Manuale di gestione documentale

di Equitalia Giustizia S.p.A.

del 08/08/2025

Regole tecniche per il protocollo informatico,
ai sensi del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005,
e delle Linee Guida Agid sulla formazione, gestione e conservazione dei doc. informatici.

Sommario

1. Premessa 4
1.1 Principali norme di riferimento 5
1.2 Definizioni 5
2 Principi Generali 11
2.1 Politiche di sicurezza 11
2.2 Aree organizzative omogenee e modello organizzativo 12
2.3 Caselle di posta elettronica certificata istituzionale e Domicilio Digitale 12
2.4 Responsabile della gestione documentale 13
3 Il Documento 14
3.1 Tipologia dei documenti 14
3.2 Documento informatico e documento amministrativo informatico 15
3.3 Formazione del documento informatico – Modalità 17
3.4 Formazione del documento informatico – Metadati 18
3.5 Formazione del documento informatico – Formati file 19
3.6 Sottoscrizione di documenti informatici 21
3.7 Verifica delle firme con il PDP 22
3.8 Posta elettronica certificata (PEC) 22
3.9 Requisiti degli strumenti informatici di scambio 23
3.10 Documento analogico 24
3.11 Documento in entrata 25
3.12 Documento in uscita 25
3.13 Documento interno (tra uffici) 25
3.14 Fascicolo – Definizione e funzione 26
3.15 Fascicolo – Formazione, implementazione e gestione 26
3.16 Piano di classificazione 26
3.17 Descrizione delle funzionalità del PDP in relazione alla conservazione ed alla immodificabilità delle registrazioni di protocollo 27
4 Protocollo informatico – Corrispondenza in entrata 28
4.1 Ricezione di documenti informatici sulle caselle PEC 28
4.2 Ricezione di documenti cartacei a mezzo posta e/o corriere 28
4.3 Documenti ricevuti prima via fax/e-mail e poi in originale su supporto cartaceo 29
4.4 Errata ricezione di documenti 29
4.5 Registrazione e relativa segnatura dei documenti in ingresso 29
4.6 Registrazione di un Protocollo differito 31
4.7 Assegnazione, visualizzazione e presa in carico dei documenti ricevuti 31
4.8 Smistamento 32
4.9 Fascicolazione 32
4.10 Rigetto e riassegnazione 32
4.11 Documenti esclusi dalla protocollazione 32
4.12 Documenti soggetti a registrazione particolare 33
5 Protocollo Informatico - Corrispondenza in uscita e a rilevanza interna 35
5.1 Descrizione del flusso di lavorazione dei documenti in uscita e interna (tra uffici) 35
5.2 Verifica formale dei documenti 35
5.3 Trasmissione di documenti informatici 35
5.4 Inserimento delle ricevute di trasmissione nel fascicolo 36
6 Regole generali per la formazione protocollo informatico, gestione registri particolari e componenti del sistema di gestione documentale 36
6.1 Registro giornaliero di protocollo 37

6.2 Livello di riservatezza 37
6.3 Segnatura di protocollo dei documenti 38
6.4 Annullamento delle registrazioni di protocollo 38
6.5 Protocollo di emergenza (art. 63 del D.P.R. 28 dicembre 2000, n. 445) 39
6.6 Modalità di protocollazione in emergenza 39
6.7 Import del registro di emergenza 40
6.8 Registri particolari di Protocollo 40
7 Piano di conservazione 41
7.1 Manuale di conservazione 42
8 Piano di Sicurezza per la gestione documentale 42
8.1 Generalità 43
8.2 Formazione dei documenti - Aspetti di sicurezza 44
8.3 Gestione dei documenti informatici in ambito PDP 45
8.4 Componente organizzativa della sicurezza per la gestione documentale 45
8.5 Componente fisica della sicurezza per la gestione documentale 46
8.6 Componente logica della sicurezza per la gestione documentale 46
8.7 Componente infrastrutturale della sicurezza per la gestione documentale 46
8.8 Gestione delle registrazioni di sicurezza per la gestione documentale 47
8.9 Trasmissione e interscambio dei documenti informatici 47
8.10 Trasmissione e interscambio dei documenti informatici 48
8.11 Trasmissione e interscambio dei documenti informatici 48
9. Gestione profili abilitativi, Manutenzione e Disaster Recovery 48
9.1 Accesso ai documenti informatici 48
9.2 Utenti interni – accesso al registro di protocollo 49
9.3 Utenti esterni ad Equitalia Giustizia S.p.A. 51
9.4 Manutenzione PdP 51
9.5 Disaster recovery 52

1. Premessa

Il DPCM del 3 dicembre 2013 - recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 711 del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005" - prevede l'obbligo per le pubbliche amministrazioni di cui all'articolo 2, comma 2 del D. Lgs. 82/2005 di "adottare il manuale di gestione (…), su proposta del Responsabile della gestione documentale" (art. 3).

Successivamente, l'Agenzia per l'Italia Digitale (di seguito AgiD) ha pubblicato le nuove Linee Guida sulla Formazione, Gestione e Conservazione del Documento Informatico (di seguito Linee Guida). Le suddette Linee Guida sono state emanate il 9 settembre 2020 e si applicano ai soggetti indicati nell'Art. 2, commi 2 e 3, del Codice dell'Amministrazione Digitale (CAD). Le Linee Guida sono state modificate da AgiD il 17 maggio 2021.

Il presente Manuale - conformemente a quanto disciplinato al punto 3.5 delle Linee Guida AgID descrive sia il sistema di gestione informatica dei documenti sia le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Pertanto, esso si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti.

Più in particolare, il Manuale disciplina le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti della società Equitalia Giustizia S.p.A. È inoltre funzionalmente connesso al presente Manuale il Manuale di conservazione, di cui al par. 4.6 delle Linee Guida AgiD, che illustra il sistema di conservazione dei documenti informatici della Società.

Il Manuale, attraverso l'integrazione delle procedure di gestione dei procedimenti amministrativi, di accesso agli atti e di archiviazione dei documenti partendo dal protocollo informatico, realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno della società anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa.

Infatti, l'attività di protocollazione - certificando "provenienza e data di acquisizione" del documento che viene identificato in maniera univoca – rappresenta un passo obbligato per tutti i flussi documentali che intercorrono tra diversi soggetti.

---

[1] D. Lgs 82/2005: Art. 40 bis "Protocollo informatico"; Art. 41 "Procedimento e fascicolo informatico"; Art. 47 "Trasmissione dei documenti tra le pubbliche amministrazioni"; Art. 71 "Linee Guida".

1.1 Principali norme di riferimento

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445: Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto legislativo 22 gennaio 2004, n. 42: Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68: Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- Decreto legislativo 7 marzo 2005, n. 82, successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217: Codice dell'amministrazione digitale;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445: Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto legislativo 22 gennaio 2004, n. 42: Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68: Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- Regolamento Europeo n. 679/2016 (GDPR): protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

1.2 Definizioni

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 durante lo svolgimento dell'attività.

Esso si distingue in:

Archivio corrente:

Il complesso dei documenti relativi ad "affari" e procedimenti amministrativi in corso di istruttoria e di trattazione o comunque per i quali esiste un interesse attuale;

Archivio di deposito:

Il complesso dei documenti relativi ad "affari" e procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento.

Archivio informatico:

è l'insieme di documenti informatici, di fascicoli informatici, nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.

Area Organizzativa Omogenea: (di seguito AOO) si intende un insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato.

Codice/CAD: si intende il decreto legislativo 7 marzo 2005 n. 82 successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217 – Codice dell'amministrazione digitale (CAD).

PdP: (Prodotto di Protocollo informatico) è il sistema informativo utilizzato da Equitalia Giustizia S.p.A. per la gestione del protocollo, le cui Strutture permettono l'acquisizione, la registrazione, l'archiviazione, la ricerca e la consultazione delle diverse tipologie di documenti trattati nell'ambito dei processi amministrativi e/o aziendali, sia interni e sia di scambio con l'esterno.

Documento amministrativo: Ai sensi 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.

In base al tipo di supporto e di modalità di formazione i documenti amministrativi possono essere analogici o digitali.

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 mano, macchina da scrivere, ecc.) o con strumenti informatici (es. lettera scritta con Word o con altri programmi di videoscrittura). Per versione analogica di documento informatico si intende la copia cartacea di un documento prodotto su supporto informatico.

Documento informatico: si intende "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" [Cfr. art. 1, comma 1 lett. p) del D.lgs. n.82/2005]. In particolare, l'art. 20 del decreto legislativo del 7 marzo 2005, n.

82, recante "Codice dell'amministrazione digitale" come modificato da ultimo, con D.lgs. 217/2017 prevede che:

> 1-bis. Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida"
>
> 3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, in conformità alle Linee Guida. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.
>
> 4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.
>
> 5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.
>
> 5-bis. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle Linee Guida.

L'originale informatico può essere dotato di firma digitale, di firma elettronica o non firmato. Per versione informatica del documento analogico si intende invece copia del documento su supporto informatico.

Documento amministrativo informatico: ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa.

Documenti interni: si intendono i documenti sia analogici che informatici scambiati tra le diverse strutture organizzative di cui si compone la società.

Documento uscita: si intende la corrispondenza, compresa di eventuali allegati, inviati ad un soggetto esterno sia pubblico che privato.

Documento ingresso: si intende la corrispondenza in ingresso acquisita dalla struttura protocollante con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

Dati personali: Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» (Cfr. art. 4 punto 1, Regolamento UE 2016/679);

Dati Particolari: Ai fini di questo disciplinare si considerano dati particolari:

- i "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (Cfr. art.9 punto1, Regolamento UE 2016/679);
- i "dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza" (Cfr. art.10, Regolamento UE 2016/679);

Interoperabilità: si intende quel particolare servizio che consente di mettere in comunicazione due o più sistemi di protocollo.

Linee Guida: emanate da AgiD il 17 maggio 2021 sostituiscono le "Regole tecniche per il protocollo informatico ai sensi dell'art. 71 del CAD di cui al decreto legislativo n.82 del 2005.

Manuale di Gestione documentale: (di seguito denominato MdG) è lo strumento che descrive il sistema di gestione informatica dei documenti.

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

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.

Posta Elettronica Certificata (PEC): è un sistema di comunicazione via e-mail, attraverso la quale è possibile inviare e ricevere documentazione elettronica 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.

Protocollo differito: permette il differimento della decorrenza giuridica dei termini di ingresso del documento rispetto alla data di registrazione, dichiarandone espressamente la data effettiva di ingresso 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.

Registro di emergenza: (art. 63 del D.P.R. 28 dicembre 2000, n. 445): è il registro su cui viene registrata la corrispondenza nel caso in cui non sia possibile utilizzare il sistema documentale per eventi eccezionali.

Responsabile del Procedimento Amministrativo (RPA): si intende il personale che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare.

Responsabile della gestione documentale: (di seguito RGD) è il soggetto che assicura la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi ai sensi dell'art. 61 del DPR 445/2000 e che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

Segnatura di protocollo: 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.

Società: per società si intende Equitalia Giustizia S.p.A.;

Testo Unico: si intendono le disposizioni dettate dal decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Titolario di Classificazione: è uno schema generale di voci logiche per organizzare i documenti dell'archivio, anche quelli non soggetti a protocollazione che consente 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.

Unità Organizzative di registrazione di Protocollo: (di seguito UOP) rappresentano gli uffici che svolgono attività di registrazione di protocollo. In Equitalia Giustizia esse coincidono con le strutture protocollanti.

Assegnazione - L'operazione di individuazione strutture competenti per la trattazione del procedimento amministrativo o dell'"affare" cui i documenti si riferiscono.

Fascicolazione - L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti "affari" o procedimenti amministrativi.

Fascicolo - Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento/processo amministrativo o ad una stessa materia o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, ai fini decisionali o informativi, tutti i documenti utili allo svolgimento delle attività.

I fascicoli costituiscono il tipo di unità archivistica più diffuso e sono costituiti, in base alle esigenze di servizio, secondo criteri che sono stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento.

Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc. Nel fascicolo possono trovarsi insiemi di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc.);

Firma digitale - Un particolare tipo di firma elettronica basata 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 (art. 1, comma 1, lettera s) del d.lgs. 7 marzo 2005, n. 82);

Firma elettronica - L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come

metodo di autenticazione informatica (art. 1, comma 1, lettera q) del d.lgs. 7 marzo 2005, n. 82).

ELENCO DEGLI ACRONIMI

AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale
D.lgs.	Decreto legislativo
DPCM	Decreto del Presidente Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
IPA	Indice delle Pubbliche Amministrazioni
PEC	Posta Elettronica Certificata
RGD	Responsabile della gestione documentale
SCDI	Sistema di conservazione dei documenti informatici
SGDD	Sistema di gestione documentale digitale
UOP	Unità Organizzativa di registrazione di Protocollo

2 Principi Generali

Politiche di gestione, archiviazione e conservazione documentale.

La Società adotta politiche di gestione e conservazione dei documenti coerenti con la normativa vigente e in particolare, con il CAD e con le Linee Guida emanate da AGID.

La gestione e la conservazione hanno come obiettivo la tutela dei documenti nel loro valore giuridico-probatorio mantenendone nel tempo l'integrità e l'affidabilità.

Al fine di assicurare l'efficace attuazione delle politiche, la Società assicura la formazione e l'aggiornamento professionale al personale coinvolto nei processi di gestione documentale, con riferimento alle regole e agli strumenti informatici adottati per la gestione dei documenti e ai processi operativi della Società.

2.1 Politiche di sicurezza

La Società adotta politiche di Sicurezza che tengono conto delle minacce alla stessa e della relativa evoluzione, in linea con la normativa vigente, anche in tema di protezione dei dati personali, e con le specifiche raccomandazioni, segnalazioni e Linee Guida pubblicate dall'AGID.

Più precisamente, la Società promuove le iniziative finalizzate al continuo miglioramento relative a:

- valutazione dei rischi;
- definizione e applicazione di adeguati piani di difesa;
- attivazioni di strumenti tecnici ed organizzativi su tutta la filiera;
- monitoraggio e aggiornamento costante di processi, procedure, prassi e strumenti;
- informazione e formazione del personale.

2.2 Aree organizzative omogenee e modello organizzativo

Per la gestione dei documenti si è adottato un modello organizzativo che ha un'unica Area Organizzativa Omogenea (AOO).

L'AOO è composta da una o più strutture organizzative per la gestione del protocollo informatico, dei flussi documentali e degli archivi (cd. strutture protocollanti). All'interno dell'AOO il sistema di protocollazione è unico.

Per la corrispondenza in ingresso, il sistema di protocollazione è accentrato presso la Funzione Segreteria Generale, ad eccezione della corrispondenza indirizzata alle Strutture di business, che è protocollata direttamente da queste ultime.

Ciò, fatto salvo quanto previsto per la documentazione riservata e/o per tipologie particolari di corrispondenza, che seguono le regole specifiche di protocollazione, in coerenza con la normativa interna tempo per tempo vigente[2]

Il sistema è sempre decentralizzato per la corrispondenza in uscita, che viene effettuata direttamente dalle singole Strutture.

2.3 Caselle di posta elettronica certificata istituzionale e Domicilio Digitale

La Società è censita, ai sensi di legge, nell'Indice delle Pubbliche Amministrazioni (IPA).

[2] Rientra in tale tipologia la corrispondenza inviata all'Organismo di Vigilanza della Società, agli appositi canali dedicati, ovvero, secondo quanto previsto dal MOG vigente, che viene registrata in entrata dalla Funzione Internal Audit ai sensi di quanto prescritto dal Funzionigramma aziendale tempo per tempo vigente. V. infra par. "Documenti soggetti a registrazione particolare".

L'indice delle pubbliche amministrazioni (IPA) è accessibile tramite il relativo sito internet - indicepa.gov.it - da parte di tutti i soggetti pubblici o privati.

La Società comunica tempestivamente all'IPA ogni successiva modifica intervenuta.

La Società è dotata di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'indice delle Pubbliche Amministrazioni (IPA): legale societario@pec.equitaliagiustizia.it.

Tale casella costituisce il domicilio digitale della Società.

2.4 Responsabile della gestione documentale

La Società nomina il Responsabile della gestione documentale, il quale assicura la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del DPR n. 445/2000. Il Responsabile si avvale delle strutture organizzative della Società preposte alla gestione documentale e del protocollo (cd. strutture protocollanti), nonché del supporto della Funzione Innovazione e Servizi ICT, in coerenza con quanto previsto dal Funzionigramma aziendale tempo per tempo vigente.

In particolare, il Responsabile della gestione ha il compito di:

- predisporre lo schema del Manuale di gestione con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del Manuale sul sito Internet della società;
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico;
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il Responsabile della conservazione, il Responsabile per la transizione digitale e il Responsabile della Funzione Innovazione e Servizi ICT, nonché, per le misure di sicurezza relative al trattamento dei dati personali, con la Funzione Internal Audit;
- abilitare gli addetti delle strutture protocollanti all'utilizzo del PdP e definire per ciascuno di essi il tipo di profilazione (ad esempio consultazione, modifica, ecc.);

- 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;
- conservare 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 operazioni di annullamento della registrazione di protocollo;
- aprire e chiudere il registro di protocollazione di emergenza.

Tutte le attività in ambito gestione documentale sono svolte in coordinamento con il Responsabile della conservazione (cfr. par. 4.5 delle Linee Guida Agid), con il Responsabile per la Transizione Digitale, con il Responsabile per la Protezione dei Dati personali e con il supporto delle altre figure/strutture della Società per quanto di rispettiva competenza.

3 Il Documento

Il documento, comunemente, viene definito quale scrittura atta a fornire una prova o convalida in ambito burocratico, amministrativo, giuridico.

In ambito giuridico è generalmente considerato come una "res", ovvero come qualsiasi cosa idonea a rappresentare e far conoscere un fatto che è destinato a produrre effetti giuridici diversi a seconda dei requisiti che possiede.

Nel linguaggio informatico il documento indica, solitamente, i files di contenuti (per esempio di Word) ovvero una "res signata", cioè un oggetto che reca una serie di segni tracciati, volti a conferirgli portata rappresentativa.

3.1 Tipologia dei documenti

Nell'ambito del processo di gestione documentale, il documento in base alle modalità di formazione è classificabile in:

- documenti analogici;
- documenti informatici.

A loro volta i documenti analogici ed informatici, si possono distinguere:

- documenti in entrata;
- documenti in uscita;
- documenti interni (tra uffici).

3.2 Documento informatico e documento amministrativo informatico

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Il documento amministrativo informatico è ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa.

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

Il documento informatico assume la caratteristica di immodificabilità se prodotto in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

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

L'associazione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione; tuttavia le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.

Tali considerazioni si estendono al documento amministrativo informatico, fermo restando che le caratteristiche di integrità ed immodificabilità sono garantite anche mediante la registrazione nel protocollo informatico della Società e negli ulteriori registri particolari.

I messaggi di posta elettronica certificata costituiscono di per sé un documento informatico, oltre che un mezzo di scambio di comunicazioni e documenti, in

quanto la relativa trasmissione/ricezione è giuridicamente rilevante e permette di avere prova opponibile dell'invio e della consegna del messaggio di posta.

Il messaggio e gli allegati trasmessi/ricevuti con PEC assumono lo stesso valore legale della raccomandata con avviso di ricevimento. In tal caso, l'avvenuta consegna del messaggio elettronico consente, tra l'altro, di ricorrere contro terzi.

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

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

Il duplicato del documento informatico è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto. I duplicati informatici hanno il medesimo valore giuridico del documento informatico da cui sono tratti. Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un pubblico ufficiale a ciò autorizzato.

La copia di documento informatico è un documento informatico che, mediante processi e strumenti idonei, assicura la corrispondenza della copia alle informazioni del documento informatico di origine attraverso l'utilizzo di uno dei formati idonei ai sensi della normativa vigente.

La copia di documento informatico è, dunque, un documento informatico che muta il formato del documento originario o che muta il supporto del documento originario informatico.

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

La copia su supporto informatico di documenti analogici può essere costituita da:

- copia informatica di documento analogico, avente contenuto identico a quello del documento analogico ma forma diversa;
- copia per immagine su supporto informatico di documento analogico, avente contenuto e forma identici all'originale.

Entrambe le tipologie di documento hanno la medesima efficacia probatoria degli originali analogici solo se la loro conformità è attestata da un pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico prodotta secondo le regole tecniche.

I file delle immagini dei documenti analogici, prodotti mediante scansione e archiviati sui sistemi informatici della Società, non assumono quindi la medesima efficacia probatoria dell'originale; rimangono quindi fermi gli obblighi di gestione e di conservazione previsti dalla normativa dei documenti analogici originali.

Il documento informatico come peraltro quello analogico, salvo standard specifici, deve, in genere, recare:

- la denominazione e il logo della società;
- l'indicazione completa della struttura che ha prodotto il documento;
- l'indirizzo completo della società (via, numero, CAP, città, provincia);
- il codice fiscale/P.IVA della società;
- luogo di redazione del documento;
- la data, (giorno, mese, anno);
- il numero di protocollo;
- il numero di repertorio (se disponibile);
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- se trattasi di documento informatico, sottoscrizione digitale del Responsabile e/o del responsabile del provvedimento finale;
- se trattasi di documento analogico, sottoscrizione autografa del Responsabile e/o responsabile del provvedimento finale;
- Informazioni complete sul destinatario (nome, cognome, sede legale, etc.);
- I modelli di riferimento delle principali tipologie di documenti sono presenti sulla intranet aziendale.

3.3 Formazione del documento informatico – Modalità

Il documento informatico è formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software: in tal caso il documento informatico assume le caratteristiche di immodificabilità e di

integrità con la sottoscrizione con firma digitale/firma elettronica qualificata o con l'apposizione di una validazione temporale o con il trasferimento a soggetti terzi con PEC con ricevuta completa o con il versamento ad un sistema di conservazione; in caso di formazione attraverso strumenti Office (es. word) il file va prodotto in formato PDF/A per la sottoscrizione con firma digitale;

- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni provenienti da una o più banche dati, anche appartenenti a più soggetti inter-operanti, secondo una struttura logica predeterminata e memorizzata in forma statica: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

3.4 Formazione del documento informatico – Metadati

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi "metadati", secondo quanto richiesto dalle Linee Guida.

I metadati costituiscono i dati associati ai documenti, che ne descrivono il contesto, il contenuto e la struttura, così da permetterne la gestione nel tempo

in conformità a quanto definito dalla norma. Gli obiettivi fondamentali dei metadati sono:

- garantire l'identificazione permanente dei singoli oggetti informativi, ad es.: identificativo univoco (numero di protocollo, data, autore, ecc.); garantire l'identificazione permanente delle relazioni tra gli oggetti informativi, ad es.: indici di classificazione;
- conservare le informazioni che supportano l'intellegibilità degli oggetti informativi, ad es.: procedimento amministrativo cui il documento è connesso.
- In prima istanza i metadati possono essere suddivisi nelle seguenti macrocategorie:
    - Descrittiva: ha lo scopo di facilitare il recupero e l'identificazione dell'oggetto digitale;
    - Gestionale: ha lo scopo di supportare la gestione dell'oggetto digitale all'interno di una collezione;
    - Strutturale: ha lo scopo di collegare fra loro i componenti di oggetti informativi complessi.

Peraltro, il documento una volta formato avrà un suo percorso di esistenza che lo porterà ad essere gestito da diversi sistemi e applicazioni con la contestuale produzione e associazione di ulteriori informazioni.

Un altro aspetto da tenere in considerazione, dunque, è che i metadati non vengono attribuiti ai documenti e in generale agli oggetti digitali tutti nel medesimo tempo, ma tendono ad accumularsi nel corso della vita degli stessi per tracciarne l'utilizzo, ad esempio gli accessi, le modifiche, i trasferimenti, le copie, nonché le modalità della sua conservazione.

3.5 Formazione del documento informatico – Formati file

Il presente paragrafo fornisce indicazioni sui Formati File accettati e gestiti dalla Società. I formati descritti, coerentemente ai requisiti definiti dalla normativa vigente, sono stati scelti fra quelli che possono maggiormente garantire il principio di interoperabilità fra i sistemi di gestione documentale e conservazione privilegiando, fra le diverse opportunità, quelli già approvati dagli organismi di standardizzazione internazionale quali ISO e ETSI.

Ciò premesso, dal punto di vista tecnico, le scelte sono state effettuate valutando le seguenti caratteristiche:

- Apertura;

- Sicurezza;
- Portabilità;
- Funzionalità;
- Supporto allo sviluppo;
- Diffusione.
- Di seguito si riporta l'elenco dei formati gestiti dalla Società:
    - PDF - PDF/A: Il PDF è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Un documento PDF può essere firmato digitalmente attraverso il formato ETSI PAdES o CAdES. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A. Il PDF/A è stato sviluppato con l'obiettivo specifico di rendere possibile la conservazione documentale a lungo termine su supporti digitali;
    - TIFF: di questo formato vi sono diverse versioni, con specifiche pubbliche e non soggette ad alcuna forma di limitazione. Il formato è utilizzato per la conversione in digitale di documenti cartacei;
    - JPG: tale formato è il più utilizzato per la memorizzazione di fotografie ed è quello più comune su World Wide Web e consente, inoltre, di associare metadati ad un'immagine;
    - Office Open XML (OOXML): il formato dispone di alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML. I metadati associabili ad un documento che adotta tale formato sono previsti dallo standard ISO 29500:2008;
    - Open Document Format (ODF): il formato è uno standard aperto, basato sul linguaggio XML, per la memorizzazione di documenti;
    - Extensible Markup Language (XML): (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi;
    - TXT: ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere adottata;
    - Formati Messaggi di posta elettronica: ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, lo

standard a cui fare riferimento è RFC 2822/MIME. Per quanto concerne il formato degli allegati al messaggio, valgono le indicazioni di cui ai precedenti paragrafi.

3.6 Sottoscrizione di documenti informatici

I requisiti di immodificabilità e di integrità del documento informatico possono essere assicurati anche con l'apposizione di una firma elettronica qualificata, di una firma digitale o firma elettronica avanzata.

La sottoscrizione dei documenti informatici prodotti dalla Società è apposta con un processo di firma elettronica digitale (qualificata), in conformità alle disposizioni dettate dalla normativa vigente.

La firma digitale è un particolare tipo di firma elettronica avanzata e qualificata (ai sensi del Regolamento Europeo eIDAS) basata su un certificato qualificato e realizzata mediante un dispositivo sicuro di firma (token, usb, smart card, usb, hsm) con un sistema di chiavi asimmetriche a coppia (una pubblica ed una privata) 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 del documento informatico. La firma digitale può essere utilizzata anche in modalità remota e/o automatica.

Il CAD stabilisce anche che "l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria", prevedendo quindi l'onere probatorio a carico del titolare del dispositivo di firma per l'eventuale disconoscimento della stessa.

La firma digitale viene assegnata ai dipendenti della Società, secondo i criteri di attribuzione definiti, in relazione alle responsabilità assegnate, e secondo le procedure di ciascuna certification authority (CA), previo riconoscimento del titolare anche tramite delegati interni alla Società da parte delle certification authority.

CAdES CMS Advanced Electronic Signature	PAdES PDF Advanced Electronic Signature	XAdES XML Advanced Electronic Signature
Qualsiasi File .doc, .xls, .exe, .pdf, etc.	Solo file .pdf	Solo file .xml
L'estensione del file firmato è p7m	L'estensione del file firmato è pdf	L'estensione del file firmato è xml

La firma elettronica "semplice" invece garantisce l'identificazione informatica dell'utilizzatore esclusivamente in forma di PIN o insieme di Username e Password (come nel caso delle e-mail); tale firma non assume valore di sottoscrizione e la relativa efficacia probatoria è liberamente valutabile dall'autorità giudiziaria.

La firma autografa può essere apposta sui documenti analogici e sulle copie analogiche di documenti informatici.

3.7 Verifica delle firme con il PDP

Nel PDP sono previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare.

La sequenza delle operazioni previste è la seguente: - apertura della busta "virtuale" contenente il documento firmato digitalmente; - verifica della validità del certificato; - verifica della firma (o delle firme multiple).

La busta "virtuale" è costruita secondo lo standard PKCS#7 e contiene il documento, la firma digitale ed il certificato rilasciato dalla autorità di certificazione unitamente alla chiave pubblica del sottoscrittore del documento.

3.8 Posta elettronica certificata (PEC)

La Società utilizza la PEC quale sistema gestionale e di comunicazione, ai sensi del CAD, in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili a terzi ad ogni effetto di legge.

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche.

L'utilizzo della Posta Elettronica Certificata (PEC) consente di:

- firmare elettronicamente il messaggio;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica certificata; dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti alla stessa e ad altre amministrazioni.

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema di protocollazione del ricevente. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato.

I messaggi di ritorno sono classificati in:

- Invio Telematico (Segnatura.xml)
- Accettazione
- Consegna
- Ricezione Conferma Protocollazione.

Nel caso in cui venga annullata la registrazione di protocollo del documento in uscita telematicamente tramite PEC, il sistema provvede a inviare sia al mittente che al destinatario dello stesso la ricevuta di annullamento della protocollazione.

Detti messaggi sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME.

Il documento informatico trasmesso per via telematica si intende uscita e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa vigente e alle relative regole tecniche sono opponibili ai terzi.

La trasmissione del documento informatico a mezzo PEC ha un valore legale equiparato ad una raccomandata con ricevuta di ritorno.

Ai sensi del combinato disposto degli articoli 40-bis e 57-bis, comma 1 del CAD vi è l'obbligo della registrazione di protocollo per le comunicazioni che pervengono alla casella di PEC istituzionale ed alle caselle di PEC dichiarate all'Indice degli indirizzi delle amministrazioni pubbliche (IPA).

Le attività di protocollazione dei documenti trasmessi alle caselle di posta elettronica sono demandate alle strutture protocollanti.

3.9 Requisiti degli strumenti informatici di scambio

Scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi è 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 delle AOO;

- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

3.10 Documento analogico

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

Per documenti analogici originali unici si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta.

Ai sensi delle norme vigenti, per particolari tipologie di documenti analogici originali unici, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un pubblico ufficiale a ciò autorizzato.

Pertanto, tutti i documenti cartacei su cui vengono apposti manualmente dati di registrazione a protocollo, sigle e firma autografa, sono documenti analogici.

Il duplicato di un documento analogico è la riproduzione di un documento analogico originale distrutto o smarrito che lo sostituisce a tutti gli effetti legali.

La copia di un documento analogico è la trascrizione o riproduzione dell'originale. Si distingue in copia semplice, imitativa e conforme. La copia semplice è la pura trascrizione dell'originale senza riguardo agli elementi formali. La copia imitativa riproduce sia il contenuto che la forma (es. fotocopia).

La copia conforme è la copia certificata come conforme all'originale da un pubblico ufficiale autorizzato ad eseguire tale attestazione nell'esercizio delle sue funzioni (copia "autentica").

La copia analogica di documento informatico è, di norma, la stampa cartacea dello stesso. La copia su supporto analogico di documento informatico, sottoscritto con firma elettronica avanzata o qualificata, per avere la stessa efficacia probatoria dell'originale da cui è tratta, deve essere certificata come conforme all'originale in tutte le sue componenti da un pubblico ufficiale ovvero deve riportare, apposto a stampa, un contrassegno, ai sensi dell'art. 23 co. 2-bis del CAD.

Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

3.11 Documento in entrata

Per "documento in entrata" si intende la corrispondenza in ingresso - compresa di eventuali allegati - trasmessa alla società nell'ambito della propria attività da un soggetto esterno pubblico o privato.

Un documento informatico può essere recapitato:

- a mezzo posta elettronica convenzionale e certificata;
- a mezzo web.

Un documento analogico può essere recapitato:

- a mezzo posta convenzionale o corriere;
- a mezzo posta raccomandata;
- per telefax o telegramma;
- con consegna diretta da parte dell'interessato o suo delegato.

La corrispondenza ricevuta via telegramma o via telefax ovvero attraverso posta elettronica certificata, per quanto riguarda la registrazione di protocollo, è trattata come un documento cartaceo.

3.12 Documento in uscita

Per "documento in uscita" si intende la corrispondenza - compresa di eventuali allegati - di rilevanza informativa e/o giuridico-probatoria prodotta dalla società nell'esercizio delle proprie funzioni ed indirizzata ad un soggetto esterno, privato o pubblico.

Di norma i documenti in uscita dovranno essere, ove possibile, trasmessi a mezzo della posta elettronica certificata se la dimensione del documento non supera la dimensione massima prevista dal sistema di posta utilizzato. Diversamente, il documento informatico viene riversato, su supporto digitale rimovibile non modificabile e trasmesso con altri mezzi di trasposto al destinatario.

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

3.13 Documento interno (tra uffici)

Per "documenti interni (tra uffici)" si intendono i documenti scambiati tra le diverse strutture organizzative di cui si compone la società. In caso di documenti tra uffici rientranti nelle tipologie per le quali è prevista la protocollazione in base

alla normativa interna tempo per tempo vigente, o scambio tra le singole strutture dei documenti informatici avviene per mezzo del PdP.

La loro registrazione deve essere effettuata una sola volta dal Responsabile mittente, mentre il destinatario del documento interno non deve effettuare una nuova registrazione del documento in arrivo.

3.14 Fascicolo – Definizione e funzione

Il fascicolo è l'unità di base dell'archivio e aggrega documenti che afferiscono allo stesso procedimento.

La corretta tenuta del fascicolo garantisce sia la sedimentazione che il diritto di accesso.

3.15 Fascicolo – Formazione, implementazione e gestione

Per ogni tipologia, la Società può conservare in un fascicolo informatico gli atti, i documenti e i dati da chiunque siano stati formati. Il fascicolo informatico deve recare l'indicazione:

- dell'AOO titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- del Responsabile del procedimento;
- dell'oggetto del procedimento;
- dell'elenco dei documenti contenuti;
- dell'indice di classificazione (e.g. titolo, classe, sottoclasse, etc.);
- del numero del fascicolo, che è identificativo di una catena numerica relativamente alla classe di riferimento dell'anno di creazione;
- della data di apertura e di chiusura del fascicolo.

L'indicazione della Struttura di competenza del Responsabile del Procedimento Amministrativo (RPA) concorrono all'identificazione del fascicolo e al riconoscimento del responsabile.

3.16 Piano di classificazione

Gli addetti alle attività di registrazione, ai fini della relativa protocollazione, provvedono alla classificazione del documento sulla base del Titolario di classificazione in essere presso la società.

Il Titolario di classificazione si articola su due livelli:

- livello per funzioni / materia;
- livello per macro-attività per ciascuna funzione.

Ogni voce del piano di classificazione comprende:

- un indice (codice alfanumerico);
- la denominazione della voce.

Laddove ne nasca l'esigenza, l'aggiornamento del piano di classificazione è gestito a cura del RGD.

Ogni proposta di revisione, anche parziale, del Titolario deve essere segnalata al RGD che la valuterà in condivisione con le competenti funzioni aziendali.

È cura del RGD informare le strutture addette alla protocollazione dell'intervenuta revisione.

Viene garantita 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.

3.17 Descrizione delle funzionalità del PDP in relazione alla conservazione ed alla immodificabilità delle registrazioni di protocollo

Il PdP è un sistema modulare, progettato per essere uno strumento completo per l'organizzazione e la gestione dei documenti in ogni fase del loro ciclo di vita, dalla loro acquisizione nel sistema fino al momento del loro versamento in conservazione.

Il piano di conservazione dei documenti e dei fascicoli informatici è a cura del soggetto produttore (AOO), in accordo con il Responsabile della Gestione Documentale e con il Responsabile della Conservazione.

Per attuare il piano di conservazione possono essere collegate le voci usate nel Titolario di classificazione, al periodo di conservazione dei documenti, per agevolare le operazioni di scarto e di conservazione degli stessi.

Il modulo di Protocollo Informatico assolve a quanto richiesto dalla normativa in materia, compreso l'aspetto relativo al calcolo dell'impronta crittografica di hash per ogni documento registrato nel sistema, assicurando la immodificabilità delle registrazioni di protocollo.

Anche la tracciatura e la storicizzazione delle modifiche effettuate sui record di registrazione sono registrate nel PdP a livello degli audit log del sistema.

I log contengono le informazioni relative a qualsiasi modifica effettuata, oltre all'autore, all'ora e alla data della stessa, storicizzando i dati modificati.

4 Protocollo informatico – Corrispondenza in entrata

La Società organizza e gestisce il servizio per la tenuta del protocollo informatico e della gestione dei flussi documentali, come previsto dall'art. 61 del DPR n. 445/2000, ai fini della corretta tenuta del sistema di gestione analogica e informatica dei documenti, dei flussi documentali e degli archivi, nonché il coordinamento degli adempimenti previsti dalla normativa vigente.

Ogni qualvolta venga emanata o modificata una delle normative interne della Società che direttamente o indirettamente contenga delle disposizioni in merito alla protocollazione è necessario un previo coinvolgimento di tutte le strutture interessate.

Il sistema di protocollo assicura la tracciabilità di tutte le registrazioni effettuate e dei relativi flussi documentali.

4.1 Ricezione di documenti informatici sulle caselle PEC

I documenti digitali ricevuti sulla casella PEC istituzionale vengono gestiti dalla Funzione Segreteria Generale, protocollati ed assegnati ad una o più Strutture di competenza ed eventualmente per conoscenza ad altre Strutture.

Se una Struttura riceve sulla propria PEC un documento, dovrà inoltralo alla struttura protocollante per la conseguente protocollazione ed assegnazione, a meno che non si tratti di documentazione riservata che è gestita in base a quanto previsto dalla normativa interna tempo per tempo vigente.

4.2 Ricezione di documenti cartacei a mezzo posta e/o corriere

Successivamente al completamento di tutte le fasi inerenti ai controlli di sicurezza della posta pervenuta, la struttura aziendale competente a ricevere tali tipologie di documenti in ingresso provvede a smistarla alle strutture protocollanti per le conseguenti attività di protocollazione descritte nei paragrafi successivi.

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

4.3 Documenti ricevuti prima via fax/e-mail e poi in originale su supporto cartaceo

I documenti anticipati a mezzo fax/e-mail sono protocollati secondo le regole descritte nel presente capitolo.

Se in seguito si riceve lo stesso documento in originale, è necessario attribuirgli la stessa segnatura di protocollo del documento ingresso via fax/e-mail. Se l'originale viene nuovamente registrato con un diverso numero di protocollo, è necessario annullare tale registrazione.

Se si riscontrano differenze sia pure minime tra il documento in ingresso via fax/e-mail e l'originale, si devono considerare documenti diversi e quindi l'originale deve essere registrato con un nuovo numero di protocollo.

La segnatura deve essere apposta sul documento e la relativa copertina nonché il rapporto di trasmissione devono essere inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.

Sia il fax/e-mail che l'originale vanno inseriti nel fascicolo.

4.4 Errata ricezione di documenti

Qualora pervengano documenti indirizzati a soggetti diversi dalla Società, gli stessi dovranno essere restituiti al mittente secondo le seguenti modalità:

- per i documenti informatici pervenuti a mezzo e-mail, l'operatore di protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa Società" protocollandolo sia in ingresso che in uscita;
- per i documenti cartacei la relativa busta viene restituita alla posta. Se la busta viene aperta per errore, il documento è protocollato sia in ingresso che in uscita inserendo nel campo oggetto la dicitura tipo "documento pervenuto per errore".

4.5 Registrazione e relativa segnatura dei documenti in ingresso

Per registrazione si intende l'insieme delle procedure e degli elementi attraverso i quali i documenti vengono trattati sotto il profilo strettamente giuridico - probatorio, assumendo l'addetto al protocollo la funzione certificativa della effettiva ricezione e spedizione dei documenti.

La registrazione deve essere effettuata, di norma, entro la giornata di arrivo o comunque tempestivamente. I documenti che arrivano il venerdì dopo l'orario di chiusura della Società o di sabato e nei festivi, sono protocollati il giorno

lavorativo successivo. Le protocollazioni avvenute con oltre 7 giorni solari dal ricevimento sono motivate mediante inserimento di un'apposita annotazione a sistema.

Dopo l'avvenuta registrazione gli elementi del documento protocollato sono riconducibili a due tipologie:

- elementi immodificabili;
- elementi modificabili.

Gli elementi immodificabili servono ad attribuire a ciascun documento data, forma e provenienza certa attraverso la registrazione delle informazioni rilevanti sul piano giuridico - probatorio.

Pertanto, il sistema informatico impedisce la loro modifica una volta registrati.

Essi sono:

- data di registrazione;
- numero di protocollo (assegnato automaticamente e immutabile);
- corrispondente (mittente per documento in arrivo; destinatario per documento in uscita);
- oggetto;
- impronta del documento informatico;
- numero degli allegati;
- descrizione degli allegati.
- Tipologia di documento;
- Recapito del mittente.

Gli elementi modificabili sono:

- Struttura di competenza;
- responsabile del procedimento amministrativo (RPA);
- classificazione archivistica in base al Titolario;
- fascicolo (ove applicabile);
- collegamenti ad altri documenti diversi da quello di inserimento;
- alcuni tipi di annotazione.

4.6 Registrazione di un Protocollo differito

La registrazione differita di protocollo in ingresso è consentita solo nel caso:

- Corrispondenza in ricezione nei giorni festivi;
- Corrispondenza in ricezione nei giorni feriali ma al di fuori dell'orario di lavoro;
- di eccessivo carico di lavoro;

non sia possibile effettuare la protocollazione nel medesimo giorno in cui è pervenuta la corrispondenza. Tale facoltà è comunque limitata ai casi in cui non venga pregiudicato il diritto del terzo (ad esempio, in caso di scadenza termini di ricevimento fissati in un bando; in tale ultima ipotesi sarà comunque garantita la registrazione della data effettiva di ricezione della corrispondenza informatica o analogica.

Il protocollo differito consiste nel differimento del termine di registrazione. Come indicato in precedenza, le protocollazioni avvenute con oltre 7 giorni solari dal ricevimento sono motivate mediante inserimento di un'apposita annotazione a sistema.

4.7 Assegnazione, visualizzazione e presa in carico dei documenti ricevuti

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

La struttura assegnataria dei documenti ricevuti ne ha notizia tramite widget dedicato e/o tramite messaggio di posta elettronica (configurabile dall'utente).

Indipendentemente dalla ricezione della suddetta notifica, gli utenti abilitati al sistema di protocollo devono costantemente monitorare l'eventuale assegnazione di documenti protocollati in ingresso.

Il Responsabile/Struttura di competenza, attraverso l'utilizzo dell'applicazione di protocollo informatico ed in base alle abilitazioni previste, provvede alla presa in carico del documento allo stesso assegnato e potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- assegnare per Competenza, laddove ritenga necessario l'interessamento di ulteriori Responsabili/Strutture;
- assegnare per Conoscenza, laddove ritenga necessario l'interessamento di ulteriori Responsabili/Struttura e/o risorse solo per opportuna informazione.

La "presa in carico" dei documenti informatici viene registrata dal sistema.

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.

4.8 Smistamento

Lo smistamento dei documenti all'interno della Società avviene, di norma, attraverso il sistema di assegnazione del PdP coerentemente con l'organigramma e il Funzionigramma aziendale.

Gli originali dei documenti cartacei, preventivamente scansionati ed inseriti nel PdP, saranno conservati di norma presso la Struttura protocollante.

4.9 Fascicolazione

La struttura protocollante provvede alla fascicolazione. Ciò, ad eccezione della fascicolazione della corrispondenza in arrivo di competenza della Funzione Contenzioso Business che è effettuata direttamente da quest'ultima struttura, una volta che la Funzione Segreteria Generale abbia completato le attività di protocollazione.

Il Responsabile, al quale è stato assegnato il documento, provvede a verificare la classificazione e la fascicolazione e, se lo ritiene opportuno, a modificarli.

4.10 Rigetto e riassegnazione

Il Responsabile della struttura assegnataria, se ritiene che il documento assegnatogli non è di propria competenza, deve eseguire il rigetto dell'assegnazione, a sistema, indicando le motivazioni del rigetto.

4.11 Documenti esclusi dalla protocollazione

In coerenza con le previsioni dell'art. 53, comma 5 del DPR 445/2000 sono esclusi dalla registrazione a protocollo delle seguenti tipologie:

- Gazzette ufficiali;
- Bollettini Ufficiali e Notiziari;
- Giornali, riviste e libri;
- Materiali statistici;
- Materiali pubblicitari;

- Offerte / preventivi inviati spontaneamente da terzi e non richiesti, in quanto non afferenti a indagini esplorative e a procedimenti per l'acquisizione di beni e servizi;
- Inviti a manifestazioni che non attivino procedimenti amministrativi.
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.);
- Allegati, se accompagnati da lettera di trasmissione;
- Fatture cartacee (Spedizione tramite le funzionalità della piattaforma di e-Procurement);
- Fatture Elettroniche (gestite su piattaforma dedicata Microsoft Dynamics 365 Business Central);
- Documentazione cartacea proveniente dagli Istituti finanziari contenente estratti conto e/o altri documenti;
- Tutti i documenti dello SNA, che sono pubblicati nella Intranet.

4.12 Documenti soggetti a registrazione particolare

Conformemente alle policy della Società per utilizzo degli strumenti elettronici, per gli accessi alle risorse e ai dati, con particolare riferimento agli obblighi di riservatezza nel trattamento delle informazioni, sono riportate di seguito le modalità operative per la protocollazione e gestione di particolari tipologie di documenti in ingresso:

- Corrispondenza "riservata" o "personale": la corrispondenza che riporta come destinatario soltanto il nominativo di una persona - senza alcun riferimento alla Struttura di appartenenza, a un progetto, a un prodotto - oppure che riporta in chiaro la dicitura "riservata" o "personale" o simili non viene aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli alla struttura protocollante di riferimento nell'arco della medesima giornata dell'avvenuta consegna;
- Corrispondenza indirizzata agli Organi della Società: tutta la corrispondenza indirizzata, anche solo genericamente, al Presidente, all'Amministratore Delegato, agli Organi sociali ed all'Organismo di Vigilanza non deve essere mai aperta. L'addetto alla funzione di protocollo provvederà a consegnarla all'interessato in attesa di indicazioni in merito alla protocollazione;

- Corrispondenza dell'OdV: La corrispondenza indirizzata all'Organismo di Vigilanza, così come previsto dal Modello di Organizzazione, Gestione e Controllo, ai sensi del D. lgs. n. 231/2001, viene consegnata al Responsabile della Funzione Internal Audit. La Funzione Internal Audit provvede alla protocollazione ed a consegnare la documentazione all'OdV, per le valutazioni di competenza;
- Segnalazioni in materia di whistleblowing: le segnalazioni di whistleblowing sono regolate dalla specifica procedura emessa dalla Società;
- Corrispondenza indirizzata alle Funzioni Risorse Umane e Strumentali e Internal Audit ed ad altri soggetti che all'interno dell'azienda ricoprono incarichi specifici: l'addetto all'attività di protocollo provvederà a consegnarla alla Funzione interessata in attesa di indicazioni in merito alla protocollazione;
- Lettere anonime: le lettere anonime vanno consegnate al Responsabile della Funzione Internal Audit. La Funzione Internal Audit, una volta visionato il contenuto della documentazione, provvede alla sua protocollazione e a riferire agli organi aziendali competenti.
- Buste di gara: la documentazione relativa alle procedure di gara eseguite in base al codice dei contratti pubblici viene gestita tramite la piattaforma informatica dedicata.
- Per quanto concerne l'ulteriore documentazione in entrata relativa agli affidamenti ai sensi del Codice degli Appalti, il RUP o il supporto al RUP, ove presente, inoltrano alla struttura protocollante la documentazione da registrare. La contrattualistica sottoscritta è sempre soggetta a registrazione di protocollo aziendale.

I documenti e le comunicazioni ricevuti via posta elettronica (e-mail) non certificata privi di sottoscrizione possono, a discrezione della Struttura di competenza, essere oggetto di protocollazione. Laddove gli stessi siano sottoscritti con firma digitale (o con altro mezzo idoneo ad accertarne la fonte di provenienza) sono da considerarsi originali a tutti gli effetti di legge e nel caso in cui il contenuto sia rilevante al fine giuridico - probatorio sono soggette a protocollazione.

I documenti informatici prodotti o gestiti da applicativi e procedure informatizzate, anche di altri Enti / Autorità / Società, a supporto di specifici processi della Società, possono essere soggetti a registrazione particolare, anche tramite gli applicativi di altri Enti / Autorità laddove consentito dalla specifica normativa vigente.

Per i documenti informatici classificati come "riservati" in quanto contenenti "informazioni e dati che possono essere trattati esclusivamente da un ristretto numero di persone, sulla base di specifiche indicazioni dei responsabili della Società", la protocollazione deve essere fatta nel sistema documentale con modalità "riservato" che consente la visibilità e l'intervento sul protocollo ai soli assegnatari dello stesso.

5 Protocollo Informatico - Corrispondenza in uscita e a rilevanza interna

5.1 Descrizione del flusso di lavorazione dei documenti in uscita e interna (tra uffici)

Per documenti in uscita si intendono quelli prodotti dalle singole strutture della società aventi rilevanza giuridico-probatoria e destinati ad essere trasmessi ad un soggetto esterno, pubblico o privato.

Per documenti interni (tra uffici) si intendono quelli prodotti dalle singole strutture della società e destinati ad altre strutture della società. Tali documenti sono soggetti a protocollazione limitatamente ad alcune tipologie individuate dalla normativa interna tempo per tempo vigente.

Il documento in uscita, ove possibile, dovrà essere in formato digitale secondo gli standard illustrati in precedenza e spedito a mezzo posta elettronica certificata.

5.2 Verifica formale dei documenti

Ogni singola struttura della società è autorizzata a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita.

Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dalle singole strutture.

5.3 Trasmissione di documenti informatici

Il canale preferenziale ai fini dell'invio del documento in uscita è la PEC.

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi al DPCM 3 dicembre 2013 in materia di protocollo informatico, artt. 16 e 17 e al D.lgs. n. 2 novembre 2005, in particolare a quanto previsto nell' allegato tecnico.

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica. Per la spedizione dei documenti informatici la struttura protocollante si avvale dei

servizi di autenticazione e marcatura temporale offerti da un certificatore accreditato iscritto nell'elenco pubblico tenuto dal AGID.

Per la spedizione dei documenti informatici, la struttura protocollante si avvale di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, che può essere offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche.

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 dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.

5.4 Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito, le ricevute dei messaggi telefax, le ricevute delle raccomandate, le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo fascicolo.

6 Regole generali per la formazione protocollo informatico, gestione registri particolari e componenti del sistema di gestione documentale

Ai sensi dell'art. 53 comma 5 del DPR 28 dicembre 2000, n. 445, la registrazione di protocollo è un'operazione obbligatoria per "i documenti ricevuti o spediti dall'amministrazione e tutti i documenti informatici".

Nel rispetto della normativa vigente, il protocollo è unico e la numerazione delle registrazioni di protocollo è unica e progressiva per ogni anno, indipendentemente dal modello organizzativo adottato dalla società.

La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo. 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 numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca solo numero di protocollo. Quindi, non è consentita la protocollazione di un documento già protocollato.

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

6.1 Registro giornaliero di protocollo

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 nei confronti dei terzi.

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

Il registro giornaliero di protocollo è trasmesso in via automatizzata entro la giornata lavorativa successiva al sistema di conservazione, garantendole l'immodificabilità del contenuto.

I principali metadati del registro giornaliero di protocollo sono riportati nella tabella seguente.

Tabella Metadati registro giornaliero di protocollo
ID (identificativo documento)
Protocolli annullati (Si/No)
Tipologia Arrivo/Uscita/Interno
Numero protocollo
Classificazione
Mittente/Destinatario
Unità Organizzativa (assegnatari)
Oggetto
Annotazioni
Numero Fascicolo
Dettaglio Allegati
Dettaglio per protocollista
Riferimenti ai documenti privi di allegati

6.2 Livello di riservatezza

Qualora l'addetto alla protocollazione valuti il documento come riservato, seleziona il flag nell'apposito campo.

6.3 Segnatura di protocollo dei documenti

La 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.

La registrazione e la segnatura costituiscono un'operazione unica e contestuale aventi entrambe la natura di atto pubblico.

L'operazione di segnatura deve consentire l'identificazione univoca e certa nel formato previsto dalle norme vigenti.

Gli elementi della segnatura devono essere apposti sui documenti prodotti da registrare in uscita, sui documenti in ingresso e sui documenti scambiati internamente.

I dati della segnatura di protocollo di un documento informatico sono il codice identificativo della società, la data ed il numero di protocollo del documento.

Nel PdP la segnatura viene associata al record del documento in simultaneità alla sua registrazione; infatti nella visualizzazione di un documento registrato, in alto deve comparire la segnatura di protocollo formata dalla seguente nomenclatura:

Prot. n. xxxxxxx del gg/mm/aaaa (AAAA–SIGLA AOO-NUMERO PROT.).

Per i documenti cartacei in ingresso e in uscita, l'acquisizione dell'immagine del documento analogico viene effettuata prima dell'apposizione della segnatura.

Una volta completata la scansione e generato il numero di protocollo tramite il sistema informatico, la data e il numero di protocollo vengono riportati manualmente sul documento originale, mediante timbratura e annotazione a mano.

6.4 Annullamento delle registrazioni di protocollo

L'annullamento di una registrazione di protocollo è un'operazione del tutto eccezionale, consentita solo in coerenza con quanto previsto dalla normativa vigente in materia, previa autorizzazione del Responsabile della Gestione Documentale. Non è mai consentito l'annullamento o la modifica di un campo modificabile di un documento che è già stato spedito al destinatario.

L'annullamento di una registrazione di protocollo avviene attraverso l'apposizione della dicitura "annullato".

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico, permettendo le attività di visualizzazione e stampa.

Per richiedere l'annullamento occorre che il Responsabile della Funzione che ha effettuato la registrazione di protocollo effettui un'apposita richiesta scritta, firmata digitalmente, indicando il motivo dell'annullamento. Se è stata prodotta una nuova registrazione in sostituzione di quella da annullare, nella richiesta di annullamento deve essere indicato anche il nuovo numero di protocollo. Se non sussistono motivi ostativi, il Responsabile della Gestione Documentale autorizza l'annullamento, dando indicazione alla struttura competente di eseguire l'annullamento stesso.

6.5 Protocollo di emergenza (art. 63 del D.P.R. 28 dicembre 2000, n. 445)

Il Registro di emergenza è il registro unico su cui viene registrata la corrispondenza nel caso in cui non sia possibile utilizzare il sistema informatico per eventi eccezionali, ad esempio qualora si verifichi:

- un guasto all'applicativo utilizzato per le attività di protocollazione;
- un guasto al sistema informatico;
- una mancanza prolungata di energia elettrica tale da non consentire lo svolgimento, entro la fine della giornata, delle operazioni di protocollazione, è necessario attivare un protocollo di emergenza su supporto cartaceo.

A tal fine, il RGD deve:

- redigere il verbale di attivazione;
- dare comunicazione alle strutture protocollanti della attivazione della procedura di emergenza;

Al termine dell'emergenza il RGD deve;

- revocare l'autorizzazione al protocollo di emergenza;
- dare comunicazione alle strutture protocollanti della revoca della procedura di emergenza.

6.6 Modalità di protocollazione in emergenza

Ricevuta la comunicazione di attivazione della procedura di emergenza, si deve procedere alla registrazione della corrispondenza utilizzando il registro di emergenza.

La numerazione del registro di emergenza è distinta da quella del protocollo ufficiale, è unica per l'intero anno e ricomincia dal numero successivo all'ultimo generato per ogni attivazione.

Ogni documento è individuato dal numero assegnato nel registro di emergenza a partire dal n. 1.

Ricevuta la comunicazione di revoca, la Funzione Segreteria Generale deve inserire le registrazioni di emergenza nel protocollo informatico ordinario, riportare nel campo note il numero e la data del protocollo di emergenza e conservare il registro di emergenza.

Il documento protocollato secondo la presente procedura di emergenza reca due numerazioni: quella del registro di emergenza e quella del protocollo ordinario. Eventuali termini decorreranno dalla data in cui è stata effettuata la protocollazione sul registro di emergenza.

6.7 Import del registro di emergenza

Una volta terminata la situazione di emergenza si deve provvedere all'import del Registro di emergenza nel PdP.

L'importazione dei dati del registro di emergenza nel sistema di protocollo è effettuata in modalità manuale dalla Funzione Segreteria Generale avendo cura di inserire nel campo "annotazione" le informazioni relative al periodo di emergenza.

In alternativa il RGD potrà raccogliere il Registro di emergenza, per poi trasmetterlo alla Funzione Innovazione e Servizi ICT che provvederà alla trasformazione degli stessi in formato XML ed al successivo caricamento.

6.8 Registri particolari di Protocollo

Oltre ai registri di cui ai punti precedenti, la cui istituzione è obbligatoria, Equitalia Giustizia S.p.A. utilizza un Registro particolare dedicato alla memorizzazione delle copie digitali dei sotto - fascicoli giudiziari della gestione crediti di giustizia.

I Registri particolari assicurano modalità di registrazioni analoghe a quelle assicurate dalla segnatura di protocollo dei documenti.

In particolare, è assicurata la consequenzialità dei numeri di registrazione attribuiti in forma automatica e la non modificabilità delle registrazioni: è infatti lo stesso sistema automatizzato, che produce massivamente queste tipologie di documenti, che genera e appone la segnatura su ciascun documento.

7 Piano di conservazione

I documenti ed i fascicoli sono gestiti e raccolti in archivi che possono essere distinti in:

- archivio corrente, rappresentato dal sistema di gestione documentale ove vengono raccolti, gestiti e conservati i documenti prodotti e ricevuti dall'azienda, fino all'esaurimento degli ordinari flussi di lavorazione che li riguardano;
- archivio di deposito, rappresentato dal sistema di conservazione, logicamente distinto dal sistema di gestione documentale, ove vengono riversati i documenti, una volta che sono esauriti i flussi di lavorazione ordinaria che li riguardano, ai fini della conservazione a lungo termine, per obblighi normativi o altri interessi storici aziendali.

La conservazione dei documenti digitali prevista normativamente viene effettuata sul sistema di conservazione in base a quanto indicato nell' apposito manuale di conservazione. Le componenti funzionali del sistema di conservazione assicurano il trattamento dell'intero ciclo di gestione, dal versamento allo scarto, dell'oggetto conservato (documento, fascicolo) nell'ambito del processo di conservazione, promuovendo una convergenza funzionale da eventuali diversi canali di versamento (principio di centralità di archivio).

Il sistema di conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla normativa di riferimento, indipendentemente dall'evolversi del contesto tecnologico.

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi (o lotti), volumi ed archivi di conservazione.

Il sistema di conservazione opera secondo modelli organizzativi definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale.

I documenti sono conservati, anche sulla base delle tempistiche previste dalla normativa di riferimento, nel sistema di conservazione secondo precise regole operative, su supporti elettronici certificati dal responsabile della conservazione. Ogni oggetto conservato è tenuto costantemente sotto controllo dal sistema, che ne garantisce la leggibilità e la disponibilità per un periodo prestabilito in fase di configurazione.

Il processo di conservazione dei documenti termina con l'apposizione da parte del conservatore della firma digitale e della marca temporale quali strumenti di "certificazione" opponibile a terzi sull'insieme di documenti destinati alla conservazione e su un'evidenza informatica (file di chiusura) contenente i metadati e le impronte (hash) dei documenti stessi. Il file di chiusura generato dal sistema risponde ai canoni dello standard UNI 11386:2010 (SInCRO).

È, infatti, la tecnologia della firma digitale che permette di garantire l'autenticità e di rendere immodificabile un oggetto informatico. La firma associata alla marcatura temporale permette di datare in modo certo l'oggetto conservato.

La conservazione di documenti nel sistema è riassumibile nelle seguenti fasi di processo:

- definizione delle regole di conservazione che il documento deve osservare, generalmente dipendono dalla tipologia documentale a cui è associato;
- verifica delle regole di conservazione ed esecuzione delle operazioni necessarie (firma, marca) in base alla tipologia documentale di appartenenza del documento;
- acquisizione del documento nel sistema;
- verifica automatica delle scadenze e dell'integrità dei documenti;
- archiviazione del documento in un pacchetto digitale (creazione del cd. "supporto" virtuale);
- creazione delle copie del supporto virtuale (copie automatiche di backup);
- verifica delle scadenze e dell'integrità dei supporti e del loro contenuto.

Il processo di conservazione è basato sulla tipologia documentale: ad essa si collegano tutti i modelli necessari all'esecuzione delle operazioni automatiche o manuali.

7.1 Manuale di conservazione

Il manuale di conservazione illustra dettagliatamente il modello organizzativo adottato, i soggetti coinvolti e i ruoli svolti dagli stessi, la descrizione dei processi relativi alle varie tipologie di documenti posti in conservazione, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

8 Piano di Sicurezza per la gestione documentale

Il piano di sicurezza per la gestione documentale è teso a garantire che i documenti e le informazioni, gestiti dal PDP siano resi disponibili, integri e riservati mediante opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Tutti i dati risiedono sul server, quindi sia la lavorazione che la consultazione dei documenti non avverrà in locale sulle postazioni client (di protocollazione e di consultazione), ma avverrà da remoto richiamando i dati presenti sul server, salvo eventuale download dei file sulla propria postazione di lavoro da parte dell'utente autorizzato a quel PDP.

Ogni utente potrà accedere solo alla documentazione per cui risulta incaricato alla consultazione.

8.1 Generalità

Il piano di sicurezza per la gestione documentale, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i documenti e le informazioni trattati e sulle direttive strategiche stabilite dal vertice della società, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza;

Il piano di sicurezza per la gestione documentale è soggetto a revisione con cadenza periodica e comunque in occasione delle modifiche di contesto interno ed esterno che possano impattare sul piano stesso o di eventi comunque rilevanti. Il RGD ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare:

- la sicurezza dell'impianto tecnologico dell'AOO;
- la riservatezza dei documenti e delle informazioni registrate nelle banche dati;
- l'univoca identificazione degli utenti interni ed esterni;
- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di acceso e conservazione dei documenti e delle informazioni;
- assegnazione ad ogni utente per accedere al protocollo aziendale ed agli altri componenti del sistema documentale, di una credenziale di

autenticazione personale composta da una user-id, da una componente riservata (password) e di un profilo di autorizzazione;

- cambio delle password con frequenza almeno ogni 90 giorni;
- la continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei documenti e delle informazioni da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;

8.2 Formazione dei documenti - Aspetti di sicurezza

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

- l'identificabilità del soggetto che ha formato il documento e la AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con altre AOO, ove presenti;

I documenti dell'AOO sono prodotti con l'ausilio di applicativi che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, XML e TIFF. I documenti informatici prodotti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) 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 e sottoscritto con firma digitale. Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per

la validazione temporale e per la protezione dei documenti informatici di cui al cap. 2.1 Documento informatico delle Linee Guida Agid. L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti informatici, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'AOO.

8.3 Gestione dei documenti informatici in ambito PDP

Il sistema operativo del PdP utilizzato dalla società è conforme alle specifiche previste dal DPCM 3 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi degli articoli 40 Bis, 41, 47, 57 bis e 71 del CAD di cui al D.lgs n. 82/2005. Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.
- Il sistema di gestione informatica dei documenti:
- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in ingresso ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ingresso dalla società e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati.

8.4 Componente organizzativa della sicurezza per la gestione documentale

La componente organizzativa della sicurezza legata alla gestione del protocollo e del sistema documentale, si riferisce principalmente alle attività svolte nell'ambito

del sistema informatico della società. In particolare, la definizione delle misure di sicurezza nell'ambito del sistema è attuata dalla Funzione Innovazione e Servizi ICT, in accordo con il RGD e il Responsabile per la transizione digitale, nonché, per quanto attiene al trattamento dei dati personali e al sistema di controllo interno, con la Funzione Internal Audit.

8.5 Componente fisica della sicurezza per la gestione documentale

Il sistema informatico è in hosting presso il CED Sogei e l'accesso fisico ai luoghi in cui sono custodite le risorse del sistema è limitato al solo personale autorizzato da Sogei secondo le proprie procedure.

8.6 Componente logica della sicurezza per la gestione documentale

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 nel Sistema di Normativa Aziendale.

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

- i file dei documenti sono accessibili solo tramite il server di application Layer.

Dal punto di vista degli accessi, per tutti gli accessi al sistema documentale, è prevista una procedura di abilitazione e profilazione utenti, gestita dalla Funzione Innovazione e Servizi ICT.

Per la gestione degli accessi, viene seguita la logica del minimo privilegio equivalente.

8.7 Componente infrastrutturale della sicurezza per la gestione documentale

Il sistema informatico è basato sull'infrastruttura di seguito descritta.

La server farm è gestita dal fornitore Sogei e protetta da una DMZ accessibile dalla sola rete di Equitalia Giustizia S.p.A..

8.8 Gestione delle registrazioni di sicurezza per la gestione documentale

Le registrazioni di sicurezza – LOG - sono costituite da informazioni di diverso tipo (ad es. dati o transazioni) presenti o transitate sui componenti del sistema documentale che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad 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 generati dall' application server;
- dai log generati dal web server.

8.9 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 ad essere rese pubbliche. Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario. Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO 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 la società 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.

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.

8.10 Trasmissione e interscambio dei documenti informatici All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende quel particolare servizio che consente di mettere in comunicazione due o più sistemi di protocollo.

8.11 Trasmissione e interscambio dei documenti informatici All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

9. Gestione profili abilitativi, Manutenzione e Disaster Recovery

9.1 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale. Queste, in sintesi, sono: la consultazione, l'inserimento, la modifica; Le regole per la composizione delle password e per il blocco delle utenze sono mutuate dalle regole configurate su Active directory.

Per ogni informazione di dettagli relativa alla disciplina degli accessi alle risorse informatiche si rimanda alla documentazione disponibile nel Sistema Normativo Aziendale.

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password, in parte riportate di seguito, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo. In particolare, il PdP adottato dalla società: 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 PdP può accedere solamente ai documenti che sono stati assegnati alla sua Struttura di competenza. Ove necessario il sistema permette di associare profili con un livello differente di accesso ai documenti in base alle esigenze organizzative aziendali; il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dalla società.

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

9.2 Utenti interni – accesso al registro di protocollo

I livelli di autorizzazione si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione ai diritti di intervento sul documento (modifica e annullamento delle informazioni). La gestione delle utenze rispetta i criteri di seguito illustrati.

Esistono diversi profili dei diritti di accesso sia in termini di visibilità dei documenti che per possibilità di inserimento, modifica e annullamento delle informazioni di protocollo.

L'assegnazione del profilo dei diritti di accesso viene effettuata centralmente dal personale della Funzione Innovazione e Servizi ICT su specifica richiesta del Responsabile della struttura di appartenenza. Le richieste vengono in genere inviate utilizzando un sistema di ticketing. La modifica dei profili viene eseguita manualmente. Nel caso che l'operazione comporti la cancellazione di un utente responsabile a cui sono stati assegnati documenti è possibile effettuare il passaggio dei diritti di accesso su tali documenti ad altro soggetto.

La "Visibilità" dei documenti è condizionata, oltre che dal profilo abilitativo assegnato all'utente, anche dalla modalità con la quale è stata eseguita la registrazione.

In particolare, il documento può essere registrato come:

- Pubblico: visibile a tutti gli utenti che abbiano assegnato il diritto di visione del relativo documento;
- Riservato: visibile solo agli utenti che abbiano assegnato il diritto di visione del relativo documento e la visibilità dei documenti riservati. L'utente potrà inserire, ove necessario, il termine fino al quale detto documento debba restare riservato.

In fase di registrazione i campi «Riservato» e «Dati Sensibili[3]» sono visualizzati solo dagli utenti a cui sono stati assegnati i diritti per la registrazione di tali categorie di documenti.

L'operatore abilitato all'inserimento, durante la fase di registrazione, assegna i documenti agli utenti assegnatari interessati per competenza al processo amministrativo.

L'utente principale assegnatario (Responsabile) dei documenti protocollati ha possibilità di riassegnare gli stessi a nuovi utenti assegnatari coinvolti nel processo amministrativo. Nel caso in cui sia effettuata la registrazione di un documento riservato, la visibilità è riservata ai soli assegnatari del documento protocollato. Gli eventuali diritti di intervento o di nuova assegnazione di un documento protocollato in forma riservata sono fruibili dal solo assegnatario principale (Responsabile) o dall'utente che ha protocollato il documento se inserito tra gli assegnatari dello stesso. Se l'utente abilitato all'inserimento che ha protocollato il documento, in forma riservata, non è inserito tra gli assegnatari, successivamente alla registrazione, perde i diritti di visibilità e quindi anche di intervento sul documento. Ogni operazione di inserimento, assegnazione, lettura, intervento sui documenti (modifica e annullamento) viene storicizzata dal sistema.

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 all'abilitazione per la fascicolazione e la archiviazione dei documenti (in raccoglitori), ai diritti di visibilità di particolari Repertori e ai diritti di inserimento e intervento in relazione ai documenti protocollati in essi contenuti.

Almeno una volta all'anno, il **Responsabile della Gestione Documentale** con il supporto di chi gestisce le autorizzazioni nei sistemi informatici, controlla che:

- Le **utenze attive** nel sistema di gestione documentale siano corrette.
- Le **autorizzazioni assegnate** siano coerenti con il ruolo e la posizione delle persone in azienda.

Durante questo controllo, viene confrontato:

- l'elenco degli utenti abilitati nel sistema con l'elenco del personale aziendale in servizio e con quello del personale esterno che ha accesso al sistema.

[3] Per dati sensibili si intendono: i dati particolari di cui all'articolo 9 del Regolamento UE 2016/679 ed i dati giudiziari di cui all'articolo 10 del medesimo Regolamento.

Se vengono trovate **anomalie**, queste vengono:

- segnalate alla **Funzione Internal Audit**,
- spiegate con le motivazioni,
- e corrette, se necessario.

9.3 Utenti esterni ad Equitalia Giustizia S.p.A.

Diritto di accesso ai documenti amministrativi informatici

Il diritto di accesso è "il diritto degli interessati di prendere visione e di estrarre copia dei documenti amministrativi" (Art. 22, comma 1, lett. a), L. 241/90).

La digitalizzazione del procedimento amministrativo comporta, quindi, che anche il diritto di accesso ai documenti amministrativi debba essere esercitabile mediante l'uso delle tecnologie dell'informazione e della comunicazione. Ciò comporta che, a seconda del soggetto interessato, variano le modalità di accesso ai fascicoli/documenti relativi al procedimento. Sussiste l'obbligo di rendere accessibili, in ogni momento, agli interessati, le informazioni relative ai provvedimenti e ai procedimenti che li riguardano, ivi comprese quelle relative allo stato della procedura, i relativi tempi e l'ufficio competente in ogni singola fase (art. 1, co. 30, L. 190/2012).

La stessa disciplina si applica per analogia anche all'accesso civico di cui al D.lgs. 33/2013.

Privati

Non è attualmente previsto l'accesso diretto al sistema di gestione documentale da parte di soggetti esterni che ne abbiano titolo. Le richieste di accesso dovranno essere inviate ai canali dedicati da Equitalia Giustizia.

L'istanza presentata dovrà essere protocollata nel sistema del PdP e verrà inclusa nel fascicolo ove sono presenti le informazioni richieste. La comunicazione delle informazioni richieste dovrà essere protocollata e le informazioni saranno fornite tramite PEC o secondo le modalità condivise.

9.4 Manutenzione PdP

In relazione all'esigenza 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 della Funzione Innovazione e Servizi ICT

gestire l’autorizzazione all’accesso ai server e le modalità di gestione dei rilasci / fix.

9.5 Disaster recovery

Il Servizio di gestione del Protocollo e gli altri servizi applicativi basati sulle componenti del sistema documentale sono erogati e garantiti dal data center di Sogei della sede di Roma secondo le procedure di Disaster recovery previste contrattualmente.