2.1.2. Documenti in uscita

Per documenti in uscita s'intendono i documenti informatici giuridicamente rilevanti, compresi di eventuali allegati, prodotti all'interno dell'AOO esclusivamente con mezzi informatici e su supporti informatici e inviati, esclusivamente in formato digitale, a privati, a società, a Enti o ad altre Pubbliche Amministrazioni.

I documenti in uscita vengono trasmessi, dopo essere stati protocollati e classificati, tramite la PEC istituzionale ai destinatari dotati di indirizzo PEC di cui agli elenchi (INI-PEC, ANPR, iPA, ecc.) previsti dalle norme, oppure comunicato dagli stessi destinatari, oppure mediante specifiche applicazioni gestionali.

Nel caso in cui, invece, sia necessaria e/o inevitabile la spedizione della versione analogica del "documento in uscita", il documento viene prodotto con strumenti informatici, quindi stampato, sottoscritto in forma autografa e successivamente protocollato.

2.1.3. Documenti tra uffici (interni dell'AOO)

Per documenti tra uffici s'intendono i documenti prodotti all'interno dell'AOO e indirizzati ai propri uffici nell'ambito della stessa AOO. Essi si distinguono in:

- documenti di preminente carattere informativo (interno informale);
- documenti di preminente carattere giuridico rilevante (interno formale, per es. le comunicazioni relative alla gestione del personale).

I documenti interni di preminente carattere informativo sono appunti, memorie informali, brevi comunicazioni scambiate tra uffici e, in quanto tali, non vanno di norma protocollati né registrati. Pur non essendo preclusa la registrazione tramite protocollo informatico, questa tipologia di documenti deve essere normalmente trasmessa con posta elettronica ordinaria.

I documenti interni a carattere giuridicamente rilevante o comunque a rilevanza interna sono quelli redatti per documentare fatti inerenti all'attività svolta o alla regolarità delle azioni amministrative o qualsiasi altro documento, dal quale possano nascere diritti, doveri o legittime aspettative di terzi e, come tali, devono essere protocollati (per es. lettera di dimissioni, giustificativi, richieste di part-time, ecc.).

I documenti interni vengono, di norma, protocollati e classificati da una UOR interna mittente, ma a tale procedura sono abilitati anche le UU e le UOP.

La registrazione dei documenti tra uffici deve essere effettuata una sola volta dal mittente, mentre il destinatario non deve effettuare una nuova registrazione come documento in entrata.

2.2. Documenti analogici

Per documento analogico s'intende un documento formato utilizzando un supporto fisico che assume valori continui, come le tracce su carta (per es. documenti cartacei), come le immagini su film (per es. pellicole mediche), come le magnetizzazioni su nastro (per es. cassette e nastri magnetici audio e video) su supporto non digitale. Di seguito si farà riferimento a un documento amministrativo analogico, vale a dire a quel documento, di norma cartaceo, prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o *text editor* o word processor e poi stampata), nell'ambito dell'attività amministrativa.

In quest'ultimo caso si definisce "originale" il documento cartaceo, nella sua redazione definitiva, perfetta e autentica negli elementi sostanziali e formali, in possesso di tutti i requisiti di garanzia e di informazione del mittente e del destinatario, stampato su carta intestata e munito di firma autografa.

Si definisce minuta l'originale del documento conservato agli atti dell'AOO o UO mittente, cioè nel fascicolo relativo al procedimento o all'affare trattato.

I documenti analogici su supporto cartaceo dotati di firma autografa prodotti dalla AOO o da una UO, aventi per destinatario un ente o soggetto terzo, sono di norma redatti in due esemplari, un originale per il destinatario e una minuta in originale da conservare agli atti del mittente.

I documenti analogici su supporto cartaceo dotati di firma autografa prodotti dalla AOO o da una UO, aventi per destinatario un ufficio interno alla AOO, sono redatti in un unico esemplare.

Un documento analogico può essere convertito in documento informatico tramite opportune procedure di digitalizzazione.

2.3. Repertori

Nell'ambito del sistema documentale, si definiscono ***repertori*** quelle serie di documenti che, prodotti internamente o ricevuti dall'esterno, seguono una propria numerazione progressiva nell'anno solare di riferimento, indipendentemente dalla numerazione di protocollo assegnata. Per cui, di norma, a ciascun documento registrato a repertorio viene assegnato dal sistema documentale anche un numero di protocollo del Registro generale.

I repertori attivati presso l'AOO SOSE sono descritti ed elencati nell'***ALLEGATO 3***.

I documenti vengono registrati a repertorio dalle rispettive UOR o UOP competenti che li istruiscono e ne stabiliscono, d'intesa con il RGD, limiti e criteri di consultazione. Alcuni archivi (per es. le comunicazioni per il personale, ordini di servizio) sono resi pubblici e consultabili da tutti i dipendenti anche attraverso la intranet aziendale.

2.4. Documenti pubblici o riservati

Tutte le tipologie di documento già menzionate (documenti in entrata, in uscita, tra uffici, non protocollati o a repertorio) possono essere registrate secondo due stati di visibilità, pubblico o riservato.

- ***Documenti pubblici***

Documenti che non contengono dati personali e che, tuttavia, possono essere visualizzati solo dagli utenti destinatari per competenza o conoscenza o dagli utenti con specifiche credenziali di accesso al sistema documentale.

- ***Documenti riservati***

Documenti che contengono dati personali o relativi ad affari societari, i quali non possono essere divulgati a terzi non autorizzati.
Tali documenti possono essere visualizzati solo dagli utenti destinatari per competenza o conoscenza e abilitati alla visualizzazione di documenti riservati (personali o dell'ufficio).

2.5. Formazione dei documenti – Aspetti operativi

I documenti dell'AOO vengono sempre prodotti con sistemi informatici.

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

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

Il **formato** del documento deve essere:

- sempre informatico (PDF) quando trasmesso, sempre via PEC, a un'altra Società o Pubblica Amministrazione;
- informatico (PDF) quando trasmesso a privati (via PEC o posta elettronica ordinaria) o professionisti (via PEC) di cui si conosce l'indirizzo digitale;
- informatico (PDF) quando trasmesso all'interno della Società;
- analogico quando trasmesso a privati, di cui non si conosce l'indirizzo di posta elettronica, o a professionisti che richiedono una firma autografa (per es. atti notarili o legali).

La **firma** del documento deve essere:

- digitale del RP e/o del responsabile del provvedimento finale, se trattasi di documento digitale, destinato a un'altra Società pubblica o Pubblica Amministrazione;
- sottoscrizione autografa del RP e/o del responsabile del provvedimento finale, se trattasi di documento analogico, destinato a privati o professionisti come specificato per il formato del documento;
- sottoscrizione elettronica semplice se trattasi di documento formale interno.

La firma (e le eventuali sigle se si tratta di documento analogico) necessarie alla redazione e perfezione sotto il profilo giuridico del documento in uscita devono essere apposte prima della sua protocollazione.

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dal responsabile della UOR.

Il documento deve consentire l'identificazione della Società mittente attraverso le seguenti informazioni:

- la denominazione e il logo della Società;
- l'indicazione completa della UOR che ha prodotto il documento;
- l'indirizzo completo della Società (via, numero civico, CAP, città, provincia);
- il numero di telefono della UOR;

- il codice fiscale/p. iva della AOO.

Il documento deve inoltre recare almeno le seguenti informazioni:

- il luogo di redazione;
- la data (giorno, mese, anno);
- il numero di protocollo;
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- il nominativo e la firma del RP e/o del responsabile del procedimento come su specificato;
- informazioni complete sul destinatario (nome, cognome, sede legale, ecc.).

SEZIONE 3 – FLUSSI OPERATIVI

- FLUSSO DI LAVORAZIONE E REGISTRAZIONE DEI DOCUMENTI
- SMISTAMENTO E ASSEGNAZIONE DEI DOCUMENTI
- PRODUZIONE E ARCHIVIAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO

FLUSSO DI LAVORAZIONE E REGISTRAZIONE DEI DOCUMENTI

Il presente capitolo tratta il flusso di lavorazione dei documenti ricevuti, spediti o interni, e le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione. L'UOR, come la UOP e l'UU, non effettua fotocopie o stampe della corrispondenza trattata, sia in ingresso che in uscita.

3.1. Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno dell'AOO si fa riferimento ai diagrammi di flusso riportati nell'***ALLEGATO 4***.

Tali flussi sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico - probatoria. Essi si riferiscono ai documenti:

- ricevuti dalla AOO, dall'esterno o dall'interno;
- inviati dalla AOO, all'esterno o anche all'interno della stessa AOO in modo formale.

I flussi di lavorazione dei documenti sono il risultato del processo di censimento, di descrizione e di reingegnerizzazione dei processi dell'AOO, quale fase propedeutica a un efficace ed efficiente impiego del sistema di protocollazione informatica e gestione documentale all'interno della AOO medesima.

L'***ALLEGATO 4*** contiene il disegno dei flussi di lavorazione dei documenti per le due tipologie (in entrata – esterni e interni –, in uscita – esterni e interni –) e la descrizione delle relative attività.

3.2. Flusso dei documenti ricevuti dall'AOO

3.2.1. Provenienza esterna dei documenti

I documenti che vengono trasmessi da soggetti esterni all'AOO sono, oltre a quelli richiamati nel capitolo precedente, i telefax, i telegrammi, le e-mail e i supporti digitali rimovibili. Questi documenti vengono recapitati alla/e UOP designata/e. I documenti che transitano attraverso il servizio postale vengono ritirati/consegnati quotidianamente secondo modalità già in uso e consolidate.

3.2.2. Provenienza di documenti interni formali

Per sorgente interna dei documenti s'intende qualunque RP o UOR che invia formalmente la propria corrispondenza ad altra UOR o UU della stessa AOO.

Il documento può essere solo di tipo informatico, secondo i formati standard illustrati nel precedente capitolo e i mezzi di recapito della corrispondenza considerati sono la posta elettronica ordinaria o certificata.

Se al documento interno formale sono associati allegati che superano la dimensione massima prevista per i documenti nel sistema di posta elettronica della AOO, si procede a un riversamento (nelle forme dovute) su supporto elettronico rimovibile da consegnare al destinatario del documento.

3.2.3. Ricezione di documenti informatici via posta certificata istituzionale

La ricezione dei documenti informatici, assicurata tramite la casella di posta elettronica certificata istituzionale, è accessibile solo alle UOP in cui si è organizzata l'AOO e ad alcuni referenti direzionali.

Quando i documenti informatici pervengono alla UOP, la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo.

Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità già in uso presso l'AOO.

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti relativamente a standard di formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime e accessorie. La ricezione comprende anche le attività di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.

Gli addetti della UOP controllano quotidianamente i messaggi pervenuti nella casella di PEC e verificano se sono da protocollare.

3.2.4. Ricezione di documenti informatici via posta elettronica ordinaria o PEC non istituzionale

Il messaggio ricevuto su una casella di posta elettronica ordinaria o PEC non istituzionale o comunque non destinata alla UOP, deve essere inoltrato alla casella di posta istituzionale di SOSE, inviando anche un messaggio, per conoscenza, al mittente con l'indicazione della casella di posta corretta (info@pec.sose.it).

3.2.5. Ricezione di documenti informatici tramite fax server

La ricezione di documenti informatici può avvenire tramite il sistema di fax server di cui è dotata l'AOO. I documenti informatici così pervenuti non devono essere stampati e devono essere trattati con le stesse modalità previste per i documenti ricevuti via posta elettronica certificata.

3.2.6. Ricezione di documenti informatici su supporti rimovibili

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, l'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. La protocollazione di tali documenti si limita alla lettera di accompagnamento.

Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

3.2.7. Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti cartacei pervenuti a mezzo posta, ritirati dagli uffici postali dal personale dell'AOO, oppure, consegnati tramite corriere o tramite singoli cittadini/clienti/fornitori alla reception, vengono tutti inoltrati alla UOP di riferimento.

Le buste o contenitori vengono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario presenti sugli stessi.

La corrispondenza "riservata personale" non viene aperta né protocollata, ma viene consegnata al destinatario che ne valuterà il contenuto ed eventualmente, in caso avesse valore istituzionale, provvederà a inoltrarla alla UOP per la registrazione.

La corrispondenza ricevuta via telegramma o le ricevute di ritorno della posta raccomandata, per ciò che concerne la registrazione di protocollo, vengono trattate

come un documento cartaceo e allegate al protocollo del documento inviato a mezzo raccomandata.

Quando la corrispondenza non rientra nelle categorie su indicate si procede all'apertura delle buste o dei plichi e si eseguono ulteriori controlli preliminari alla registrazione.

La corrispondenza cartacea in entrata viene normalmente aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata. La busta si allega e si archivia con il documento cartaceo per mantenere l'evidenza dei timbri postali.

3.2.8. Errata ricezione di documenti informatici

Nel caso in cui pervengano sulla casella di posta istituzionale dell'AOO (certificata o meno) o in una casella non istituzionale messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore di protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa Società".

3.2.9. Errata ricezione di documenti cartacei

Nel caso in cui pervengano erroneamente a una UOP documenti indirizzati ad altri soggetti, possono verificarsi le seguenti possibilità:

- busta indirizzata ad altra AOO di Pubblica Amministrazione:
  a. si spedisce all'AOO corretta;
  b. se la busta viene aperta per errore il documento, viene protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si spedisce alla AOO destinataria apponendo sulla busta la dicitura "Pervenuta e aperta per errore";
- busta indirizzata ad altro soggetto (persona fisica non appartenente all'AOO o giuridica diversa dall'AOO):
  a. si restituisce alla posta;
  b. se la busta viene aperta per errore il documento, viene protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia al mittente apponendo sulla busta la dicitura "Pervenuta e aperta per errore".

3.2.10. Attività di protocollazione dei documenti

Superati tutti i controlli precedenti i documenti, digitali o analogici, vengono protocollati e registrati nel protocollo generale secondo gli standard e le modalità dettagliate nei capitoli successivi.

3.2.11. Rilascio di ricevute attestanti la ricezione di documenti informatici

Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di PEC utilizzato dalla AOO oppure dal servizio di fax, ciascuno con gli standard specifici. Nel caso di ricezione di documenti informatici per mezzo di posta elettronica ordinaria, la notifica al mittente dell'avvenuto recapito viene effettuata se la notifica è stata richiesta dal mittente stesso.

Non si prevede di effettuare l'invio al mittente della ricevuta di avvenuta protocollazione informatica.

3.2.12. Rilascio di ricevute attestanti la ricezione di documenti cartacei

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

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

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

- fotocopiare (gratuitamente) la prima pagina del documento;
- apporre sulla copia così realizzata il timbro della società con la data e l'ora d'arrivo e la sigla dell'operatore.

3.2.13. Archiviazione dei documenti informatici

I documenti informatici vengono archiviati nel sistema di protocollazione informatica in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.

I documenti ricevuti per via telematica, se privi di vincoli specifici, vengono resi disponibili agli UU, attraverso la rete interna dell'AOO, subito dopo l'operazione di smistamento e di assegnazione. Vengono, se previsto, inviati, periodicamente, in conservazione.

3.2.14. Archiviazione delle rappresentazioni digitali di documenti cartacei

I documenti ricevuti su supporto cartaceo vengono acquisiti in formato immagine attraverso un processo di scansione.

Il processo di scansione avviene in diverse fasi:

- acquisizione delle immagini in modo tale che a ogni documento, anche se composto da più pagine, corrisponda un unico *file*;
- verifica della leggibilità e della qualità delle immagini acquisite;
- collegamento delle immagini alle rispettive registrazioni di protocollo in modo non modificabile;
- memorizzazione delle immagini su supporto informatico, in modo non modificabile.

Le rappresentazioni digitali dei documenti cartacei vengono archiviate, secondo le regole vigenti, all'interno del sistema di protocollazione informatica in modo non modificabile.

Anche i documenti con più destinatari vengono riprodotti in formato immagine e inviati solo in formato elettronico.

In ogni caso non vengono riprodotti in formato immagine i documenti di cui all'elenco nei capitoli successivi.

Tutte le UOP sono abilitate all'operazione di scansione dei documenti.

I documenti cartacei, dopo l'operazione di riproduzione in formato immagine e la protocollazione, vengono archiviati presso la UOP in modalità cronologica.

3.2.15. Classificazione, assegnazione e presa in carico dei documenti

Gli addetti alla UOP eseguono la prima classificazione (o classificazione di primo livello) del documento sulla base del titolario di classificazione adottato presso l'AOO e provvedono a inviarlo alla UOR di destinazione che:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore - il documento è ritrasmesso alla UOP di origine;
- in caso di verifica positiva, esegue l'operazione di presa in carico smistandola al proprio interno all'UU o direttamente al RP.

3.3. Flusso dei documenti inviati dall'AOO

3.3.1. Sorgente interna dei documenti

Per sorgente interna dei documenti s'intende l'unità organizzativa mittente interna all'AOO che trasmette, tramite la UOP di riferimento, la corrispondenza, nelle forme e nelle modalità più opportune, a un Ente o una Pubblica Amministrazione - Centrale o Periferica -, a un contribuente - persona fisica o giuridica -, a un cliente/fornitore dell'AOO ovvero ad altro ufficio (UU o UOR) della stessa AOO.

Per documenti in uscita s'intendono quelli giuridicamente rilevanti, prodotti dal personale degli uffici dell'AOO, nell'esercizio delle proprie funzioni, e inviati a uno o più dei destinatari su indicati.

Il documento è in formato digitale "realizzato" secondo gli standard illustrati nei precedenti capitoli.

I mezzi di recapito della corrispondenza considerati sono quelli che prevedono la trasmissione del documento nel suo formato digitale senza, tranne casi particolari ed eccezionali, il ricorso alla stampa; la PEC è il mezzo prioritario di trasmissione.

Nel caso di trasmissione interna di allegati, al documento di cui sopra, che possono superare la capienza della casella di posta elettronica si procede a un riversamento (con le modalità previste dalla normativa vigente), su supporto rimovibile da consegnare al destinatario contestualmente al documento principale.

I documenti in uscita possono contenere l'invito al destinatario a riportare i riferimenti della registrazione di protocollo nella lettera con cui eventualmente risponde.

3.3.2. Verifica formale dei documenti

Solo specifiche UOP sono autorizzate dall'AOO, per il tramite del RGD, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita.

Le UOR provvedono a eseguire al loro interno le verifiche di conformità della documentazione che deve essere trasmessa e predispongono, eventualmente, le bozze di protocollazione.

3.3.3. Registrazione di protocollo e segnatura

La protocollazione e la segnatura della corrispondenza in uscita, sia essa in formato digitale sia, eventualmente, in formato analogico, è effettuata direttamente dalle UOP abilitate.

Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo possono essere effettuate in bozza dal RP.

3.3.4. Trasmissione di documenti informatici

I documenti informatici sono trasmessi all'indirizzo dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno alla AOO).

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici, coerentemente con quanto previsto nelle procedure di sicurezza aziendale, non possono duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate a essere rese pubbliche.

3.3.5. Trasmissione di documenti cartacei a mezzo posta

La UOP provvede direttamente a tutte le operazioni di spedizione della corrispondenza provvedendo anche all'affrancatura e all'eventuale pesatura, alla ricezione e alla verifica delle eventuali distinte di raccomandate.

3.3.6. Trasmissione di documenti cartacei a mezzo fax

Sul documento trasmesso via fax può essere apposta la dicitura: "La trasmissione via fax del presente documento non prevede l'invio del documento originale".

Solo su richiesta del destinatario verrà trasmesso anche l'originale.

3.3.7. Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito, ovvero le ricevute dei messaggi fax, ovvero le ricevute digitali del sistema di PEC utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo protocollo/fascicolo.

3.4. Registrazione dei flussi documentali

L'organizzazione dei flussi documentali si basa su tre operazioni: la registrazione dei documenti (operazione obbligatoria), la loro fascicolazione e trasmissione in conservazione (operazioni legate alla natura dei documenti).

Il sistema di gestione dei flussi documentali deve quindi:

- fornire informazioni sul legame esistente tra ciascun documento registrato, l'eventuale fascicolo e il singolo procedimento cui esso è associato;
- consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento e il relativo responsabile, nonché la gestione delle fasi del procedimento;
- consentire lo scambio di informazioni con altri sistemi di gestione dei flussi documentali se presenti all'interno della AOO al fine di determinare lo stato e l'iter dei procedimenti complessi.

Il primo passo è quindi la registrazione dei documenti nel sistema di protocollo informatico.

3.4.1. Registrazione a protocollo

La registrazione a protocollo per ogni documento ricevuto o spedito dall'AOO è effettuata mediante la memorizzazione nel sistema di protocollo informatico delle seguenti informazioni e non modificabili:

- data di registrazione;
- numero di protocollo;

- corrispondenti esterni/interni (mittente per il documento in entrata; destinatario o destinatari per quello in uscita);
- oggetto del documento;
- numero e descrizione degli allegati.

La classificazione del documento, invece, costituisce un dato obbligatorio ma modificabile, perché risponde a una finalità gestionale e non a rilevanza giuridica.

A registrazione ultimata il sistema appone sul record del documento un'impronta digitale (**segnatura**), cioè una sequenza di caratteri alfanumerici che identificano in maniera univoca il documento.

3.5. Documenti esclusi dalla registrazione a protocollo informatico

Sono esclusi dalla registrazione al protocollo informatico ai sensi dell'art. 53, comma 5 del DPR 20 dicembre 2000, n.445 le seguenti tipologie documentali:

- Gazzette Ufficiali, bollettini e notiziari della P.A.
- note di ricezione di circolari e disposizioni materiali statistici;
- atti preparatori interni
- giornali, riviste, libri
- materiali pubblicitari
- comunicazioni di cortesia (auguri, congratulazioni, ringraziamenti, condoglianze, ecc.)
- offerte/preventivi di terzi non richiesti
- inviti a manifestazioni;
- tutti i documenti già soggetti a registrazione particolare dell'amministrazione;
- allegati, se non accompagnati da lettera di trasmissione, nonché ogni altra documentazione priva di rilevanza giuridica.

Sono inoltre esclusi dalla registrazione al protocollo informatico i documenti soggetti "a registrazione particolare" di cui al successivo punto 5.7.

3.6. Repertori

La registrazione di documenti a repertorio, trattandosi esclusivamente dei documenti elettronici di cui al capitolo 4, viene effettuata direttamente presso le UOR competenti, opportunamente abilitate a tali inserimenti. I documenti per i quali è necessaria anche l'acquisizione di una o più firme autografe, in assenza di firma digitale, contestualmente alla loro registrazione, vengono acquisiti via scanner, classificati, registrati e assegnati per competenza alle stesse UOR che hanno predisposto l'atto.

L'eventuale originale analogico, cioè il documento nella sua redazione definitiva, perfetta e autentica negli elementi sostanziali e formali, viene conservato nel fascicolo corrispondente presso la UOR responsabile.

3.7. Documenti soggetti a registrazione particolare

Per i procedimenti o gli affari o le operazioni legali e societarie per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto, all'interno dell'AOO, un registro di protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati. In questo ambito rientrano:

- documenti relativi a vicende di persone o a fatti privati o particolari;

- documenti di carattere politico e di indirizzo, documenti relativi a operazioni societarie e a procedimenti legali che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi aziendali;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa e societaria;
- documenti anonimi, individuati ai sensi dell'art. 8, commi 4, e 141 del codice di procedura penale;
- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241 e dall'art. 8 del DPR 27 giugno 1992, n. 352, nonché dalla legge n. 196/2003 (e successive modifiche e integrazioni) e dal GDPR n.2016/679.

Tale tipo di registrazione, effettuata su un registro in formato elettronico, consente, comunque, di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti; in particolare la classificazione, la fascicolazione, la repertorizzazione. Il numero di protocollo assegnato può seguire una codifica stabilita dai responsabili abilitati alla consultazione e registrazione del protocollo riservato.

SMISTAMENTO E ASSEGNAZIONE DEI DOCUMENTI

3.8. Attività di smistamento e assegnazione

L'attività di smistamento consiste nell'operazione d'invio, dalla UOP alla UOR competente in base alla classificazione di primo livello del titolario, del documento elettronico protocollato e segnato e la contestuale trasmissione del materiale documentario oggetto di trattazione.

Con l'assegnazione si attribuisce la responsabilità del procedimento a un soggetto fisico che si identifica nel RP designato.

Preso atto dell'assegnazione, il RP verifica la competenza e, se esatta, prende in carico il documento che gli è stato assegnato.

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

La UOR competente è incaricata della gestione del procedimento a cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento che prende avvio dal documento decorrono comunque dalla data di protocollazione.

Il sistema di protocollazione informatica memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante è utile anche ai fini di individuare i tempi del procedimento e i conseguenti riflessi sotto il profilo della responsabilità.

3.9. Assegnazione dei documenti ricevuti

I documenti ricevuti dalla UOP, sia digitali che analogici, e resi disponibili in formato digitale, sono assegnati alla UOR competente attraverso i canali telematici dell'AOO al termine delle operazioni di registrazione, segnatura di protocollo, memorizzazione su supporti informatici interni al sistema documentale in modo non modificabile.

La UOR competente ha notizia dell'assegnazione di detti documenti tramite un messaggio di posta elettronica interna trasmesso automaticamente dal PPI.

Il responsabile della UOR è in grado di visualizzare i documenti, attraverso le funzionalità del sistema documentale e, in base alle abilitazioni possedute, potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare come assegnatario il RP competente per la materia a cui si riferisce il documento e assegnare il documento in questione.

La "presa in carico" dei documenti informatici viene registrata dal sistema documentale in modo automatico e la data di ingresso dei documenti nelle UOR competenti coincide con la data di assegnazione degli stessi.

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

3.10. Corrispondenza di particolare rilevanza

Quando un documento pervenuto appare di particolare rilevanza (per es. proveniente da un'istituzione politica o dal vertice o dalla direzione generale di una pubblica amministrazione), indipendentemente dal supporto utilizzato, è preventivamente inviato in visione alla segreteria di Direzione (Amministratore Delegato) che o la

trattiene o provvede a individuare la UOR competente a trattare il documento, fornendo eventuali indicazioni per l'espletamento della pratica.

3.11. Modifica delle assegnazioni

Nel caso di assegnazione errata, la UOR/UU che riceve il documento comunica l'errore alla UOP, che procederà a una nuova assegnazione.

Nel caso in cui un documento assegnato erroneamente a una UOR afferisca a competenze attribuite ad altra UOR, l'abilitazione al relativo cambio di assegnazione è attribuita alla UOP.

Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

3.12. Assegnazione dei documenti inviati

Il documento in uscita può essere protocollato dalle UOP autorizzate che, dopo la protocollazione, lo assegnano all'ufficio proponente.

Tale assegnazione è generata automaticamente dal PPI ed è la conferma dell'avvenuta protocollazione del documento.

PRODUZIONE E ARCHIVIAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

3.13. Registro informatico di protocollo (RIP)

Il sistema di protocollazione consente la produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. L'assegnazione delle informazioni nelle operazioni di registrazione e segnatura di protocollo è effettuata dal sistema in unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati.

De facto, **il registro di protocollo** è un atto che attesta la data e l'effettivo ricevimento o invio di un documento ed **è idoneo a produrre effetti giuridici a favore o a danno delle parti**. Per tale ragione, al fine di tutelare l'integrità e la regolarità delle registrazioni, ai sensi del DPCM 3 dicembre 2013, il PPI produce, automaticamente, una copia digitale del registro e la trasmette all'azienda incaricata della conservazione.

3.14. Unicità del protocollo informatico

Nell'ambito dell'AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo adottato dall'AOO medesima.

La numerazione si chiude al 31 dicembre di ogni anno solare e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.

Il numero di protocollo è costituito da almeno sette cifre numeriche.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.

Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in entrata e per il documento in uscita.

Non è consentita la protocollazione di un documento già protocollato (all'interno del sistema documentale aziendale).

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

3.15. Registro giornaliero di protocollo

Il PPI provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato, al termine della giornata lavorativa o al più tardi il giorno successivo, e conservato, ai sensi del DPCM 3 ottobre 2013, a cura di un soggetto responsabile della conservazione delle copie, appositamente nominato dall'AOO.

L'operazione di riversamento viene espletata automaticamente dal PPI verso il sistema di conservazione.

3.16. Registrazione di protocollo

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi e interni, digitali e analogici).

Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il PPI, consistente nella memorizzazione dei dati obbligatori.

Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente che ha prodotto il documento;
- il destinatario del documento;
- l'oggetto del documento;
- la classificazione.

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.

Tali dati facoltativi sono descritti nei paragrafi seguenti.

3.16.1. Documenti informatici

I documenti informatici vengono ricevuti e trasmessi, in modo formale, sulla/dalla casella di PEC istituzionale della AOO.

La registrazione di protocollo di un documento informatico eventualmente sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità e ha verificato la validità della firma. Nel caso di documenti informatici in uscita, l'operatore esegue anche la verifica della validità amministrativa della firma.

Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto o inviato.

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere a ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia a uno o più file a esso allegati.

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

3.16.2. Documenti analogici (cartacei e supporti rimovibili)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza (il servizio postale pubblico e/o privato o con consegna diretta alla UOP).

La registrazione di protocollo di un documento analogico ricevuto, così come illustrato nel seguito, viene sempre eseguita, se giuridicamente rilevante, in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.

Nel caso di corrispondenza in uscita l'UOP esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

3.17. Elementi facoltativi delle registrazioni di protocollo

Il RGD, con proprio provvedimento e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può modificare e integrare gli elementi facoltativi del protocollo.

La registrazione degli elementi facoltativi del protocollo, con determinazione del RGD può essere modificata, integrata e cancellata in base alle effettive esigenze delle UOR o delle UOP.

I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il PPI registri tali modifiche.

Di seguito vengono riportati gli elementi integrativi e facoltativi finalizzati all'archiviazione e gestione della documentazione:

- luogo di provenienza o di destinazione del documento
- mezzo di ricezione/spedizione (ordinaria, espressa, corriere, raccomandata con ricevuta di ritorno, telefax, posta elettronica, ecc.)
- indirizzi di posta elettronica e recapito telefonico
- codice fiscale e/o partita IVA
- numero degli allegati
- nominativo dei destinatari delle copie per conoscenza
- UOR/UU competente
- identificativo del RP
- indicazione del livello di sicurezza se diverso da quello standard applicato dal sistema di protocollazione
- classificazione del documento (titolo, classe e fascicolo)
- numero di repertorio della serie (verbali, circolari, ordini e note di servizio, comunicazioni di direzione e rapporti).

3.18. Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione. La segnatura è l'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile.

3.18.1. Documenti informatici

Le informazioni minime incluse nella segnatura sono di seguito elencate:

- codice identificativo dell'AOO
- tipologia del documento rispetto al flusso (E/U/I)
- numero di protocollo del documento e data.

La struttura e i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.

L'AOO che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.

3.18.2. Documenti analogici/cartacei

Nel caso di documenti cartacei in entrata l'operazione di segnatura viene eseguita dopo l'acquisizione dell'immagine dei documenti, in modo da acquisirne le informazioni di protocollazione da riportare nel "segno" apposto al documento cartaceo sulla prima pagina dell'originale.

I documenti in uscita devono essere gestiti e protocollati come documenti informatici. Quelli per i quali non è possibile la trasmissione nel formato digitale di produzione e devono essere necessariamente riprodotti in formato cartaceo, riporteranno, dopo la protocollazione, la relativa segnatura.

3.19. Annullamento delle registrazioni di protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrati in forma non modificabile - per correggere errori verificatisi in sede d'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 dall'applicazione, comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento, le motivazioni e il richiedente l'annullamento.

In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data e il soggetto che è intervenuto.

Solo il RGD è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo al RPI.

L'annullamento di una registrazione di protocollo generale deve essere richiesto dal responsabile della UOR o dall'UOP con specifica nota, adeguatamente motivata, indirizzata al RGD ovvero al RPI abilitato. Il diritto per l'effettuarsi dell'operazione di annullamento è assegnato esclusivamente al RGD e ai suoi RPI delegati.

Analoga procedura di annullamento va eseguita quando, stante le funzioni primarie di certificazione riconosciute dalle norme alla UOP, emerge che a uno stesso documento in ingresso, ricevuto con mezzi di trasmissione diversi quali, ad esempio, fax, originale cartaceo o posta elettronica siano stati attribuiti più numeri di protocollo (sia stata, cioè, effettuata una protocollazione multipla dello stesso documento).

3.20. Modifica file/immagini di un protocollo

La funzione di modifica di una registrazione di protocollo per errata associazione delle immagini del documento o del file associato a protocolli in entrata, uscita o interni o a repertorio dovrà essere espressamente richiesta dal responsabile della UOR interessata al RGD ovvero al RPI abilitato. Il diritto per l'effettuazione dell'operazione di modifica file o immagini di un record di protocollo è assegnato esclusivamente al RPI. In seguito alla modifica di file e immagini associate a un record di protocollo il sistema ricalcola automaticamente l'impronta digitale del record lasciando traccia, per trasparenza amministrativa, dell'intervento occorso.

3.21. Livello di riservatezza

L'operatore che effettua la registrazione di protocollo di un documento attribuisce allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal sistema.

Il RP chiede all'Amministratore l'apertura di un nuovo fascicolo con i relativi livelli di riservatezza.

Il livello di riservatezza applicato a un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore o uguale. I documenti che invece hanno un livello di riservatezza superiore lo mantengono.

3.22. Alcuni casi particolari di registrazioni di protocollo

In questo paragrafo vengono elencati alcuni casi particolari di registrazione di protocollo, casi che non sono da ritenersi né esaustivi né tanto meno vincolanti nella stesura del presente Manuale di Gestione.

3.22.1. Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma inoltrati alla UOP di riferimento come documenti senza firma, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

3.22.2. Assegni e altri valori di debito o credito

Le buste contenenti eventuali assegni o altri valori di debito o credito con i relativi documenti di accompagnamento devono essere separate dall'altra posta in entrata, i documenti devono essere protocollati immediatamente specificando i valori tra gli allegati e trasmessi, insieme ai valori, alla UOR competente.

3.22.3. Protocolli urgenti

La richiesta di protocollare urgentemente un documento è collegata a una necessità indifferibile e di tipo straordinario.

Solo in questo caso il RGD si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento in formato digitale da spedire.

Tale procedura viene osservata sia per i documenti in entrata che per quelli in uscita, raccomandando, per questi ultimi, che non devono essere protocollati anticipatamente documenti diversi dall'originale (ad esempio bozze del documento), fatti pervenire alla UOP.

3.22.4. Corrispondenza personale

Si intende corrispondenza personale quella costituita da documenti contenuti in buste o plichi che riportano come destinatario soltanto il nominativo di una persona dipendente della società senza alcun riferimento alla funzione, all'ufficio di appartenenza, a un progetto, a un prodotto o servizio dell'AOO oppure che riportano in chiaro la dicitura "riservata personale" o "personale".

La corrispondenza personale come su descritta non viene aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti debbano essere comunque protocollati provvede a trasmetterli alla UOP di riferimento per la protocollazione.

3.22.5. Documenti riferibili a offerte

La corrispondenza che riporta l'indicazione "offerta" - "preventivo" o simili deve essere gestita come specificato al punto 5.2.4.

3.22.6. Domande di assunzione e curriculum vitae

Le domande di assunzione e i relativi curricula devono essere trasmesse esclusivamente in formato digitale nell'apposita casella di posta elettronica ordinaria indicata nel bando pubblicato sul sito istituzionale e archiviate in altri sistemi informatici fuori dal protocollo.

3.22.7. Messaggi di posta elettronica ordinaria

Considerato che l'attuale sistema di posta elettronica ordinaria non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata come segue:

- ricezione, come allegato, di un documento scansionato munito di firma autografa: fermo restando che il RP deve verificare la provenienza certa dal documento, in caso di mittente non verificabile, il RP valuta, caso per caso, l'opportunità di protocollare il documento inviato via e-mail;
- ricezione, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale; il documento e/o il messaggio sono considerati come un documento digitale inviato con qualunque mezzo di posta;
- ricezione di una e-mail contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

3.22.8. Documenti non firmati

L'operatore di protocollo, conformandosi alle regole stabilite dal RGD attesta la data, la forma e la provenienza per ogni documento.

Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "mittente sconosciuto o anonimo" oppure "documento non sottoscritto".

Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.

È poi compito della UOR di competenza e, in particolare, del RP valutare se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

3.22.9. Protocollazione di un numero consistente di documenti cartacei

Quando si presenti la necessità o si preveda di dover protocollare un numero consistente di documenti, sia in ingresso che in uscita, deve esserne data comunicazione alle UOP

con congruo anticipo, onde concordare tempi e modi di protocollazione e assegnazione (se in ingresso) o di spedizione (se in uscita).

3.22.10. Differimento delle registrazioni

Le registrazioni di protocollo dei documenti pervenuti presso l'AOO destinataria sono effettuate nella giornata di arrivo e comunque non oltre la giornata lavorativa successiva a quella del ricevimento di detti documenti.

Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del RGD, che autorizza le UOP a differire le operazioni relative agli altri documenti.

Il protocollo differito consiste nel differimento dei termini di registrazione. Il protocollo differito si applica solo ai documenti in entrata e per tipologie omogenee che il RGD descrive nel provvedimento sopra citato.

3.22.11. Documenti digitali pervenuti erroneamente

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all'AOO non competente, l'addetto provvede o ad annullare il protocollo stesso o a protocollare il documento in uscita indicando nell'oggetto "protocollato per errore" e rispedisce il messaggio al mittente.

3.22.12. Documenti cartacei pervenuti erroneamente

Nel caso in cui sia protocollato un documento cartaceo erroneamente inviato all'AOO, l'addetto provvede o ad annullare il protocollo stesso o 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".

3.22.13. 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 e gli eventuali allegati.

Tale verifica spetta al RP che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

I documenti pervenuti a integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RP, sono inseriti nell'eventuale relativo fascicolo.

SEZIONE 4 – CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

- SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE DEI DOCUMENTI
- GESTIONE DEI PROCEDIMENTI

SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE DEI DOCUMENTI

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, si avvale del piano di classificazione (titolario), cioè di quello che si suole definire "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente (o della società), al quale viene ricondotta la molteplicità dei documenti prodotti".

3.23. Titolario (o piano di classificazione)

Con l'entrata in funzione del protocollo e con l'avvio del sistema di gestione informatica dei documenti, viene adottato un titolario di classificazione unico (valido sia per il protocollo informatico sia per quello riservato), predisposto per l'AOO, con lo scopo di organizzare in maniera omogenea i documenti che si riferiscono a medesimi procedimenti secondo una logica di processo e a prescindere dal modello organizzativo adottato dall'AOO stessa.

3.23.1. Titolario

Il piano di classificazione, assieme al repertorio dei fascicoli, è lo strumento che permette di:

- organizzare tutti i documenti secondo uno schema logico, con riferimento ai processi (missione) e alle attività (competenze) svolte dall'AOO;
- applicare criteri di trasparenza favorendo la reperibilità del documento rispetto
  - ai macro-processi e processi aziendali
  - al funzionigramma aziendale
  - all'argomento e ai contenuti.

Si ribadisce che un sistema di classificazione è caratterizzato dalla:

- autonomia, rispetto all'organigramma aziendale perché quest'ultimo può variare nel tempo;
- stabilità, legata alla missione e ai processi dell'AOO e non al suo apparato burocratico e organizzativo;
- staticità, che deve quindi essere valutata in rapporto alla effettiva stasi delle norme che regolano le attività dell'AOO;
- inefficienza retroattiva del titolario.

Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello**.** Il titolario di SOSE si suddivide semplicemente in titoli e classi.

Il titolo individua i processi primari dell'organizzazione; la successiva partizione, le classi, corrisponde a specifiche fasi/attività che rientrano concettualmente nel processo descritto dal titolo.

Titoli e classi sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del vertice aziendale con propria decisione o su proposta del RGD.

Il titolario è uno strumento suscettibile di aggiornamento: esso deve, infatti, descrivere i processi e le attività dell'AOO, soggette a modifiche in forza di leggi, norme e regolamenti.

L'aggiornamento del titolario compete al RGD quando ne ricorrono i presupposti.

Dopo ogni modifica del titolario, il RGD informa tutti i soggetti abilitati all'operazione di classificazione dei documenti e impartisce loro le istruzioni per il corretto utilizzo della nuova classificazione.

Il titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione. È comunque possibile inserire come "Documenti non protocollati", soprattutto a livello di repertori, documenti con valenza storica e importanti nelle attività correnti dell'AOO: per es. gli organigrammi e i funzionigrammi aziendali, circolari e ordini di servizio, disposizioni e determinazioni dei vertici aziendali.

Il sistema di protocollazione garantisce la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.

Ogni proposta di revisione, anche parziale (per es. integrazione), del titolario deve essere segnalata al RGD che la valuterà. È cura del RGD informare le strutture addette alla protocollazione dell'intervenuta revisione.

Le variazioni sono introdotte ogni qualvolta si renda necessaria una modifica o miglioramento.

Il titolario in vigore è contenuto nell'***ALLEGATO 1***.

3.23.2. Classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordinamento logico, in relazione ai processi e alle attività dell'AOO.

Essa è eseguita a partire dal titolario di classificazione facente parte del piano di conservazione dell'archivio.

Tutti i documenti ricevuti e prodotti dalle UOP/UOR dell'AOO, indipendentemente dal supporto sul quale vengono formati, vengono classificati in base al sopra citato titolario.

Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo e classe), l'eventuale numero di fascicolo.

Le operazioni di classificazione vengono svolte interamente dalle UOP/UOR destinatarie/istruttori di atti.

3.24. Fascicolazione

In un sistema di gestione e tenuta dei documenti conta non solo il documento in quanto tale, ma l'insieme delle relazioni che questo ha con tutti gli altri (cioè l'intero archivio) e, più in particolare, con quelli che riguardano un medesimo affare o un medesimo procedimento.

La classificazione e la fascicolazione dei documenti sono gli strumenti che nel sistema documentale consentono il rispetto del vincolo archivistico, favorendo la sedimentazione stabile dei documenti prodotti e acquisiti dall'AOO nel corso delle proprie attività.

L'operazione di fascicolazione, sia nel caso di documenti in entrata, che in uscita o interni deve essere effettuata dalle UOP su proposta del Responsabile del relativo procedimento.

3.24.1. Apertura e tenuta del fascicolo

La fascicolazione è l'attività di riconduzione logica di un documento all'interno dell'unità archivistica che ne raccoglie i precedenti, al fine di mantenere vivo il vincolo archivistico che lega ogni singolo documento al relativo iter.

Tale attività permette di costruire un archivio basato sull'organizzazione funzionale dei documenti in unità complesse stabili nel tempo (i fascicoli), che riflettono la concreta attività del soggetto produttore.

Ogni fascicolo è individuato dai seguenti elementi:

- anno di istruzione;
- numero di fascicolo, cioè un numero sequenziale all'interno della classe del titolario, attribuito da 1 a n con cadenza annuale;
- oggetto, cioè una stringa di testo per descrivere compiutamente l'affare o il procedimento, o più di questi, insieme.

I fascicoli, che fanno riferimento a procedimenti o affari che si prolungano su più esercizi, possono essere reiterati, d'intesa e con il supporto del RGD, per gli anni successivi al primo, con una nuova numerazione.

3.24.2. Tipologia di fascicoli

Le tipologie di fascicoli possono essere quattro:

a. fascicoli degli Enti (di PA)
b. fascicoli di aziende (non PA)
c. fascicoli di procedimenti e/o gestionali
d. fascicoli del personale.

I fascicoli amministrativi e gestionali vengono aperti e gestiti nell'ambito della UOR che li istruisce.

I fascicoli relativi a enti e aziende sono in genere i fascicoli gestiti dalle funzioni di business dell'AOO.

I fascicoli del personale, invece, sono fascicoli nominativi, intestati al singolo dipendente e contengono tutta la documentazione relativa alla loro carriera. Inoltre, il numero di fascicolo del dipendente è dato, generalmente, dal loro numero di matricola.

3.24.3. Chiusura del fascicolo

Il fascicolo viene chiuso al termine del procedimento o con l'esaurimento dell'affare o della relazione.

La data di chiusura si riferisce alla data dell'ultimo documento prodotto.

Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.

Gli elementi che individuano un fascicolo sono gestiti dal Responsabile competente, il quale è tenuto pertanto all'aggiornamento del repertorio dei fascicoli.

3.24.4. Repertorio dei fascicoli

Il repertorio dei fascicoli rappresenta l'elenco ordinato e aggiornato dei fascicoli istruiti all'interno di ciascuna classe e riporta, per ciascun fascicolo, i seguenti dati (primi 4 obbligatori, gli altri opzionali):

a. anno di istruzione
b. classificazione completa (titolo e classe)

c. numero di fascicolo (ed eventuali altre ripartizioni)
d. anno di chiusura
e. oggetto (ed eventualmente l'oggetto di sotto-fascicoli, inserti, ecc.)
f. annotazione del passaggio all'archivio storico o, in alternativa, l'avvenuto scarto.

Il repertorio dei fascicoli è un registro annuale; inizia il 1° gennaio e termina il 31 dicembre.

3.24.5. Versamenti dei fascicoli chiusi

I responsabili delle UOR o dei procedimenti sono tenuti alla corretta conservazione e custodia dei documenti relativi agli affari e ai procedimenti di propria competenza nei relativi fascicoli e ad assicurare la corrispondenza dell'archivio elettronico consultabile on-line rispetto a quello cartaceo.

Periodicamente (di norma una volta l'anno), ogni ufficio dell'AOO deve trasferire a un archivio di deposito i fascicoli relativi ad affari e a procedimenti conclusi.

Ricevuti i fascicoli e controllato il rispettivo repertorio, il gestore dell'archivio di deposito predispone un elenco di consistenza e procede a:

1. versarli nell'archivio di deposito (fisico) in base al loro anno di istruzione, classificazione e numero di fascicolo;
2. archiviarli nel sistema documentale elettronico per la loro chiusura affinché dalle ricerche on-line risulti che il corrispettivo fascicolo fisico non si trova più nella UOP/UOR di competenza ma è già stato versato nell'archivio di deposito.

I fascicoli del personale vanno versati dall'archivio corrente all'archivio di deposito l'anno successivo alla data di cessazione dal servizio del dipendente.

3.25. Conservazione dei documenti

I documenti e i fascicoli sono archiviati sul PPI e inviati al sistema di conservazione sulla base delle regole stabilite nel piano di cui al Manuale di conservazione. Il piano stabilisce le tempistiche di conservazione e di scarto tenendo conto sia della normativa di riferimento sia dell'analisi interna effettuata dal RGD congiuntamente con le UOR/UU responsabili del trattamento dei documenti.

GESTIONE DEI PROCEDIMENTI

Quanto di seguito accennato in termini di base informativa dei procedimenti dell'AOO, costituisce il riferimento per qualsiasi successivo impiego delle tecnologie informatiche di gestione dei flussi documentali (*work flow*).

3.26. Workflow documentale

Il workflow è la descrizione di un processo (business process) ed è costituito da una serie di attività elementari (task), eventualmente cicliche o alternative, da eseguire per ottenere un preciso risultato.
In ambito documentale, i sistemi di workflow coordinano tutte le operazioni che riguardano l'elaborazione e la trasmissione dei documenti, specificando le attività e i ruoli di tutti gli appartenenti al processo di lavoro. Un workflow documentale segue un documento durante tutto il suo ciclo di vita, fornendo un'azione di controllo costante per la sua compilazione.

3.27. Matrice delle correlazioni

I procedimenti vengono descritti nella "Mappa dei processi aziendali" all'interno del Sistema di Gestione della Qualità (SGQ), di cui l'organizzazione aziendale cura l'aggiornamento, estemporaneo e/o periodico.

I procedimenti costituiscono i processi attraverso i quali si esplica l'attività istituzionale dell'AOO.

La definizione del singolo procedimento rappresenta il modello astratto di riferimento per lo svolgimento dell'attività amministrativa.

Il risultato concreto di questa attività sono i documenti opportunamente aggregati in fascicoli, ognuno dei quali è relativo a un singolo affare/procedimento.

3.28. Catalogo dei procedimenti

La gestione delle attività e dei procedimenti e il loro eventuale *iter* sono definiti così come previsto dalle norme legislative, nonché dall'eventuale regolamento interno emanato dall'AOO.

A tal fine l'AOO, per favorire la trasparenza dell'azione amministrativa, per semplificare i procedimenti e per schematizzare le descrizioni, assimila il Catalogo dei procedimenti alla Mappa dei processi aziendali presente nel suo SGQ.

3.29. Avvio dei procedimenti e gestione degli stati di avanzamento

Mediante l'assegnazione dei fascicoli alle UOR/UU di volta in volta competenti le UOP o i RP provvedono a dare avvio ai relativi procedimenti.

La registrazione degli stati di avanzamento dei procedimenti può avvenire in modalità manuale o automatica.

Nel primo caso, gli stati di avanzamento sono aggiornati dal RP.

Nel secondo caso, è il software che registra automaticamente i passaggi dei documenti contenuti nei fascicoli e lo stato di avanzamento del procedimento.

SEZIONE 5 – DISPOSIZIONI FINALI

- PIANO DI SICUREZZA
- PROTOCOLLO DI EMERGENZA
- ACCESSO AL PROTOCOLLO INFORMATICO
- APPROVAZIONE E AGGIORNAMENTO DEL MANUALE DI GESTIONE

PIANO DI SICUREZZA

Il piano di sicurezza informatica relativo alla formazione, gestione, trasmissione, interscambio e archiviazione elettronica dei documenti nell'ambito del protocollo informatico, in quanto parte del più ampio Piano di Sicurezza Informatica del sistema informativo di SOSE, viene predisposto e aggiornato sistematicamente dall'Unità ICT & DT della Società.

Il piano della sicurezza garantisce che:

- i documenti e le informazioni trattati dalla AOO 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.

Le misure di sicurezza specifiche adottate dal protocollo informatico sono riportate nell'***ALLEGATO 5***- Piano di sicurezza specifico del sistema di protocollazione informatica.

PROTOCOLLO DI EMERGENZA

3.30. Il registro di emergenza

Il RGD ovvero il responsabile dell'AOO autorizza, ai sensi dell'art. 63 del DPR 445/2000, lo svolgimento anche manuale delle operazioni di registrazione di protocollo su un registro di emergenza, ogni qualvolta che, per cause tecniche, non sia possibile utilizzare la normale procedura informatica.

Nel caso di gravi e persistenti danni alla rete intranet o altre cause che rendano impossibile utilizzare il protocollo informatico per oltre 48 (quarantotto) ore, ogni registrazione verrà effettuata su un supporto alternativo denominato REGISTRO DI EMERGENZA.

Il registro di emergenza si attiva su supporto cartaceo presso un'unica UOP aziendale. Il numero di protocollo assegnato ai documenti partirà da 1(uno). Una volta ripristinato il servizio informatico, il RGD, coadiuvato dal RPI o altro delegato, dovrà, prima che il protocollo informatico sia stato riattivato, importare sia il contenuto del Registro di emergenza, scansionato, all'interno del PPI protocollandolo, sia i documenti registrati in emergenza.

A ogni documento importato sarà assegnato un nuovo numero di protocollo (mantenendo tuttavia il riferimento al numero di protocollo e alla data assegnata dal registro di emergenza). I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale.

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

Solo dopo aver concluso l'importazione, il PPI potrà essere di nuovo attivato per l'utilizzo da parte di tutte le UOP e le UOR.

3.31. Modalità di apertura del registro di emergenza

Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il RGD imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare.

Sul registro di emergenza vengono riportate: la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo informatico.

Per semplificare e normalizzare la procedura di apertura del registro di emergenza il RGD può predisporre un eventuale modulo su cui riportare la causa dell'interruzione, la data e l'ora dell'attivazione del registro di emergenza, i numeri di protocollo iniziale e finale.

Qualora l'impossibilità di utilizzare la procedura web si prolunghi oltre le quarantotto ore, per cause di eccezionale gravità, il RGD autorizza l'uso del registro di emergenza per periodi successivi di durata non superiore a una settimana.

3.32. Modalità di utilizzo del registro di emergenza

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro, il numero totale di operazioni registrate manualmente.

La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del protocollo informatico dell'AOO.

Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono gli stessi previsti dal protocollo generale.

Durante il periodo di interruzione del protocollo informatico generale, il RGD si informa costantemente sui tempi di ripristino da parte del fornitore del sistema di protocollazione o del fornitore del servizio server e di rete.

3.33. Modalità di chiusura e recupero del registro di emergenza

È compito del RGD verificare la chiusura del registro di emergenza.

È compito del RGD, o di un suo delegato, riportare dal registro di emergenza al registro di protocollo generale le protocollazioni relative ai documenti protocollati in emergenza attraverso la UOP abilitata.

Una volta ripristinata la piena funzionalità del protocollo informatico, il RGD provvede alla chiusura del registro di emergenza, annotando, sullo stesso il numero delle registrazioni effettuate e la data e l'ora di chiusura.

AUTENTICAZIONE E PRIVILEGI D'USO DEL PROTOCOLLO INFORMATICO

Il presente capitolo riporta i criteri e le modalità per l'autenticazione e per il rilascio delle abilitazioni per l'utilizzo del sistema applicativo di protocollazione e di accesso ai documenti (profilo o privilegi d'uso).

3.34. Generalità

L'autenticazione al sistema di gestione documentale segue la logica del single-sign-on. Con tale logica si permette, a tutti i dipendenti di Sose, di autenticarsi una sola volta accedendo alla propria stazione di lavoro potendo utilizzare tutte le risorse informative per le quali è stato abilitato; nel caso specifico risulta utile e vantaggiosa un'unica autenticazione per postazione di lavoro, intranet, internet, posta elettronica e protocollo informatico.

Il profilo d'uso, definito e governato all'interno del sistema di protocollazione informatica, è differenziato in base alla UOR di appartenenza e alle tipologie di possibili attività e operazioni assegnate ai singoli dipendenti, indipendentemente dalla qualifica.

I diversi profili d'uso vengono definiti, d'intesa con il vertice aziendale, dal RGD, che si può eventualmente avvalere del RPI o altro utente delegato.

3.35. Abilitazioni interne per l'utilizzo dei servizi di protocollo

Le informazioni raccolte per controllare i privilegi d'uso sono quelle strettamente necessarie per l'identificazione dell'utente.

L'autenticazione è governata e integrata con il sistema di active directory al fine di garantirne la sicurezza.

Tutte le utenze dell'AOO sono configurate con un *time-out* che provvede a disconnettere automaticamente la postazione di lavoro dopo 10/15 minuti di inattività.

Il sistema applicativo del protocollo impedisce le sessioni multiple con lo stesso utente.

3.36. Profili d'uso

Gli utenti del servizio di protocollo una volta identificati e autenticati sono suddivisi in 5 (cinque) diverse tipologie di profili d'uso dell'applicazione di protocollo, sulla base delle rispettive competenze e della struttura organizzativa.

- ✓ **PROFILO UTENTE AMMINISTRATORE**, è il profilo assegnato all'utente con ruolo di Amministratore di sistema definiti all'interno del documento "Elenco Amministratori di sistema", che differisce da quello nominale. Nel caso del RGD, questo può avere l'accesso come Amministratore ai fini dello svolgimento delle funzioni e compiti previsti dalla legge, in particolare nelle ipotesi di audit o controllo della configurazione di sistema: con tale profilo è possibile effettuare operazioni di annullamento di protocollo, accedere alla lista di controllo degli accessi per operazioni di e abilitazione o disabilitazione, assegnare o modificare i profili interni degli utenti, accedere ai log di sistema, creare nuovi fascicoli o modificarne la denominazione, effettuare operazioni di ripristino e salvataggio, attivare e disattivare il registro di emergenza;
- ✓ **PROFILO UTENTE STANDARD UOP**, è il profilo assegnato ai singoli componenti della UOP; con tale profilo è possibile inserire e protocollare i documenti (in entrata, in uscita e tra uffici) nel PPI, visualizzare i propri documenti protocollati, inserirli in un fascicolo, assegnarli a una UOR o a un RP, modificarne i parametri modificabili; con tale profilo può essere o non può essere (a seconda della tipologia di UOP)

possibile creare nuovi fascicoli, ma non è possibile essere destinatari come responsabili di un procedimento (RP);

- ✓ **PROFILO UTENTE STANDARD UOR**, è il profilo assegnato ai singoli componenti della UOR/UU; con tale profilo è possibile inserire e protocollare i documenti interni (tra uffici) nel sistema documentale, visualizzare i propri documenti protocollati, inserirli in un fascicolo, modificarne i parametri modificabili; con tale profilo non è possibile creare nuovi fascicoli, ma è possibile essere destinatari di un documento come responsabili di un procedimento (RP);
- ✓ **PROFILO UTENTE RESPONSABILE**, è il profilo assegnato ai responsabili delle UOR/UU o persone delegate; con tale profilo è possibile inserire e protocollare i documenti interni (tra uffici) nel PPI, visualizzare sia i propri documenti protocollati assegnati sia quelli assegnati ai propri diretti collaboratori, inserire i documenti in un fascicolo, assegnare i documenti, modificarne i parametri modificabili; con tale profilo non è possibile modificare i profili assegnati ai propri collaboratori;
- ✓ **PROFILO UTENTE SPECIALE**, è il profilo assegnato a particolari responsabili di UOR/UU o persone delegate o a particolari funzioni; con tale profilo è possibile svolgere le stesse operazioni previste per il profilo utente responsabile ed è possibile, inoltre, svolgere operazioni trasversali o esclusive sui fascicoli dell'AOO e su specifici repertori.

3.37. Creazione e gestione delle utenze e dei relativi profili d'uso

Al fine di procedere alla creazione delle utenze è necessario distinguere due diversi momenti: la prima attivazione dell'intero sistema documentale e la gestione in fase di esercizio.

Nel primo caso si prevede un caricamento massivo effettuato in autonomia da parte del RGD oppure con intervento del fornitore del PPI sulla base di una opportuna tabella fornita dal RGD.

Nel secondo caso ogni modifica o singola nuova creazione viene effettuata dal RGD o da persona da questi delegata e abilitata alla definizione dei profili d'uso.

3.38. Ripristino delle credenziali di autenticazione

In caso di smarrimento della password, per la logica del single-sign-on, l'utente deve avanzare formale richiesta al gestore delle stazioni di lavoro nell'ambito della funzione ICT & DT.

APPROVAZIONE E AGGIORNAMENTO DEL MANUALE DI GESTIONE

3.39. Modalità di approvazione e aggiornamento del manuale

Il CdA di SOSE adotta il presente Manuale di Gestione su proposta del RGD.

Il presente manuale potrà essere aggiornato a seguito di:

- una sopravvenuta nuova normativa o modifica di una esistente;
- 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;
- modifiche apportate negli allegati dal RGD.

Nel caso di avvicendamento del RGD, il nuovo Responsabile deve prendere visione del manuale di gestione, verificare le regole in esso contenute ed eventualmente modificarle aggiornando il manuale stesso. sostanziali modifiche apportate nell'ambito dell'architettura del sistema.

3.40. Regolamenti abrogati

Con la pubblicazione del presente manuale vengono annullati tutti i regolamenti interni all'AOO nelle parti contrastanti con lo stesso.

3.41. Pubblicità del Manuale di Gestione

Il presente manuale potrà, come previsto dalla normativa, essere reso disponibile alla consultazione del pubblico attraverso il sito istituzionale dell'AOO.

Inoltre, copia del presente manuale è:

- fornita a tutte le UOP e alle UOR e sarà disponibile a tutto il personale dell'AOO mediante la rete intranet aziendale;
- inviata agli organi di governance dell'AOO.

3.42. Operatività del Manuale di Gestione

Il presente manuale è operativo a partire dal giorno della sua pubblicazione sulla intranet aziendale e sul sito istituzionale.

SEZIONE 6 – ALLEGATI

ALLEGATO 1

TITOLARIO DI CLASSIFICAZIONE DEI DOCUMENTI AZIENDALI[1]

Titolo I. Attività di Governance

Questo titolo raccoglie tutta la documentazione riguardante le relazioni esterne e gli affari amministrativi, istituzionali e di governo.

1. Comunicazione e relazioni esterne
2. Amministrazione e Controllo di gestione
3. Rapporti con la società di revisione
4. Gestione della compliance

Titolo II. Organi di governo e controllo

Questo titolo contiene tutta la documentazione interna riguardante gli organi nell'esercizio delle loro funzioni direttive, consultive ed elettive (verbali, pareri, nomine, delibere, atti preparatori).

1. Amministratore Delegato
2. Presidenza
3. Consiglio di Amministrazione
4. Collegio sindacale

Titolo III. Relazioni commerciali e convenzioni

In questo titolo viene raccolta tutta la documentazione riguardante le attività relative ai rapporti e ai contratti con gli enti di PA centrale e periferica e con le diverse organizzazioni con cui l'azienda avvia relazioni economiche.

1. Rapporti e contratti con PA centrale (Agenzie Fiscali, MEF, DF, …)
2. Rapporti e contratti con PA territoriale
3. Commerciale e marketing

Titolo IV. Fabbisogni standard

Il titolo raccoglie tutta la documentazione riguardante il processo di predisposizione, elaborazione e pubblicazione dei fabbisogni standard.

1. Pianificazione
2. Rapporti periodici e schede di monitoraggio
3. Interscambio informativo con stakeholder di progetto[2]
4. Convocazione incontri

Titolo V. Studi di settore

In questo titolo viene raccolta tutta la documentazione riguardante le attività di elaborazione e rilascio degli Studi di Settore.

---

1 Il presente titolario è un sistema di classificazione per l'ordinamento dei documenti in archivio. Per dargli stabilità, è stato svincolato dall'organigramma aziendale (mutevole nel tempo) e riferito, invece, ai processi e alle attività aziendali.

2 RGS, IFEL, ANCI, UPI, CTFS

1. Pianificazione
2. Rapporti periodici e schede di monitoraggio
3. Convocazione incontri
4. Interscambio informativo con stakeholder di progetto
5. Commissione degli esperti

Titolo VI. Analisi fiscali ed economiche

In questo titolo viene raccolta tutta la documentazione riguardante le attività di analisi fiscali ed economiche.

1. Prodotti per istituzioni e imprese
2. Elaborazione rapporti

Titolo VII. Risorse umane

Il titolo è dedicato alle funzioni relative alla gestione del personale, sia esso dipendente o meno. Per i documenti relativi a ciascun dipendente viene istruito un fascicolo nominativo cosiddetto "del personale".

1. Assunzioni e cessazioni
2. Richieste di assenza[3]
3. Mobilità e part time
4. Viaggi e trasferte
5. Gestione della formazione
6. Quiescenza e TFR
7. Rapporti sindacali
8. Contenzioso del lavoro e disciplina
9. Servizi a domanda individuale[4]
10. Gestione personale non dipendente e collaboratori

Titolo VIII. Studi, ricerche e consulenze

In questo titolo viene raccolta tutta la documentazione riguardante le attività di ricerca e consulenza.

1. Pianificazione e analisi
2. Elaborazione rapporti e documentazione

Titolo IX. Legale e contenzioso

In questo titolo viene raccolta tutta la documentazione riguardante le attività relative alla gestione di tutte le tipologie di contenzioso e della consulenza legale in genere.

1. Contenzioso
2. Pareri e consulenze legali
3. Denunce e azioni legali
4. Affari e operazioni societarie

Titolo X. Approvvigionamenti

5 Domande agli Enti previdenziali
6 Rientrano in questa classe i documenti per prestiti, sussidi, borse di studio, ecc.

Questo titolo comprende le funzioni riguardanti la titolarità e gestione del patrimonio, di natura sia mobile che immobile, all'acquisizione e gestione di beni e servizi strumentali allo svolgimento delle attività aziendali.

1. Gestione contratti (beni immobili, mensa, …)
2. Acquisizioni e forniture di beni, servizi e lavori

Titolo XI. Sistemi informativi

All'interno di questo titolo verranno classificati i documenti riguardanti la gestione dei sistemi informativi a livello di infrastrutture, di applicazioni, di dati, di flussi elaborativi e di sicurezza.

1. Acquisizione e gestione dei flussi di dati
2. Comunicazioni di progetto con clienti e fornitori
3. Assistenza utenti
4. Assistenza Enti locali

Titolo XII. ISA – Indice Sintetico di Affidabilità

In questo titolo viene raccolta tutta la documentazione riguardante le attività di elaborazione e rilascio degli ISA.

1. Pianificazione
2. Rapporti periodici e schede di monitoraggio
3. Convocazione incontri
4. Interscambio informativo con stakeholder di progetto
5. Commissione degli esperti

ALLEGATO 2

DEFINIZIONI

Archivio
L'archivio è il complesso organico di documenti, fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore/assegnatario durante lo svolgimento dell'attività. (cfr. art. 1 Allegato 1, D.P.C.M. 3 dicembre 2013)
Esso si distingue in:
· archivio corrente;
· archivio storico.

Archivio informatico
L'archivio informatico è l'insieme di documenti informatici, di fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico (cfr. art. 1 Allegato 1, D.P.C.M. 3 dicembre 2013)

Assegnatario
Struttura organizzativa o persona alla quale viene assegnato un documento per competenza o per conoscenza. Costituisce un'informazione oggetto di registrazione di protocollo.

Assegnazione
Attribuzione di ciascun documento alle strutture organizzative o risorse aziendali competenti per la trattazione nel merito.

Attributo di riservatezza
Informazione oggetto di registrazione di protocollo che indica il livello di riservatezza del documento (riservato o riservatissimo/segreto). Se non specificato il documento si intende non riservato.

Codice
Per codice si intende il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale (CAD). (cfr. art. 1 Allegato 1, D.P.C.M. 3 dicembre 2013)

Documento amministrativo
Ai sensi dell'art.1, comma 1 lettera a) del DPR 445/2000, si definisce documento amministrativo ogni rappresentazione, comunque formata, grafica, informatica o di qualsiasi altra specie del contenuto di atti, anche interni, utilizzati ai fini dell'attività amministrativa.

Documento analogico
Per documento analogico si intende la "rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti". (Cfr. art. 1 comma 1 lett. p-bis del D.lgs. n.82/2005)
Il documento analogico è prodotto con strumenti analogici (es. a penna/matita, con macchina da scrivere, ecc.) o con strumenti informatici (es. con MS Office o con altri programmi di videoscrittura).
Per versione analogica di documento informatico si intende la copia cartacea di un documento prodotto con strumenti informatici.

Documento informatico
Si definisce documento informatico "il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti". (Cfr. art. 1, comma 1 lettera p) del D.lgs. n.82/2005)
L'idoneità del documento informatico a soddisfare il requisito della forma scritta e la sua validità ed efficacia probatoria sono disciplinate agli artt. 20 e segg. del D.lgs. n. 82/2005, come da ultimo modificato con D.lgs. n. 179/2016.

Documento interno
Per documento interno si intende un documento, sia analogico che informatico, scambiato tra le risorse interne e le diverse strutture organizzative dell'AOO SOSE.

Documento inviato
Per documento inviato si intende la corrispondenza, compresa di eventuali allegati, inviata, di norma, per mezzo della posta elettronica ordinaria o certificata a un soggetto esterno sia pubblico che privato.

Documento ricevuto
Per documento ricevuto si intende la corrispondenza in ingresso acquisita dalla AOO con diversi mezzi e modalità in base allo strumento di trasporto utilizzato dal mittente.

Fascicolazione
Attribuzione a ciascun documento gestito dal Prodotto di Protocollo Informatico (PPI) di una codifica che ne individua l'insieme omogeneo di appartenenza (fascicolo).

Firma digitale
Firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Gestione documentale
Insieme delle attività finalizzate al trattamento dei documenti formati e acquisiti da SOSE in modo da garantirne la certezza documentale, l'assegnazione e l'ordinata conservazione.

Mittente
Soggetto che forma un documento. Costituisce un'informazione oggetto di registrazione obbligatoria di protocollo.

Oggetto
Indicazione in forma sintetica del contenuto di un documento. Costituisce una informazione oggetto di registrazione obbligatoria di protocollo.

Procedimento

Si intende una pluralità di atti tra loro autonomi, scanditi nel tempo e destinati alla emanazione di un provvedimento finale.

Profilo utente
Insieme omogeneo delle specifiche abilitazioni necessarie per lo svolgimento delle attività predefinite nel Sistema di gestione documentale digitalizzato che ciascun dipendente è chiamato a svolgere, in relazione alla posizione funzionale che riveste e/o alle specifiche competenze attribuitegli.

Protocollo informatico
Si intende:
- sia il registro in formato elettronico su cui si annota in ordine cronologico la corrispondenza e, pertanto, contenente i dati di classificazione, organizzazione e digitalizzazione dei documenti;
- sia l'insieme delle regole, delle risorse e delle attività necessarie alla realizzazione di un sistema automatico per la gestione elettronica dei flussi documentali.

Prodotto di Protocollo Informatico
Si intende il prodotto *Docway4* (nel Manuale denominato PPI - Prodotto di Protocollo informatico), il sistema informativo utilizzato da SOSE per la gestione del protocollo le cui funzioni permettono l'acquisizione, la registrazione, l'archiviazione, la ricerca e la consultazione delle diverse tipologie di documenti trattati nell'ambito dei processi aziendali di SOSE, sia interni e sia di scambio con l'esterno.

Posta Elettronica Certificata (PEC)
È il sistema di comunicazione via e-mail, attraverso cui è possibile inviare e ricevere documentazione digitale con valore legale equiparato alla Posta Raccomandata con ricevuta di ritorno (A/R). Il termine "Certificata" indica la caratteristica per cui il gestore del servizio PEC rilascia al mittente della e-mail una ricevuta di consegna che costituisce prova legale dell'avvenuta spedizione del messaggio ed eventuali allegati e attesta nello specifico:
- data e orario dell'operazione di invio del messaggio
- la certezza del contenuto (il messaggio non può essere alterato)
- la certificazione della consegna al destinatario.

Posta Elettronica Ordinaria (PEO)
È il sistema di comunicazione convenzionale via e-mail, attraverso cui è possibile inviare e ricevere documentazione digitale generalmente priva del carattere di ufficialità e per la quale non sussistono obblighi particolari di conservazione.

Protocollo differito
Il protocollo differito permette il differimento della decorrenza giuridica dei termini di entrata del documento rispetto alla data di registrazione, dichiarandone espressamente la data effettiva di entrata e le motivazioni della ritardata protocollazione.

Registrazione
È l'attività che permette l'assegnazione automatica al documento di un numero di protocollo progressivo e unico all'interno di ogni anno solare.

Registro di emergenza

È il registro su cui viene registrata la corrispondenza nel caso in cui non sia possibile utilizzare il PPI per eventi eccezionali. (art. 63 del D.P.R. 28 dicembre 2000, n. 445)

Registro giornaliero di protocollo
Registro dove sono riportati giornalmente, per ciascun documento formato o acquisito, gli estremi di protocollo e le informazioni oggetto di registrazione di protocollo.

Regole tecniche
Si intendono le disposizioni dettate dal D.P.C.M. 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli art. 40-bis, 41, 47, 57 bis e 71 del Codice di Amministrazione Digitale di cui al Decreto Legislativo n. 82 del 2005".

Repertorio
Si definiscono repertori quelle serie di documenti che, prodotti internamente o ricevuti dall'esterno, seguono una propria numerazione progressiva nell'anno solare di riferimento, indipendentemente dalla numerazione di protocollo assegnata.

Responsabile della conservazione
È il soggetto responsabile delle attività finalizzate a definire e attuare le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione.

Segnatura
È l'attività che permette l'apposizione al documento, in forma permanente e non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare in maniera univoca ciascun documento.

Sose
Si intende la società Soluzioni per il Sistema Economico S.p.A.

Testo Unico
Si intendono le disposizioni dettate dal DPR 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (cfr. art. 1, Allegato 1, D.P.C.M. 3 dicembre 2013)

Titolario
Il titolario di classificazione rappresenta uno schema generale di voci logiche per organizzare i documenti protocollati, in modo da consentirne il facile reperimento, la soggettazione e l'indicizzazione degli stessi e rappresenta uno strumento a garanzia del diritto d'accesso ai documenti amministrativi riconosciuto dalla legge 241/1990.

Strutture organizzative di registrazione di protocollo
Le strutture organizzative di registrazione di protocollo (nel testo del Manuale denominate UOP) rappresentano gli uffici che svolgono attività di registrazione di protocollo in entrata e, se autorizzate (a seconda della profilazione), in uscita.

ALLEGATO 3

REPERTORI

I repertori definiti all'interno del sistema di protocollazione comprendono le seguenti serie documentarie:

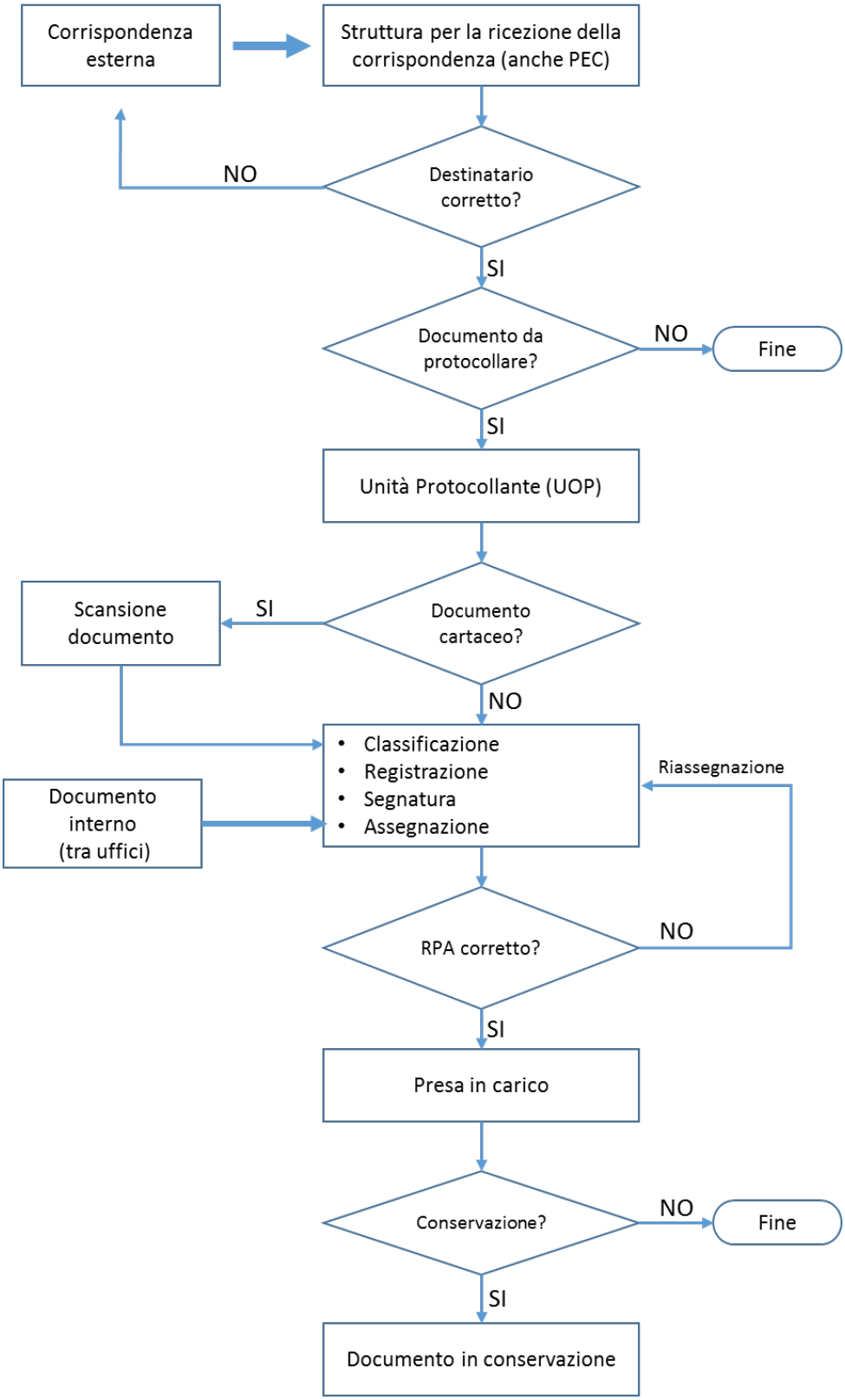
- Verbali del Consiglio di Amministrazione
- Verbali del Collegio Sindacale
- Verbali dell'Assemblea dei Soci
- Verbali e comunicazioni della Società di revisione
- Ordini di servizio, incarichi e nomine
- Comunicazioni al personale
- SGQ – Manuale e procedure della qualità
- SGQ – Verbali ispettivi di conformità
- SGQ – Rapporti di non conformità e azioni correttive/preventive
- Audit report e Rapporti all'OdV
- Verbali dei Comitati interni
- Registri per il trattamento dei dati personali, sensibili e giudiziari

I documenti vengono registrati a repertorio dalle rispettive UOR o UOP competenti che li istruiscono e ne stabiliscono, d'intesa con il RGD, limiti e criteri di consultazione. Alcuni archivi (per es. gli Ordini di Servizio o le Comunicazioni al personale o il Manuale e le procedure del SGQ), pur possedendo la caratteristica di repertori, possono essere resi pubblici e consultabili da tutti i dipendenti anche attraverso la intranet aziendale.

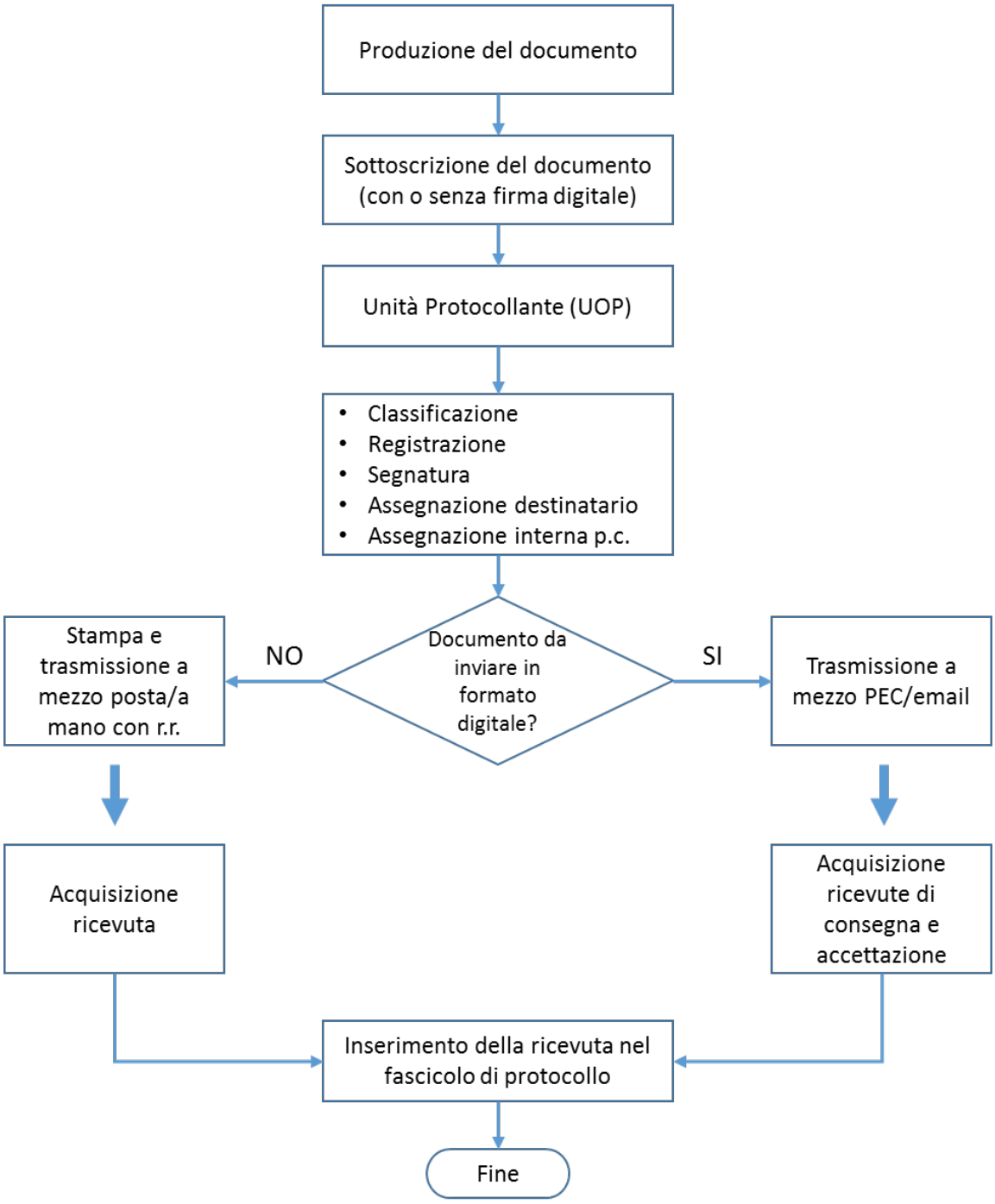
ALLEGATO 4

FLUSSI OPERATIVI

FLUSSO GENERALE DI LAVORAZIONE DEI DOCUMENTI IN ARRIVO



FLUSSO DI LAVORAZIONE DEI DOCUMENTI IN PARTENZA



ALLEGATO 5

PIANO DI SICUREZZA SPECIFICO DEL SISTEMA DI PROTOCOLLAZIONE INFORMATICA

Vengono di seguito riportate le 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.

a. Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dall'AOO siano disponibili, integre e riservate;
- 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 all'evoluzione tecnologica, alla loro natura e alle specifiche caratteristiche del trattamento.

b. Politiche di sicurezza e protocollo informatico

La progressiva diffusione delle tecnologie informatiche all'interno dell'azienda, e in particolare il libero accesso alla rete Internet dei personal computer, espone SOSE e i suoi dipendenti e collaboratori a responsabilità di natura patrimoniale, nonché penali qualora attraverso l'utilizzo di tali tecnologie si incorra in violazioni di legge (disciplina sulla protezione dei dati personali su tutte) con inevitabili conseguenze per la sicurezza e l'immagine aziendali.

Le misure e le politiche per la sicurezza di SOSE si basano sui risultati dell'analisi dei rischi cui sono esposti i dati (personali e non), e conseguentemente i documenti trattati, e sulle direttive strategiche stabilite dal vertice dell'AOO.

Il piano definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno dell'AOO;
- le modalità di accesso al sistema di protocollazione informatica e relativa gestione documentale;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza di cui alle politiche aziendali per la sicurezza informatica;
- i piani specifici di formazione del personale;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione con cadenza periodica. Esso può essere modificato anticipatamente a seguito di eventi rilevanti o gravi. Il RGD ha adottato le misure tecniche e organizzative, stabilite dalla struttura responsabile della sicurezza informatica dell'AOO, di seguito specificate, al fine di assicurare:

- la sicurezza dell'impianto tecnologico dell'AOO;

- la riservatezza delle informazioni registrate nelle banche dati;
- l'univoca identificazione degli utenti interni ed esterni;
- la protezione della Intranet aziendale;
- la protezione dei sistemi di accesso e conservazione delle informazioni;
- l'assegnazione a ogni utente, che deve accedere al protocollo informatico e agli altri componenti della postazione di lavoro, di una credenziale (*single-sign-on*) di autenticazione personale composta da un nome utente e da una componente riservata (*password*) e, per il protocollo, di un profilo di autorizzazione;
- le modalità di modifica delle password definite nelle Politiche di Sicurezza aziendali;
- la continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo;
- la conservazione, a cura dell'Unità ICT & DT, delle copie di riserva dei dati e dei documenti, in locali diversi da quelli in cui sono installati i sistemi di elaborazione di esercizio;
- l'archiviazione giornaliera, in modo non modificabile, delle copie del registro giornaliero di protocollo, dei file di log di sistema, di rete e applicativi contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata;
- il monitoraggio delle operazioni di backup attraverso sistemi di alert;
- la consultazione, solo in caso di necessità, dei dati personali, registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollo informatico e gestione dei documenti, da parte del RGD e/o dal titolare dei dati e/o dalla funzione di audit interno e, ove previsto, dalle forze dell'ordine;
- la gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- l'impiego e manutenzione di un adeguato sistema antivirus e di gestione degli aggiornamenti (patch e service pack) correttivi dei sistemi operativi.

c. Formazione dei documenti – Aspetti relativi alla sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici devono poter garantire:

- l'identificabilità del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando disponibile e prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti a essere gestiti mediante strumenti informatici e a essere registrati mediante 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 e con AOO diverse.

I documenti dell'AOO vengono generalmente 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 e XML. I documenti informatici redatti dall'AOO con altri prodotti di *text editor* vengono convertiti, prima della loro eventuale sottoscrizione con firma digitale o dopo la firma autografa, nei formati standard (PDF e XML), 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 potrà essere sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno dell'AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al DPCM 13 gennaio 2004 ("Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici").

I documenti informatici, prima di essere inviati a qualunque altra postazione di lavoro interna all'AOO, sono sottoposti a un controllo antivirus, presente su tutte le postazioni dell'AOO, onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'AOO.

d. Gestione dei documenti informatici

Il sistema applicativo del protocollo informatico è conforme alle specifiche previste dalla normativa vigente (DPR 3 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi del CAD di cui al D.lgs. n. 82/2005 e ss.mm.).

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.

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, in uscita e interni;
- 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 trattamento dei dati personali, con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione adottato.

e. Componente organizzativa della sicurezza

La componente organizzativa della sicurezza legata alla gestione del protocollo e dei relativi documenti, si riferisce principalmente alle attività svolte presso il sistema informatico di SOSE. In particolare, la definizione delle misure di sicurezza nell'ambito del sistema è attuata dalla struttura ICT, in ottemperanza a quanto previsto dalla normativa vigente, ed esplicitata nei documenti relativi alle politiche aziendali e nei regolamenti interni. Il RGD, in virtù del regime di single-sign-on previsto su tutte postazioni di lavoro aziendali, ha valutato l'opportunità di adeguarsi alle politiche aziendali di sicurezza.

f. Componente fisica della sicurezza

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico, e quindi anche del protocollo informatico e relativi documenti, è regolato secondo i seguenti criteri basati su due livelli:

- l'accesso alla sede di SOSE avviene tramite badge, rilasciato per i dipendenti e per gli ospiti previa identificazione;
- l'accesso al Data Center di Roma, via Mentore Maggini 48C, può avvenire esclusivamente con un secondo badge rilasciato ai dipendenti e ai manutentori appositamente abilitati.

g. Componente logica della 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 è garantita in generale dal rispetto e dall'attuazione delle politiche di sicurezza, sia per la configurazione e gestione della rete, sia per la configurazione e gestione dei dispositivi e delle dotazioni informatiche, contenute nei regolamenti interni di SOSE, nonché, in maniera più ampia, relativamente alla protezione dei dati personali, nelle politiche di trattamento stabilite dal Titolare e/o dal Responsabile per il trattamento dei dati personali.

In particolare, la componente logica della sicurezza, nell'ambito del sistema di protocollazione informatica è gestita, dal punto di vista architetturale dalle seguenti componenti:

- architettura multi-layer: consente di tenere separati i livelli funzionali di presentazione, dell'applicazione e dei dati;
- i file dei documenti sono accessibili solo tramite il livello applicativo del PPI.

Dal punto di vista degli accessi al protocollo informatico, è prevista una procedura di abilitazione e profilazione utenti, gestita dal RGD in funzione dei processi aziendali e delle prerogative stabilite dal comitato interno di compliance per determinate risorse e funzioni aziendali.

Per la gestione degli accessi base (profilazione), viene seguita la logica del minimo privilegio, concedendo gli accessi consentiti e regolamentati dalle specifiche procedure interne di SOSE. Gli amministratori di sistema sono appositamente nominati e il loro operato è soggetto a registrazione, ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e ss.mm.

h. Componente infrastrutturale della sicurezza

Il sistema informatico in cui è inserito il sistema di protocollazione e gestione dei documenti è basato sulla seguente infrastruttura:

- un Data Center progettato per tenere separati i livelli funzionali, dell'applicazione e dei dati;
- componenti hardware/software di alta affidabilità, capaci di gestire i fault sui singoli server.

i. Gestione delle registrazioni di sicurezza

Le registrazioni di sicurezza, o Log, sono costituite da informazioni di diverso tipo (ad es. dati o connessioni) presenti o transitate sui componenti del sistema di protocollazione che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano a oggetto le operazioni effettuate sul sistema

stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico, sensori di rete e firewall;
- dalle registrazioni dei singoli componenti.

Le modalità di conservazione delle registrazioni relative agli eventi di sicurezza sono definite nel documento che descrive le Procedure di backup dei dati.

j. 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 cognizione della corrispondenza telematica, 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 a essere 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 e i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, 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 di cui si avvale SOSE 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 di amministrazioni 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 dal decreto legislativo del 30 giugno 2003, n. 196 e ss.mm e dal GDPR n.2016/679. 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.

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione, oltre all'antivirus presente su tutte le postazioni di lavoro, rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

k. Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (nome utente e password) alla postazione di lavoro aziendale e un sistema di autorizzazione per il protocollo informatico basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate a un utente del servizio di protocollo e gestione dei relativi

documenti. Queste, in sintesi, sono: la consultazione, l'inserimento, la modifica, l'annullamento. Le regole per la composizione delle password e per il blocco delle utenze sono mutuate dalle regole configurate sul sistema di gestione centralizzata degli utenti.

Per ogni informazione di dettaglio relativa alla disciplina degli accessi alle risorse informatiche si rimanda alla normativa interna e alle linee guida dell'Agenzia per l'Italia digitale (AgID)

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo. In particolare, il PPI adottato da SOSE:

- 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 al fine di non consentire modifiche non autorizzate. Ciascun utente del PPI può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) a esso eventualmente subordinati. Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato da SOSE.

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

I. Accesso al registro di protocollo per utenti interni all'AOO

L'autorizzazione all'accesso al registro di protocollo è regolata tramite i seguenti strumenti:

- *liste di competenza*, gestite dal RGD, per la definizione degli utenti abilitati ad accedere a determinate classi del titolario;
- *ruoli degli utenti*, gestiti dal RGD, per la specificazione delle macro-funzioni alle quali vengono abilitati;
- protocollazione "*particolare o riservata*", gestita dal RGD, relativa a documenti **sottratti alla consultazione** da parte di chi non sia espressamente abilitato.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di RGD o RPI.

L'utente assegnatario dei documenti protocollati è invece abilitato a una vista parziale sul registro di protocollo. Tale vista è definita dalle voci di titolario associate alla lista di competenza in cui l'utente è presente (sia come singolo, sia come ufficio).

L'operatore che gestisce lo smistamento dei documenti può definire riservato un protocollo e assegnarlo per competenza a un utente.

Nel caso in cui sia effettuata una protocollazione riservata la visibilità completa sul documento è possibile solo all'utente a cui il protocollo è stato assegnato per competenza e ai soggetti che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo).

Tutti gli altri utenti (anche se inseriti nella giusta lista di competenza) possono accedere solo ai dati di registrazione (ad esempio: progressivo di protocollo, data di protocollazione) mentre vedono mascherati i dati relativi al profilo del protocollo (ad esempio: classificazione).

Ogni profilo abilitativo istituito può essere integrato da ulteriori specifiche abilitazioni/diritti per l'utilizzo di funzioni che non mutano le caratteristiche principali del profilo stesso. Ci si riferisce in questo caso ai diritti di visibilità di particolari Repertori e ai diritti di inserimento e intervento in relazione ai documenti protocollati in essi contenuti.

m. Utenti esterni all'AOO

Non vengono rese disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti e al protocollo informatico dell'AOO da parte di utenti non appartenenti all'AOO stessa.

n. Manutenzione del PPI

Ai fini della necessità di intervenire sul sistema di protocollo per le operazioni di manutenzione ordinaria e/o evolutiva, ove sia necessaria la guida o anche l'azione diretta del fornitore, è cura dell'Unità ICT & DT gestire l'autorizzazione all'accesso ai server. Lo stesso iter formale viene osservato anche nelle circostanze in cui si presenti l'eventuale necessità di dover far accedere utenti collaudatori privati esterni a SOSE qualificati per le verifiche funzionali alla certificazione di qualità del sistema di protocollazione.

Il fornitore del PPI, ai sensi del decreto legislativo del 30 giugno 2003, n. 196 e ss.mm. e del GDPR n.2016/679 è stato nominato responsabile esterno del trattamento dei dati personali.