Manuale operativo

di GESTIONE DOCUMENTALE

e CONSERVAZIONE A NORMA

24 novembre 2023

Compilato: G. LAZZARINI
G. NUNZIALE

Rivisto: G. LAZZARINI
G. NUNZIALE

Autorizzato: M. BETTINI

Versione: 1
Variante: 1

Compendio:	Il presente Manuale descrive il sistema di gestione informatica dei documenti di Venis e fornisce le istruzioni per la formazione dei documenti informatici, per il corretto funzionamento del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi, ivi compresa la conservazione dei documenti informatici.
Riferimenti:	Nella compilazione del presente documento si è fatto riferimento a: • *Standard di documentazione del Sistema Qualità Venis (VAQ-AQ-SQ-01)*
Altri documenti correlati:	
Parole chiave:	
Moduli associati:	Nessuno
Principali modifiche rispetto alla versione precedente:	Aggiornamento delle classi documentali inviate in conservazione
Marchi registrati:	Citati.

INDICE

1. INTRODUZIONE

Il presente Manuale di Gestione Documentale e Conservazione (in seguito denominato "Manuale"), previsto dal paragrafo 3.1.2. delle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* emanate dall'AgID il 10 settembre 2020 (in seguito denominate "Linee Guida"), descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

La presente versione del Manuale sostituisce la precedente versione del 16 febbraio 2022 e viene adottata per garantire il necessario adeguamento al quadro normativo in materia di gestione documentale, e per rendere coerenti le istruzioni in esso riportate all'evoluzione del sistema e degli applicativi informatici adottati.

Gli allegati al presente Manuale possono essere modificati o sostituiti per gli eventuali successivi adeguamenti di natura tecnica o organizzativa, riportando in calce la data dell'ultimo aggiornamento.

2. DISPOSIZIONI PRELIMINARI

2.1. RIFERIMENTI NORMATIVI

Il presente Manuale è adottato ai sensi delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, emanate dall'Agenzia per l'Italia Digitale con determinazione del Direttore generale del 9 settembre 2020, n. 407 e pubblicate il 10 settembre 2020, come modificate dalla determinazione del 17 maggio 2021 n. 371.

Gli allegati alle Linee Guida sono parte integrante delle stesse e contengono disposizioni relative a:

1) Glossario dei termini e degli acronimi;
2) Formati di file e riversamento;
3) Certificazione di processo;
4) Standard e specifiche tecniche;
5) Metadati;
6) Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

Ulteriori norme rilevanti ai fini della gestione documentale sono:

- ✓ le disposizioni in materia di formazione dei documenti informatici, anche di natura amministrativa, e di digitalizzazione dell'attività amministrativa di cui al d.lgs. 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale*" (di seguito anche solo "CAD");
- ✓ le disposizioni in materia di documentazione amministrativa di cui al d.P.R. 28 dicembre 2000, n. 445 *'Disposizioni legislative in materia di documentazione amministrativa"* (di seguito anche solo "TUDA");
- ✓ le norme sul procedimento amministrativo di cui alla l. 7 agosto 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- ✓ le disposizioni sulla trasparenza di cui al d.lgs. 14 marzo 2013, n. 33 "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";

- ✓ le disposizioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno di cui al Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014 (Regolamento "eIDAS");
- ✓ le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 *"Regolamento generale sulla protezione dei dati"* ("GDPR") e d.lgs. 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali*".

2.2. FINALITÀ, CONTENUTI E METODOLOGIA DEL DOCUMENTO

Il presente Manuale, ai sensi del paragrafo 3.5. delle Linee guida, descrive il sistema di gestione informatica dei documenti della Società Venezia Informatica e Sistema S.p.A. (d'ora in avanti anche solo "**Società**" o "**VENIS**") e fornisce le istruzioni per la formazione dei documenti informatici, per il corretto funzionamento del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi, ivi compresa la conservazione dei documenti informatici.

Il presente Manuale non concerne i documenti del Comune di Venezia, di cui VENIS S.p.A. è società strumentale, anche nei casi in cui sono formati e gestiti tramite servizi e strumenti software sviluppati e gestiti da VENIS per conto del Comune. Per tali documenti, resta in capo al Comune di Venezia la competenza e la responsabilità per il corretto espletamento delle attività di gestione documentale.

Il Manuale è un documento interno di contenuto sia organizzativo che operativo, utile quale strumento di supporto ai processi decisionali e operativi e, pertanto, è destinato alla più ampia diffusione presso tutto il personale della Società.

Con la pubblicazione nella sezione "Società Trasparente" del sito internet istituzionale (sottosezione "Atti Generali"), il Manuale è reso noto anche esternamente alla Società. In quest'ottica, il Manuale costituisce altresì un documento pubblico funzionale al perseguimento del principio di trasparenza dell'attività amministrativa.

2.3. APPROVAZIONE E MODALITÀ DI AGGIORNAMENTO DEL MANUALE

Il presente Manuale e i suoi allegati sono approvati, su proposta del **Responsabile della Gestione Documentale** (d'ora in avanti anche solo "**RGD**") d'intesa con il **Responsabile della Conservazione** (d'ora in avanti anche solo "**RC**"), con determinazione del Condirettore Generale della Società, cui l'Assemblea dei soci ha

conferito deleghe e relativi poteri, compresi quelli relativi all'approvazione degli atti organizzativi dell'ente.

I successivi aggiornamenti del Manuale devono essere approvati con le medesime modalità. L'aggiornamento degli allegati, quando non comporta modifiche sostanziali ai contenuti del presente Manuale, è effettuato con provvedimento del RGD d'intesa con il RC. Sono da considerarsi modifiche sostanziali quelle aventi a oggetto il Titolario (vedi Allegato 4).

Il Manuale e gli allegati sono pubblicati sul sito istituzionale della Società, nella sezione "Società Trasparente", sottosezione "Atti generali".

3. ORGANIZZAZIONE

3.1. AREA ORGANIZZATIVA OMOGENEA E UNITÀ ORGANIZZATIVE

VENIS si configura come un'unica Area Organizzativa Omogenea ("**AOO**") denominata *UFFICIO 1 Ufficio protocollo Venis S.p.A.* (codice univoco: A88EA83). L'AOO e gli indirizzi di posta elettronica a essa associati sono indicati nell'Indice PA.

Le Unità Organizzative ("**Uffici**" o "**UUOO**") che afferiscono alla AOO sono riportate nell'Allegato 1 (Macrostruttura e Uffici), che potrà essere oggetto di modifiche e integrazioni per effetto di successivi interventi sulla struttura organizzativa aziendale. Le UUOO sono individuate in modo da rispecchiare la macrostruttura della Società.

3.2. RESPONSABILE DELLA GESTIONE DOCUMENTALE E ALTRI SOGGETTI RESPONSABILI

VENIS, nell'ottica di gestire modo integrato tutte le fasi del ciclo di vita dei documenti informatici, ha individuato un'unica figura, dotata di competenze giuridiche, informatiche e archivistiche, a cui affidare le funzioni e i compiti del RGD al par. 3.4 delle Linee guida (vedi Allegato 2 – Provvedimenti di nomina).

I compiti del RGD sono definiti nell'atto di nomina e nel presente Manuale. In particolare, il RGD:

a) è preposto, ai sensi dell'art. 61 TUDA, al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi della AOO unica della Società;

b) provvede, d'intesa con il RC (di cui al successivo par. 3.3) e il Responsabile per la Transizione Digitale (**RTD**), previo parere del Responsabile per la Protezione dei Dati personali (**RPD**), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;

c) monitora i processi e le attività che governano le fasi di formazione e gestione dei documenti informatici e definisce, d'intesa con il RC, i formati da adottare per la formazione e i metadati, ulteriori a quelli obbligatoriamente previsti dall'allegato 5 alle Linee Guida AgID, da associare al fine di assicurare la corretta conservazione nel tempo dei documenti informatici;

d) valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;

e) vigila sul rispetto delle norme e delle procedure durante le operazioni di registrazione di protocollo, di segnatura di protocollo e produzione del registro giornaliero di protocollo;

f) assicura l'accesso al sistema di gestione documentale, provvedendo alla definizione delle abilitazioni di accesso, e vigila sul rispetto delle misure di sicurezza e di protezione dei dati;

g) effettua un periodico censimento degli strumenti software di gestione documentale in uso presso la Società e, di concerto con il RTD, ne verifica la conformità alla normativa vigente.

Ulteriori e specifici compiti del RGD sono indicati nelle sezioni pertinenti del presente Manuale. Il RGD, ferma restando la propria responsabilità, può delegare in tutto o in parte i propri compiti al personale posto sotto la propria direzione.

3.3. RESPONSABILE DELLA CONSERVAZIONE

La Società ha individuato una figura dotata di competenze giuridiche, informatiche e archivistiche, a cui affidare le funzioni e i compiti del RC di cui al par. 4.5 delle Linee guida (vedi Allegato 2 – Provvedimenti di nomina).

Il RC svolge tutti i compiti previsti dal richiamato par. 4.5 delle Linee guida che non siano stati espressamente affidati al Conservatore (cfr. cap. 11 del presente Manuale). In particolare, il RC:

a) assicura, d'intesa con il RGD, la produzione e la trasmissione dei pacchetti di versamento al sistema di conservazione;

b) esegue il monitoraggio in merito al corretto funzionamento del sistema di conservazione dei documenti informatici, provvedendo altresì a segnalare tempestivamente al conservatore gli eventuali guasti e le proposte di miglioramento del sistema medesimo;

c) provvede, sotto il profilo organizzativo e gestionale, ad assicurare l'interfacciamento e il collegamento del proprio sistema con il sistema di conservazione digitale dei documenti informatici gestito dal Conservatore;

d) comunica al Conservatore i nominativi e le funzioni del personale abilitato all'accesso al sistema di conservazione, per verificare il corretto svolgimento dell'attività di conservazione e per consultare ed eventualmente estrarre i documenti depositati e le prove di conservazione, secondo le modalità previste nella documentazione tecnica relativa all'affidamento del servizio.

Resta fermo che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al RC, chiamato altresì a svolgere le necessarie attività di verifica e controllo sulla corretta esecuzione del servizio di conservazione da parte del Conservatore.

Il RC cura il costante aggiornamento delle disposizioni di cui Cap. 11. del presente Manuale e sottopone al RGD eventuali necessità di aggiornamento.

3.4. SISTEMA INFORMATICO DI GESTIONE DOCUMENTALE DI VENIS

Il Sistema informatico di gestione documentale di VENIS si avvale dei seguenti strumenti software:

- ✓ *Egrammata*, è la soluzione software per la tenuta del protocollo informatico, acquisito con licenza d'uso e utilizzato *on premises* (cioè installato presso i server della Società);
- ✓ *Gamma Enterprise*, è il software per la gestione del magazzino e dei flussi amministrativi (ordini, fatture, ecc.), utilizzato *on premises*. Il software consente inoltre il versamento automatizzato dei documenti su *server cloud*;
- ✓ *ViaLibera*, è il software per la formazione e gestione degli atti di bilancio (bilancio europeo e nota integrativa), utilizzato *on premises*;
- ✓ *InazPaghe*, è il software in licenza d'uso utilizzato *on premises* per la generazione dei cedolini e della documentazione ad assi correlata;
- ✓ *SIA – Determine e Commesse* e *Nota Spese*, è il software sviluppato da VENIS tramite cui sono gestiti la formazione delle determine aziendali ed le note spese del personale.
- ✓ *DMS – KNOS*, è il gestore documentale utilizzato per il controllo di specifici workflow aziendali (Modulo Approvazione Fatture, pratiche cliente, ordine fornitore, ordini cliente, ecc.). Il sistema colloquia ed è integrato nativamente con Gamma Enterprise.

La puntuale descrizione delle componenti e delle funzionalità dei software è contenuta nei rispettivi manuali digitali disponibili all'interno dei software stessi.

3.5. ABILITAZIONI DI ACCESSO

Per la gestione dei documenti è adottato un modello operativo che prevede la partecipazione attiva di più soggetti ed uffici utenti abilitati a svolgere soltanto le

operazioni di loro competenza. Le abilitazioni sono rilasciate/revocate dal Responsabile.

Ad ogni documento, inoltre, all'atto della registrazione nel sistema di protocollo informatico si può associare una Access Control List (ACL) che consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso. Per default il sistema segue la logica dell'organizzazione, nel senso che ciascun utente può accedere solamente ai documenti che sono stati assegnati alla sua struttura di appartenenza, o agli uffici ad esso subordinati. Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato. Il livello di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti, distinto per abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni, è attribuito dal Responsabile.

3.6. SOGGETTI DELEGATI ALLE ATTIVITÀ DI PROTOCOLLAZIONE

Le attività di protocollazione dei documenti, sia in ingresso che in uscita, sono effettuate esclusivamente dal personale della Segreteria, presso cui è incardinato il servizio per la gestione del protocollo informatico. A tutti i dipendenti dell'ufficio è assegnata un'utenza per l'abilitazione d'accesso al Sistema di protocollo informatico. Il personale dell'ufficio opera sotto la direzione e la supervisione del RGD di cui al par. 3.2.

4. FORMAZIONE DEI DOCUMENTI – MODALITÀ DI FORMAZIONE

4.1. MODALITÀ DI FORMAZIONE DEI DOCUMENTI INFORMATICI

I documenti informatici della Società sono formati secondo le modalità individuate nella presente Parte del Manuale.

In particolare, i documenti informatici possono essere formati mediante una delle seguenti modalità.

a) creazione e redazione tramite l'utilizzo di strumenti di software o servizi cloud qualificati (ad esempio, mediante programmi di scrittura delle suite *Microsoft Office* o *Libre Office*, o mediante l'utilizzo delle componenti del Sistema di gestione documentale);

b) acquisizione:
- della copia per immagine di un documento analogico su supporto informatico (ad esempio, mediante scansione di documento cartaceo);

- della copia informatica di un documento analogico (ad esempio, acquisizione del documento tramite lettore OCR);

- del duplicato di un documento informatico per via telematica o da supporto informatico (ad esempio, mediante download da posta elettronica o da chiave usb);

c) memorizzazione su supporto informatico delle informazioni risultanti da transazioni o processi informatici, oppure delle informazioni risultanti dall'acquisizione telematica di dati attraverso moduli o formulari resi disponibili all'utente (ad esempio, memorizzazione dei dati immessi in un *form* reso disponibile online agli utenti, oppure formazione delle fatture elettroniche tramite SDI);

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni secondo una struttura logica predeterminata e memorizzata in forma statica (ad esempio, generazione del registro di protocollo giornaliero).

Di seguito sono fornite indicazioni specifiche per ciascuna delle modalità sopra descritte.

4.1.1. Creazione e redazione tramite software di documenti informatici

Gli uffici della Società dispongono dei seguenti strumenti software per la creazione dei documenti informatici mediante redazione:

- ✓ programmi della suite *Microsoft Office*: *Word*, *Excel*, *Access*, *Powerpoint*, ecc.;
- ✓ programmi della suite *Libre Office*: *Writer*, *Calc*, *Base*, *Impress*, ecc.

Il testo del documento informatico creato dagli uffici della Società deve essere redatto utilizzando esclusivamente i modelli approvati.

4.1.2. Documento amministrativo informatico

I documenti amministrativi informatici sono i documenti creati, redatti o acquisiti dalla Società nell'ambito di attività regolata dalle norme sul procedimento amministrativo (in particolare: procedimenti ai sensi del Codice dei contratti pubblici, procedimenti in materia di accesso documentale, attività in materia di trasparenza e anticorruzione).

I documenti amministrativi informatici creati e redatti da VENIS devono recare i seguenti elementi:

1. denominazione della Società;
2. autore e ufficio responsabile;
3. oggetto del documento;
4. riferimenti a procedimento, affare o fascicolo;
5. sottoscrizione;
6. data e luogo;
7. numeri di pagina;
8. indicazione degli allegati (se presenti);
9. identificazione e dati dei destinatari (se si tratta di documento in uscita);
10. dati della Società (compresi indirizzo e recapiti, se si tratta di documento in uscita);
11. mezzo di spedizione (se documento in uscita).

4.1.3. Documenti informatici che non hanno natura amministrativa

I documenti informatici che non hanno natura amministrativa (ad es. atti di gestione del personale, scritture private, ecc.), devono recare i medesimi elementi, eccetto gli eventuali riferimenti al procedimento amministrativo.

4.1.4. Scelta del formato e modalità di sottoscrizione

Il formato del documento informatico creato dalla Società deve essere scelto tra i seguenti formati standard: **.pdf**, **.pdf/a**, **.odt**, **.docx**, **.xlsx**, **.ods**, **.xml**. Eventuali formati differenti possono essere utilizzati in relazione a specifiche e comprovate esigenze. Il formato del documento informatico, in ogni caso, deve essere preferibilmente individuato tra quelli previsti nell'allegato 2 alle Linee guida dell'AgID.

Le versioni del documento precedenti alla versione definitiva (bozze, minute, ecc.), possono essere salvate in un formato che ne consente la modificabilità (ad esempio, .docx o .odt). La versione definitiva del documento, invece, è sempre preferibile sia in formato PDF.

4.1.5. Modalità di sottoscrizione elettronica

I documenti di maggiore rilevanza giuridico-amministrativa (ad esempio, gli atti degli organi societari, i contratti, gli atti formati nell'ambito dell'attività di carattere amministrativo, ecc.), prima della firma, devono essere convertiti in formato PDF/A (PDF non modificabile). I documenti in formato PDF e PDF/A sono sottoscritti con firma PADES.

Nel caso il documento definitivo sia di un formato diverso dal PDF, la sottoscrizione avviene con firma CADES (.p7m).

4.2. ACQUISIZIONE DI DOCUMENTI INFORMATICI

La formazione di documenti informatici per acquisizione può avvenire secondo una delle seguenti modalità:

a) acquisizione di un documento informatico per via telematica o su supporto informatico (ciò avviene, ad esempio, quando si effettua il download di un documento dalla casella di posta elettronica, oppure, quando si trasferisce un documento da un dispositivo di archiviazione esterno, come una penna usb);

b) acquisizione della copia per immagine su supporto informatico di un documento analogico (ciò avviene, ad esempio, quando si effettua la scansione di un documento cartaceo, memorizzandolo in un formato digitale);

c) acquisizione della copia informatica di un documento analogico (ciò avviene, ad esempio, quando un documento di testo analogico viene riversato in formato digitale tramite lettore OCR per il riconoscimento ottico dei caratteri).

In caso di acquisizione di copia informatica del documento originale (analogico o informatico), al fine di assicurarne l'efficacia giuridico-probatoria, occorre attestare la conformità della copia all'originale da cui è estratta (con le modalità indicate nelle disposizioni successive).

In caso di acquisizione di un duplicato informatico, ai sensi dell'art. 23-*bis* del CAD, esso ha la stessa efficacia giuridico-probatoria del documento informatico originale, pertanto non è richiesta l'attestazione di conformità.

4.3. COPIE PER IMMAGINI DI DOCUMENTI ANALOGICI

La copia per immagine su supporto informatico di un documento analogico e prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti.

4.3.1. Attestazione di conformità delle copie per immagine

Qualora si decidesse di non conservare il documento analogico originale, potrà essere effettuata l'attestazione di conformità della copia per immagine all'originale:

a. da un pubblico ufficiale (notaio), tramite apposizione dell'attestazione di conformità in calce al documento o su foglio separato ma congiunto al documento, poi firmato digitalmente;

b. oppure, mediante la certificazione del processo di dematerializzazione, in conformità a quanto previsto dall'allegato 3 delle Linee guida AgID.

4.4. DUPLICATI, COPIE ED ESTRATTI INFORMATICI DI DOCUMENTI INFORMATICI

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi (così avviene, ad esempio, quando si duplica un documento trasferendolo dall'hard disk del proprio personal computer a un dispositivo di archiviazione esterno quale una chiave usb). Tale modalità di formazione della copia del documento informatico non richiede alcuna attestazione di conformità all'originale, perché vi è perfetta coincidenza tra le due evidenze informatiche (verificabile tramite il confronto dell'*hash* dei documenti, che deve coincidere).

La copia di un documento informatico, invece, è un documento il cui contenuto è il medesimo dell'originale, ma con una diversa evidenza informatica rispetto al documento da cui è tratto (come quando si trasforma un documento in formato PDF. in un documento in diverso formato, ad esempio, .docx). Tale operazione è anche detta "riversamento" da un formato digitale verso un altro. Affinché la copia conservi la medesima efficacia giuridico-probatoria del documento informatico originale, è necessario attestarne la conformità all'originale secondo le modalità indicate al par. 4.3.1

4.5. ACQUISIZIONE DI ISTANZE TRAMITE MODULI ONLINE

Le istanze (es. accesso documentale) provenienti dagli utenti possono essere formate anche tramite la compilazione di moduli e *form* messi a disposizione sul sito web della Società e resi accessibili previa identificazione dell'utente con gli strumenti di identificazione SPID, CIE e CNS. I dati immessi dall'istante sono acquisiti e memorizzati su supporto informatico. Le istanze così formate sono acquisite dal Sistema di protocollo informatico di VENIS e costituiscono a tutti gli effetti documenti amministrativi informatici, trattati come documenti in entrata soggetti a registrazione di protocollo.

I file di log relativi agli accessi e alle attività svolte dagli utenti sono conservati secondo le stesse modalità di conservazione delle istanze ricevute tramite PEC.

4.6. FORMAZIONE DI REGISTRI E REPERTORI

I registri e repertori tenuti da VENIS, ivi compreso il registro giornaliero di protocollo, sono formati mediante la generazione/raggruppamento in via automatica e

memorizzazione in forma statica dell'insieme delle registrazioni effettuate dal sistema di gestione documentale.

5. FORMAZIONE DEI DOCUMENTI – DISPOSIZIONI COMUNI A TUTTE LE MODALITÀ DI FORMAZIONE

5.1. DISPOSITIVI DI FIRMA ELETTRONICA

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica la Società fornisce la firma digitale ai soggetti da essa delegata a rappresentarla. La Società, in particolare, garantisce che tutti i dipendenti e i titolari di cariche che firmano i documenti amministrativi informatici (di cui par. 4.1.2) siano dotati di dispositivi di firma elettronica e la utilizzino per la formazione in originale di documenti informatici.

L'utilizzo del dispositivo di firma è strettamente personale e riconducibile al suo titolare. Pertanto, il dispositivo non deve essere ceduto, né devono essere diffuse le chiavi dei certificati.

Ogni titolare di dispositivo di firma verifica periodicamente la validità e la data di scadenza del certificato di firma, al fine di provvedere tempestivamente al rinnovo.

Quando la firma è apposta utilizzando un certificato prossimo alla scadenza, il titolare ne dà avviso al Responsabile, affinché provveda a costituire un riferimento temporale giuridicamente probante, così da attestare che la firma è stata apposta in un momento in cui il certificato era valido. In particolare, costituiscono riferimento temporale giuridicamente valido le seguenti attività sul documento firmato:

- apposizione di marca temporale;
- apposizione della segnatura di protocollo;
- versamento in conservazione.

Documenti, dati e altre informazioni trasmesse in cooperazione applicativa con le Pubbliche Amministrazioni non richiedono la sottoscrizione digitale o l'apposizione della marca temporale.

5.2. IDENTIFICAZIONE UNIVOCA DEL DOCUMENTO INFORMATICO

Ogni documento informatico deve essere identificato in modo univoco e persistente.

L'identificazione univoca dei documenti è effettuata con l'associazione al documento dell'impronta crittografica hash. Per i documenti soggetti a registrazione di protocollo, l'associazione è effettuata tramite le apposite funzioni del Sistema di protocollo

informatico della Società. Per i documenti non protocollati, l'associazione è effettuata tramite le apposite funzioni degli strumenti software in uso per la formazione degli atti. In ogni caso l'impronta crittografica deve essere basata su una funzione di hash conforme alle tipologie di algoritmi previste nell'allegato 6 alle Linee guida (cfr. p. 2.2, tab. 1).

5.3. ASSOCIAZIONE DEGLI ALLEGATI AL DOCUMENTO PRINCIPALE

Gli allegati sono congiunti in modo univoco al documento informatico principale tramite l'associazione delle impronte hash dei documenti allegati al documento principale.

Al documento principale, inoltre, devono essere associati i seguenti metadati:

- numero allegati;
- indice allegati;
- identificativo del documento allegato (IdDoc);
- titolo dell'allegato (Descrizione).

A ciascun allegato, invece, deve essere associato il metadato identificativo del documento principale (IdDoc).

Le operazioni di associazione degli allegati, quando possibile, sono effettuate in modo automatizzato dallo strumento software utilizzato per la formazione del documento principale.

In alternativa, è possibile associare gli allegati al documento principale manualmente, riportando in calce al documento stesso l'elenco degli allegati, indicando per ciascuno l'oggetto e la relativa impronta *hash*. L'associazione sarà assicurata una volta che il documento informatico principale sia divenuto immodificabile (ad esempio, dopo l'apposizione della firma digitale – cfr. par. 5.6. del presente Manuale).

5.4. ACCESSIBILITÀ DEL DOCUMENTO INFORMATICO

Per garantire l'accessibilità dei documenti informatici ai soggetti portatori di disabilità, anche ai fini della pubblicazione e dell'accesso documentale, i soggetti responsabili della formazione del documento seguono le indicazioni contenute nella "Guida pratica per la creazione di un documento accessibile" di cui all'Allegato 3 (Guida al documento informatico accessibile) al presente Manuale.

5.5. METADATI DEL DOCUMENTO INFORMATICO

Al documento informatico e al documento amministrativo informatico devono essere associati i metadati obbligatori previsti dall'allegato 5 alle Linee guida dell'AgID. Ulteriori metadati facoltativi sono associati ai documenti relativi alle procedure esperite ai sensi del codice dei contratti pubblici (CIG e CUP).

I metadati devono essere associati prima che il documento informatico acquisisca le caratteristiche di immodificabilità e integrità, dunque prima della sottoscrizione, della memorizzazione nel sistema o del versamento in conservazione.

5.6. IMMODIFICABILITÀ E INTEGRITÀ DEL DOCUMENTO INFORMATICO

Affinché sia garantito il valore giuridico-probatorio del documento informatico, ne deve essere assicurata l'immodificabilità e l'integrità.

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nelle fasi di accesso, gestione e conservazione.

L'immodificabilità e l'integrità dei documenti informatici della Società possono sono garantite:

- ✓ per i documenti di cui è richiesta la sottoscrizione, dall'apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- ✓ per i documenti di cui non è richiesta la sottoscrizione, dalla memorizzazione nel sistema di gestione documentale, purché sia garantito il rispetto delle misure di sicurezza previste (cfr. cap. 12. del presente Manuale);
- ✓ per tutte le tipologie documentali, dal versamento nel sistema di conservazione.

In ogni caso, il versamento nel sistema di conservazione è il metodo che offre le maggiori garanzie di immodificabilità e integrità dei documenti informatici nel tempo. Pertanto, è essenziale che tutti i documenti siano versati in conservazione, secondo i tempi e le modalità descritte nel cap. 11 del presente Manuale.

Il Responsabile assicura che i documenti informatici a cui è apposta una firma elettronica siano versati in conservazione prima che scada il certificato di firma.

6. FORMAZIONE DEI DOCUMENTI – DISPOSIZIONI SULLA FORMAZIONE DI DOCUMENTI ANALOGICI

6.1. COPIE ANALOGICHE DI DOCUMENTI INFORMATICI

Dei documenti amministrativi informatici (cfr. par. 4.1.2.), può essere necessario effettuare copie analogiche affinché siano spedite a mezzo posta ai soggetti che non hanno eletto domicilio digitale ai sensi dell'art. 3-*bis*, CAD o che non hanno un domicilio digitale iscritto negli elenchi di cui agli articoli 6-*bis*, 6-*ter* e 6-*quater* del CAD.

In tali casi, al fine di conferire alla copia medesima efficacia giuridico probatoria del documento originale, ai sensi dell'art. 3, d.lgs. n. 39/1993, la copia analogica dovrà essere accompagnata dall'indicazione della fonte del documento originale e del soggetto responsabile dell'immissione, riproduzione, trasmissione o emanazione del documento stesso. Quando il documento originale informatico è sottoscritto con firma digitale o altra firma elettronica qualificata, la firma è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile.

La copia analogica, dunque, dovrà contenere apposita dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto come documento nativo digitale ed è disponibile presso la Società (ad es.: "*Copia è tratta da documento informatico, predisposto come documento nativo digitale da [nome responsabile], Responsabile dell'Ufficio* [indicazione UO]. *Il documento originale informatico è archiviato nel sistema informatico di VENIS S.p.A., presso cui è disponibile per l'accesso'*").

Quando possibile, la dicitura deve essere integrata con indicazioni sulle modalità per effettuare l'accesso online al documento informatico.

6.2. CASI IN CUI È AMMESSA LA FORMAZIONE DI DOCUMENTI ORIGINALI ANALOGICI

Fermo restando l'obbligo di produrre i propri documenti amministrativi in originale informatico (cfr. par. 4.1.2.), nella prospettiva di una gestione omogenea e integrata dell'archivio della Società, il personale è tenuto a preferire gli strumenti informatici per la formazione di tutti i documenti prodotti. Documenti in originale analogico potranno essere prodotti solo nel caso in cui il soggetto che li sottoscrive non sia munito di un dispositivo di firma digitale.

Fanno eccezione le seguenti tipologie documentali, formate in originale analogico e conservate presso i locali deputati all'archivio:

- provvedimenti dell'Amministratore Unico;
- verbali delle Assemblee e, in generale, i libri sociali.

7. GESTIONE DOCUMENTALE – FLUSSI DOCUMENTALI ESTERNI

7.1. RICEZIONE TELEMATICA DI DOCUMENTI INFORMATICI IN ENTRATA

I documenti informatici in entrata, pervenuti tramite la casella PEC aziendale, sono oggetto di registrazione di protocollo secondo quanto previsto nella Sezione seconda della presente Parte del Manuale. Una volta che ne sia accertata la provenienza (secondo la normativa vigente o, comunque, in base a criteri di attendibilità e riconducibilità al mittente dichiarato), i documenti sono validi anche, eventualmente, ai fini delle attività disciplinate dalle norme sul procedimento amministrativo.

I documenti informatici trasmessi per via telematica nell'ambito di procedimenti amministrativi (cfr. par. 4.1.2), quali istanze, dichiarazioni e comunicazioni devono ritenersi valide a tutti gli effetti di legge nei casi previsti dall'art. 65, CAD. È fatto salvo il caso di individuazione di particolari modalità di trasmissione nell'ambito del procedimento (ad es. nelle gare telematiche).

7.2. CANALI DI RICEZIONE

La ricezione di comunicazioni e documenti informatici è assicurata tramite i seguenti canali:

- casella PEC: protocollo@pec.venis.it (abilitato esclusivamente alla ricezione PEC);
- acquisizione di istanze, redatte anche tramite *form*, formate e trasmesse tramite il sito web aziendale.
- cooperazione applicativa tra pubbliche amministrazioni;
- altri canali di trasmissione, anche di posta elettronica ordinaria, indicati per specifici procedimenti o attività.

L'indirizzo di posta elettronica certificata è riportato nell'Indice delle Pubbliche Amministrazioni e pubblicizzato sul sito web istituzionale.

7.3. FORMATI ACCETTATI

Sono accettati documenti informatici esclusivamente nei formati standard in uso presso la Società (cfr. par. 4.1), nonché gli ulteriori formati previsti dall'allegato 2 alle Linee guida.

Specifiche limitazioni formati accettati possono essere previste per specifici procedimenti o attività, purché le limitazioni siano ragionevoli e giustificate da obiettive esigenze legate alla gestione dei documenti. Il personale addetto alla protocollazione effettua un controllo preliminare sulla conformità del formato dei documenti in entrata è effettuato dal personale addetto alla protocollazione prima della registrazione di protocollo. Qualora pervengano documenti in formati non ammessi, la circostanza deve essere indicata in nota al momento della registrazione di protocollo. Quando si riscontra un formato non accettato, ne deve essere data comunicazione al mittente.

L'accettazione di formati che di norma non sono accettati deve essere consentita nel caso in cui, per obiettive esigenze rappresentate dal mittente, il documento non possa riversato in altro formato tra quelli ammessi.

In caso di trasmissione di documenti informatici illeggibili (ad es. perché il file risulta danneggiato), il personale addetto provvede a comunicare al mittente la mancata accettazione della trasmissione, specificando il motivo.

7.4. CONTROLLO DEI CERTIFICATI DI FIRMA

Il personale a cui è assegnato il documento verifica la validità dei certificati di firma e, in caso di certificato scaduto o revocato, lo segnala al personale addetto alla protocollazione, affinché indichi la circostanza in nota alla registrazione di protocollo (v. procedura di modifica di cui al par. 8.9 del presente Manuale).

7.5. TRASMISSIONE TELEMATICA DI DOCUMENTI INFORMATICI IN USCITA

Per la trasmissione telematica di documenti a imprese e professionisti tenuti obbligatoriamente all'iscrizione in albi o elenchi, è in ogni caso da preferire la trasmissione per via telematica. Per le comunicazioni da trasmettere via PEC, il domicilio digitale è estratto dall'indice INI-PEC (www.inipec.gov.it).

Se il destinatario ha eletto uno specifico domicilio digitale, la comunicazione è trasmessa all' indirizzo di posta elettronica dichiarato (anche ordinaria).

I documenti che devono essere prodotti entro un determinato termine, o dalla cui trasmissione dipendo particolari effetti giuridici – quali, ad es., diffide, messe in mora o in generale, messaggi idonei a impegnare la Società verso terzi – sono sempre trasmessi a mezzo PEC.

I documenti informatici in uscita sono trasmessi a mezzo PEC solo dopo essere stati classificati, fascicolati e protocollati secondo le disposizioni della presente Parte del Manuale.

La trasmissione di dati e altre informazioni in cooperazione applicativa è soggetta a protocollazione o a registrazione particolare secondo le medesime regole per la registrazione di protocollo dei documenti.

7.6. USO DELLA POSTA ELETTRONICA ORDINARIA

La posta elettronica ordinaria (PEO) può essere utilizzata – anzi, è preferibile – per convocare riunioni, inviare comunicazioni di servizio o notizie dirette ai dipendenti in merito a informazioni generali di organizzazione, diffondere circolari e ordini di servizio (gli originali si conservano nel fascicolo specifico), documenti informatici, copie di documenti cartacei.

La PEO, inoltre, è utilizzata per spedire copie dello stesso documento a più destinatari.

A chi ne fa richiesta deve sempre essere data la risposta dell'avvenuto ricevimento.

Non è possibile inviare messaggi dalla casella di posta elettronica personale quando il contenuto di questi impegni la Società verso terzi. La trasmissione di documenti che necessita di una ricevuta di invio e di consegna è effettuata tramite il sistema di posta elettronica certificata.

7.7. COMUNICAZIONI E TRASMISSIONE DI DOCUMENTI CON ALTRE PUBBLICHE AMMINISTRAZIONI

La trasmissione di comunicazioni e documenti verso altre pubbliche amministrazioni avviene sempre per via telematica, agli indirizzi di posta elettronica, anche ordinaria, dei singoli uffici. Gli indirizzi di spedizione sono rilevati tramite la consultazione dell'Indice delle Pubbliche Amministrazioni (indicepa.gov.it) di cui all'art. 6-ter del CAD.

I documenti che devono essere prodotti entro un determinato termine sono sempre trasmessi a mezzo PEC.

7.8. DISPOSIZIONI SUI DOCUMENTI ANALOGICI

I documenti su supporto analogico possono pervenire alla Società attraverso:

- il servizio postale;

- la consegna diretta, presso la sede, al personale addetto;
- il fax. La ricezione dei fax avviene mediante un software che inoltra lo stesso ad uno specifico indirizzo di posta elettronica istituzionale.

Le buste delle comunicazioni cartacee sono conservate insieme ai documenti in esse contenuti.

8. GESTIONE DOCUMENTALE – PROTOCOLLO INFORMATICO

8.1. SISTEMA DI PROTOCOLLO INFORMATICO

VENIS, per la protocollazione dei documenti, utilizza il Sistema di protocollo informatico Egrammata. La puntuale descrizione funzionale e operativa del Sistema di protocollo informatico è illustrata nel manuale di utilizzo disponibile in formato digitale all'interno del software stesso.

8.2. FUNZIONI DEL RESPONSABILE DELLA GESTIONE DOCUMENTALE IN MATERIA DI PROTOCOLLO INFORMATICO

La corretta tenuta del protocollo informatico è garantita dal RGD. In particolare, il Responsabile, nella veste di responsabile del protocollo informatico:

a. coordina la gestione del Sistema di protocollo informatico;
b. assegna al personale addetto alla protocollazione l'abilitazione all'utilizzo delle funzioni di protocollo del Sistema;
c. esercita il controllo generale sui flussi documentali esterni e interni;
d. assicura la corretta esecuzione delle attività di protocollazione;
e. autorizza l'attivazione del protocollo di emergenza;
f. autorizza con comunicazione formale le operazioni di annullamento delle registrazioni di protocollo;
g. vigila sull'osservanza della normativa e delle disposizioni del presente Manuale da parte del personale addetto.

Le attività di protocollazione sono eseguite dagli utenti delegati dal Responsabile. La modalità di individuazione dei soggetti delegati alle attività di protocollazione è definita al par. 3.6 del presente Manuale.

8.3. REGISTRO GENERALE DI PROTOCOLLO

Nell'ambito della AOO il Registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo.

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

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

Il numero di protocollo è associato in modo univoco e immodificabile al documento, pertanto esso individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Non è consentita la protocollazione di un documento già protocollato.

8.4. REGISTRO GIORNALIERO DI PROTOCOLLO

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso è prodotto automaticamente dal Sistema di protocollo informatico, che provvede altresì al versamento automatico al Sistema di conservazione.

8.5. DOCUMENTI SOGGETTI A REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI ESCLUSI

Tutti i documenti prodotti e ricevuti da VENIS, indipendentemente dal supporto sul quale sono formati, sono registrati al protocollo, ad eccezione di quelli indicati successivamente.

Ai sensi dell'articolo 53 del TUDA sono esclusi dalla registrazione di protocollo:

- Gazzette Ufficiali, Bollettini Ufficiali, notiziari della Pubblica Amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, stampe varie, plichi di libri;
- biglietti augurali, inviti a manifestazioni e documenti di occasione vari che non attivino procedimenti amministrativi;
- bolle accompagnatorie;
- richiesta/invio comunicazioni informali.

Non sono soggetti a protocollazione, inoltre, gli atti e i documenti registrati in repertori e registri differenti dal registro di protocollo ai sensi del par. 8.15. del presente Manuale.

Le ricevute di accettazione e di consegna di un messaggio inviato tramite PEC non devono essere protocollate, ma devono essere associate alla registrazione di protocollo del documento trasmesso/ricevuto a cui la ricevuta stessa si riferisce.

8.6. DISPOSIZIONI PER PARTICOLARI TIPOLOGIE DI DOCUMENTI

La protocollazione della documentazione di gara e delle offerte, scaricabili dalle piattaforme e-procurement dei mercati elettronici della Pubblica Amministrazione, della Regione o da altre piattaforme conformi alla normativa vigente, non è necessaria quando i gestori di tali sistemi assicurano la conservazione a tempo indeterminato della documentazione relativa alle singole gare. In tali casi si ritiene comunque opportuna, anche se non necessaria, la protocollazione della richiesta d'offerta o dell'ordine diretto di acquisto e dell'offerta dell'impresa aggiudicataria acquisendo, per questa, tutti i documenti relativi e specificando, negli appositi campi, data e ora di arrivo.

8.7. REGISTRAZIONE DI PROTOCOLLO

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare in forma non modificabile al fine di garantirne l'identificazione univoca e certa. Ai sensi dell'art. 53, comma 1, TUDA, metadati di registrazione di protocollo sono:

a. numero di protocollo del documento, generato automaticamente dal sistema;
b. data di registrazione di protocollo, assegnata automaticamente dal sistema;
c. il mittente, per i documenti ricevuti, e il destinatario (o i destinatari), per i documenti spediti;
d. oggetto del documento;
e. data e protocollo del documento ricevuto, se disponibili;
f. l'impronta del documento informatico.

A suddetti metadati registrati in forma non modificabile, inoltre, possono essere aggiunti (a seconda dei casi) i seguenti ulteriori metadati:

a. tipologia di documento;
b. classificazione (titolo e classe) sulla base del Titolario (vedi Allegato 4);
c. fascicolo di appartenenza;

d. assegnazione interna (per competenza o per conoscenza);
e. data e ora di arrivo;
f. allegati;
g. livello di riservatezza;
h. mezzo di ricezione o invio;
i. annotazioni;
j. (eventualmente) estremi del provvedimento di differimento della registrazione;
k. (se necessario) elementi identificativi del procedimento amministrativo.

8.8. MODALITÀ DI REGISTRAZIONE

La registrazione di protocollo di un documento è eseguita dopo averne verificato l'autenticità, la provenienza e l'integrità.

La registrazione dei documenti ricevuti, spediti e interni è effettuata in un'unica operazione, utilizzando le apposite funzioni previste dal Sistema di protocollo informatico.

Il Sistema genera automaticamente il numero progressivo e la data di protocollazione associata. Alla registrazione di protocollo, inoltre, sono associate le ricevute generate dal sistema di protocollo informatico. Le ricevute di accettazione e di consegna di un messaggio inviato tramite PEC non devono essere protocollate, ma devono essere associate alla registrazione di protocollo del documento trasmesso/ricevuto a cui la ricevuta stessa si riferisce.

L'eventuale indicazione dell'ufficio utente, ovvero del soggetto destinatario del documento, va riportata nella segnatura di protocollo.

8.8.1. Documenti con più destinatari e copie per conoscenza

Al documento indirizzato a più destinatari deve essere assegnato un solo e unico numero di protocollo. I destinatari possono essere descritti in elenchi associati al documento.

Dei documenti analogici prodotti/pervenuti, di cui necessita la distribuzione interna alla Società, si faranno copie informatiche degli stessi.

8.8.2. Protocollazione della posta ordinaria

In casi particolari, eventualmente da valutare d'intesa con il personale addetto alla protocollazione, è possibile protocollare i messaggi di posta elettronica ordinaria, provvedono a scaricare il file .EML contenente messaggio in entrata. In tali casi, dunque, l'operatore addetto alla protocollazione in ingresso provvede alla registrazione del messaggio inoltrato in allegato, assicurandosi che siano registrati i relativi dati.

8.9. ANNULLAMENTO E MODIFICHE DELLA REGISTRAZIONE DI PROTOCOLLO

La registrazione degli elementi obbligatori del protocollo non può essere modificata né integrata, né cancellata, ma soltanto annullata attraverso l'apposita procedura conforme all'art. 54 del TUDA. In particolare, i metadati indicati al par. 8.7. del presente Manuale, lettere da a) a f), non sono modificabili, ma eventualmente annullabili.

Ogni annullamento della registrazione deve:

- essere autorizzato con comunicazione formale del Responsabile;
- comportare la memorizzazione di data, ora e estremi della comunicazione formale di annullamento;
- consentire sempre la memorizzazione e la visibilità delle informazioni oggetto di annullamento.

Nell'inviare il documento già oggetto di precedente registrazione, poi annullata, nelle note di trasmissione si dovrà dichiarare che: "*Il presente documento sostituisce il documento prot. n.* [...] *di data* [...]".

Le richieste di annullamento rivolte al Responsabile devono essere motivate. Le richieste sono accolte, di norma, in casi di mero errore materiale (quali ad es. la doppia registrazione, la registrazione di documenti che non diano seguito a procedimenti o ad attività amministrative proprie dell'ente, la registrazione errata che necessiterebbe di modifiche sostanziali dei campi obbligatori). Solo il Responsabile ha il potere di autorizzare l'annullamento delle registrazioni di protocollo, ovvero di dare disposizioni in tal senso.

Come previsto dal par. 3.1.5. delle Linee Guida AgID, il Sistema di protocollo informatico deve assicurare che le uniche informazioni modificabili di una registrazione di protocollo siano quelle relative a:

- classificazione (titolo e classe);

- assegnazione interna alla Società (per competenza o per conoscenza).

Le operazioni di modifica posso essere svolte dal personale addetto alla protocollazione, anche senza previa autorizzazione del Responsabile.

L'annullamento e le modifiche avvengono secondo la procedura guidata dal Sistema, che consente di mantenere traccia di ogni operazione, così come richiesto alla normativa.

8.10. GESTIONE DEGLI ALLEGATI

Il numero e la descrizione degli allegati sono elementi essenziali per l'efficacia di una registrazione. Tutti gli allegati devono pervenire con il documento principale al fine di essere inseriti nel Sistema di protocollo informatico ed essere sottoposti a registrazione.

Gli allegati dei documenti ricevuti tramite il canale PEC sono gestiti in forma automatizzata dal Sistema di protocollo informatico. Negli altri casi, l'associazione degli allegati al documento principale avviene con le modalità indicate al par. 5.3 del presente Manuale.

Non è ammessa l'associazione al documento informatico già registrato di allegati non indicati nella registrazione di protocollo.

8.11. TEMPI DI REGISTRAZIONE E CASI DI DIFFERIMENTO

La registrazione della documentazione in entrata deve avvenire in giornata o comunque non oltre il giorno lavorativo successivo a quello di arrivo. Ai fini della gestione del protocollo non sono in ogni caso considerati lavorativi il sabato e la domenica.

In casi eccezionali ed imprevisti che non permettono di evadere la corrispondenza ricevuta e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi (ad esempio per la registrazione di un consistente numero di domande di partecipazione ad un concorso in scadenza), con motivato provvedimento del Responsabile è autorizzato il differimento dei termini di registrazione (protocollo differito).

Il protocollo differito si applica solo ai documenti in entrata e per tipologie omogenee che il Responsabile deve descrivere nel provvedimento di autorizzazione. Il provvedimento individua i documenti da ammettere alla registrazione differita, le

cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.

Al momento della registrazione differita devono essere indicati in nota alla registrazione gli estremi del provvedimento di differimento. In ogni caso, della ricezione del documento informatico fa fede la ricevuta di consegna generata dal gestore della casella PEC.

Ai fini del computo di termini previsti dalla legge o da altri atti (es. bandi, contratti, ecc.), resta fermo quanto previsto dall'art. 45 del CAD, ai sensi del quale il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

8.12. SEGNATURA DI PROTOCOLLO

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa, come indicate all'art. 53, comma 1, TUDA.

Le operazioni di segnatura sono effettuate contemporaneamente alla registrazione di protocollo o ad altra registrazione cui il documento è soggetto.

I requisiti necessari di ciascuna segnatura di protocollo sono:

a. indicazione del mittente;
b. codice identificativo dell'AOO mittente;
c. codice identificativo del registro;
d. numero progressivo di protocollo;
e. data di registrazione;
f. oggetto del messaggio di protocollo;
g. classificazione del messaggio di protocollo;
h. indicazione del fascicolo in cui è inserito il messaggio di protocollo.

Per i documenti informatici trasmessi alle Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file XML conforme alle indicazioni previste al p. 2 e ss. dell'allegato

6 alle Linee guida dell'AgID e, in particolare, deve rispettare lo schema di cui all'Appendice A (v. p. 4.1. "Segnatura di protocollo XML Schema").

8.13. PROTOCOLLO RISERVATO

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

- documenti contenenti categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento UE 2016/679 che rivelano 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 (ad es. documenti che contengono certificati medici con diagnosi o patologie, certificati di invalidità, documenti attestanti l'adesione a partiti politici, documenti contenenti sfratti esecutivi e pignoramenti, ecc.), dati personali relativi a condanne penali e reati o a connesse misure di sicurezza;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati o procurare pregiudizio a terzi o al buon andamento dell'attività amministrativa (tipologie documentarie definite all'art. 24 della legge n. 241/1990).
- segnalazioni indirizzate al RPCT ai sensi della normativa in materia di whistleblowing.

I documenti registrati con tali forme appartengono al protocollo riservato della Società, costituito dalle registrazioni sul Sistema di protocollo il cui accesso è consentito solamente agli utenti autorizzati.

Le tipologie di documenti da registrare nel protocollo riservato sono codificate all'interno del Sistema di protocollo informatico a cura del Responsabile.

8.14. REGISTRO DI EMERGENZA

Nei casi in cui non sia possibile l'utilizzo del registro di registro di protocollo informatico, il Responsabile provvede alla formazione del registro di emergenza su supporto analogico, redatto secondo lo schema di cui all'Allegato 5 (Modello registro di emergenza). L'utilizzo del registro di protocollo emergenza, ai sensi dell'art. 63 del TUDA, è autorizzato dal Responsabile, o in assenza dal suo Vicario, in situazioni nelle quali per cause tecniche non sia possibile utilizzare il registro generale di protocollo

informatico e la sospensione del servizio si protragga per un tempo tale da poter pregiudicare la registrazione a protocollo in giornata. In tali casi, il Responsabile dà immediata comunicazione a tutti gli uffici della temporanea sospensione dell'utilizzo della procedura informatizzata ordinaria di protocollazione.

Il registro di protocollo di emergenza ha una numerazione progressiva propria, perciò ai documenti protocollati su tale registro, una volta riversati, saranno associati due numeri di protocollo, quello del registro di emergenza e quello del registro di protocollo generale. Le registrazioni sul registro di emergenza avvengono, quando possibile, secondo le medesime regole e con le stesse modalità adoperate per le registrazioni sul registro generale di protocollo.

Sul registro di emergenza, inoltre, sono riportati:

- gli estremi del provvedimento di autorizzazione all'utilizzo del registro;
- la causa, la data e l'ora di inizio dell'interruzione;
- il numero totale di registrazioni effettuate nel corso di ogni giornata di utilizzo;
- la data e l'ora del ripristino della funzionalità del sistema
- ogni altra annotazione ritenuta rilevante.

Al ripristino della piena funzionalità del Sistema di protocollo informatico, il Responsabile provvede alla chiusura del registro di emergenza, annotando il numero delle registrazioni effettuate, la data e l'ora di chiusura, e dà disposizioni per il riversamento delle registrazioni sul registro di protocollo generale.

8.15. DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

La registrazione particolare dei documenti richiede lo svolgimento delle medesime operazioni di gestione documentale effettuate per la registrazione di protocollo, ivi incluse la classificazione e la fascicolazione.

Sono soggette a registrazione particolare nei repertori e registri all'uopo istituiti le tipologie di documenti di seguito riportate:

- Delibere degli organi collegiali (Libro sociale);
- Determinazioni dirigenziali;
- Corrispondenza riservata (Repertorio Xfile del protocollo informatico);
- Circolari interne (Repertorio CA);
- Ordini di servizio (Repertorio CA).

I registri e repertori diversi dal protocollo contengono le seguenti informazioni:

- tipologia del registro o repertorio;
- numero di registro o repertorio (cronologico e progressivo);
- elementi identificativi dell'atto (soggetto o soggetti, oggetto, data);
- dati di classificazione e di fascicolazione;
- annotazioni.

Al fine di garantire i medesimi effetti della registrazione di protocollo, i registri e repertori di cui al presente paragrafo sono conservati con modalità analoghe a quelle del registro giornaliero di protocollo informatico.

Il Responsabile, al fine di dare attuazione ai principi di unicità e onnicomprensività del registro di protocollo, valuta periodicamente l'opportunità di sopprimere le forme di registrazione particolare non necessarie per legge, prevedendo in sostituzione esclusivamente la registrazione di protocollo.

8.16. DISPOSIZIONI SULLA PROTOCOLLAZIONE DI DOCUMENTI ANALOGICI

Il personale addetto a effettuare la registrazione di protocollo informatica in entrata è competente anche per la protocollazione dei documenti analogici in entrata (consegnati a mano o pervenuti tramite servizio postale). Di tale documentazione è effettuata una copia per immagine su supporto informatico (scansione in formato pdf/A) prima della registrazione.

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è cura del personale addetto alla protocollazione rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal protocollo informatico. La ricevuta della consegna di un documento analogico può essere prodotta con qualsiasi mezzo che ne attesti il giorno della consegna. A chi ne fa domanda, compatibilmente con le esigenze del servizio, deve essere anche riportato il numero di protocollo assegnato al documento. In questo caso l'operatore deve provvedere immediatamente alla registrazione dell'atto.

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

- il numero e la data di protocollo;
- l'indicazione dell'AOO;

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

Qualora per ragioni organizzative o tecniche non sia possibile protocollare immediatamente il documento, l'addetto al protocollo comunica al mittente o ad altra persona incaricata il termine entro il quale il documento verrà protocollato, impegnandosi – se richiesto – a far pervenire la ricevuta all'indirizzo o recapito indicato dal mittente stesso (anche tramite e-mail). La ricevuta può essere altresì ritirata dall'interessato o da persona espressamente delegata nei giorni successivi.

8.16.1. Registrazione, segnatura, annullamento

Alla registrazione di protocollo dei documenti cartacei si applicano, in quanto compatibili, le medesime regole previste per la registrazione dei documenti informatici.

Le lettere anonime sono soggette a registrazione di protocollo, eventualmente riservato, indicando nel campo del mittente la dicitura "Anonimo".

Per i documenti analogici la segnatura è apposta con timbro ed etichetta riportante i dati indicati al par. 8.12., lett. da a) a e).

Sul documento analogico soggetto ad annullamento della registrazione si deve riportare a margine il numero di protocollo e la data dell'autorizzazione di annullamento. La segnatura (timbro ed etichetta) deve essere barrata con la dicitura "*annullato*".

8.16.2. Corrispondenza contenente dati sensibili

I documenti contenenti categorie particolari di dati o soggetti a riservatezza, pervenuti in modalità cartacea, dopo essere stati scansionati e allegati alla registrazione effettuata con protocollo riservato, devono essere inseriti in busta chiusa recante la dicitura "contiene dati sensibili" e successivamente consegnati soggetto competente in base all'assegnazione.

8.16.3. Corrispondenza personale o riservata

La corrispondenza nominativamente intestata è regolarmente aperta dagli incaricati della registrazione di protocollo dei documenti in arrivo, ad eccezione di quella diretta ai titolari di cariche. Se la corrispondenza riveste carattere "riservato" o "personale", e ciò è desumibile prima dell'apertura della busta, questa viene inviata chiusa direttamente al destinatario priva di registrazione. Se il carattere "riservato" o "personale" della corrispondenza viene desunto dopo averne preso visione, il plico viene richiuso e inviato al destinatario privo di registrazione. L'eventuale registrazione di protocollo potrà essere effettuata in un momento successivo.

8.16.4. Corrispondenza cartacea non di competenza della Società

La corrispondenza cartacea che non è evidentemente di competenza della Società (es. altro destinatario) non va aperta e va riconsegnata al Servizio postale. In caso di errata apertura, la busta va richiusa indicando la dicitura "aperta per errore", apponendo timbro datario e riconsegnata al Servizio postale.

9. GESTIONE DOCUMENTALE – CLASSIFICAZIONE, FASCICOLAZIONE E ACCESSO AI DOCUMENTI ED AI FASCICOLI INFORMATICI

9.1. CLASSIFICAZIONE DEI DOCUMENTI

I documenti formati e acquisiti da VENIS sono classificati mediante indicazione del titolo e della classe secondo i criteri previsti nel Titolario (vedi Allegato 4). I documenti devono essere classificati prima della registrazione di protocollo. Non è ammessa la registrazione di protocollo di documenti non classificati.

La classificazione dei documenti è effettuata dal personale addetto alla protocollazione.

9.2. FASCICOLAZIONE DEI DOCUMENTI

Al fine di garantire la consultazione dei documenti informatici, questi sono raccolti in fascicoli informatici. I fascicoli eventualmente possono essere organizzati in sottofascicoli.

I documenti soggetti a protocollazione sono inseriti nel pertinente fascicolo tramite l'apposita funzione del Sistema di gestione documentale. Quando è necessario aprire un nuovo fascicolo informatico, l'utente abilitato alla creazione dei fascicoli provvede all'apertura del fascicolo in cui inserire il documento.

Per i documenti in entrata, quando occorre provvedere all'apertura di un nuovo fascicolo informatico e vi sia incertezza sul criterio di fascicolazione da adottare, il personale addetto alla protocollazione provvede di concerto l'ufficio a cui è assegnato il documento.

I fascicoli informatici possono essere organizzati:

a. per affare, quando i documenti raccolti nel fascicolo, accomunati secondo un criterio di classificazione basato sulla competenza amministrativa, non sono tutti riferibili a un singolo procedimento amministrativo. Il fascicolo per affare deve avere una data di apertura e una durata circoscritta;

b. per attività, quando i documenti raccolti nel fascicolo attengono allo svolgimento di un'attività amministrativa semplice, che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale;

c. per persona (fisica o giuridica), quando i documenti raccolti nel fascicolo, anche con classificazioni diverse, sono riferibili a un medesimo soggetto. Sono fascicoli di tipo "aperto", con durata pluriennale e indeterminata;

d. per procedimento amministrativo, quando i documenti raccolti nel fascicolo rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

I fascicoli informatici devono recare, in quanto compatibili i metadati obbligatori delle aggregazioni documentali previsti nell'allegato 5 alle Linee guida AgID.

Nelle more dell'implementazione di modalità automatizzate creazione e gestione dei fascicoli, organizzate secondo il piano di fascicolazione della Società, gli utenti tenuti alla formazione dei fascicoli informatici assicurano che siano associati almeno i seguenti metadati, distinti per tipologia di fascicolo.

Il fascicolo informatico organizzato per procedimento amministrativo (da creare in caso di attività disciplinata da norme sul procedimento amministrativo – cfr. par. 4.1.2.) deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo (procedimento amministrativo);
3. codice IPA Amministrazione/ente titolare (campo "Ruolo");
4. codice IPA Amministrazioni/ente partecipanti (campo "Ruolo");
5. dati identificativi del responsabile (nome, cognome, codice IPA dell'Amministrazione/ente di appartenenza, domicilio digitale).

Il fascicolo informatico organizzato per affare deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo (affare);
3. codice IPA Amministrazione/ente titolare (campo "Ruolo");
4. codice IPA Amministrazioni/enti partecipanti (campo "Ruolo")
5. dati identificativi del responsabile (nome, cognome, codice IPA dell'ente di appartenenza, domicilio digitale).

Il fascicolo informatico organizzato per persona deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo ("persona fisica" o "persona giuridica");
3. dati anagrafici della persona a cui fa riferimento il fascicolo (almeno nome e cognome per le persone fisiche, denominazione per le persone giuridiche, denominazione e codice IPA per le PA);
4. dati identificativi del responsabile (nome, cognome, codice IPA dell'ente di appartenenza, domicilio digitale).

Il fascicolo informatico organizzato per attività deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo (attività);
3. dati identificativi del responsabile/assegnatario dell'attività (nome, cognome, codice IPA dell'ente di appartenenza, domicilio digitale).

9.3. ACCESSO AI FASCICOLI ED AI DOCUMENTI INFORMATICI

L'accesso ai fascicoli e ai documenti informatici da parte di utenti esterni alla società è consentito ai sensi della normativa vigente in materia di accesso (l. n. 241/1990, d.lgs. n. 33/2013, regolamento interno), nei limiti in cui sia applicabile alla Società.

Agli utenti riconosciuti ed abilitati alla consultazione sono rese disponibili tutte le informazioni necessarie e sufficienti all'esercizio del diritto di accesso ai documenti amministrativi, in conformità alle disposizioni normative e regolamentari vigenti.

10. GESTIONE DOCUMENTALE – FLUSSI DOCUMENTALI INTERNI

10.1. ASSEGNAZIONE DEI DOCUMENTI IN ENTRATA AGLI UFFICI

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate. I criteri di assegnazione automatica sono definiti dal Responsabile, sentiti gli uffici interessati.

I documenti non assegnati automaticamente sono assegnati agli uffici interessati dal personale addetto alla protocollazione in base all'oggetto del documento e alla classificazione. Quando un documento è di interesse anche per più uffici, si provvede a più assegnazioni, sia "per competenza" che "per conoscenza".

10.2. COMUNICAZIONI INTERNE

Lo scambio di documenti tra i dipendenti e gli uffici è effettuato per mezzo di posta elettronica ordinaria e degli ulteriori strumenti di trasmissione messi a disposizione del personale dalla Società.

Le comunicazioni personali sono trasmesse a mezzo posta elettronica ordinaria. Quando la comunicazione indirizzata a più destinatari, in ragione del contenuto e degli invii multipli, potrebbe comportare la divulgazione di dati personali, il mittente provvede a invii individuali o in copia conoscenza nascosta (ccn).

Lo scambio di documenti internamente di norma non richiede la protocollazione del messaggio. Scambi di documenti tra gli uffici possono essere effettuati anche attraverso rete intranet e cartelle condivise. In ogni caso, nelle attività di trasmissione e scambio dei documenti tutto il personale deve utilizzare esclusivamente gli strumenti di comunicazione messi a disposizione dalla Società.

Non è consentito l'utilizzo di servizi di messaggistica istantanea (es. Whatsapp, Telegram, ecc.) per lo scambio di documenti nell'ambito dell'attività lavorativa.

10.3. PUBBLICAZIONI IN SOCIETÀ TRASPARENTE

Tutti gli atti prodotti dalla Società che, ai sensi della normativa vigente, sono soggetti a pubblicazione nella sezione Società trasparente, sono trasmessi per la pubblicazione solo dopo che il documento sia divenuto immodificabile (cfr. par. 5.6 del presente Manuale).

11. CONSERVAZIONE DEI DOCUMENTI

11.1. SISTEMA DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI

VENIS, per la conservazione dei documenti informatici e degli altri oggetti della conservazione, si avvale dei sistemi di conservazione di conservatori esterni ai sensi dell'art. 44, comma 1-quater, CAD.

Il servizio di conservazione dei documenti informatici di Venis è stato affidato ai Conservatori:

- Infocert S.p.A. (Registro di Protocollo);
- TeasmSystem S.p.A. (Fatture attive);
- Namirial S.p.A. (Libro Giornale, Libro Inventario, LUL Cedolini e Fogli Presenze, Verbali, Registri IVA, Documenti di Protocollo).

Le attività affidate al Conservatore sono puntualmente indicate nella convenzione per l'affidamento del servizio.

Per la descrizione delle attività del processo di conservazione non definite nel presente Manuale, così come consentito dal par. 4.6 delle Linee Guida, è fatto rinvio al manuale di conservazione del Conservatore nonché agli ulteriori documenti tecnici concernenti l'affidamento del servizio di conservazione.

11.2. RESPONSABILE DELLA CONSERVAZIONE

Come precisato al par. 3.3. del presente Manuale, Venis ha individuato il RC dei documenti informatici, cui sono affidati i compiti ivi indicati.

È compito del RC assicurare il rispetto della normativa vigente da parte del Conservatore e degli obblighi contrattuali dallo stesso assunti, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile agisce d'intesa con il RPD dell'ente.

Il RC, ferma restando la propria responsabilità, può delegare in tutto o in parte una o più attività di propria competenza relative alla conservazione, affidandole a soggetti interni alla Società dotati di adeguate competenze. Gli atti di delega devono individuare le specifiche attività e funzioni delegate.

11.3. OGGETTO DELLA CONSERVAZIONE

Gli oggetti della conservazione sono:

- i documenti informatici formati dalla Società e i rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- i fascicoli informatici e rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- il registro del protocollo informatico;
- le fatture attivegli altri registri e repertori tenuti dalla Società;
- LUL – cedolini e fogli presenza;
- altri registri e repertori tenuti dalla Società (verbali CdA, Assemblea, Collegio).

E, a breve:

- i documenti di protocollo;
- le comunicazioni Aziendali;
- il libro giornale;
- il libro inventario;
- Registri IVA.

Gli oggetti della conservazione sono trattati dal sistema di conservazione del Conservatore in pacchetti informativi che si distinguono in:

a) pacchetti di versamento;

b) pacchetti di archiviazione;

c) pacchetti di distribuzione.

Il Responsabile provvede ad associare a ogni pacchetto di versamento almeno i seguenti metadati:

1. identificativo univoco e persistente del pacchetto di versamento;
2. riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
3. denominazione del soggetto responsabile della produzione del pacchetto;
4. impronta del pacchetto di versamento;
5. numero dei documenti compresi nel pacchetto.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie di documentarie oggetto del servizio di conservazione sono dettagliatamente nel Manuale del Conservatore.

11.4. FORMATI AMMESSI PER LA CONSERVAZIONE

I formati ammessi per la conservazione sono individuati nell'allegato 2 alle Linee guida dell'AgID.

Il Responsabile, prima del versamento in conservazione, valuta i casi in cui è opportuno procedere al riversamento del documento in diverso formato, purché conforme ai formati indicati adatti alla conservazione nell'allegato 2 alle Linee guida. In tal caso, la corrispondenza fra il formato originale e quello di riversamento deve essere garantita attraverso attestazione di conformità apposta secondo le modalità indicate al par. 4.3.1 del presente Manuale. I documenti originali cartacei sottoscritti con firma autografa non possono essere scartati se alla copia informatica non è apposta l'attestazione di conformità all'originale.

11.5. MODALITÀ E TEMPI DI TRASMISSIONE DEI PACCHETTI DI VERSAMENTO

Il versamento dei documenti avviene secondo le seguenti tempistiche:

- versamento manuale a cadenza variabile, per cui ciascun dlegato invia in conservazione la documentazione individuata;
- versamento automatizzato a determinate scadenze, che per il registro di protocollo giornaliero avviene entro le 24 ore successive al momento della produzione. Il RC, d'intesa con il RGD, può individuare altre tipologie di versamento automatizzato a determinate scadenze per particolari tipologie di documenti.

11.6. MEMORIZZAZIONE DEI DATI E DEI DOCUMENTI INFORMATICI E SALVATAGGIO DELLA MEMORIA INFORMATICA

I dati e i documenti informatici sono memorizzati nei data center aziendali, fino all'eventuale versamento nel sistema di conservazione o allo scarto.

Le procedure di memorizzazione sono le seguenti:

a) salvataggio immediato su server di rete collocato presso la sede aziendale;

b) alla fine di ogni giorno sono create, a cura del Centro Servizi aziendale, copie di backup della memoria informatica della società, che vengono poi riversate su supporti di memorizzazione tecnologicamente avanzati e conservati nel Data Center aziendale adibito a Disaster Recovery, secondo quanto previsto dalle procedure di salvataggio dati descritte all'interno del Piano di sicurezza informatica della Società (vedi. **Allegato 6**).

11.7. ACCESSO AL SISTEMA DI CONSERVAZIONE

Gli utenti espressamente autorizzati dal RC, anche su indicazione del RGD, possono accedere al Sistema tramite credenziali personali rilasciate dal Conservatore e comunicate al singolo utente. L'accesso al Sistema consente di consultare i documenti digitali versati nel Sistema e le configurazioni specifiche adottate.

11.8. SELEZIONE E SCARTO DEI DOCUMENTI

Periodicamente, secondo quanto previsto in accordo con il Conservatore, viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale.

11.9. CONSERVAZIONE, SELEZIONE E SCARTO DEI DOCUMENTI ANALOGICI

La documentazione analogica corrente è conservata a cura da ciascun Ufficio fino al trasferimento in archivio di deposito.

I documenti analogici sono conservati nei locali della Società. Il Responsabile cura il versamento nell'archivio di deposito delle unità archivistiche non più utili per la trattazione degli affari in corso, individuate dagli uffici produttori. I fascicoli non soggetti a operazioni di scarto sono conservati nell'archivio di deposito secondo i termini di legge.

Periodicamente il Responsabile valuta l'opportunità, anche sotto il profilo economico, di provvedere al riversamento in formato digitale di tutti o parte dei documenti analogici presenti negli archivi.

11.10. MISURE DI SICUREZZA E MONITORAGGIO

Il Manuale di conservazione e il piano della sicurezza del Conservatore descrivono le modalità con cui il fornitore del servizio assicura gli obiettivi di sicurezza richiesti per

la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i backup degli archivi e il *Disaster recovery*.

Il Conservatore provvede altresì al periodico monitoraggio al fine di verificare lo stato delle componenti infrastrutturali del sistema e l'integrità degli archivi.

Il RC vigila affinché il Conservatore provveda alla conservazione integrata dei documenti, dei fascicoli e dei metadati associati nelle fasi di gestione e di conservazione. A tal fine, con cadenza almeno annuale, richiede al Conservatore l'esibizione di un campione di documenti o fascicoli.

Nel caso siano riscontrate irregolarità, provvede a sollecitare il Conservatore affinché vi ponga rimedio, anche attraverso gli strumenti contrattuali previsti negli atti di affidamento del servizio.

12. SICUREZZA E PROTEZIONE DEI DATI PERSONALI

12.1. SICUREZZA DEI SISTEMI INFORMATICI DI VENIS

Gli strumenti software indicati al par 3.4. del presente Manuale, utilizzati per la formazione e gestione dei documenti informatici, sono resi accessibili al personale della Società secondo il sistema di rilascio delle abilitazioni di accesso (cfr. par. 3.6.).

Le componenti architetturali e di sicurezza del sistema informatico di VENIS sono descritte nell'Allegato 6 al presente Manuale.

12.2. AMMINISTRATORE DI SITEMA

Il ruolo di Amministratore del Sistema del sistema di protocollo informatico è svolto dal RGD.

Negli altri casi, l'amministratore di sistema (o *Domain Administrator*), gestisce gli accessi al Sistema di gestione documentale previa autorizzazione del RGD, sulla base delle indicazioni fornite da ciascun Responsabile d'area competente.

12.3. USO DEL PROFILO UTENTE PER L'ACCESSO AI SISTEMI INFORMATICI

Per l'accesso ai sistemi informatici della Società è necessaria l'assegnazione di un profilo utente. Ogni profilo è protetto da un sistema di credenziali (username e password). Al momento della creazione del profilo utente, sono attribuiti all'utente lo username e una password temporanea. Al primo accesso dell'utente, viene richiesto l'inserimento di una nuova password, mentre lo username resta invariato.

L'uso di ogni profilo utente è strettamente personale e ogni dipendente, sotto la propria responsabilità, è tenuto a custodire e non diffondere le proprie credenziali. Ciascun dipendente deve associare al proprio profilo una password di almeno otto cifre, che preveda almeno una lettera maiuscola, una lettera minuscola, un numero e un segno (ad esempio: #, !, ?, -, &, ecc.). La password non deve mai coincidere con altre password associate ad altri profili o utenze (ad esempio, non si deve usare la stessa password del proprio account email personale).

L'Amministratore di sistema provvede affinché, almeno a cadenza semestrale, per ogni profilo utente sia richiesto il rinnovo della password.

Nell'accesso ai sistemi, nell'uso dei profili utente e nell'utilizzo di risorse e strumenti informatici, tutto il personale è tenuto a osservare le previsioni del ***Disciplinare interno contenente le norme di comportamento per l'accesso e l'utilizzo dei sistemi e delle risorse informatiche***. È responsabilità di ogni dipendente osservare scrupolosamente le indicazioni del disciplinare, che deve essere consultato nella versione più aggiornata.

12.4. ACCESSO ALLA POSTAZIONI DI LAVORO, AI LOCALI E AGLI ARCHIVI DI VENIS

L'archivio della Società è collocato nella sede aziendale, in locali opportunamente chiusi al pubblico, le cui chiavi di accesso sono custodite dal personale addetto. La consultazione avviene esclusivamente in presenza del personale.

Per quanto riguarda l'accesso ai locali che ospitano i data center aziendali, si rinvia alle previsioni del Piano di sicurezza (vedi Allegato 6).

13. ALLEGATI

Allegato 1 – Macrostruttura e Uffici

Allegato 2 – Provvedimenti di nomina

Allegato 3 – Guida alla formazione del documento accessibile

Allegato 4 – Titolario

Allegato 5 – Modello di registro di emergenza

Allegato 6 – Piano di sicurezza informatica