MANUALE DI GESTIONE DOCUMENTALE

Precedente Versione	Data emissione	Modifiche apportate	Nominativo
Det. S.S. n. 155 dd. 03.10.2019	07/04/2022	Aggiornamento 2022	Consiglio Direttivo

Approvato con deliberazione del Consiglio
Direttivo n. 44 dd. 07.04.2022
IL SEGRETARIO CONSORZIALE
f.to dott.ssa Luisa Ferrazza

Sommario

Premessa 4
Sezione 1 - Aspetti organizzativi 4
Sezione 1.1 L'area organizzativa omogenea e le responsabilità 4
Sezione 1.2 - Strumenti informatici per la formazione, la gestione e la conservazione dei documenti informatici 5
Sezione 1.3 - Modello operativo adottato per la gestione dei documenti 6
Sezione 1.4 – Identificazione dei documenti ricevuti ed inviati 6
Sezione 1.5 – Responsabile della gestione documentale 7
Sezione 2 – Documenti 7
Sezione 2.1 – Formazione dei documenti 7
Sezione 2.1.1 - Documento amministrativo 7
Sezione 2.1.2 - Documento cartaceo 7
Sezione 2.1.3 - Documento informatico 7
Sezione 2.1.4 - Documento amministrativo informatico 10
Sezione 2.1.5 – Sottoscrizione dei documenti informatici 10
Sezione 2.2 - Individuazione dei formati utilizzati 10
Sezione 3 – Protocollo informatico, registrazioni particolari e gestione dei flussi documentali 10
Sezione 3.1 – Registro di protocollo 10
Sezione 3.2 – Registrazione di protocollo 11
Sezione 3.3 – Documenti non soggetti a registrazione di protocollo 11
Sezione 3.4 – Segnatura di protocollo 11
Sezione 3.5 – Documenti soggetti a registrazione particolare 12
Sezione 3.6 – Annullamento e modifica delle registrazioni di protocollo 12
Sezione 3.7 – Registro di emergenza 12
Sezione 3.8 – Fatture elettroniche 13
Sezione 3.9 – Documenti inerenti a gare telematiche 13
Sezione 3.10 – Documenti originali plurimi 13
Sezione 3.11 – Lettere anonime 13
Sezione 3.12 – Lettere prive di firma o con firma illeggibile 13
Sezione 3.13 – Documenti con file protetti da password o con collegamenti attivi a siti web 13
Sezione 3.14 – Allegati da scaricare tramite link temporanei 14
Sezione 3.15 – Gestione dei flussi documentali cartacei in arrivo 14
Sezione 3.15.1 – Acquisizione di documenti cartacei 14
Sezione 3.15.2 – Apertura e cernita della corrispondenza in arrivo 14
Sezione 3.15.3 – Corrispondenza cartacea non di competenza dell'amministrazione 14
Sezione 3.15.4 – Scannerizzazione per acquisizione dei documenti cartacei 14
Sezione 3.15.5 – Rilascio di ricevute attestanti la ricezione di documenti su supporto cartaceo 14
Sezione 3.16 – Documenti informatici in arrivo: acquisizione e formato dei documenti 14
Sezione 3.17 – Documenti informatici in partenza 15
Sezione 3.18 – Inoltro di documenti informatici già protocollati verso strutture dell'Ente 15
Sezione 3.19 – Invio di documenti informatici verso strutture dell'Ente tramite registrazione di protocollo interno 15

Sezione 3.20– Inoltro di documenti informatici non protocollati 15
Sezione 3.21 – Metadati 15
Sezione 4 – Azioni di classificazione e selezione 15
Sezione 4.1 – Azioni di classificazione 15
Sezione 4.2 – Fascicolazione dei documenti 16
Sezione 4.2.1 – Regole generali sulla gestione del fascicolo elettronico 16
Sezione 4.2.2 – Descrizione del fascicolo 17
Sezione 4.2.3 – Processo di assegnazione dei documenti ai fascicoli 17
Sezione 5 – Misure di sicurezza e protezione dei dati personali 17
Sezione 5.1 – Accesso ai dati, informazioni e documenti informatici 17
Sezione 5.1.1 – Accessibilità da parte degli utenti appartenenti all'AOO 17
Sezione 5.1.2 – Accessibilità da parte degli utenti non appartenenti all'AOO (diritto di accesso agli atti) 18
Sezione 5.2 – Tutela dei dati personali 18
Sezione 5.3 – Requisiti minimi di sicurezza dei sistemi di protocollo informatico e misure di sicurezza 18
Sezione 6 – Conservazione 18
Sezione 6.1 – Responsabile della Conservazione 19
ELENCO ALLEGATI 21
ALLEGATO A – Documenti soggetti a registrazione particolare 22
ALLEGATO B – Registro di emergenza (RDE) 23
ALLEGATO C – Glossario 28
ALLEGATO D – Titolario 33
ALLEGATO E – Piano di sicurezza 36

Premessa

Il presente “Manuale di gestione documentale” (d’ora in avanti Manuale) risponde agli obblighi normativi introdotti dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emesse dall’Agenzia per l’Italia Digitale (AGID) al paragrafo 3.5. Tali Linee Guida sono entrate in vigore il 10 settembre 2020 e trovano piena applicabilità a partire dal 1 gennaio 2022.

Il loro duplice scopo è quello di:

1. aggiornare le attuali regole tecniche in base all’art. 71 del Codice dell’amministrazione digitale (CAD – D.Lgs 82/2005), concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici già precedentemente regolate nei DPCM del 2013 e 2014;
2. incorporare in un’unica linea guida le regole tecniche e le circolari in materia, addivenendo ad un “unicum” normativo che disciplini gli ambiti sopracitati, nel rispetto della disciplina in materia di Beni culturali.

Come precisato dal Consiglio di Stato - nell’ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, n. 2122/2017 del 10.10.2017 - le Linee Guida adottate da AGID, ai sensi dell’art. 71 del CAD, hanno carattere vincolante e assumono valenza erga omnes. Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all’art. 2, comma 2 del CAD, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell’art. 17 del CAD.

L’obiettivo del presente Manuale è quello di dotare l’Amministrazione di uno strumento che descriva e regolamenti il sistema di gestione documentaria, con particolare riferimento alle procedure relative alla formazione, alla gestione e alla conservazione dei documenti.
Il Manuale disciplina la gestione e la tenuta dei documenti in tutte le fasi del loro “ciclo di vita” (dalla fase di acquisizione/produzione fino all’archiviazione), coinvolgendo tutte le strutture dell’Amministrazione. Fornisce inoltre le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Regolamenta inoltre le fasi operative per la gestione informatica dei documenti, nel rispetto della normativa vigente in materia di trasparenza degli atti amministrativi, di tutela della privacy e delle politiche di sicurezza.

Il Consorzio, nell’organizzare autonomamente la propria attività utilizza le tecnologie dell’informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione.

Per perseguire gli obiettivi di informatizzazione dei flussi documentali previsti dalla normativa vigente, le pubbliche Amministrazioni debbono dotarsi di alcuni strumenti che consentano loro l’acquisizione e la spedizione di documenti informatici dei quali sia possibile verificare la provenienza e l’effettivo recapito. Tali strumenti devono essere in grado di attuare un’effettiva interoperabilità fra i sistemi documentari delle varie amministrazioni pubbliche.

Al fine di garantire lo sviluppo del processo di digitalizzazione, l’Ente provvede a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini, delle imprese e delle altre pubbliche amministrazioni.

Sezione 1 - Aspetti organizzativi

Sezione 1.1 L’area organizzativa omogenea e le responsabilità

L’Amministrazione ha provveduto al proprio accreditamento presso l’Indice delle Amministrazioni pubbliche e delle aree organizzative omogenee (https://www.indicepa.gov.it/ipa-portale/).
Gli uffici del Consorzio sono organizzati in un'unica Area Organizzativa Omogenea (AOO), costituita da un insieme di Unità Organizzative Responsabili (UOR), corrispondenti ai servizi presenti nell’organigramma, che usufruiscono in modo omogeneo e coordinato degli stessi servizi per la gestione dei flussi documentari.
All’interno delle UOR i dipendenti assumono la responsabilità nella trattazione di affari e procedimenti amministrativi nell’ambito delle competenze loro affidate.

Nell'ambito della AOO è istituito l'Ufficio per la tenuta del protocollo informatico e della gestione dei flussi documentali (di seguito denominato "Ufficio protocollo"). Il servizio è unico per l'intero Ente ed ha competenza sulla gestione dei documenti informatici, ai fini della corretta registrazione di protocollo, classificazione, conservazione, selezione e ordinamento.

Il servizio svolge i seguenti compiti:

a) garantisce che le operazioni di registrazione e segnatura di protocollo, classificazione ed indicizzazione dei documenti si svolgano nel rispetto delle disposizioni della normativa vigente;
b) gestisce le anagrafiche presenti all'interno del sistema di gestione documentale e protocollazione, garantendone il continuo aggiornamento;
c) gestisce il titolario, necessario per la corretta catalogazione dei documenti informatici;
d) gestisce la corretta formazione e tenuta dell'archivio corrente, ovvero dei fascicoli e dei registri relativi ad affari in corso di trattazione e conservati presso ciascuno ufficio dell'Amministrazione;
e) garantisce la corretta produzione e la conservazione del registro di protocollo;
f) si assicura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate nei termini temporali previsti dal Piano di Continuità operativa;
g) conserva il registro di emergenza (allegato B);
h) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali e le attività di gestione degli archivi;
i) gestisce le operazioni di annullamento e di modifica, previa autorizzazione del Responsabile della gestione documentale.

Sezione 1.2 - Strumenti informatici per la formazione, la gestione e la conservazione dei documenti informatici

L'Ente si avvale di strumenti informatici per la formazione dei documenti e per lo scambio degli stessi all'interno ed all'esterno dell'AOO, applicando le modalità di trasmissione indicate nell'allegato 6 delle Linee Guida "Comunicazione tra AOO di documenti amministrativi protocollati".

Il sistema di gestione e di protocollazione dei documenti usato è PITre (Protocollo Informatico Trentino), della Provincia Autonoma di Trento con supporto tecnico di Trentino Digitale spa, presente nel catalogo dei software a riuso di AGID https://developers.italia.it/it/software/p_tn-provinciaautonomatrento-pitre. Tale sistema consente non solo l'interscambio di documentazione fra i diversi servizi dell'amministrazione, ma anche fra sistemi di altre amministrazioni conformi ai nuovi standard.

Il software PITre garantisce:

a) la protezione del sistema nei confronti di agenti esterni;
b) l'impermeabilità dei dati e delle informazioni ad essi correlate (metadati);
c) coerenza e stabilità dei livelli di abilitazione di ruolo;
d) il trasferimento di dati e informazioni da utente a sistema, da sistema a utente e da utente a utente;
e) l'efficacia dei sistemi di back-up dei dati;
f) la produzione delle stampe giornaliere dei registri (di protocollo e di repertorio) e l'invio in conservazione delle stesse;
g) l'invio in conservazione dei documenti e del set di metadati prescritti dalla normativa.

Il sistema, inoltre, garantisce l'accesso alle informazioni contenute nel sistema di gestione documentale in conformità ai criteri di divulgazione dei documenti e fascicoli riservati previsti dalla normativa. In particolare, l'operatore che crea un documento non protocollato nel sistema, o effettua la registrazione di protocollo di un documento, indica il livello di riservatezza ritenuto necessario, se diverso da quello stabilito e applicato automaticamente dal sistema in base alla configurazione dell'organigramma.

L'accesso al sistema di protocollo informatico è consentito esclusivamente agli utenti abilitati, previa univoca identificazione e autenticazione. Gli utenti del sistema hanno autorizzazioni di accesso differenziate in base alle loro competenze e alle tipologie di operazioni stabilite dall'ufficio di appartenenza.
A ogni utente sono assegnate:

- specifiche credenziali di accesso, costituite da un UserID (nome utente) e da una password (privata, definita autonomamente dall'utente);
- uno o più ruoli, per ciascuno dei quali sono definite, in base alle competenze e ai compiti istituzionali, le specifiche funzioni che gli utenti di PITre possono svolgere nel sistema e il livello di visibilità sui documenti e sui fascicoli.

Il sistema di gestione documentale prevede la disconnessione automatica dall'applicazione dopo 20 minuti di inattività. È impossibile accedere a sessioni multiple su postazioni differenti con la stessa UserID.

Il manuale utente del sistema di protocollo informatico e gestione documentale PITre è disponibile online.

Quando un utente cessa il rapporto di lavoro o di guida dell'Ente, il Consorzio richiede l'estinzione delle credenziali ad esso riferite.

Sezione 1.3 - Modello operativo adottato per la gestione dei documenti

I responsabili dei Servizi in cui si articola l'Amministrazione hanno specificamente il compito di:

a) costituire e gestire i fascicoli e le serie documentarie riferentisi ad affari in corso di trattazione, di loro competenza;
b) curare l'accesso interno ed esterno alla documentazione affidata loro in carico;
c) collaborare con l'Ufficio Protocollo per il trasferimento all'Archivio della documentazione relativa ad affari esauriti.

Il modello organizzativo prevede un unico sistema per l'erogazione dei servizi di gestione documentaria ed in particolare un unico registro di protocollo, tenuto informaticamente. Le operazioni di registrazione di protocollo in arrivo sono effettuate dall'Ufficio protocollo, mentre le registrazioni in partenza e interne sono effettuate autonomamente da ciascun Responsabile di Servizio.

Gli utenti sono abilitati a svolgere soltanto le operazioni di propria competenza, secondo le abilitazioni definite: sola visualizzazione, visualizzazione e protocollazione in uscita, protocollazione sia in entrata che in uscita. Il sistema di gestione informatica dei documenti prevede, infatti, livelli di accesso differenziati per quanto riguarda inserimento, ricerca, consultazione e modifica dei dati.

Nell'ambito della AOO, la numerazione delle registrazioni di protocollo è unica e progressiva: non si differenzia fra documenti in ingresso, in uscita o interni e si rinnova ogni anno solare.
Il numero di protocollo e la data di protocollo sono generati tramite il sistema di protocollo informatico, non modificabili e sono assegnati automaticamente a ciascun documento registrato. Ad ogni documento è assegnano un solo numero, che non può essere utilizzato per la registrazione di altri atti, anche se correlati allo stesso. Questi ultimi vengono introdotti all'interno del fascicolo al quale si riferiscono.

Tutti i documenti registrati dal sistema informatico vengono classificati in base alla codifica identificata nel titolario, che rappresenta l'intera attività dell'Ente.

Sezione 1.4 – Identificazione dei documenti ricevuti ed inviati

In generale i documenti si distinguono in base allo stato di trasmissione in:

- documenti in entrata/arrivo: si intendono i documenti pervenuti dall'amministrazione nell'esercizio delle proprie funzioni;
- documenti in uscita/partenza: si intendono i documenti prodotti dall'amministrazione nell'esercizio delle proprie funzioni e inviati a soggetti esterni, pubblici e privati, all'amministrazione;
- documenti interni: si intendono i documenti amministrativi prodotti nell'ambito dell'attività dell'Ente.

Tutti i documenti in arrivo e in partenza devono essere protocollati, con le tipologie rispettivamente "Arrivo" e "Partenza" se si tratta di corrispondenza da/per soggetti esterni all'Ente, con la tipologia "Interno" se si tratta di corrispondenza fra servizi del Consorzio. Qualora un documento sia indirizzato sia a strutture interne sia a soggetti esterni, esso è protocollato con la tipologia "Partenza".

I documenti in arrivo ed inviati dell'Amministrazione possono seguire i seguenti canali:

a) interoperabilità PITre: gli enti che utilizzano il sistema di gestione e protocollazione PITre possono scambiarsi le comunicazioni tramite interoperabilità. Tali documenti vengono registrati, gestiti ed archiviati al pari delle comunicazioni ricevute tramite pec istituzionale;

b) casella istituzionale di posta elettronica certificata (pec): l'Amministrazione ha provveduto all'istituzione di una casella istituzionale di posta elettronica certificata, reperibile sul sito del Consorzio. La casella pec viene caricata quotidianamente all'interno del sistema PITre per la protocollazione delle e-mail ricevute;

c) caselle di posta elettronica: ciascun dipendente è dotato di casella di posta elettronica. Le comunicazioni interne non vengono protocollate. Eventuali comunicazioni ricevute e di rilevanza per l'Ente vengono inoltrate all'Ufficio protocollo per la registrazione in PITre;

d) documenti cartacei ricevuti dai cittadini: i cittadini che non utilizzano la casella pec o e-mail per inviare le proprie comunicazioni od istanze, possono presentare i propri documenti in formato cartaceo. Questi vengono tempestivamente protocollati dall'Ufficio protocollo, scannerizzati ed inseriti all'interno del sistema di gestione documentale.

Sezione 1.5 – Responsabile della gestione documentale

All'interno dell'Ente è nominato il responsabile della gestione documentale.

Il responsabile della gestione documentale assolve i seguenti compiti:

a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantisce che le operazioni di registrazione e di segnatura di protocollo si volgano nel rispetto delle disposizioni della normativa vigente;
c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo;
d) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
e) conserva le copie del salvataggio dei dati e del registro di emergenza in luoghi sicuri differenti;
f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le attività di gestione degli archivi;
g) autorizza le operazioni di annullamento di protocollo;
h) vigila sull'osservanza delle disposizioni della normativa vigente in materia da parte del personale autorizzato e degli incaricati:
i) predispone, d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale di cui all'art.17 del CAD e acquisito il parere del responsabile della protezione dei dati personali, il manuale di gestione documentale.

Sezione 2 – Documenti

Sezione 2.1 – Formazione dei documenti

Sezione 2.1.1 - Documento amministrativo

Per documento amministrativo si intende ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale.

Sezione 2.1.2 - Documento cartaceo

Per documento cartaceo s'intende tutta la documentazione prodotta con strumenti analogici (ad esempio, una lettera scritta a mano) o con strumenti informatici (ad esempio, una lettera prodotta tramite sistema di videoscrittura) e stampata. In quest'ultimo caso, come originale, si considera quello cartaceo stampato e, di norma, sottoscritto con firma autografa. Per originale si intende la stesura definitiva del documento, perfetto nei suoi elementi sostanziali e formali.

Sezione 2.1.3 - Documento informatico

La gestione del ciclo di vita di un documento informatico è un processo che può essere suddiviso in tre fasi principali:

1. Formazione;
2. Gestione;
3. Conservazione.

Il documento informatico è formato mediante una delle seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 delle Linee Guida;
b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico deve essere identificato in modo univoco e persistente. Nel caso della Pubblica Amministrazione, l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento. L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di hash che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 regole di processamento.
Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immodificabilità e l'integrità sono garantite da una o più delle seguenti operazioni:
- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9 delle Linee Guida;
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera b) l'immodificabilità ed integrità sono garantite da una o più delle seguenti operazioni mediante:
- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9 delle Linee Guida;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo le sopracitate lettere c) e d) le caratteristiche di immodificabilità e di integrità sono garantite da una o più delle seguenti operazioni:
- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
- produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati del documento informatico è definito nell'allegato 5 "Metadati" delle Linee Guida. Possono essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici.

Ai sensi dell'art. 40, comma 1 del CAD, le pubbliche amministrazioni sono tenute a produrre documenti nativi digitali.

L'Ente forma gli originali dei propri documenti con mezzi informatici secondo l'art. 71 del CAD e i suoi relativi rimandi, ossia secondo le seguenti modalità:

- utilizzo di applicativi di videoscrittura;
- utilizzo di appositi strumenti software;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o attraverso presentazione telematica di dati mediante moduli standard o formulari;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni provenienti da una o più basi dati, anche in modalità interoperativa;
- acquisizione di un documento informatico per via telematica o su supporto informatico, della copia per immagine su supporto informatico di un documento analogico, della copia informatica di un documento analogico.

Nella formazione dei documenti informatici effettuata nei diversi gestionali, può essere attuato un controllo delle versioni degli stessi. In tal caso viene tenuta traccia dei loro passaggi fino alla versione definitiva inviata alla registrazione e, ove richiesto, vengono conservate le versioni stesse.

Gli atti formati con strumenti informatici, i dati e i documenti informatici dell'Ente costituiscono informazione primaria ed originale di cui è possibile effettuare, su diversi tipi di supporto, copie e duplicati per gli usi consentiti dalla legge.

La copia per immagine su supporto informatico di un documento analogico è 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 o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia. Nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis del CAD, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.
Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

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; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato. La copia di un documento informatico 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 con estensione ".doc" in un documento ".pdf".

L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine. Nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto. Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

Sezione 2.1.4 - Documento amministrativo informatico

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico, salvo quanto specificato nel presente paragrafo.

La Pubblica Amministrazione forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel presente manuale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni dalle imprese attraverso le tecnologie dell'informazione e della comunicazione, oppure provenienti da o inviate a domicili digitali eletti, oppure presentate per via telematica. Tali istanze, dichiarazioni e comunicazioni sono identificate e trattate come i documenti amministrativi informatici. Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità proprie del documento informatico, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo, nonché i metadati relativi alla classificazione e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza. Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, secondo quanto previsto dall'Allegato 5 delle Linee guida.

In applicazione dell'art.23-ter comma 5-bis del CAD16, i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

Sezione 2.1.5 – Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma elettronica conforme alle disposizioni di legge.

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma elettronica, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione.

Sezione 2.2 - Individuazione dei formati utilizzati

L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati previsti dalla normativa di settore, in modo da assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la durata nel tempo dei dati in termini di accesso e di leggibilità.

L'Ente per la formazione dei documenti informatici, delle copie e degli estratti informatici può adottare i formati indicati nell'allegato 2 delle Linee Guida.
Non vengono utilizzati ulteriori formati per la formazione dei documenti. Ne consegue che non si rende necessaria la valutazione di interoperabilità prevista annualmente nell'allegato 2 delle Linee Guida, paragrafo 3.

Non si effettuano riversamenti periodici da una tecnologia verso un'altra al fine di mitigare l'obsolescenza dei formati dei file nel lungo/ lunghissimo periodo.

Sezione 3 – Protocollo informatico, registrazioni particolari e gestione dei flussi documentali

Sezione 3.1 – Registro di protocollo

Il registro di protocollo è un atto pubblico che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento. Ha cadenza annuale, cioè inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

L'addetto dell'Ufficio Protocollo verifica la produzione del registro giornaliero informatico di protocollo su supporto informatico (file), costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Il registro del protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Le informazioni che caratterizzano il registro di protocollo sono quelle relative alla registrazione di protocollo di cui alla sezione 3.2, a cui si aggiungono le informazioni inerenti l'assegnazione interna all'amministrazione e la eventuale classificazione.

Sezione 3.2 – Registrazione di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione e per tutti i documenti informatici che non rientrano tra le tipologie escluse (alla sezione 3.3) e che non sono oggetto di registrazione particolare da parte dell'amministrazione, al fine di garantirne l'identificazione univoca e certa.

La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni:

a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
d) oggetto del documento, registrato in forma non modificabile;
e) data e protocollo del documento ricevuto, se disponibili;
f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

I documenti devono essere protocollati tempestivamente.

La registrazione della documentazione in ingresso di norma resta in carico all'Ufficio Protocollo che provvede alla protocollazione.

Eventuali allegati, privi di relativa lettera accompagnatoria, che dovessero pervenire in un momento successivo alla presentazione della nota ufficiale, devono essere protocollati. Le integrazioni documentarie, pervenute in data successiva alla registrazione della lettera accompagnatoria, devono essere protocollate.

La protocollazione in uscita è sempre decentrata all'Ufficio che produce l'atto. Eccezionalmente, in caso di necessità o per carenza di personale, può essere demandata all'Ufficio Protocollo.

Sezione 3.3 – Documenti non soggetti a registrazione di protocollo

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

Sezione 3.4 – 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. Essa consente di individuare ciascun documento in modo inequivocabile. Le informazioni minime previste sono:

a) il progressivo di protocollo;
b) la data di protocollo;
c) l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa.

Le operazioni di segnatura e registrazione di protocollo sono effettuate contemporaneamente.
Tutti i documenti ricevuti dall'Amministrazione in formato analogico (cartaceo) devono riportare le suddette informazioni tramite etichetta, timbro di protocollo o, eccezionalmente, con apposizione manuale. I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura di protocollo, sono acquisiti in formato immagine attraverso processo di scansione con finalità gestionali.

I documenti originati in formato digitale, ricevuti dall'Amministrazione, non dovranno riportare alcun tipo di informazione relativa al protocollo all'interno del testo. Le informazioni relative al protocollo vengono associate

al file ricevuto in automatico dal software PITre. Il sistema prevede la possibilità di stampa del file ricevuto integrato dai dati relativi alla segnatura di protocollo apposta sull'immagine pervenuta.

I documenti in partenza, creati dall'Amministrazione in formato analogico, devono necessariamente riportare la segnatura di protocollo tramite etichetta o scritti all'interno del documento.

I documenti prodotti dall'Amministrazione in formato digitale non riportano alcuna informazione relativa al protocollo all'interno del testo prodotto, ma vengono associati ai dati di protocollo all'interno del software PITre e raggiungono il destinatario provvisto di posta elettronica o l'ente in cooperazione applicativa corredati dei relativi dati di segnatura.

Sezione 3.5 – Documenti soggetti a registrazione particolare

I documenti che possono essere sottoposti ad altre forme di registrazione sono registrati per mezzo di appositi repertori. L'allegato A ricomprende l'elenco dei documenti soggetti a registrazione particolare alla data di approvazione del presente manuale.

Sono riportati, inoltre, i registri particolari individuati per la gestione del trattamento delle registrazioni particolari.

A tali documenti vengono associati i metadati obbligatori presenti nell'Allegato 5 delle Linee Guida.

Sezione 3.6 – Annullamento e modifica delle registrazioni di protocollo

L'annullamento di un protocollo avviene solamente per i seguenti motivi: registrazione di un protocollo in arrivo anziché in uscita e viceversa, errore nell'identificazione del mittente o del destinatario, errore formale nell'oggetto. Le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa.

Le uniche informazioni modificabili di una registrazione di protocollo sono l'assegnazione interna all'amministrazione e la classificazione.

Per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni, il sistema storicizza tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili.

Nel caso si rendesse necessario creare nuove versioni per documenti che sono già stati spediti a corrispondenti esterni all'amministrazione, deve essere attribuito un nuovo numero di protocollo ed effettuata una nuova trasmissione. Nelle note di trasmissione ad altre strutture, o nella lettera di accompagnamento, nel caso di spedizione verso l'esterno, si dovrà specificare che: "Il presente documento sostituisce il documento prot. n. _____ di data _____".

Sezione 3.7 – Registro di emergenza

Ogniqualvolta, per cause tecniche, non sia possibile utilizzare il sistema, è necessario prendere contatti con l'Ufficio Protocollo e il Responsabile della gestione documentale per gli eventuali provvedimenti da adottare. Il Responsabile della gestione documentale autorizza lo svolgimento delle operazioni di registrazione su registri di emergenza. Le istruzioni relative all'utilizzo del registro di emergenza sono riportate nell'allegato B.

In condizioni di emergenza si applicano le seguenti modalità di registrazione e di recupero dei dati:

a) sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;
b) qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre quattro ore, per cause di eccezionale gravità, il Responsabile della gestione documentale può autorizzare l'uso del registro di emergenza per periodi successivi. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione;
c) per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate;
d) la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario;
e) le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

Sezione 3.8 – Fatture elettroniche

Le fatture sono gestite secondo le disposizioni normative vigenti. La fattura elettronica passiva (nata in formato digitale e firmata digitalmente):

- arriva alle Strutture provviste di codice IPA, mediante il sistema d'interscambio (SdI), direttamente all'interno del sistema di gestione documentale PITre;
- è registrata automaticamente nel repertorio delle fatture elettroniche passive;
- può essere inserita in un fascicolo digitale;
- è sottoposta a processo di conservazione a norma entro i termini previsti dalla normativa vigente.

La fattura elettronica attiva (nata in formato digitale e firmata digitalmente) viene gestita tramite il gestionale della contabilità e affidata per la conservazione secondo specifica convenzione.

Sezione 3.9 – Documenti inerenti a gare telematiche

La protocollazione della documentazione di gara e delle offerte, scaricabili dalle piattaforme e-procurement dei mercati elettronici della Pubblica Amministrazione, istituiti ai sensi di legge, non è necessaria quando i gestori di tali sistemi assicurano la conservazione sostitutiva a norma di legge e a tempo indeterminato, della documentazione relativa alle singole gare. In tali casi si ritiene peraltro opportuno, ancorché non necessario, 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.

Sezione 3.10 – Documenti originali plurimi

Al documento originale plurimo indirizzato a più destinatari deve essere assegnato un solo e unico numero di protocollo. Il documento viene poi trasmesso tramite PITre per competenza ai vari destinatari.

Sezione 3.11 – Lettere anonime

Le lettere anonime sono soggette a registrazione di protocollo. Nel campo del mittente s'indicherà la dicitura "Anonimo".

Sezione 3.12 – Lettere prive di firma o con firma illeggibile

Le lettere prive di firma e quelle con firma illeggibile sono soggette a registrazione di protocollo. Nel campo delle "note" delle lettere pervenute prive di firma, con mittente comunque identificabile, si indicherà l'irregolarità riscontrata ("Firma mancante"). Nel campo delle "note" delle lettere con firma illeggibile, si indicherà la dicitura "Firma illeggibile".

Sezione 3.13 – Documenti con file protetti da password o con collegamenti attivi a siti web

Non è consentito l'inserimento nel sistema di gestione documentale di file protetti da password in quanto non gestibili in termini di conservazione.
Parimenti non è consentito produrre documenti nel testo dei quali compaiano collegamenti attivi (*link* attivi) a siti web poiché il documento è completo solo se corredato dai contenuti ad esso collegati (che di fatto ne costituiscono allegati), dei quali in questo caso non è possibile garantire la stabilità nel tempo. In questo caso il documento viene protocollato con una nota di irregolarità da inserire sul profilo del documento ed il responsabile del procedimento dovrà provvedere a richiedere la regolarizzazione al mittente affinché tutti i contenuti siano presenti nel documento (o nei suoi allegati) senza link a contenuti esterni.
Se possibile l'Ufficio Protocollo provvede direttamente a caricare i file indicati nel link esterno, indicando in tal caso anche la nota "moduli scaricati da protocollista". È cura del responsabile del procedimento verificare l'esattezza dei file caricati.

I link attivi a siti web sono invece considerati regolari quando hanno uno scopo meramente indicativo (ad esempio il rimando ad una legge o ad un approfondimento), poichè il contenuto del documento rimane in questo caso autosufficiente a prescindere dal contenuto web collegato.

Sezione 3.14 – Allegati da scaricare tramite link temporanei

Nel caso di e-mail in arrivo con files da scaricare tramite dropbox, wetransfer, o simili, l'Ufficio protocollo provvede ad acquisire i relativi files inserendo una nota nel profilo protocollo "allegati scaricati da protocollista". È cura del responsabile del procedimento verificare l'esattezza dei file caricati.

Se i files sono troppo pesanti e non si possono acquisire l'Ufficio Protocollo inserisce nel profilo di protocollo la seguente nota "allegati non scansionabili e salvati sul server, indicando il percorso".

Sezione 3.15 – Gestione dei flussi documentali cartacei in arrivo

Sezione 3.15.1 – Acquisizione di documenti cartacei

I documenti cartacei possono essere acquisiti tramite i seguenti canali:

a) servizio postale o servizio di corriere;
b) consegna diretta agli uffici.

Sezione 3.15.2 – Apertura e cernita della corrispondenza in arrivo

Una volta pervenuta all'Ufficio protocollo, la corrispondenza viene suddivisa distinguendo preliminarmente tra:

a) corrispondenza da non protocollare, che viene inoltrata direttamente;
b) corrispondenza da protocollare.

I documenti da protocollare o da sottoporre ad altra forma di registrazione sono presi in carico dall'Ufficio protocollo che provvede, prima della protocollazione, a individuare la corrispondenza che ha carattere di urgenza.

Sezione 3.15.3 – Corrispondenza cartacea non di competenza dell'amministrazione

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

La corrispondenza cartacea che invece riporta l'indirizzo corretto sulla busta, ma non è di competenza dell'Amministrazione, a seguito dell'apertura e valutazione, va richiusa indicando la dicitura "aperta e non di competenza", apponendo timbro datario e riconsegnata al Servizio postale o al mittente.

Sezione 3.15.4 – Scannerizzazione per acquisizione dei documenti cartacei

I documenti cartacei pervenuti, una volta registrati e protocollati, vengono scannerizzati ed inseriti nel sistema di gestione documentale e di protocollo. La copia per immagine, provvista della segnatura di protocollo, viene successivamente trasmessa per competenza o conoscenza ai destinatari tramite PITre.

A partire da un documento già protocollato in PITre si avvia l'operazione di acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico file in formato pdf o più, nel caso di presenza di allegati. L'associazione tra documenti scansionati e la registrazione di protocollo è effettuata automaticamente dal sistema ed è immediatamente verificabile. Il sistema, inoltre, provvede automaticamente alla memorizzazione dei file in modo non modificabile.

Sezione 3.15.5 – Rilascio di ricevute attestanti la ricezione di documenti su supporto cartaceo

Qualora un documento cartaceo sia consegnato personalmente dal mittente o da altra persona incaricata, l'Ufficio protocollo provvede a protocollare ed acquisire il documento in PITre. Stampa poi la prima pagina del documento acquisito, comprensivo della segnatura di protocollo, e lo consegna quale ricevuta di ricezione del documento. In alternativa alla stampa della prima pagina acquisita, l'utente protocollatore può fotocopiare la prima pagina del documento ricevuto ed apporre l'etichetta stampata da PITre contente le informazioni relative alla segnatura di protocollo.

Sezione 3.16 – Documenti informatici in arrivo: acquisizione e formato dei documenti

I documenti acquisiti dall'Amministrazione vengono accettati solo se in uno dei formati previsti dall'Allegato 2 delle Linee Guida. Se il documento ricevuto proviene da uno sei soggetti indicati dall' art. 2 comma 2 del CAD

(a cui le Linee Guida si riferiscono) e deve essere pubblicato online, questo deve essere anche redatto in modalità accessibile. Se così non fosse, l'Ufficio protocollo provvede a richiedere al mittente la revisione del documento in formato accessibile. Se non perviene entro il termine indicato, l'Ente procede comunque con la pubblicazione.

Sezione 3.17 – Documenti informatici in partenza

Il protocollo in uscita va utilizzato per registrare documenti in formato elettronico nel caso in cui almeno un destinatario sia esterno. Nel caso di destinatari esterni e interni, il documento va protocollato con protocollo in uscita. Gli eventuali destinatari interni vengono raggiunti da una semplice trasmissione in PITre. In questo caso il destinatario interno non deve protocollare in ingresso e non riceve il cartaceo anche se il provvedimento è firmato con firma autografa.

Sono previsti casi eccezionali concordati con l'amministrazione per gestire la protocollazione e spedizione di documenti prodotti da sistemi informativi automatizzati ove è consentito che il documento spedito sia acquisito in formato elettronico, con la dicitura "F.to". Le ricevute di presa in carico e consegna sono acquisite automaticamente in PITre. come allegati al documento registrato.

Sezione 3.18 – Inoltro di documenti informatici già protocollati verso strutture dell'Ente

Nel caso di documenti informatici ricevuti, e già sottoposti a registrazione di protocollo, che devono essere inoltrati ad altre strutture dell'ente, si effettua una operazione di trasmissione verso la persona interessata, specificando nelle note il motivo della trasmissione.

La ricezione, con contestuale accettazione da parte del destinatario, di documentazione informatica trasmessa per competenza, vale a tutti gli effetti quale sua presa in carico lavorativo. L'eventuale rifiuto deve essere motivato.

Sezione 3.19 – Invio di documenti informatici verso strutture dell'Ente tramite registrazione di protocollo interno

Nel caso in cui i destinatari di un documento amministrativo siano solo strutture interne all'Amministrazione, è necessario che il documento venga registrato con protocollo interno. L'Ufficio protocollo esegue la registrazione e invia il documento tramite trasmissione al destinatario.

La ricezione, con contestuale accettazione da parte del destinatario, di documentazione informatica trasmessa per competenza, vale a tutti gli effetti quale sua presa in carico lavorativo. L'eventuale rifiuto deve essere motivato.

Sezione 3.20– Inoltro di documenti informatici non protocollati

I documenti registrati a sistema senza protocollazione, a carattere meramente informativo, possono essere inoltrati a strutture o a singoli destinatari attraverso la trasmissione.

Sezione 3.21 – Metadati

Al documento informatico ed al documento amministrativo informatico è associato l'insieme obbligatorio dei metadati previsti dall'Allegato 5 delle Linee Guida per ciascuna tipologia di documenti.

Sezione 4 – Azioni di classificazione e selezione

Sezione 4.1 – Azioni di classificazione

La classificazione è l'attività di organizzazione logica di tutti i documenti che entrano a far parte del sistema documentario del Consorzio, a prescindere dalle modalità di acquisizione o produzione. Per mezzo di essa si stabilisce la posizione che ogni documento assume nell'archivio in formazione, permettendo, in tal modo, una sedimentazione che rispecchi lo sviluppo dell'attività svolta dall'Ente.

I documenti vanno sempre classificati, anche se non sono protocollati.

Il codice di classificazione è elemento obbligatorio (e modificabile) della registrazione di protocollo, ed è riportato:

- sul documento in arrivo, nello spazio appositamente riservato, in caso di documento nativo cartaceo;

- nel profilo di protocollo in caso di documento nativo digitale;
- sul documento in partenza nel profilo di protocollo.

La classificazione si effettua sulla scorta del Titolario di classificazione.

Il titolario di classificazione si articola, secondo uno schema che va dal generale al particolare, in titoli (nodi di primo livello), classi (nodi di secondo livello) e sottoclassi (nodi di terzo livello).
Tale schema rappresenta un sistema logico che suddivide i documenti secondo le funzioni istituzionali esercitate dal Consorzio, indipendentemente dagli uffici che le esercitano, dato che l'organizzazione di questi può variare nel tempo, mentre le funzioni dell'Ente si mantengono costanti.
Il Titolario non è retroattivo: non si applica, cioè, ai documenti prodotti prima della sua introduzione. Per agevolare le operazioni di classificazione nell'allegato D del presente Manuale è riportato l'indice del Titolario di classificazione con relativa descrizione delle classi.

Sezione 4.2 – Fascicolazione dei documenti

Di norma il documento si collega naturalmente e logicamente ad uno o più precedenti e ad uno o più susseguenti documenti, relativi ad un medesimo affare, attività, soggetto (persona fisica/giuridica) od oggetto, dando luogo alla formazione di un fascicolo.
Il fascicolo è quindi l'insieme ordinato di documenti relativi ad un medesimo affare particolare, ad una medesima attività generale o ad un medesimo soggetto/oggetto. Il fascicolo può riferirsi ad uno o più procedimenti amministrativi.

Ogni documento che dà avvio ad un nuovo procedimento o si riferisce ad un nuovo affare deve dar luogo ad un nuovo fascicolo, entro il quale devono essere ricondotti anche tutti i documenti che, successivamente acquisiti o prodotti, si riferiscano al medesimo affare, attività o persona.

La fascicolazione è obbligatoria per tutti i documenti, anche quelli non protocollati. Ogni utente fascicola i documenti di propria competenza.

Qualora si ritenga necessario, la documentazione contenuta nei fascicoli può essere articolata in sottofascicoli. In questo ultimo caso i sottofascicoli sono visualizzabili solamente dal profilo di protocollo poiché sul timbro o etichetta di protocollo compare esclusivamente il fascicolo di riferimento.

Sezione 4.2.1 – Regole generali sulla gestione del fascicolo elettronico

Ogni documento che dà avvio ad un nuovo procedimento o che si riferisce ad un nuovo affare deve dar luogo ad un nuovo fascicolo, al quale devono essere ricondotti anche tutti i documenti che, successivamente acquisiti o prodotti, si riferiscano al medesimo affare.

Il fascicolo viene creato a cura di ciascun utente, per competenza.

L'operazione di apertura di un fascicolo e di collocazione di ciascun documento all'interno del fascicolo di assegnazione è detta fascicolazione.
Il fascicolo deve essere aperto in corrispondenza del nodo di Titolario di classificazione più basso (Classe).

All'atto dell'apertura del fascicolo il sistema rilascia la seguente segnatura: <anno di apertura del fascicolo/indice di classificazione/numero di repertorio di fascicolo>. Esempio: 2020-2.3-1.

Le informazioni essenziali contenute in ciascuna registrazione sono:
- anno di apertura del fascicolo
- classe del fascicolo
- numero di repertorio del fascicolo (numero progressivo all'interno di ogni nodo del Titolario di classificazione).

Quando si crea un fascicolo in PITre, il sistema assegna automaticamente un numero al fascicolo: la numerazione è annuale e progressiva all'interno di ogni classe del Titolario.
È vietato creare fascicoli destinati a contenere tutta la documentazione proveniente da un determinato ente a prescindere dall'oggetto (ad esempio un fascicolo della corrispondenza con la Provincia Autonoma di Trento, oppure con il Comune X).

È prassi creare dei fascicoli permanenti che rimangono correnti ben oltre la durata dei singoli affari o procedimenti dai quali sono composti, sono fascicoli che si riferiscono ad uno stesso soggetto od oggetto (ad esempio una persona, un edificio, ecc.).
Il caso più comunemente diffuso di fascicoli permanenti sono i fascicoli del personale dipendente.
Per ciascun dipendente viene istruito un fascicolo nominativo, aperto all'atto dell'assunzione in cui sono inseriti tutti i documenti che fanno riferimento al rapporto di lavoro intercorrente tra l'Amministrazione e la persona stessa. Il fascicolo del personale viene creato dall'Ufficio Personale con un grado di riservatezza tale da risultare visibile solamente all'Ufficio stesso.

Sezione 4.2.2 – Descrizione del fascicolo

La descrizione del fascicolo è di cruciale importanza per una corretta tenuta del sistema documentale. Deve rispettare le regole comuni volte ad omogeneizzare i criteri di registrazione, per questo valgono per la descrizione dei fascicoli valgono gli stessi principi enunciati per la corretta redazione degli oggetti dei documenti. In particolare, si deve garantire:

- una corretta strutturazione delle informazioni, seguendo un ordine che procede dal generale al particolare: la prima parte della descrizione è costituita dall'argomento generale del fascicolo, mentre la seconda parte è costituita dalle informazioni specifiche del procedimento;
- un giusto equilibrio tra sintesi e specificità: la descrizione del fascicolo deve riportare le parole chiave utili ai fini della ricerca delle informazioni;
- l'uso normalizzato di sigle, numeri e date, nonché del carattere maiuscolo;
- l'adozione di un lessico Consorzio e condiviso;
- il rispetto delle disposizioni vigenti in materia di protezione dei dati personali e del segreto d'ufficio.

Sezione 4.2.3 – Processo di assegnazione dei documenti ai fascicoli

All'atto dell'assegnazione di un documento, l'utente stabilisce se:

- il documento sia riconducibile ad un affare o procedimento in corso e sia pertanto da ricondurre ad un fascicolo già aperto;
- il documento si riferisca ad un nuovo affare o procedimento per il quale sia necessario aprire un nuovo fascicolo.

Se il documento si ricollega ad un affare o procedimento in corso, l'utente:

- cerca il fascicolo avvalendosi dei filtri di ricerca del sistema;
- seleziona il fascicolo individuato;
- inserisce il documento nel fascicolo selezionato.

Se il documento dà avvio ad un nuovo fascicolo, l'utente:

- esegue l'operazione di apertura del fascicolo (in collaborazione con il Responsabile del procedimento);
- provvede alla trasmissione del fascicolo al Responsabile competente;
- inserisce il documento nel fascicolo aperto.

Tutti i documenti sono conservati all'interno di ciascun fascicolo secondo l'ordine cronologico di registrazione, ovvero in base al numero di protocollo ad essi attribuito o, se assente, in base alla propria data. Il fascicolo viene chiuso di norma al termine del procedimento amministrativo o all'esaurimento dell'affare/attività. La data di chiusura si riferisce a quella dell'ultimo documento inserito nel fascicolo e viene memorizzata dal sistema con la selezione del pulsante che attiva la funzione di chiusura del fascicolo.

Sezione 5 – Misure di sicurezza e protezione dei dati personali

Sezione 5.1 – Accesso ai dati, informazioni e documenti informatici

Sezione 5.1.1 – Accessibilità da parte degli utenti appartenenti all'AOO

Per ogni documento, all'atto della registrazione, il sistema consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso, nel rispetto della normativa in materia di trattamento e tutela dei dati personali. Ogni dipendente dell'Ente può consultare i documenti relativi ad affari di propria competenza ad esso assegnati e quei documenti di carattere generale e infrastrutturale necessari a concludere il procedimento. Il controllo degli accessi al sistema di gestione informatica dei documenti è assicurato mediante le modalità descritte nel Piano per la sicurezza dei documenti informatici allegato al presente Manuale (allegato E). Sulla base della struttura

organizzativa e funzionale dell'Ente, il Responsabile della gestione documentale attribuisce almeno i seguenti livelli di autorizzazione:

a) abilitazione alla consultazione;
b) abilitazione all'inserimento;
c) abilitazione alla modifica delle informazioni e/o all'annullamento dell'intero protocollo.

I dipendenti, in quanto funzionari pubblici, sono tenuti a rispettare il segreto d'ufficio e quindi a non divulgare notizie di natura riservata, a non trarre profitto personale o a procurare danno a terzi e all'amministrazione di appartenenza dalla conoscenza di fatti e documenti riservati.

Sezione 5.1.2 – Accessibilità da parte degli utenti non appartenenti all'AOO (diritto di accesso agli atti)

L'accesso agli atti nell'Ente è garantito secondo la normativa vigente in materia.
Sul sito istituzionale dell'Ente, all'interno della sezione "Amministrazione Trasparente", sono riportate le modalità di accesso, sia civico che generalizzato.

Sezione 5.2 – Tutela dei dati personali

L'Ente, a norma del Regolamento generale sulla protezione dei dati personali 679/2016 dell'Unione Europea (d'ora in poi Regolamento 679/2016/UE), è Titolare dei dati personali, intesi come "….qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

I trattamenti di dati personali effettuati dall'Ente sono elencati nel Registro delle attività dei trattamenti e nella documentazione prodotta ai sensi del medesimo Regolamento.

I dati personali sono contenuti nella documentazione sia analogica che informatica prodotta e ricevuta dall'Ente che, in qualità di Titolare del trattamento dei dati stessi, è responsabile per quanto riguarda le decisioni in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. L'Ente dà attuazione al dettato del Regolamento 679/2016/UE con atti formali aventi rilevanza interna ed esterna quali le informative e le nomine a incaricato, a designato o a responsabile esterno per il trattamento dei dati.

L'Ente si organizza per garantire che i certificati e i documenti prodotti riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisiti.

Sezione 5.3 – Requisiti minimi di sicurezza dei sistemi di protocollo informatico e misure di sicurezza

Il sistema di protocollo informatico, eventualmente integrato in un sistema di gestione informatica dei documenti, assicura il rispetto delle disposizioni in materia di sicurezza predisposte da AGID (misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017) e delle disposizioni in materia di protezione dei dati personali.

In particolare, il sistema di protocollo informatico deve garantire:

a) l'univoca identificazione ed autenticazione degli utenti;
b) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;
c) il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il Responsabile della gestione documentale predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR). Il piano contiene altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali (data breach).

Sezione 6 – Conservazione

Sulla base di un accordo di collaborazione stipulato con l'Istituto per i Beni Artistici, Culturali e Naturali della Regione Emilia-Romagna e la Provincia autonoma di Trento, cui il Consorzio ha aderito, l'Ente invia i propri

documenti informatici, gestiti all'interno del sistema PITre, al sistema di conservazione gestito dal Polo archivistico regionale dell'Emilia-Romagna – ParER.

L'invio in conservazione dei documenti informatici avviene secondo le seguenti scadenze temporali:

- le stampe giornaliere del registro di protocollo e dei repertori entro il giorno successivo;
- le fatture elettroniche entro i termini stabiliti dalla normativa fiscale;
- tutti gli altri documenti informatici un anno dopo rispetto alla data di registrazione.

La presa in carico dei documenti informatici da parte del sistema di conservazione comporta il consolidamento degli stessi documenti nel sistema di gestione documentale PITre.
Il consolidamento inibisce ogni modifica, con l'obiettivo di mantenere inalterate le caratteristiche dei documenti che sono già stati presi in carico dal sistema di conservazione.

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime;
c) gli archivi informatici con i metadati associati.

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

a) pacchetti di versamento;
b) pacchetti di archiviazione;
c) pacchetti di distribuzione.

L'intero processo di conservazione dei documenti informatici è dettagliatamente descritto nel manuale di conservazione del Consorzio, a cui si rimanda.

Sezione 6.1 – Responsabile della Conservazione

All'interno dell'Ente è designato il Responsabile della Conservazione.

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
In particolare, il responsabile della conservazione:

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

k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali45;
m) predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sul servizi affidati in outsourcing dalle PA

Sezione 7 – Disposizioni finali

Sezione 7.1 – Applicabilità

Le indicazioni contenute nel presente Manuale trovano piena applicazione a partire dal 1° gennaio 2022.

Sezione 7.2 – Revisione

Il presente Manuale è rivisto ogniqualvolta sia necessario un aggiornamento o si presentino modifiche sostanziali nell'operatività del Consorzio, su iniziativa del Responsabile della gestione documentale. La modifica o l'aggiornamento di uno o tutti i documenti allegati al presente manuale non comporta la revisione del manuale stesso. Atteso il rapido evolversi della legislazione in materia di gestione documentale e di digitalizzazione della Pubblica Amministrazione, si evidenzia che le disposizioni normative citate, in vigore al momento dell'approvazione, potrebbero subire variazioni prima dell'aggiornamento del presente Manuale.

Sezione 7.3 – Pubblicazione e divulgazione

Il Manuale di gestione documentale del Consorzio dei Comuni del B.I.M. Sarca Mincio Garda è pubblicato sul sito istituzionale nella Sezione Amministrazione Trasparente, come previsto dal D.Lgs. 33/2013. Il provvedimento di adozione/approvazione o di revisione viene pubblicato nell'albo on line dell'Ente.

ELENCO ALLEGATI

A. Documenti soggetti a registrazione/archiviazione particolare
B. Registro di emergenza (RDE)
C. Glossario
D. Titolario
E. Piano di sicurezza

ALLEGATO A – Documenti soggetti a registrazione/archiviazione particolare

Sono soggetti a registrazione particolare o numerazione ed archiviazione i seguenti tipi di documenti:

1. Atti pubblici (repertorio) e atti privati (protocollo)
2. Delibere Assemblea
3. Delibere Consiglio Direttivo
4. Determinazioni dei Responsabili dei Servizi
5. Verbali Assemblea Generale
6. Fatture elettroniche

ALLEGATO B – Registro di emergenza (RDE)

ISTRUZIONI OPERATIVE PER L'USO DEL REGISTRO DI EMERGENZA (RDE) DEL P.I.TRE

INDICE

1. Operazioni preliminari
2. Quando si usa il registro di emergenza – RDE
3. Chi decide quando usare il registro di emergenza
4. Cosa bisogna fare per usare il RDE
5. Come si compila il file di excel RDE
6. Come predisporre il documento protocollato con il RDE
7. Se l'interruzione di P.I.TRE dura più di un giorno
8. Quando riprende la protocollazione con P.I.TRE
9. Prima cosa da fare alla ripresa del servizio
10. La ripresa del servizio di protocollazione
11. Utilizzo del foglio cartaceo RDE
12. Inserimento in P.I.TRE delle registrazioni effettuate sul RDE
13. Completamento dei protocolli importati
14. Completamento del documento cartaceo
15. Salvataggio del registro di emergenza in P.I.TRE
16. Modulo di Autorizzazione e revoca uso RDE

1. OPERAZIONI PRELIMINARI

Stampare:

- questo manualetto,
- il foglio di excel RDE (che vale come registro di emergenza) in formato A3,
- il modulo di autorizzazione/revoca.

Salvare sul PC:

- questo manualetto,
- il foglio di excel RDE (che vale come registro di emergenza),
- il modulo di autorizzazione/revoca.

Tutti questi documenti sono pubblicati sul sito https://www.pi3.it/portal/server.pt/directory/registro_di_emergenza_-_rde/1725?DirMode=1.

2. QUANDO SI USA IL REGISTRO DI EMERGENZA – RDE

Se non funziona il programma P.I.TRE, ma è possibile usare il PC, aprire il foglio di excel RDE salvato sul pc. Se manca l'energia elettrica, usare il RDE che è stato stampato.

3. CHI DECIDE QUANDO USARE IL REGISTRO DI EMERGENZA

In caso di interruzione del sistema di protocollo P.I.TRE, Trentino Digitale comunica, tramite posta elettronica, l'impossibilità di utilizzare P.I.TRE In tutti gli altri casi (ad esempio se manca la corrente elettrica nella sede della struttura) è il Responsabile della gestione documentale che decide quando attivare il registro di emergenza.

4. COSA BISOGNA FARE PER USARE IL RDE

Per prima cosa occorre compilare la prima parte del modulo di Autorizzazione all'uso dell'RDE e farlo firmare al Responsabile della gestione documentale (modulo "Autorizzazione e revoca uso RDE").

È il responsabile della gestione documentale che autorizza, sempre, l'uso del protocollo di emergenza: il modulo deve essere compilato anche se c'è la comunicazione di Trentino Digitale.

5. COME SI COMPILA IL FILE DI EXCEL RDE

È importante non fare variazioni di formattazione celle, aggiunta o eliminazione colonne, ecc..

Il foglio ha una struttura più semplice rispetto al protocollo normale. Per ogni documento registrato occorre compilare una riga, seguendo le descrizioni riportate nella riga di intestazione. I dati da riportare sono:

a) data protocollo emergenza: indicare nella cella la data in cui si esegue la registrazione di emergenza nel formato <gg/mm/aaaa>;

b) ora protocollo emergenza: indicare nella cella l'ora in cui si esegue la registrazione di emergenza nel formato <hh.mm.ss>. L'informazione sui secondi non è obbligatoria, pertanto nel caso in cui non fosse inserito tale dato, il sistema automaticamente valorizza il campo con "hh.mm.00";

c) numero protocollo emergenza: indicare nella cella il numero progressivo della registrazione di emergenza che si sta eseguendo nel formato <n>. La numerazione del registro d'emergenza parte dal numero 1 e prosegue per tutti i documenti che sarà necessario registrare, fino alla ripresa del servizio centralizzato del sistema P.I.Tre;

d) stringa protocollo emergenza: indicare la segnatura di emergenza nel formato <PITRE/codice amministrazione/ userID/numero progressivo del protocollo di emergenza all'interno del foglio excel (la numerazione parte da 1) di 7 cifre preceduto da zeri>; esempio P.I.TRE/A116/A116MROSSI/0000001;

e) codice RF: indicare nella cella il codice del RF (Raggruppamento Funzionale = UO) che deve essere presente in segnatura. Ad esempio se la registrazione in emergenza è eseguita da un ruolo appartenente al RFS007 indicare tale codice nella cella;

f) tipo protocollo (A/P): indicare A per i protocolli in ingresso; P per i protocolli in uscita; gli interni non sono gestiti;

g) oggetto: indicare nella cella l'oggetto del documento per il quale si sta eseguendo la registrazione di protocollo di emergenza (massimo 2000 caratteri);

h) mittente: se il protocollo è di tipo A (arrivo/ingresso) indicare la descrizione del mittente. Nota bene: il corrispondente sarà trattato come occasionale e quindi, per ottimizzare le ricerche di documenti per mittente, si suggerisce di procedere, alla ripresa del servizio di protocollo elettronico, alla modifica in P.I.TRE del corrispondente, associando quello presente in rubrica;

i) destinatario: se il protocollo è di tipo P (partenza/uscita) indicare la descrizione del destinatario. Nel caso sia necessario inserire più destinatari principali, separare i destinatari con punto e virgola (;). Nota bene: il corrispondente sarà trattato come occasionale e quindi, per ottimizzare le ricerche di documenti per destinatario, si suggerisce di procedere, alla ripresa del servizio di protocollo elettronico, alla modifica in P.I.TRE del corrispondente, associando quello presente in rubrica;

j) destinatario per conoscenza: indicare la descrizione del corrispondente destinatario per conoscenza. Nel caso sia necessario inserire più destinatari per conoscenza separare i destinatari con punto e virgola (;). Nota bene: il corrispondente sarà trattato come occasionale e quindi per ottimizzare le ricerche di documenti per destinatario per conoscenza, si suggerisce di procedere, alla ripresa del servizio di protocollo elettronico, come sopra e cioè alla modifica in P.I.TRE del corrispondente, associando quello presente in rubrica;

k) codice amministrazione: è il codice dell'amministrazione che sta eseguendo l'operazione di protocollazione in emergenza: indicare M365;

l) codice Registro: è il codice dell'Area Organizzativa Omogenea (o Registro) sulla quale si sta eseguendo la registrazione di protocollo: indicare M365;

m) data protocollo mittente: indicare la data del protocollo mittente nel formato <gg/mm/aaaa> (solo per i documenti in ingresso);

n) numero protocollo mittente: indicare la stringa completa di segnatura del protocollo mittente (solo per i documenti in ingresso);

o) data arrivo: indicare la data di arrivo del documento nel formato <gg/mm/aaaa>(solo per i documenti in ingresso). Il dato non è obbligatorio;

p) ora arrivo: indicare l'ora di arrivo nel formato <hh.mm.ss> (l'informazione sui secondi non è obbligatoria pertanto nel caso in cui non fosse inserito tale dato il sistema automaticamente valorizza il campo con "hh.mm.00"), (solo per i documenti in ingresso). Il dato non è obbligatorio;

q) codice classifica: indicare il solo codice della voce di titolario con cui si vuole classificare il documento nel formato <1.2.3> (es. 4.1.2). Non deve essere indicato il codice del fascicolo.

Se si usa il file elettronico, salvare il foglio excel RDE sul disco locale della postazione di lavoro dell'utente che l'ha utilizzato, avvalendosi del comando "salva con nome" e nominando il file "RDE del giorno XXX" e indicando il giorno dell'emergenza in cui lo si è compilato. Se invece si usa il RDE cartaceo, compilare l'intestazione con la data del giorno del registro di emergenza.

6. COME PREDISPORRE IL DOCUMENTO PROTOCOLLATO CON IL RDE

Sul documento cartaceo si indicherà la segnatura di emergenza che è la seguente: <Cod. amministrazione>/<RFstruttura(solo se presente)>-<Anno>-RDE/<UserId dell'utente protocollatore>/<numero protocollo RDE>

Esempio senza RF: A116/2012-RDE/A116MROSSI/0000001

Esempio con RF: A116/RFS139-2012-RDE/A116MROSSI/0000001

7. SE L'INTERRUZIONE DI P.I.TRE DURA PIÙ DI UN GIORNO

Deve essere usato un foglio RDE diverso per ogni giornata, ricominciando la numerazione da 1.

8. QUANDO RIPRENDE LA PROTOCOLLAZIONE CON P.I.TRE

- Quando Trentino Digitale comunica tramite la casella di posta elettronica il ripristino del sistema P.I.TRE e dei relativi servizi di protocollazione;
- In tutti gli altri casi è il Responsabile della gestione documentale che decide quando è terminata l'emergenza.

9. PRIMA COSA DA FARE ALLA RIPRESA DEL SERVIZIO

Occorre compilare la seconda parte del modulo che revoca l'uso del RDE e farlo firmare al Responsabile della gestione documentale (modulo "Autorizzazione e revoca uso RDE").

È il Responsabile della gestione documentale che deve revocare l'uso del protocollo di emergenza. (anche se c'è la comunicazione di Trentino Digitale).

10. LA RIPRESA DEL SERVIZIO DI PROTOCOLLAZIONE

Nel momento in cui il servizio viene ripristinato, l'utente dovrà salvare e chiudere il foglio excel usato per RDE precedentemente creato sul disco locale della postazione di lavoro. Alla ripresa del servizio si utilizza il sistema P.I.TRE per le nuove registrazioni di protocollo. La normativa vigente, infatti, prevede che si possa utilizzare immediatamente il registro ufficiale di protocollo, avendo cura però di recuperare le registrazioni di emergenza appena possibile.

11. UTILIZZO DEL FOGLIO CARTACEO RDE

Se è stato utilizzato il Registro di emergenza cartaceo, ad esempio per mancanza di energia elettrica, al termine dell'emergenza, si devono riportare tutti i dati scritti sul registro cartaceo nel foglio di excel RDE, per poi procedere con la successiva importazione in P.I.TRE (di cui al punto 12).

12. INSERIMENTO IN P.I.TRE DELLE REGISTRAZIONI EFFETTUATE SUL RDE

Il ruolo abilitato all'utilizzo della funzione d'importazione (di solito il protocollo o la segreteria) procede all'importazione del file utilizzato come RDE nel sistema P.I.TRE.

Entrati in P.I.TRE si va alla voce di menù "Gestione" e quindi "Import RDE". Compare la pagina per l'importazione. Cliccando su "Sfoglia" si cerca il file di excel RDE salvato con le registrazioni effettuate, lo si seleziona e si seleziona "Apri". Quindi si clicca sul pulsante "Avvia RDE". (Per maggiori dettagli vedere la Guida Operativa con le istruzioni particolareggiate.)

Al termine dell'importazione il sistema restituisce un rapporto con l'esito dell'importazione: verrà presentata una schermata generale, e quindi i dettagli per i documenti in arrivo/ingresso e per quelli in partenza/uscita. OK significa è andato tutto bene; KO c'è qualche errore nell'importazione.

Nel caso di errori nell'importazione, verificare le indicazioni fornite dal rapporto (log) e, se necessario, contattare il CSD di Trentino Digitale per aprire una richiesta di assistenza.

13. COMPLETAMENTO DEI PROTOCOLLI IMPORTATI

Entrare in P.I.TRE e in Ricerca / Documenti / Completa, nella parte dedicata all'emergenza, ricercare la data in cui sono state effettuate le registrazioni di emergenza, nel campo "Data segn. emergenza".

Si trovano tutti i documenti importati e si procede a completare le operazioni che mancano:

- fascicolare;
- associare l'immagine del documento (scansionare) e gli eventuali allegati;
- sostituire il mittente/destinatario occasionale importato con quello presente in rubrica per migliorare le ricerche successive;
- trasmettere, inserire eventuali note, ecc.

14. COMPLETAMENTO DEL DOCUMENTO CARTACEO

Il documento cartaceo deve riportare la segnatura RDE e il numero di protocollo in P.I.TRE, quindi si deve segnare, accanto al numero di protocollo dato con il RDE, anche il numero di protocollo assegnato dal sistema P.I.TRE.

Esempio di segnatura: <Cod.amministrazione>/<RFstruttura>*-<Anno>-RDE/<UserId utente protocollatore>/<numero protocollo RDE> – <numero di protocollo PITRE>
*se presente

A116/RFS139*-2012-RDE/A116MROSSI/0000001 – 0077777

*se presente

15. SALVATAGGIO DEL REGISTRO DI EMERGENZA IN P.I.TRE

Il foglio di excel RDE utilizzato è da registrare come documento grigio/non protocollato in P.I.TRE, classificandolo nella voce di Titolario relativa all'Archivio Generale associando il file excel e mettendo nell'oggetto: "Registro di emergenza del giorno gg/mm/aaaa".

Anche il modulo di autorizzazione e revoca all'utilizzo del RDE compilato e firmato, è da registrare sempre come documento grigio/non protocollato, classificandolo nella voce di Titolario relativa all'Archivio Generale associando la scansione del documento con l'indicazione nell'oggetto "Autorizzazione e revoca all'uso del registro di emergenza del giorno gg/mm/aaaa".

Nel caso di interruzione del servizio di P.I.TRE per più giorni consecutivi, si avrà un foglio excel RDE per ogni giorno di interruzione, mentre si registrerà un unico documento di autorizzazione e revoca all'utilizzo del RDE,

che avrà come oggetto in P.I.TRE “Autorizzazione e revoca all’uso del registro di emergenza dal giorno gg/mm/aaaa al giorno gg/mm/aaaa”.

16. MODULO DI AUTORIZZAZIONE E REVOCA USO RDE

Ente: (indicare il nome dell’Ente)

AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO DI EMERGENZA
(art. 63 del D.P.R. n. 445/2000)

Ai sensi dell’art. 63 del D.P.R. 445/2000, preso atto che non è possibile utilizzare la normale procedura informatica di protocollazione informatica per la seguente causa, (indicare la causa)

in data (indicare la data) alle ore (indicare l’ora),

si autorizza lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza.

Luogo e data, (indicare luogo e data)

Il Responsabile della gestione documentale (firma del Responsabile)

REVOCA AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO DI EMERGENZA
(art. 63 del D.P.R. n. 445/2000)

Preso atto che, in data (indicare la data) alle ore (indicare l’ora)

è stato ripristinato il normale funzionamento della procedura informatica, si revoca l’autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza.

Si dispone il tempestivo inserimento delle informazioni relative ai documenti protocollati in emergenza nel sistema informatico, con automatica attribuzione della numerazione di protocollo ordinaria, mantenendo la correlazione con la numerazione utilizzata in emergenza.

Luogo e data, (indicare luogo e data)

Il Responsabile della gestione documentale (firma del Responsabile)

ALLEGATO C – Glossario

- Allegato: documento unito a un altro documento o a una pratica con funzione di prova, memoria, chiarimento o integrazione di notizie.
- Anagrafica: dati personali relativi all'identificazione dei mittenti e dei destinatari di un documento, memorizzati nel database del software di protocollo e compilati nel rispetto delle linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico.
- Annullamento: operazione che consente a un utente abilitato di annullare una registrazione di protocollo.
- Archivio: il complesso dei documenti prodotti o comunque acquisiti da un ente durante lo svolgimento della propria attività. A fini gestionali l'archivio s'intende diviso in: Archivio corrente, per la parte relativa agli affari in corso; Archivio di deposito, per la parte di documenti relativi ad affari esauriti da meno di quarant'anni; Archivio storico, per la parte di documenti relativi ad affari esauriti da oltre quarant'anni. L'archivio, pur caratterizzandosi in tre momenti diversi, è da considerarsi una sola unità. Con archivio si intende anche il luogo fisico di conservazione della documentazione.
- Area Organizzativa Omogenea (AOO): insieme definito di unità organizzative di un'amministrazione che usufruiscono in modo omogeneo e coordinato di comuni servizi per la gestione dei flussi documentari. In particolare, una AOO utilizza per il servizio di protocollazione un'unica sequenza numerica, rinnovata ogni anno solare.
- Assegnazione: individuazione della persona fisica responsabile della trattazione dell'affare o del procedimento amministrativo e della gestione dei documenti nella fase corrente.
- Casella istituzionale di posta elettronica: casella di posta elettronica, istituita da un'AOO, per la ricezione dall'esterno e per la spedizione all'esterno dei documenti da sottoporre a registrazione di protocollo.
- Certificato elettronico: insieme di attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche.
- Copia: riproduzione di un documento originale non avente valore giuridico. La copia semplice è la riproduzione di un documento originale non avente valore giuridico. La copia autentica o autenticata è la riproduzione di un documento originale avente valore giuridico in quanto la conformità all'originale, in tutte le sue componenti, viene dichiarata da un pubblico ufficiale a ciò autorizzato e la conformità risulta dalla copia del documento rilasciata o da un suo allegato.
- Copia informatica di documento cartaceo: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.
- Copia per immagine su supporto informatico di documento cartaceo: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto (es.: documento informatico ottenuto tramite scansione di un documento analogico).
- Copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari [es.: documento informatico ottenuto dalla trasformazione in PDF della sua versione originale in formato OpenOffice ODT; in questo caso infatti l'operazione di trasformazione ha prodotto una diversa sequenza di valori binari (bit) tra il documento originale (.odt) e la sua copia (.pdf)].
- Duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario [es.: documento informatico ottenuto salvando semplicemente il documento informatico esistente ad esempio su un CD o su chiavetta esterna, anche modificando il nome del file; infatti in questo caso l'operazione ha mantenuto la stessa sequenza di valori binari (bit) tra il documento originale e il suo duplicato].
- Deposito: locale nel quale un ente conserva la propria documentazione non più occorrente alla trattazione degli affari in corso.
- Documento: testimonianza di un fatto, non necessariamente di natura giuridica, compilata su tipologie diverse di supporti e varie tecniche di scrittura con l'osservanza di determinate forme che sono destinate a darle fede e forza di prova.
- Documento amministrativo: ogni rappresentazione comunque formata del contenuto di atti, anche interni, delle pubbliche Amministrazioni o comunque utilizzati ai fini dell'attività amministrativa.

- Documento cartaceo (c.d. “analogico”): documento amministrativo rappresentato su supporto cartaceo, leggibile direttamente senza l’ausilio di strumenti.
- Documento informatico: rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
- Documento informatizzato: documento in origine analogico reso digitale.
- Elenco topografico: strumento di corredo che descrive le unità archivistiche secondo la loro disposizione fisica.
- Elenco di versamento: strumento di corredo che descrive in modo sintetico le unità archivistiche, prodotto in occasione di ogni trasferimento o versamento di fascicoli e registri.
- Fascicolazione: pratica di gestione archivistica dei documenti che consente di raccogliere tutta la documentazione inerente ad uno specifico procedimento amministrativo o affare in un medesimo fascicolo. Vedi anche Fascicolo.
- Fascicolo: insieme dei documenti relativi a una determinata pratica, attività, affare o persona, collocati all’interno di una copertina in ordine cronologico.
- Firma digitale: particolare firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e 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 di un documento informatico o di un insieme di documenti informatici.
- Firma elettronica: dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.
- Flusso documentario: insieme delle operazioni cui è soggetta la documentazione prodotta o acquisita da un ente; esso comprende le fasi che vanno dalla registrazione e segnatura di protocollo alla classificazione, organizzazione, assegnazione, inserimento e conservazione dei documenti, compresi quelli non soggetti a registrazione di protocollo, nell’ambito del sistema di classificazione adottato.
- Gestione dei documenti: insieme delle attività finalizzate alla registrazione di protocollo, alla classificazione, fascicolazione, assegnazione, reperimento, conservazione, accesso e consultazione dei documenti amministrativi prodotti o comunque acquisiti da un ente nell’esercizio delle sue funzioni. Tali attività nello scenario delineato dalla normativa vigente sono integrabili con quelle volte al governo dell’Innovazione e servizi digitali e dei flussi di lavoro (workflow) di un ente.
- Gestione documentale: vedi Sistema di gestione informatica dei documenti.
- Interoperabilità: modalità di comunicazione tra P.A. dotate di sistema di protocollo informatico a norma che permette di scambiare automaticamente metadati relativi alle registrazioni di protocollo spedite e ricevute tramite la posta elettronica.
- Interoperabilità semplificata: interoperabilità tramite il sistema P.I.Tre. (ovvero senza l'ausilio del canale della posta elettronica).
- Intranet: rete interna di un ente realizzata utilizzando protocolli del tipo TCP/IPP.
- Metadati: insieme dei dati relativi alle registrazioni informatiche di documenti e fascicoli.
- Minuta: per ogni scritto nativo analogico destinato ad essere spedito vengono compilati due esemplari, uno dei quali viene spedito e pertanto entra a far parte dell’archivio del destinatario, mentre l’altro viene conservato dall’autore ed entra a far parte dell’archivio del mittente. L’esemplare che resta al mittente prende il nome di minuta.
- Nucleo minimo di protocollo: vedi Sistema di gestione documentario.
- Oggetto: in sede di redazione del documento, l’oggetto è l’enunciazione sommaria, sintetizzata in poche parole, dell’argomento di cui tratta il documento. L’oggetto viene scritto sul documento nello spazio apposito e deve essere riportato sia sul registro di protocollo dell’ente che scrive sia su quello dell’ente che riceve il documento.
- Originale: è la stesura definitiva del documento, perfetto nei suoi elementi sostanziali e formali.
- Piano di classificazione: vedi Titolario di classificazione.

- Piano di conservazione dei documenti cartacei: strumento che definisce i criteri di organizzazione, selezione periodica tramite scarto archivistico e conservazione permanente dei documenti, redatto e integrato col sistema di classificazione adottato.

- Posta elettronica certificata (PEC): è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici. "Certificare" l'invio e la ricezione – i due momenti fondamentali nella trasmissione dei documenti informatici – significa fornire al mittente, dal proprio gestore di posta, una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione. Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale. Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte viene conservata per un periodo di tempo definito a cura dei gestori, con lo stesso valore giuridico delle ricevute.

- Prontuario del Titolario di classificazione: strumento per la corretta classificazione dei documenti, costituito da un insieme di voci relative alle diverse attività svolte da un Ente, organizzate in ordine alfabetico in modo da consentire all'utente una facile fruizione del Titolario.

- Protocollazione: vedi Registrazione di protocollo.

- Registrazione di protocollo: insieme degli elementi, rilevanti sul piano giuridico-probatorio e obbligatori, desunti dai documenti prodotti o comunque acquisiti dal sistema documentario di un ente. Tali elementi, immessi nel registro di protocollo, sono costituiti da: data di registrazione, numero di protocollo, mittente o destinatario, oggetto, numero degli allegati, descrizione degli allegati.

- Registro di protocollo: atto pubblico di fede privilegiata che attesta l'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, idoneo a produrre effetti giuridici a favore o a danno delle parti. Il registro di protocollo è gestito esclusivamente mediante un sistema di gestione informatica dei documenti, disciplinato dal presente Manuale di gestione. Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il sistema di gestione informatica dei documenti è attivato un registro alternativo denominato registro di protocollo di emergenza.

- Registro di protocollo di emergenza: Vedi Registro di protocollo.

- Repertorio: registro in cui sono annotati in ordine cronologico documenti e atti che presentano gli stessi elementi formali (ad esempio circolari, delibere di un organo collegiale, contratti, ecc.), indipendentemente dall'oggetto trattato. Tale forma di registrazione ha valore giuridico-probatorio ed è da ritenersi alternativa alla registrazione di protocollo.

- Repertorio dei fascicoli: registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del titolario (titoli, classi, sottoclassi).

- Responsabile del Procedimento Amministrativo (RPA): persona fisica incaricata dell'istruttoria e degli adempimenti di un affare o di un procedimento amministrativo, ai sensi dell'art. 5 della legge 7 agosto 1990, n. 241 e delle corrispondenti disposizioni di legge regionali e provinciali.

- Riferimento temporale: informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.

- Riversamento sostitutivo: processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione a un altro, modificando la loro rappresentazione informatica.

- Scarto (procedura di): operazione con cui si destina al macero una parte dei documenti di un archivio.

- Scarto informale: documenti senza valore amministrativo (appunti, fotocopie, copie di norme, fac-simili di lettere o di documenti, ecc.) utilizzati nel corso dell'istruttoria delle pratiche che possono essere eliminati alla chiusura del procedimento.

- Segnatura di protocollo: apposizione o associazione al documento, in forma permanente o non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire l'individuazione di ciascun documento in modo inequivocabile. Nel documento in arrivo la segnatura viene posta di norma sul recto del documento medesimo mediante l'apposizione della segnatura di protocollo in formato digitale o l'apposizione di un'etichetta.

- Selezione: individuazione dei documenti da destinare alla conservazione permanente o, qualora ritenuti inutili, allo scarto; tale operazione viene effettuata periodicamente e comunque prima del passaggio dei fascicoli all'Archivio storico. Nel Comune la proposta di scarto è subordinata alla preventiva autorizzazione della Soprintendenza archivistica territorialmente competente.

- Sistema di gestione informatica dei documenti: insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti. Le funzionalità di un sistema di gestione documentaria possono distinguersi, partendo da un nucleo minimo, in:

1. Nucleo minimo di protocollo: prevede la gestione informatica dei documenti in modalità base. È caratterizzato dalla registrazione delle informazioni riguardanti un documento (numero, data, mittente/destinatario, oggetto, ecc.); dalla segnatura sul documento delle informazioni riguardanti il documento stesso (numero, data, AOO); dalla classificazione d'archivio per una corretta organizzazione dei documenti, corrispondenti alle funzionalità minime previste dalla normativa vigente, alle quali può eventualmente essere aggiunta anche l'indicazione dell'assegnatario sul registro di protocollo.

2. Gestione documentale: prevede la gestione informatica dei documenti in modalità avanzata. Questo termine ricomprende attività assai eterogenee, che variano a seconda del grado di funzionalità che si desideri attuare, ma che trovano una logica ben precisa per il loro accorpamento, nella comune finalità della dematerializzazione dei documenti cartacei e quindi della disponibilità degli stessi a livello informatico. Tale livello può prevedere la registrazione di protocollo dei documenti con trattamento delle immagini (scannerizzazione dei documenti cartacei); l'assegnazione per via telematica al destinatario; la gestione avanzata della classificazione dei documenti (utilizzo di thesaurus e vocabolari controllati, ecc.); il collegamento dei documenti alla gestione dei procedimenti; a queste può aggiungersi la realizzazione di una repository documentaria per quei documenti di alto contenuto informativo che meritano uno specifico trattamento (prevedendo ad esempio la creazione di abstract, l'uso di parole chiave per un'indicizzazione più dettagliata, ecc.).

3. Workflow documentario: tale livello può prevedere l'informatizzazione dei processi relativi ai flussi documentari in entrata, l'informatizzazione dei processi relativi ai flussi documentari in uscita, l'informatizzazione dei processi relativi ai flussi documentari interni.

4. Business Process Reengeneering (BPR): quest'ultimo livello prevede la reingegnerizzazione dei processi dell'ente al fine di una loro successiva informatizzazione. In particolare vengono gestiti mediante sistemi integrati di workflow tutti quei processi che possiedono i requisiti di convenienza, ovvero la complessità, la ripetitività e la stabilità dell'iter.

- Smistamento di un documento: individuazione di un'unità organizzativa responsabile (UOR) cui affidare un documento in gestione. Vedi anche Assegnazione di un documento.

- Sottofascicolo: sottoinsieme organico di documenti contenuti in un fascicolo di cui rappresenta una partizione. Ciascun sottofascicolo è iscritto nel repertorio dei fascicoli all'interno del fascicolo di appartenenza.

- Supporto ottico di memorizzazione: mezzo fisico che consente la memorizzazione di documenti informatici mediante l'impiego della tecnologia laser (dischi ottici, DVD, ecc.).

- Titolario di classificazione: quadro di classificazione costituito da un determinato numero di titoli, articolati in classi e sottoclassi, contrassegnati da simboli numerici. Si tratta di un sistema logico che suddivide i documenti secondo la funzione esercitata dall'ente che li produce o li acquisisce, permettendone l'organizzazione a seconda degli oggetti cui si riferiscono.

- Trasferimento: è l'operazione con cui periodicamente i documenti non più necessari al disbrigo degli affari correnti vengono trasferiti nell'Archivio di deposito.

- Unità Organizzativa Responsabile (UOR): Struttura organizzativa (aree, servizi, ecc.) al quale afferisce il RPA (Responsabile Procedimento Amministrativo).

- Unità archivistica: indica il documento o un insieme di documenti, rilegati o raggruppati secondo un nesso di collegamento organico, che costituiscono un'unità non divisibile (registro, fascicolo).

- Unità Organizzativa di Protocollazione (UOP): ufficio che svolge attività di registrazione di protocollo.

- Versamento: operazione con cui un ente trasferisce periodicamente i documenti che si riferiscono ad affari esauriti da oltre quarant'anni dall'Archivio di deposito a quello storico.

- Vincolo archivistico: nesso logico che unisce tutti i documenti facenti parte del medesimo affare o attività; il vincolo non può essere spezzato, pena la perdita della funzionalità del documento in rapporto all'affare o attività in relazione alle quali era stato posto in essere.

- Visibilità: possibilità per un utente abilitato di visualizzare una registrazione di protocollo.

- Workflow documentario: vedi Sistema di gestione informatica dei documenti.

- Workflow management: strumento di gestione del flusso aziendale di dati che permette incremento dell'efficienza, migliore controllo del processo e flessibilità mediante l'utilizzo di un programma software specifico. I vantaggi del workflow management sono dovuti soprattutto alla possibilità di utilizzo della rete internet per il mantenimento e organizzazione dei contatti, soprattutto quando il gruppo di lavoro è vasto e disperso nello spazio.

ALLEGATO D – Titolario

CODICE_NODO	DESCRIZIONE_TITOLO
1	AMMINISTRAZIONE GENERALE
1.1	Legislazione e circolari esplicative
1.2	Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica
1.3	Statuto
1.4	Regolamenti
1.5	Stemma, gonfalone, sigillo
1.6	Archivio generale
1.7	Sistema informativo
1.8	Informazioni e relazioni con il pubblico
1.9	Politica del personale; ordinamento degli uffici e dei servizi
1.10	Relazioni con le organizzazioni sindacali e di rappresentanza del personale
1.11	Controlli interni ed esterni
1.12	Editoria e attività informativo-promozionale interna ed esterna
1.13	Cerimoniale, attività di rappresentanza; onoreficenze e riconoscimenti
1.14	Interventi di carattere politico e umanitario; rapporti istituzionali
1.15	Adesione a forme associative
1.16	Associazionismo e partecipazione
2	ORGANI DI GOVERNO, GESTIONE, CONTROLLO, CONSULENZA E GARANZIA
2.1	Sindaco
2.2	Vice-Sindaco
2.3	Consiglio
2.4	Presidente del Consiglio
2.5	Conferenza dei capigruppo e Commissioni del Consiglio
2.6	Gruppi consiliari
2.7	Giunta
2.8	Commissario prefettizio e straordinario
2.9	Segretario e Vice-Segretario
2.10	Direttore generale e dirigenza
2.11	Revisori dei conti
2.12	Difensore civico
2.13	Commissario ad acta
2.14	Organi di controllo interni
2.15	Organi consultivi
2.16	Delegati
2.17	Consigli circoscrizionali
2.18	Presidenti dei Consigli circoscrizionali
2.19	Organi esecutivi circoscrizionali
2.20	Commissioni dei Consigli circoscrizionali
2.21	Segretari delle circoscrizioni
2.22	Commissario ad acta delle circoscrizioni
2.23	Conferenza dei Presidenti di quartiere
3	RISORSE UMANE
3.1	Concorsi, selezioni, colloqui
3.2	Assunzioni e cessazioni
3.3	Comandi e distacchi; mobilità
3.4	Attribuzione di funzioni, ordini di servizio e missioni
3.5	Inquadramenti e applicazione contratti collettivi di lavoro

3.6	Retribuzioni e compensi
3.7	Adempimenti fiscali, contributivi e assicurativi
3.8	Tutela della salute e sicurezza sul luogo di lavoro
3.9	Dichiarazioni di infermità ed equo indennizzo
3.10	Indennità premio di servizio e trattamento di fine rapporto, quiescenza
3.11	Servizi al personale su richiesta
3.12	Orario di lavoro, presenze e assenze
3.13	Giudizi, responsabilità e provvedimenti disciplinari
3.14	Formazione e aggiornamento professionale
3.15	Collaboratori esterni
4	RISORSE FINANZIARIE E PATRIMONIALI
4.1	Entrate
4.2	Uscite
4.3	Partecipazioni finanziarie
4.4	Bilancio preventivo, variazioni di bilancio, verifiche contabili
4.5	Piano esecutivo di gestione (PEG)
4.6	Rendiconto della gestione
4.7	Adempimenti fiscali
4.8	Inventari e consegnatari dei beni
4.9	Beni immobili
4.10	Beni mobili
4.11	Economato
4.12	Oggetti smarriti e recuperati
4.13	Tesoreria
4.14	Concessionari ed altri incarichi della riscossione delle entrate
4.15	Pubblicità e pubbliche affissioni
5	AFFARI LEGALI
5.1	Contenzioso
5.2	Responsabilità civile e patrimoniale verso terzi; assicurazioni
5.3	Pareri e consulenze
6	PIANIFICAZIONE E GESTIONE DEL TERRITORIO
6.1	Urbanistica: piano regolatore generale e varianti
6.2	Urbanistica: strumenti di attuazione
6.3	Edilizia privata
6.4	Edilizia pubblica
6.5	Opere pubbliche
6.6	Catasto
6.7	Viabilità
6.8	Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
6.9	Ambiente:autorizzazioni, monitoraggio e controllo
6.10	Protezione civile ed emergenze
7	SERVIZI ALLA PERSONA
7.1	Diritto allo studio e servizi
7.2	Asili nido e scuola dell'infanzia
7.3	Promozione e sostegno delle istituzioni di istruzione e delle loro attività
7.4	Orientamento professionale; educazione degli adulti; mediazione culturale
7.5	Istituti culturali (Musei, biblioteche, teatri, Scuola comunale di musica, etc.)
7.6	Attività ed eventi culturali
7.7	Attività ed eventi sportivi

7.8	Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale
7.9	Prevenzione, recupero e reintegrazione dei soggetti a rischio
7.10	Informazione, consulenza ed educazione civica
7.11	Tutela e curatela di incapaci
7.12	Assistenza diretta e indiretta, benefici economici
7.13	Attività ricreativa e di socializzazione
7.14	Politiche per la casa
7.15	Politiche per il sociale
8	ATTIVITA' ECONOMICHE
8.1	Agricoltura e pesca
8.2	Artigianato
8.3	Industria
8.4	Commercio
8.5	Fiere e mercati
8.6	Esercizi turistici e strutture ricettive
8.7	Promozione e servizi
9	POLIZIA LOCALE E SICUREZZA PUBBLICA
9.1	Prevenzione ed educazione stradale
9.2	Polizia stradale
9.3	Informative
9.4	Sicurezza e ordine pubblico
10	TUTELA DELLA SALUTE
10.1	Salute e igiene pubblica
10.2	Trattamento Sanitario Obbligatorio
10.3	Farmacie
10.4	Zooprofilassi veterinaria
10.5	Randagismo animale e ricoveri
11	SERVIZI DEMOGRAFICI
11.1	Stato civile
11.2	Anagrafe e certificazioni
11.3	Censimenti
11.4	Polizia mortuaria e cimiteri
12	ELEZIONI E INIZIATIVE POPOLARI
12.1	Albi elettorali
12.2	Liste elettorali
12.3	Elezioni
12.4	Referendum
12.5	Istanze, petizioni e iniziative popolari
13	AFFARI MILITARI
13.1	Leva e servizio civile sostitutivo
13.2	Ruoli matricolari
13.3	Caserme, alloggi e servitù militari
13.4	Requisizioni per utilità militari
14	OGGETTI DIVERSI
15	AMMINISTRAZIONI SEPARATE DEI BENI DI USO CIVICO - ASUC
15.1	Organo di governo
15.2	Amministrazione generale
15.3	Risorse umane
15.4	Risorse finanziarie e patrimoniali
15.5	Gestione dei beni mobili strumentali all'attività dell'ASUC
15.6	Affari legali
15.7	Amministrazione e gestione di terreni e fabbricati di uso civico

15.8	Amministrazione e gestione delle strade forestali
15.9	Amministrazione e gestione del patrimonio boschivo e del legname

ALLEGATO E – Piano di sicurezza

Premessa

Il presente Piano di Sicurezza (PdS) è parte integrante del Manuale di gestione documentale del Consorzio BIM del Sarca Mincio Garda.

Lo scopo del documento è quello di poter stabilire, attuare, mantenere e migliorare in modo continuo la sicurezza delle informazioni.

La sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità delle informazioni mediante l'applicazione di un processo di gestione del rischio.

1. Il piano di sicurezza

Le Pubbliche Amministrazioni, nell'ottica di sviluppare concretamente il Sistema di gestione informatica dei documenti, predispongono "Il Piano di sicurezza" relativo alla formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici, nel rispetto delle misure minime di sicurezza. Il Responsabile della gestione documentale predispone il piano prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR). Il piano contiene altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali (data breach).

La sicurezza di un sistema informativo è da intendersi come:

- La protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali.
- La limitazione degli effetti causati dall'eventuale occorrenza delle cause sopraindicate.

La sicurezza informatica è una caratteristica globale in grado di fornire il desiderato livello di disponibilità, integrità e riservatezza dei dati, informazioni, documenti e dei servizi erogati.

Gli aspetti toccati dal documento sono la descrizione delle risorse e delle configurazioni del sistema informatico e delle politiche di sicurezza in essere.

1.1 Revisione e modifica del piano di sicurezza

L'Ente effettua la revisione del piano sicurezza ogni qualvolta si renda necessario al fine di assicurarne la continua idoneità, adeguatezza ed efficacia. Le modifiche al piano di sicurezza vengono approvate dall'Ente stesso.

1.2 Revisione e modifica delle politiche di sicurezza

Tutta la documentazione, ed in particolare le politiche di sicurezza, vengono riesaminate al verificarsi di cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

Il riesame comprende una valutazione delle opportunità di miglioramento delle politiche dell'organizzazione e dell'approccio alla gestione della sicurezza delle informazioni in risposta ai cambiamenti dell'ambiente organizzativo, dei servizi erogati, delle clausole legali o dell'ambiente tecnico.

Revisione delle politiche estemporanee vengono effettuate nei seguenti casi:

- verificarsi di incidenti di sicurezza;
- variazioni tecnologiche significative;
- modifiche all'architettura informatica;
- aggiornamenti delle prescrizioni normative;
- risultati delle eventuali attività di audit interni.

2. Componenti e configurazioni del sistema informatico

In questo paragrafo vengono descritte le risorse e le configurazioni in essere che compongono o supportano il sistema informatico.

Il Comune ha nominato un Amministratore di sistema, a cui è stata affidata la gestione del sistema informatico e della rete. I suoi compiti sono:
a) la gestione dei vari sistemi informatici presenti all'interno della rete: workstation, notebook, server, sistemi di backup, sistemi disponibili in rete, posta elettronica, sistemi di navigazione del web e filtraggio;
b) l'installazione di tutti i sistemi informatici e la definizione delle configurazioni necessarie al corretto funzionamento;
c) la verifica della corretta funzionalità dei sistemi informatici, l'esecuzione degli aggiornamenti di hardware e software, la riparazione di eventuali malfunzionamenti;
d) la gestione delle procedure di autenticazione e di autorizzazione da parte degli utenti, al fine di evitare accessi indesiderati dall'esterno;
e) l'implementazione e il controllo periodico delle misure minime di sicurezza e di backup, per evitare la perdita e la compromissione di dati che possono poi comportare un "data breach", progettando altresì le necessarie attività di supporto al "disaster recovery";
f) l'assistenza a tutti gli uffici in merito alle problematiche connesse all'uso dei sistemi informatici;
g) la verifica annuale della struttura informatica e la redazione di una relazione, per ciascun ente, al fine di identificare eventuali criticità e/o non conformità.

2.1 Caratteristiche di sedi e locali

Il Consorzio BIM Sarca Mincio Garda è composto dalla sede principale.

Le porte di ingresso agli uffici vengono chiuse quando non presidiate.

Il sistema antincendio è costituito da diverse componenti (rilevatori dei fumi, estintori, ecc.) regolarmente manutentati e tenuti in efficienza secondo le normative vigenti.

2.2 Locale CED e server

Il server è posizionato in un locale posto al piano rialzato dell'edificio, all'interno degli uffici consorziali, cui possono accedere solamente le persone autorizzate. Il server risulta essere sollevato dal pavimento in quanto posto su tavolino munito di ruote. Al server è collegato un display, tastiera e mouse al fine di agevolare le operazioni di manutenzione/consultazione.

L'Ente è inoltre dotato di gruppi di continuità dedicato, in modo da permettere la tenuta o lo spegnimento controllato dei dispositivi ad essi collegati in caso di mancanza di energia elettrica.

2.3 Connettività

La gestione della linea dati è affidata a Trentino Digitale spa, la quale gestisce integralmente la rete in fibra ottica Telpat della Provincia Autonoma di Trento, a cui l'Ente si collega. Trentino Digitale spa si occupa anche di supervisionare la rete e i tentativi di accesso esterni, in modo da prevenire eventuali accessi indesiderati.

2.4 Posta elettronica

Il servizio di posta elettronica è garantito da un fornitore locale. Le caselle di posta elettronica vengono consultate con protocollo IMAP e l'amministratore di sistema cura, per quanto di competenza, la configurazione del sistema. Gli aspetti di tenuta dell'infrastruttura e di continuità di servizio sono in carico al fornitore del servizio esterno.

2.5 Posta elettronica certificata

La casella di posta elettronica certificata (PEC) è gestita tramite un servizio di fornitura esterno in cloud. La casella, rilasciata dal fornitore accreditato, è direttamente integrata al sistema di protocollo informatico, quindi, il backup dei messaggi avviene seguendo il naturale percorso di integrazione con le procedure dell'ente.

La continuità operativa e la manutenzione del servizio sono gestite a livello contrattuale con il fornitore.

2.6 Sicurezza perimetrale

Il sistema informatico dell'Ente è protetto dal firewall (Fortinet) del fornitore del servizio Internet.

2.7 Sistemi di protezione da malware

Presso le postazioni di lavoro ed il server dell'Ente è installato e attivo un sistema antivirus.

Tale software viene gestito a livello centralizzato dall'Amministratore di sistema, che ne cura gli aggiornamenti, le installazioni sulle postazioni di lavoro e, sempre ad esso, vengono notificate le eventuali infezioni/minacce rilevate.

In occasione di criticità relativa a virus o malware, l'Amministratore di sistema adotta le azioni opportune.

2.8 Sistemi e politiche di backup

La gestione dei backup viene effettuata dall'Amministratore di sistema per ciò che riguarda i dati che risiedono presso l'Ente, e dai fornitori esterni per i servizi dati in concessione esterna o su cloud.

I backup vengono eseguiti dell'intera infrastruttura su NAS di rete e su supporti USB. Un incaricato si occupa della sostituzione mensile del supporto removibile in modo da avere dei backup off-line.

2.9 Accesso logico alle reti e ai sistemi

L'accesso alla rete può avvenire esclusivamente tramite un processo di autenticazione che prevede un nome utente ed una password. La password è composta da almeno otto caratteri alfanumerici essa non deve contenere riferimenti agevolmente riconducibili all'assegnatario.

L'Amministratore di sistema gestisce l'assegnazione delle password di accesso al sistema informatico.

Nome utente e password sono strettamente personali. L'utente è tenuto a:

- non comunicare a terzi la password
- a non annotare la password su supporti posti in vicinanza della propria postazione di lavoro o comunque incustoditi.

La password di accesso alla rete viene cambiata autonomamente ogni 3 mesi secondo quanto stabilito dalla normativa vigente.

In caso di assenza, anche temporanea, del personale incaricato dei trattamenti dei dati, sui pc devono essere chiuse le procedure di accesso ai dati o attivato il blocco attraverso lo screen saver con password.

Le credenziali di accesso ai sistemi informatici sono rilasciate su richiesta dell'Ente.

2.10 Sistemi di autenticazione

Gli utenti autorizzati accedono alle risorse informative dell'Ente tramite diversi livelli di autenticazione, a seconda dei privilegi autorizzativi che vengono loro rilasciati.

In generale, l'accesso alle postazioni di lavoro, ai sistemi di navigazione internet e ai documenti residenti sul file server (cartelle di rete condivise), viene disciplinato in fase di rilascio delle credenziali da parte

dell'Amministratore di sistema, previa apposita richiesta fatta pervenire dall'Ente, nella quale vengono specificate le funzioni dell'utente.

2.11 Modalità di accesso remoto

L'Amministratore di sistema si occupa della gestione e del controllo degli accessi effettuati da parte di terze parti e manutentori esterni del sistema informatico.

Le autorizzazioni di accesso vengono definite in sede contrattuale e vengono effettuate le apposite nomine in caso di accesso con profili di amministrazione.

Di volta in volta, in base alle specifiche attività da effettuare, l'Amministratore di sistema autorizza l'accesso alle risorse, fisiche e logiche, del sistema informatico con credenziali identificate e con livelli di autorizzazione minimi per l'attività che deve essere effettuata.

2.12 Telelavoro e smart working

La modalità del lavoro da remoto (sia in caso di telelavoro che di smart working) è abilitata in casi di emergenza o a seguito dell'attivazione di particolari progetti, per il periodo di tempo stabilito tra l'Ente ed il dipendente interessato. L'amministratore di sistema si occupa di predisporre strumenti di lavoro e connessioni adeguati e sicuri, su indicazione dell'Ente.

2.13 Inventario degli asset e postazioni di lavoro

Attraverso SW applicativo specifico in uso, le postazioni di lavoro vengono tenute in costante aggiornamento. L'Amministratore di sistema, periodicamente, segnalerà eventuali criticità e fornirà proposte, ove possibile, per l'aggiornamento delle stesse o, se si rileva uno stato di obsolescenza, suggerirà attività maggiormente incisive.

2.14 Notebook, smartphone e altri supporti mobili

Agli utenti possono essere forniti dispositivi mobili, quali: notebook, supporti di memorizzazione esterna mobili quali chiavette USB, dischi esterni, e altro.

La corretta gestione di questi strumenti, la custodia e le metodologie di protezione delle informazioni in esse contenute sono gestite dall'Ente stesso, attraverso adeguate azioni di informazione agli utenti finali sui rischi che possono occorrere nell'utilizzo di tali strumenti.

I notebook di proprietà dell'Ente sono crittografati, conformemente a quanto prevede la normativa in materia di sicurezza dei dati.

Tutti i supporti mobili, nel momento del non utilizzo, devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in un armadio/cassetto chiuso a chiave.

3. Privacy

L'Ente, a norma del Regolamento generale sulla protezione dei dati personali 679/2016 dell'Unione Europea, è Titolare dei dati personali, intesi come "….qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

I trattamenti di dati personali effettuati dall'Ente sono elencati nel Registro delle attività dei trattamenti e nella documentazione prodotta ai sensi del medesimo Regolamento.

I dati personali sono contenuti nella documentazione sia analogica che informatica prodotta e ricevuta dall'Ente che, in qualità di Titolare del trattamento dei dati stessi, è responsabile per quanto riguarda le decisioni in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. L'Ente dà attuazione al dettato del Regolamento 679/2016/UE con atti formali aventi rilevanza interna ed esterna quali le informative e le nomine a incaricato, a designato o a responsabile esterno per il trattamento dei dati.

L'Ente si organizza per garantire che i certificati e i documenti prodotti riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisiti o generati.

L’accesso agli atti nell’Ente è garantito secondo la normativa vigente in materia. Sul sito istituzionale dell’Ente, all’interno della sezione “Amministrazione Trasparente”, sono riportate le modalità di accesso, sia civico che generalizzato.

4. Data Breach

Il Consorzio BIM Sarca Mincio Garda ha attivato la procedura per la gestione della violazione dei dati personali (data breach) come da direttive prot. n. 1921 dd. 28.08.2020.

In tale documento, a cui si rimanda, sono indicati i passaggi e le comunicazioni da effettuare nel caso in cui si verifichi una possibile violazione dei dati personali.

5. Formazione del personale

Il personale dell’Ente è formato ed informato per quanto riguarda formazione, gestione, trasmissione, accesso e conservazione dei documenti. È inoltre aggiornato in tema di sicurezza sull’utilizzo del personal computer, sull’accesso alla rete e sui comportamenti da tenere per prevenire la diffusione di phishing, malware e virus.

L’eventuale attività formativa è svolta principalmente internamente e riguarda i seguenti aspetti:

- cultura generale sull’utilizzo del personal computer;
- cultura generale sull’utilizzo della rete;
- utilizzo di programmi di produttività individuale;
- utilizzo di programmi di posta elettronica;
- aggiornamento sui programmi di gestione documentali;
- tutela dei dati personali;
- adeguamento alle norme sulla protezione dei dati personali e alle relative direttive.