



Via Alberti 4 – 38033 CAVALESE  
tel. 0462-241311 fax 0462-241322 C.F. 91016130220

e-mail: [info@comunitavaldifiemme.tn.it](mailto:info@comunitavaldifiemme.tn.it)  
pec: [comunita@pec.comunitavaldifiemme.tn.it](mailto:comunita@pec.comunitavaldifiemme.tn.it)  
[www.comunitavaldifiemme.tn.it](http://www.comunitavaldifiemme.tn.it)

# **Manuale di Gestione del Protocollo Informatico**

della  
Comunità territoriale della val di fiemme  
(D.P.C.M. 3.12.2013 – art. 5)

Questo Manuale di Gestione è stato approvato con delibera di Comitato  
Esecutivo n. \_\_\_\_ del 10/05/2016

## INDICE GENERALE

<b>1</b>	<b>PREMESSA .....</b>	<b>5</b>
<b>2</b>	<b>RIFERIMENTI.....</b>	<b>5</b>
<b>3</b>	<b>PARTE PRIMA – PRINCIPI GENERALI .....</b>	<b>5</b>
3.1	PRINCIPI GENERALI DI GESTIONE DELLA DOCUMENTAZIONE AMMINISTRATIVA.....	5
3.2	IL SISTEMA DI GESTIONE DOCUMENTARIA DELL'AMMINISTRAZIONE.....	6
3.3	IL RUOLO DELLA TECNOLOGIA.....	6
3.4	AMBITO DI APPLICAZIONE DEL MANUALE.....	7
3.4.1	<i>Obiettivi e finalità del Manuale di Gestione .....</i>	<i>7</i>
3.5	DEFINIZIONI E GLOSSARIO .....	7
3.6	AREE ORGANIZZATIVE OMOGENEE E MODELLI ORGANIZZATIVI.....	10
3.6.1	<i>Strutture organizzative.....</i>	<i>10</i>
3.7	SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO.....	11
3.7.1	<i>Responsabile tecnico del protocollo informatico (amministratore di sistema).....</i>	<i>11</i>
3.7.2	<i>Responsabili del procedimento amministrativo.....</i>	<i>12</i>
3.7.3	<i>Utente protocollista.....</i>	<i>12</i>
3.8	CONSERVAZIONE DELLE COPIE DI RISERVA.....	12
3.9	FIRMA DIGITALE.....	12
3.10	TUTELA DEI DATI PERSONALI .....	12
3.11	CASELLE DI POSTA ELETTRONICA E INTEROPERABILITÀ.....	13
3.11.1	<i>La Posta Elettronica Certificata - PEC .....</i>	<i>13</i>
3.11.2	<i>Casella di posta istituzionale.....</i>	<i>13</i>
3.11.3	<i>Caselle di posta elettronica interne all'Amministrazione.....</i>	<i>13</i>
3.11.4	<i>Interoperabilità tra pubbliche amministrazioni.....</i>	<i>13</i>
3.12	SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI.....	14
3.13	FORMAZIONE .....	14
3.14	ACCREDITAMENTO DELL'AMMINISTRAZIONE/AOO ALL'IPA.....	14
3.15	PROCEDURE INTEGRATIVE DI CONSERVAZIONE SOSTITUTIVA .....	15
3.16	TIPI DI DOCUMENTO .....	15
3.16.1	<i>Documento amministrativo.....</i>	<i>15</i>
3.16.2	<i>Documento cartaceo .....</i>	<i>15</i>
3.16.3	<i>Documento informatico .....</i>	<i>16</i>
3.17	DISTINZIONE DEI DOCUMENTI IN BASE ALLO STATO DI TRASMISSIONE.....	16
<b>4</b>	<b>PARTE SECONDA – PROCEDURE DI GESTIONE DEI DOCUMENTI E DEI FLUSSI DOCUMENTALI.....</b>	<b>16</b>
4.1	IL REGISTRO DI PROTOCOLLO .....	16
4.2	LIVELLI ACCESSO INTERNO.....	17
4.3	UTENTE INTERNO ABILITATO ALLA CONSULTAZIONE .....	17
4.4	ELIMINIZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO.....	17
4.5	PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI .....	17
4.5.1	<i>Formazione dei documenti – Aspetti di sicurezza .....</i>	<i>17</i>
4.5.2	<i>Gestione dei documenti informatici .....</i>	<i>18</i>
4.5.3	<i>Trasmissioni e interscambio dei documenti informatici .....</i>	<i>18</i>
4.5.3.1	<i>All'esterno dell'AOO (Interoperabilità) .....</i>	<i>18</i>
4.5.3.2	<i>All'interno dell'AOO .....</i>	<i>19</i>
4.5.4	<i>Accesso ai documenti informatici .....</i>	<i>19</i>
4.5.5	<i>Conservazione di documenti informatici.....</i>	<i>19</i>
4.5.5.1	<i>Archivio di deposito .....</i>	<i>19</i>
4.5.5.2	<i>La selezione dei documenti .....</i>	<i>20</i>
4.5.5.3	<i>La conservazione dei documenti .....</i>	<i>20</i>
4.5.5.5	<i>Archivio storico .....</i>	<i>20</i>
4.5.6	<i>Backup dei dati .....</i>	<i>20</i>
4.5.7	<i>Politiche di sicurezza adottate dall'AOO.....</i>	<i>21</i>
4.5.7.1	<i>Politiche di uso accettabile del Sistema Informativo .....</i>	<i>21</i>
4.5.7.2	<i>Politiche di uso non accettabile del Sistema Informativo .....</i>	<i>21</i>

4.6	MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI	23
4.7	REGISTRAZIONE DEI DOCUMENTI	23
4.7.1	<i>Registrazione di protocollo e altre forme di Registrazione</i>	23
4.7.1.1	Registrazione di protocollo	23
4.7.1.2	Segnatura (timbro) di protocollo	24
4.7.1.3	Documenti soggetti a protocollazione	24
4.7.1.4	Annullamento o modifica di una registrazione di protocollo	24
4.7.1.5	Registrazioni differite (protocollo differito)	25
4.7.1.6	Registrazione con differimento dei termini di visibilità (riservatezza temporanea delle registrazioni di protocollo)	25
4.7.1.7	Registrazione di protocollo riservata	25
4.7.1.8	Operazioni particolari di registrazione di protocollo	25
4.8	DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI	27
4.8.1	<i>Documenti in arrivo</i>	27
4.8.1.1	Documenti cartacei	27
4.8.1.2	Documenti informatici in arrivo	28
4.8.2	<i>Documenti in partenza</i>	29
4.8.2.1	Redazione dei documenti	29
4.8.2.2	Documenti cartacei	30
4.8.2.3	Documenti informatici in partenza	30
4.8.3	<i>Documenti interni</i>	30
4.8.3.1	Registrazione di protocollo dei documenti interni	30
4.8.3.2	Trasmissione	31
4.8.4	<i>Flusso documentario tra Amministrazioni comunali aderenti a forme associative intercomunali per l'esercizio di funzioni e servizi</i>	31
4.8.5	<i>Assegnazione e presa in carico dei documenti</i>	31
4.8.5.1	Assegnazione dei documenti ricevuti in formato cartaceo o digitale	31
4.8.5.2	Modifica delle assegnazioni	31
4.9	REGOLE DI SMISTAMENTO E ASSEGNAZIONE DEI DOCUMENTI RICEVUTI	31
4.10	UNITÀ ORGANIZZATIVE RESPONSABILI DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI	31
4.11	ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE	32
4.11.1	<i>Documenti esclusi dalla protocollazione</i>	32
4.11.2	<i>Documenti soggetti a registrazione particolare</i>	33
4.12	SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE	33
4.12.1	<i>Classificazione</i>	33
4.12.1.1	Titolario di classificazione	33
4.12.1.2	Modifica del Titolario di classificazione	33
4.12.2	<i>Massimario di selezione</i>	33
4.12.3	<i>FASCICOLI</i>	33
4.12.3.1	Fascicolo e fascicolazione	33
4.12.3.2	Tipologie di fascicolo	34
4.12.3.3	Fascicoli relativi a procedimenti, affari ed attività amministrative	34
4.12.3.4	Fascicoli del personale	34
4.12.4	<i>Formazione e gestione dei fascicoli</i>	34
4.12.5	<i>Apertura e repertorizzazione del fascicolo</i>	34
4.12.6	<i>Gestione periodica dei fascicoli</i>	34
4.12.6.1	Copertina ("camicia") del fascicolo	34
4.12.7	<i>Inserimento dei documenti nel fascicolo</i>	35
4.12.8	<i>Trasferimento del fascicolo</i>	35
4.12.9	<i>Chiusura del fascicolo</i>	35
4.13	FORMAZIONE E GESTIONE DELLE SERIE DI UNITA' DOCUMENTARIE E FASCICOLI – NOZIONI DI SERIE ARCHIVISTICA	35
4.14	MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO	35
4.15	DESCRIZIONE FUNZIONALE E OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO	35

4.15.1	<i>Identificazione</i> .....	36
4.15.2	<i>Cambio password e blocco delle credenziali</i> .....	36
4.15.3	<i>Firma dei documenti e impronta informatica</i> .....	36
4.16	RILASCIO DELLE ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI .....	37
4.17	MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA.....	37
4.18	APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI...	37
4.18.1	<i>REGOLAMENTI ABROGATI</i> .....	38
4.18.2	<i>PUBBLICITÀ DEL PRESENTE MANUALE</i> .....	38
4.18.3	<i>OPERATIVITÀ DEL PRESENTE MANUALE</i> .....	38
4.19	ALLEGATI .....	38

# 1 PREMESSA

Questo documento è il Manuale di Gestione del Protocollo Informatico della **Comunità territoriale della val di fiemme**, ed è stato adottato dall'Ente ai sensi degli artt. 52 e seguenti del D.P.R. 28.12.2000 n. 445 e s.m. (Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), degli artt. 40 e seguenti del D.Lgs. 7.3.2005 n. 82 e s.m. (Codice dell'Amministrazione Digitale) e degli artt. 3 e seguenti del DPCM del 3.12.2013 (Regole tecniche per il protocollo informatico ai sensi degli articoli 40 bis, 41, 47, 57 bis e 71 del C.A.D. di cui al D.Lgs. n. 82 del 2005).

Il Manuale di gestione è suddiviso in due parti:

- La Prima Parte, che descrive i principi generali propri delle attività trattate da questo Manuale
- La Seconda Parte, che entra nel dettaglio del sistema di protocollo informatico adottato; in particolare la sezione 4.15 "Descrizione funzionale e operativa del sistema di protocollo informatico" contiene una breve guida all'uso delle funzionalità base del Sistema Informatico adottato.

# 2 RIFERIMENTI

Questo capitolo contiene l'insieme dei riferimenti normativi che nel testo del documento sono istanziati. La scelta di concentrare i riferimenti normativi in un'unica sezione è stata dettata dall'esigenza di leggibilità del documento e dalla necessità di avere uniformità di descrizione dei riferimenti legislativi/normativi.

La consultazione dei documenti è resa possibile dalla disponibilità di tali documenti nell'ambito del sito "Normattiva" il cui link è: <http://www.normattiva.it/static/index.html>, accedendo alla funzione di ricerca e inserendo gli estremi del documento è possibile visualizzare la norma, la legge o il decreto nella sua versione attuale, verificando inoltre la sua vigenza alla data di consultazione.

[1] Art. 61, comma 1 del DPR 445/2000

[2] Art. 3, comma 1 lettera b e art. 5 del DPCM 3 dicembre 2013

[3] Art. 22, della legge n. 241 del 7 agosto 1990

[4] Art. 12, comma 2, lettera c del DPCM 3 dicembre 2013

[5] Direttiva del 27 novembre 2003 del Ministero per l'Innovazione e le Tecnologie - "Impiego della posta elettronica nelle pubbliche amministrazioni"

[6] ex art. 2, comma 1, lettera a) D.lgs. 10/2002

[7] Dlgs. N. 196 del 30 giugno 2003

[8] Art. 1 del DPR 445/2000

[9] ex art. 20, comma 1 D.lgs. 82/2005

[10] Art. 50 del DPR 445/2000

[11] ex art. 43, comma 5, DPR 445/2000

[12] Accordi contrattuali Informatica Trentina – Enti aderenti al Protocollo Federato P.I.Tre

# 3 PARTE PRIMA – PRINCIPI GENERALI

## 3.1 Principi generali di gestione della documentazione amministrativa

Ai sensi di quanto previsto dall'articolo riferito in [11] tutte le pubbliche amministrazioni devono provvedere a realizzare o revisionare i propri sistemi di gestione documentaria prevedendo l'introduzione del protocollo informatico.

Gli obiettivi specifici di un sistema di gestione documentario possono essere ricondotti ai seguenti:

- La produzione e acquisizione di documenti attendibili a fini giuridici e a fini amministrativi;
- L'organizzazione e la tenuta dei documenti in modo ordinato e coerente alle funzioni esercitate;
- La trasmissione e conservazione di documenti autentici, cioè integri e di provenienza certa ed identificata;
- La rapidità e l'efficienza del reperimento delle informazioni nell'ambito dell'attività amministrativa svolta.

Per la corretta e regolare sedimentazione dei documenti prodotti e acquisiti sono necessarie regole, procedure e strumenti finalizzati a:

- Determinare i criteri e le modalità di produzione/acquisizione dei documenti e garantire l'identificazione della provenienza (attraverso registrazioni di protocollo o altri strumenti di registrazione);
- Organizzare l'ordinata sedimentazione dei documenti in rapporto alle attività amministrative cui partecipano (attraverso l'osservanza di corrette pratiche di fascicolazione);
- Conservare e trasmettere i documenti in modo sicuro, escludendo i rischi di manipolazione e dispersione (controllo sulla movimentazione, controllo sulle attività di acquisizione e spedizione dei documenti e sui flussi documentari interni, controllo sulle attività di trasferimento dei documenti tra le diverse sezioni dell'archivio, definizioni di responsabilità per la tenuta e il trattamento dei documenti, ecc.).

### 3.2 Il sistema di gestione documentaria dell'amministrazione

Il sistema di gestione documentario non si riferisce quindi solo all'insieme dei documenti prodotti o acquisiti dall'Amministrazione, ma include anche le regole, le procedure e le risorse (umane e strumentali) destinate per la formazione, l'organizzazione, il reperimento, l'utilizzo e la conservazione dei documenti. In ultima analisi, è quel sistema che garantisce il controllo generale e sistematico da parte dell'Ente sulla propria documentazione amministrativa.

La definizione di sistema documentario coinvolge almeno tre aspetti fondamentali:

- Il sedimento documentario dell'attività amministrativa nelle sue diverse forme di aggregazione ovvero singoli documenti, fascicoli, registri, serie, l'archivio nel suo complesso;
- Gli strumenti di gestione archivistica (registro di protocollo, Titolario di classificazione, repertorio dei fascicoli);
- L'organizzazione dei flussi di lavoro e della documentazione con particolare riferimento alle responsabilità proprie delle risorse umane e strumentali dell'amministrazione.

### 3.3 Il ruolo della tecnologia

Grazie alle novità introdotte dall'innovazione tecnologica, il sistema di gestione documentaria può essere sviluppato fino a integrarsi con strumenti nati con finalità diverse (organizzative, gestionali, informative ecc.), costituendo una risorsa strategica in termini di efficienza dell'azione amministrativa.

Grazie alle potenzialità tecnologiche il sistema di gestione documentaria così concepito è in grado di garantire:

- L'integrità dei documenti e delle informazioni in essi contenute;
- L'attestazione dell'avvenuta acquisizione o produzione di tutti i documenti all'interno del complesso documentario dell'Amministrazione attraverso l'attribuzione automatica di un codice univoco di identificazione mediante la registrazione di protocollo o mediante altre forme di registrazione comunque definite;
- L'ordinata sedimentazione di tutti i documenti comunque prodotti o acquisiti dall'Amministrazione mediante l'attribuzione di un indice di classificazione che rispecchi logicamente le funzioni da essa istituzionalmente esercitate e che si riverberi nella coerente aggregazione fisica dei documenti mediante l'attività di fascicolazione e formazione di serie documentarie;
- la conservazione dei documenti nel tempo, con particolare riferimento alle attività di riversamento dei dati, attuate allo scopo di garantire la fruibilità duratura dei documenti formati su supporto elettronico;
- l'individuazione e la selezione dei documenti non destinati alla conservazione permanente
- lo sviluppo delle potenzialità informative dei documenti mediante l'utilizzo di strumenti di ricerca informatici;
- l'ottimizzazione dell'intero ciclo di vita e di trattamento del documento;
- la gestione automatizzata dei procedimenti amministrativi e dei flussi di lavoro.

La normativa sul protocollo informatico delinea inoltre uno scenario in cui l'utilizzo di nuovi strumenti tecnologici (firma digitale, posta elettronica certificata, ecc.) diviene elemento essenziale del nuovo sistema documentario.

### 3.4 AMBITO DI APPLICAZIONE DEL MANUALE

#### 3.4.1 Obiettivi e finalità del Manuale di Gestione

Il “Manuale di gestione del protocollo informatico, flussi documentari e archivio” (d’ora in avanti Manuale) risponde agli obblighi normativi sanciti dall’art.5 del DPCM 3 dicembre 2013, che impone alle pubbliche amministrazioni l’adozione di uno strumento che ne descriva e ne regolamenti il sistema di gestione documentario, con particolare riferimento alla procedure relative alla formazione, all’acquisizione, alla tenuta, all’accesso, alla consultabilità e alla conservazione dei documenti sia informatici che cartacei, individuando nel contempo per ogni azione o processo i livelli di esecuzione, responsabilità e controllo.

Il Manuale disciplina quindi 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’Ente. È pertanto rivolto a tutti i dipendenti, quale strumento di lavoro e di riferimento.

Specificamente il Manuale descrive

- Il modello organizzativo di gestione documentaria adottato
- Le modalità di acquisizione/produzione dei documenti
- Le operazioni connesse alla registrazione di protocollo
- Il sistema di classificazione e fascicolazione dei documenti
- La gestione dei documenti presso gli archivi correnti
- Le operazioni di versamento dei documenti e dei fascicoli presso l’archivio di deposito
- Le modalità di accesso ai documenti
- La definizione delle linee strategiche legate al sistema archivistico ed al sistema di flusso di lavoro e delle procedure ad esso collegate.
- I requisiti di sicurezza del sistema di gestione documentario.

Il sopra citato DPCM prevede che la responsabilità del sistema di gestione documentario sia affidato ad uno specifico “servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi”. Al Servizio è demandata la responsabilità dell’applicazione del presente Manuale.

Gli aggiornamenti sono approvati con deliberazione della Giunta.

### 3.5 DEFINIZIONI E GLOSSARIO

Ai fini del presente Manuale si definiscono:

- “amministrazione” la **Comunità territoriale della val di fiemme**, di seguito indicata come **COMUNITA'**;
- “Testo Unico”, il decreto del presidente della Repubblica 20 dicembre 2000 n. 445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- “Regole tecniche”, il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell’Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005;
- “Codice”, il decreto legislativo 7 marzo 2005 n. 82 – Codice dell’amministrazione digitale;

Nel seguito si riportano definizioni e acronimi utilizzati più frequentemente nel testo:

**Allegato:** documento unito a un documento o a una pratica per prova, per chiarimento o integrazione di notizie, per memoria.

**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:** la possibilità per un utente abilitato (specificatamente il responsabile del protocollo informatico) di annullare una registrazione di protocollo.

**AOO (Area Organizzativa Omogenea):** insieme definito di unità organizzative di una 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.

**Archivio:** il complesso dei documenti prodotti o comunque acquisiti da un ente durante lo svolgimento della propria attività. A fini gestionali l’archivio si 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 quaranta anni; *archivio storico*, per la parte di documenti relativi ad affari esauriti da oltre quaranta 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.

**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'A.O.O., per la ricezione dall'esterno e per la spedizione all'esterno dei documenti da registrare a protocollo.

**Certificato elettronico:** attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche.

**Certificatore:** soggetto che presta servizi di certificazione delle firme elettroniche/digitali o che fornisce altri servizi connessi con queste ultime.

**Copia:** riproduzione di un documento originale. Non ha valore giuridico. La copia ha valore giuridico e si definisce autentica o autenticata quando è emessa da un ente che può rilasciare copie conformi all'originale e reca segni di autenticazione.

**Deposito:**

1. Locale nel quale un ente conserva la propria documentazione non più occorrente alla trattazione degli affari in corso.
2. Operazione con cui gli enti pubblici trasferiscono la propria documentazione anteriore all'ultimo quarantennio nei competenti archivi.

**Documento informatico:** rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti.

**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 di forza e 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.

**Elenco di versamento:** strumento di corredo che descrive in modo sintetico le unità archivistiche (cfr.) facilitandone la ricerca. Ogni trasferimento o versamento di fascicoli e registri è accompagnato da un apposito elenco.

**Fascicolo:** insieme dei documenti relativi ad una determinata pratica, attività, affare o persona, collocati, all'interno di una camicia (o 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:** insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

**Flusso documentario:** insieme delle attività finalizzate alla gestione della documentazione prodotta o acquisita; dalla registrazione e segnatura di protocollo, alla classificazione, organizzazione, assegnazione e reperimento e conservazione di tutti i documenti, compresi quelli non soggetti a registrazione di protocollo, nell'ambito del sistema di classificazione d'archivio adottato.

**Gestione dei documenti:** insieme delle attività finalizzate alla registrazione di protocollo, alla classificazione, alla fascicolazione, all'assegnazione, al reperimento, alla conservazione, all'accesso e alla 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 del sistema informativo e dei flussi di lavoro (workflow) di un ente.

**Gestione documentale:** vedi *Sistema di gestione informatica dei documenti*.

**Inserimento:** la possibilità per un utente abilitato di inserire i dati e provvedere ad una registrazione di protocollo.

**Interoperabilità:** possibilità di trattamento automatico, da parte del sistema di protocollo ricevente, delle informazioni trasmesse dal protocollo mittente, allo scopo di automatizzare le attività e i procedimenti amministrativi conseguenti.

**Massimario di selezione:** strumento che consente di coordinare razionalmente lo scarto archivistico (cioè la destinazione al macero) dei documenti prodotti da un ente. Il massimario riproduce l'elenco delle partizioni (titoli) e sottopartizioni (classi) del Titolare di classificazione con una descrizione più o meno dettagliata delle competenze cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascuna partizione quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nell'archivio storico) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc.

**Modifica:** la possibilità per un utente abilitato di modificare i dati gestionali di una registrazione di protocollo, con l'esclusione dei dati obbligatori.



**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 è scritto sul documento nello spazio apposito e deve essere riportato sia sul registro di protocollo dell'ente che scrive sia quello dell'ente che riceve il documento.

**Originale:** è la stesura definitiva del documento, perfetto nei suoi elementi sostanziali e formali.

**Piano di conservazione:** strumento che definisce i criteri di organizzazione, di selezione periodica e di conservazione permanente dei documenti, redatto ed integrato col sistema di classificazione adottato.

**PdP:** Prodotto 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, e idoneo a produrre effetti giuridici a favore o a danno delle parti. Ai sensi del DPR 445/2000 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 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, deliberi di un organo collegiale, contratti, ecc.) indipendentemente dall'oggetto trattato. Ai sensi del DPR 445/2000 tale forma di registrazione ha valore giuridico-probatorio ed è da ritenersi alternativa alla registrazione di protocollo.

**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.

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

**Scarto:** operazione con cui si destina al macero una parte dei documenti di un archivio.

**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 è posta di norma sul *recto* del documento medesimo mediante l'apposizione del timbro di protocollo. Non è invece indispensabile il timbro sul documento in partenza o sul documento interno, in quanto i dati della registrazione sono apposti direttamente dal RPA (cfr.) secondo le consuetudini e l'impostazione grafica della carta intestata.

**Selezione:** individuazione dei documenti da destinare alla conservazione permanente o, qualora ritenuti inutili, allo scarto (cfr.), effettuato periodicamente e comunque prima del passaggio dei fascicoli all'archivio storico. La proposta di scarto è subordinata alla preventiva autorizzazione della Soprintendenza archivistica territorialmente competente.

**Servizio archivistico:** servizio per la gestione informatica dei documenti, del protocollo, dei flussi documentari e degli archivi.

**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 la 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 desidera 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; il collegamento dei documenti alla gestione dei procedimenti; A queste può aggiungersi la: realizzazione di un 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 una indicizzazione più dettagliata, ecc.).

3. *workflow documentario*: tale livello può prevedere una o più delle seguenti attività: informatizzazione dei processi relativi ai flussi documentali in entrata; informatizzazione dei processi relativi ai flussi documentali in uscita; informatizzazione dei processi relativi ai flussi documentali interni.
4. *Business Process Reengineering (BPR)*: quest'ultimo livello prevede la reingegnerizzazione dei processi dell'ente al fine di una loro successiva informatizzazione: in particolare sono 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.

**Sottofascicolo**: insieme organico di documenti contenuti in un fascicolo di cui rappresenta una sottopartizione. Ciascun sottofascicolo è iscritto nel repertorio dei fascicoli (cfr.) 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 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 in maniera omogenea a seconda degli oggetti cui si riferiscono.

**Trasferimento**: è l'operazione con cui periodicamente (di solito una volta l'anno) i documenti non più necessari al disbrigo degli affari correnti sono trasferiti nell'archivio di deposito.

**Unità Organizzativa Responsabile (UOR)**: Servizio/Ufficio al quale afferisce il RPA (cfr.), previsto dall'art. 4 della legge 7 agosto 1990, n. 241.

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

**Unità Organizzativa di Protocollo (UOP)**: ufficio che svolge attività di registrazione di protocollo.

**Ufficio Utente (UU)**: un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

**Versamento**: è l'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.

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

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

Le Norme e i Regolamenti di riferimento sono elencati nel paragrafo 2 Riferimenti.

## 3.6 AREE ORGANIZZATIVE OMOGENEE E MODELLI ORGANIZZATIVI

### 3.6.1 Strutture organizzative

Per la gestione dei documenti, l'amministrazione individua **un'unica Area Organizzativa Omogenea (AOO)** denominata **COMUNITA'** che è composta dall'insieme di tutti gli UOP/UOR/UU. In particolare il sistema di gestione documentario si basa sul modello organizzativo della COMUNITA'.

Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, con una postazione di protocollo autorizzata alla scannerizzazione e allo smistamento dei documenti.

All'interno della AOO il sistema di protocollazione è **centralizzato** per la corrispondenza in ingresso, mentre è **decentralizzato** per la corrispondenza in uscita, per mezzo delle **Unità Organizzative Responsabile (UOR)** che all'interno dell'ente sono attualmente le seguenti:

- **Servizio Affari Generali;**
- **Servizio finanziario;**
- **Servizio personale;**
- **Servizio tecnico;**
- **Servizio attività socio-assistenziali.**

La stazione principale di protocollazione prende il nome di **Protocollo Centrale**, e nel caso specifico è individuato nel UOR **Servizio Affari Generali**.

Le **UOR** si articolano in **Unità Organizzative di protocollazione (UOP)** (ovvero gli uffici quelli che sono abilitati a svolgere attività di registrazione di protocollo in uscita), e in **Uffici Utente (UU)**.

Le strutture organizzative sono suscettibili di modifica, in caso di inserimento di nuove (AOO)/UOP/UOR/UU o di riorganizzazione delle medesime.

Le modifiche sono proposte ai vertici dell'amministrazione dal RSP d'intesa con il responsabile del sistema informativo e con il responsabile della tutela dei dati personali.

L'amministrazione si riserva la facoltà di autorizzare, in via transitoria e del tutto eccezionale, altri UOR allo svolgimento dell'attività di protocollazione.

Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente manuale e sarà sottoposto al controllo del Responsabile del Protocollo Informatico.

Nelle UOR sarà utilizzato il medesimo sistema di numerazione di protocollo e l'operatore o gli operatori incaricati dell'attività di protocollazione dovranno essere abilitati dal RSP che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

### 3.7 SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO

Nella AOO individuata dall'Ente, è istituito il servizio per la gestione del protocollo informatico, dei flussi documentari e degli archivi, denominato "**Servizio protocollo e archivio**" (d'ora in avanti **Servizio**), ai sensi di quanto riferito in [1], alla cui guida è nominato il **Responsabile del Servizio di Protocollo informatico (RSP)**, funzionalmente individuato nel **Segretario** dell'Ente.

Il **Servizio** svolge funzioni di:

- Coordinamento e di presidio per tutte le componenti dell'Amministrazione, esclusivamente per quanto attiene il Protocollo e l'Archivio di deposito storico
- Coordinamento della gestione del protocollo
- Sorveglianza sulla corretta formazione e tenuta degli archivi correnti e (ovvero dei fascicoli e dei registri conservati presso ciascun ufficio dell'Amministrazione)
- provvede alla tenuta dell'archivio di deposito dell'Ente.

In particolare il **Servizio**:

- Gestisce direttamente ed organizza la gestione del protocollo informatico in merito ai seguenti aspetti:
  - Amministrazione delle anagrafiche e dei profili di accesso al sistema;
  - Garanzia della correttezza delle operazioni di registrazione e segnatura dei documenti;
  - Gestione delle situazioni di anomalia dovute a guasti del sistema informatico, compresa la gestione del registro di emergenza;
  - Garanzia della corretta applicazione delle procedure di sicurezza;
- Cura l'adozione e l'aggiornamento del Titolario di classificazione e del Manuale;
- Cura l'adozione e l'aggiornamento del piano di conservazione dei documenti;
- Gestisce le operazioni connesse al trasferimento, al versamento e alla movimentazione dei documenti nell'archivio corrente, in quello di deposito e nell'archivio storico.

È responsabilità del Segretario:

- Autorizzare le operazioni di annullamento di numeri di protocollo e del relativo documento;
- Assicurare che sia individuato il Responsabile Tecnico del protocollo informatico (amministratore di sistema), assicurandosi che il soggetto individuato possieda le competenze necessarie ad assolvere tale ruolo;
- Individuare gli operatori di protocollo e i loro sostituti, attribuendo; il livello di autorizzazione di ciascun addetto all'accesso alle funzioni delle procedure applicative di gestione del protocollo informatico e gestione documentale distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento, alla modifica e alla cancellazione delle informazioni.

Il **Servizio** è articolato in

- Servizio di protocollo
- Archivio di deposito e storico

#### 3.7.1 Responsabile tecnico del protocollo informatico (amministratore di sistema)

Il Responsabile Tecnico del protocollo informatico è la figura che ha la possibilità di svolgere operazioni straordinarie sul sistema. In particolare, fra l'altro:

- Ripristino del sistema a seguito di eventuali interruzioni
- Monitoraggio delle operazioni compiute

- Predisposizione delle autorizzazioni di accesso al sistema per gli utenti nell'ambito dell'AOO
- Il responsabile tecnico risponde funzionalmente al Responsabile del Servizio di Protocollo. La funzione viene svolta da ditta esterna, cui è affidato anche l'incarico di Amministratore di sistema.

### 3.7.2 Responsabili del procedimento amministrativo

Spetta ai responsabili delle UOR in cui si articola l'amministrazione, individuare i responsabili dei procedimenti amministrativi (RPA) e collaborare con il Responsabile del Servizio di Protocollo per gli adempimenti previsti dalla gestione dei documenti dell'Amministrazione.

I RPA hanno specificamente il compito di

- Costituire e gestire i fascicoli e le serie documentarie che fanno riferimento ad affari in corso di trattazione;
- Curare l'accesso interno ed esterno alla documentazione affidata loro in carico;
- Collaborare con il **Servizio** per il trasferimento in archivio di deposito della documentazione relativa ad affari esauriti.

### 3.7.3 Utente protocollista

L'Utente protocollista è la figura incaricata di effettuare le operazioni di registrazione di protocollo o le altre forme di registrazione dei documenti previste dal presente Manuale.

Gli Utenti protocollisti sono collocati presso il **Protocollo Centrale** e presso le UOP abilitate.

## 3.8 CONSERVAZIONE DELLE COPIE DI RISERVA

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della giornata lavorativa, va riversato, nel rispetto della normativa vigente, su supporti informatici non riscrivibili ed è in carico ad Informatica Trentina spa che eroga il servizio di protocollo informatico in modalità ASP.

## 3.9 FIRMA DIGITALE

La normativa distingue diverse modalità di sottoscrizione dei documenti informatici. Ciascuna modalità fa riferimento a differenti varianti normative della "firma elettronica" e conferisce alla "firma" stessi livelli di efficacia probatoria.

In generale per "firma elettronica" si intende un "insieme dei dati in forma elettronica correlati in vario modo ad altri dati elettronici in maniera tale da creare un sistema di autenticazione informatica" (Rif. [6]). Le varianti possibili previste dalla normativa vigente sono: la "firma elettronica avanzata", la "firma elettronica qualificata" e la "firma digitale".

Ai sensi della normativa vigente, solo il documento informatico, sottoscritto con firma digitale, soddisfa il requisito legale della forma scritta ed ha rilevanza probatoria, è assimilato cioè ad un documento cartaceo sottoscritto con firma autografa.

In pratica il documento dotato di firma digitale consente di soddisfare i requisiti di:

- *Autenticità* (con un documento firmato digitalmente si può essere certi dell'identità del sottoscrittore);
- *Integrità* (si ha la sicurezza che il documento informativo non sia stato modificato dopo la sua sottoscrizione);
- *Non ripudiabilità* (il documento ha piena validità legale e non può essere ripudiato dal sottoscrittore).

Il Sistema Informatico adottato dall'Ente rende disponibile la funzione di Firma Digitale.

## 3.10 TUTELA DEI DATI PERSONALI

La Comunità, titolare dei dati di protocollo e dei dati personali – comuni, sensibili e/o giudiziari – contenuti nella documentazione amministrativa di propria pertinenza dà attuazione al dettato del decreto legislativo riferito in [7] con atti formali aventi rilevanza interna ed esterna.

- Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, sono stati incaricati dal titolare dei dati e, se nominato, dal responsabile.
- Relativamente agli adempimenti esterni, la Comunità si è organizzata per garantire che i certificati e i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per le sole finalità per le quali sono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui sono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente.

Le regole e le modalità operative stabilite dalla Comunità sono riportate nel Cap. 4.5 "PIANO DI SICUREZZA" a cui si rimanda.

In relazione alla protezione dei dati personali trattati al proprio interno, la Comunità dichiara di aver ottemperato a quanto previsto dal decreto legislativo riferito in [7] con particolare riferimento:

- Al principio di necessità nel trattamento dei dati;
- Al diritto di accesso ai dati personali da parte dell'interessato
- Alle modalità del trattamento e ai requisiti dei dati
- All'informativa fornita agli interessati e al relativo consenso quando dovuto;
- Alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- Alle misure minime di sicurezza.

### 3.11 CASELLE DI POSTA ELETTRONICA E INTEROPERABILITÀ

#### 3.11.1 La Posta Elettronica Certificata - PEC

La 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 venga conservata per un periodo di tempo definito a cura dei gestori, con lo stesso valore giuridico delle ricevute.

#### 3.11.2 Casella di posta istituzionale

L'indirizzo della casella di **posta elettronica certificata** è: **comunita@pec.comunitavaldifiemme.tn.it**

Il responsabile del **Servizio** provvede a rendere pubblico l'indirizzo della casella di posta istituzionale e a riportarlo nell'Indice delle amministrazioni gestito dalla Agenzia per l'Italia Digitale ai sensi dell'articolo riferito in [4]

#### 3.11.3 Caselle di posta elettronica interne all'Amministrazione

In attuazione di quanto stabilito dalla Direttiva riferita in [5] l'Amministrazione ha dotato tutti i dipendenti di una casella di posta elettronica.

#### 3.11.4 Interoperabilità tra pubbliche amministrazioni

Nell'ambito di una comunicazione tra differenti amministrazioni (ovvero tra Aree Organizzative Omogenee della stessa Amministrazione) due sistemi di protocollo interoperano quando è consentito al sistema ricevente di trattare automaticamente le informazioni trasmesse dal sistema mittente, al fine di automatizzare le attività e i processi amministrativi sottostanti.

Le condizioni necessarie all'interoperabilità tra Aree Organizzative Omogenee sono:

- L'istituzione di una casella di Posta Elettronica Certificata istituzionale per ogni Area Organizzativa Omogenea in cui si articola un'Amministrazione;
- L'istituzione di un Indice delle Pubbliche Amministrazioni e delle Aree Organizzative Omogenee presso un ente centrale; tale indice è reperibile in <http://www.indicepa.gov.it/>
- Lo scambio di dati strutturati tramite un file in formato standard allegato al messaggio.

L'istituzione di una casella di Posta Elettronica Certificata istituzionale consente agli enti di raggiungere e di farsi raggiungere dalle comunicazioni che provengono da altre amministrazioni.

L'indice centralizzato che raggruppa gli indirizzi di posta elettronica istituzionale facilita le comunicazioni tra enti.

La strutturazione dei dati sulla base di standard tecnici predefiniti (standard XML) rende possibile e automatica l'interpretazione delle comunicazioni tra pubbliche amministrazioni.

### 3.12 SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI

Per l'operatività del protocollo, viene utilizzato all'interno della AOO dell'amministrazione, il **Titolario di classificazione** approvato con delibera Giunta Provinciale n. 2957 del 27 dicembre 2012 (Allegato 1).

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

### 3.13 FORMAZIONE

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni dalla direttiva del Ministro della funzione pubblica sulla formazione e valorizzazione del personale delle pubbliche amministrazioni, l'amministrazione ha stabilito percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.

Tali iniziative formative, che afferiscono in particolare ai temi:

- Processi di semplificazione e innovazioni procedurali inerenti alla protocollazione e all'archiviazione dei documenti della AOO
- Strumenti e tecniche per la gestione digitale delle informazioni, con particolare riguardo alle politiche di sicurezza definite dall'Amministrazione/AOO
- Norme sulla protezione dei dati personali e alle direttive impartite con il documento programmatico della sicurezza

trovano la loro attuazione nell'ambito delle attività di diffusione del Protocollo Informatico Trentino – P.I.Tre, gestito da Informatica Trentina e a cui l'Ente ha aderito. In particolare gli argomenti di cui sopra sono oggetto di specifiche presentazioni nel corso delle attività di avviamento e di affiancamento all'uso del Sistema Informatico P.I.Tre.

### 3.14 ACCREDITAMENTO DELL'AMMINISTRAZIONE/AOO ALL'IPA

Ai sensi di quanto disposto dal rif. [4] l'Amministrazione/AOO si dota di una casella di Posta Elettronica Istituzionale attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della UOP incaricata; la UOP medesima provvede alla lettura quotidiana (almeno una volta al giorno), della corrispondenza ivi pervenuta e adotta gli opportuni metodi di conservazione in relazione alle varie tipologie di messaggi e ai tempi di conservazione richiesti.

L'Amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA), raggiungibile al link <http://indicepa.gov.it/>, tenuto e reso pubblico dalla Agenzia per l'Italia Digitale, fornendo le seguenti informazioni che individuano l'amministrazione stessa e le AOO in cui è articolata:

- La denominazione dell'amministrazione
- Il codice identificativo proposto per l'amministrazione
- L'indirizzo della sede principale dell'amministrazione
- L'elenco delle proprie Aree Organizzative Omogenee con l'indicazione:
  - Della denominazione
  - Del codice identificativo
  - Della casella di posta elettronica
  - Del nominativo del RSP
  - Della data di istituzione
  - Della eventuale data di soppressione
- L'elenco degli UOR e degli UU dell'A OO.

Il codice identificativo dell'amministrazione, eventualmente associato a ciascuna delle proprie AOO, è costituito dal Codice **ctvf\_tn**.

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

L'amministrazione comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività l'amministrazione comunica la soppressione ovvero la creazione di una AOO.

L'Amministrazione a cui questo Manuale di Gestione appartiene è identificata presso IPA come:

Dati Amministrazione	
Nome Esteso (Nome della Amministrazione Pubblica)	COMUNITA' TERRITORIALE DELLA VAL DI Fiemme
Categoria (Es. Comuni, Regioni, Altri Enti)	ALTRI ENTI
Provincia Sede Legale	TRENTO
Città Sede Legale	CAVALESE
Indirizzo Sede Legale	VIA ALBERTI 4
CAP Sede Legale	38033
Sito Web Istituzionale	<a href="http://WWW.COMUNITAVALDIFIEMME.TN.IT">WWW.COMUNITAVALDIFIEMME.TN.IT</a>
Indirizzo mail PEC	<b>comunita@pec.comunitavaldifiemme.tn.it</b>
Altro indirizzo mail istituzionale	INFO@COMUNITAVALDIFIEMME.TN.IT
Dati Responsabile	
Nome del Responsabile	MARIO
Cognome del Responsabile	ANDRETTA
Funzione del Responsabile	SEGRETARIO GENERALE

### 3.15 PROCEDURE INTEGRATIVE DI CONSERVAZIONE SOSTITUTIVA

Per l'esecuzione del processo di conservazione sostitutiva dei documenti l'amministrazione si uniforma alle modalità previste dalla deliberazione CNIPA n. 11/2004 e dal DPCM 3.12.2013 (Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71 comma 1 del C.A.D. di cui al D.Lgs. n. 82 del 2005).

Prima di adottare eventuali accorgimenti e procedure integrative, anche successivamente all'avvio del processo di conservazione sostitutiva dei documenti, l'amministrazione comunica al CNIPA (ora Agenzia per l'Italia Digitale) le procedure integrative che intende eventualmente adottare ai sensi dell'art. 7 della citata deliberazione.

### 3.16 TIPI DI DOCUMENTO

#### 3.16.1 Documento amministrativo

Per documento amministrativo si intende ogni rappresentazione grafica, fotocinematografica, informatica o di qualsiasi altra specie del contenuto di atti, fatti cose giuridicamente rilevanti, anche interni, prodotti e acquisiti ai fini dell'attività amministrativa, così come prevede l'articolo di legge riferito in [8]

Un documento amministrativo è dunque una rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa, così come prevede l'articolo riferito in [8]

#### 3.16.2 Documento cartaceo

Per documento cartaceo si intende tutta la documentazione prodotta con strumenti analogici (es. lettera scritta a mano o a macchina) o con strumenti informatici (es. lettera prodotta tramite sistema di videoscrittura) e stampati. 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. Di uno stesso documento possono esistere più esemplari originali. Copia del documento è trattenuta nell'archivio del soggetto che l'ha spedito.

### 3.16.3 Documento informatico

Per documento informatico si intende la rappresentazione o l'insieme di dati formati, acquisiti o convertiti in formato digitale dalle pubbliche amministrazioni per scopi e motivi pertinenti alla loro attività istituzionale.

Il documento informatico, sottoscritto con firma digitale, soddisfa il requisito legale della forma scritta ed ha rilevanza probatoria (si veda quanto riferito in [9] [8] ).

L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che ne sia data prova contraria o che la firma si basi su un certificato elettronico revocato, scaduto o sospeso.

Il valore probatorio e l'attendibilità dei documenti informatici privi di firma digitale o con firma non valida saranno liberamente valutabili dal destinatario, restando inteso che ai sensi della normativa vigente tali documenti sono assimilabili a documenti privi di sottoscrizione autografa.

## 3.17 DISTINZIONE DEI DOCUMENTI IN BASE ALLO STATO DI TRASMISSIONE

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

<b>Documenti in entrata/arrivo</b>	si intendono i documenti pervenuti o comunque acquisiti dalla Comunità nell'esercizio delle proprie funzioni
<b>Documenti in uscita/partenza</b>	si intendono i documenti prodotti dall'Amministrazione nell'esercizio delle proprie funzioni ed inviati a soggetti pubblici e privati, esterni alla Comunità
<b>Documenti interni</b>	si intendono i documenti amministrativi prodotti nell'ambito della medesima AOO. Questi si distinguono in: <ul style="list-style-type: none"> <li>• documenti di preminente carattere informativo</li> <li>• documenti di preminente carattere giuridico-probatorio</li> </ul>

## 4 PARTE SECONDA – PROCEDURE DI GESTIONE DEI DOCUMENTI E DEI FLUSSI DOCUMENTALI

### 4.1 IL REGISTRO DI PROTOCOLLO

Giuridicamente il registro di protocollo è un atto pubblico di fede privilegiata chiamato a certificare l'effettiva ricezione e l'effettiva spedizione di un documento ad una certa data, indipendentemente dalla veridicità o autenticità del documento stesso. Il registro è idoneo a produrre effetti giuridici a favore o a danno di terzi e dell'Amministrazione.

La numerazione delle registrazioni di protocollo è unica all'interno dell'AOO, progressiva e relativa all'anno solare.

La normativa vigente prescrive che il sistema informatico debba consentire la produzione del registro di protocollo, ovvero dell'elenco delle informazioni inserite con le operazioni di registrazione di protocollo nell'arco di uno stesso giorno.

La produzione del registro giornaliero di protocollo avviene su supporto informatico.

Il Responsabile del Servizio di Protocollo garantisce, ai sensi dell'art. 7 comma 5 del DCPM 3.12.2013, la trasmissione entro la giornata lavorativa successiva al sistema di **conservazione il registro giornaliero** di protocollo, garantendone l'immodificabilità del contenuto. Il *processo di conservazione* è attivato sulla base dell'accordo stipulato tra PAT, in qualità di ente capofila delle pubbliche amministrazioni aderenti al sistema informativo elettronico trentino (SINET), e IBACN, in qualità di soggetto che svolge attività di conservazione (deliberazione della Giunta provinciale di Trento n. 2219 di data 15 dicembre 2014).

Il Responsabile del Servizio di Protocollo provvede a **riversare annualmente** in un'unica soluzione le registrazioni del protocollo informatico dell'anno precedente su supporti di memorizzazione non riscrivibili (operazione quest'ultima che è eseguita in automatico da Informatica Trentina Spa).



## 4.2 Livelli accesso interno

L'accesso al sistema di protocollo informatico è consentito esclusivamente agli utenti abilitati, previa univoca identificazione e autenticazione.

La procedura del sistema di protocollo informatico risponde compiutamente ai requisiti minimi di sicurezza di cui all'art. 7 del D.P.C.M. 3 dicembre 2013.

Sono stabilite quattro possibilità di accesso interno al sistema di protocollo:

- visibilità
- inserimento
- modifica
- annullamento

Per “**visibilità**” si intende la possibilità per un utente abilitato di visualizzare una registrazione di protocollo, con l'esclusione dei documenti riservati.

Per “**inserimento**” si intende la possibilità per un utente abilitato di inserire i dati e provvedere ad una registrazione di protocollo.

Con “**modifica**” si intende la possibilità per un utente abilitato di modificare i dati gestionali di una registrazione di protocollo, con l'esclusione dei dati obbligatori.

Con “**annullamento**” si intende la possibilità per un utente abilitato (specificatamente il responsabile del protocollo informatico) di annullare una registrazione di protocollo.

## 4.3 Utente interno abilitato alla consultazione

Gli utenti interni sono abilitati ad accedere al sistema informativo limitatamente ai documenti di rispettiva competenza e con le restrizioni formalmente indicate dal RPA, compresi fra un livello massimo (tutti i documenti della stessa UOR) e minimo (esclusivamente quelli trattati dal singolo addetto).

In tal senso il RPA deve anche indicare al **Responsabile del Servizio**, per ciascun utente (addetto) il livello di accesso in modifica (inserimento dati) e in consultazione.

## 4.4 ELIMINIZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

In modo coerente con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'amministrazione sono registrati nell'ambito del registro di protocollo informatico che è unico.

L'amministrazione ha aderito alla proposta di adozione del sistema di protocollazione denominato Protocollo Informatico Trentino – P.I.Tre.

## 4.5 PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

Per quanto attiene gli aspetti di sicurezza nelle componenti infrastrutturali e logiche del sistema informatico di protocollazione, la stesura del piano per la sicurezza è di competenza di Informatica Trentina in qualità di società che eroga il servizio nei confronti dei vari Enti della Provincia Autonoma di Trento. In particolare si rimanda alla documentazione contrattuale/agli accordi intercorsi fra Informatica Trentina S.p.A. e gli Enti aderenti all'iniziativa di Protocollo Federato così come riferito in [12].

Per gli aspetti di sicurezza di competenza della AOO, la Comunità ha definito un insieme di modalità descritte nei successivi paragrafi.

### 4.5.1 Formazione dei documenti – Aspetti di sicurezza

Le risorse messe a disposizione e le procedure definite per la formazione dei documenti informatici garantiscono:

- L'**identificazione** della persona che ha predisposto il documento informatico e l'Amministrazione/AOO di riferimento; in particolare ciascun utente del Sistema Informatico in uso è identificato per mezzo di credenziali univoche di accesso al sistema costituite da un Identificatore Utente (User Id) e di una Parola d'Accesso (Password).
- La **sottoscrizione** dei documenti informatici, quando prescritta, con firma digitale secondo le normative vigenti
- L'**idoneità** dei documenti ad essere gestiti mediante strumenti informatici e a essere registrati mediante il protocollo informatico

- L'**accesso** ai documenti informatici tramite sistemi informativi automatizzati
- La **leggibilità** dei documenti nel tempo
- L'**interscambiabilità** dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti dalla AOO sono prodotti con l'ausilio di applicativi di video scrittura (Text Editor) che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, XML e TIFF.

I documenti informatici dell'AOO realizzati con altri prodotti di *text editing* sono convertiti, **prima della loro sottoscrizione con firma digitale**, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche.

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

## 4.5.2 Gestione dei documenti informatici

La gestione dei documenti informatici nell'ambito del Piano di Sicurezza dei documenti informatici considera un insieme di aspetti, elencati di seguito, la cui competenza è della Società erogatrice del Servizio P.I.Tre.

In particolare i successivi aspetti sono di competenza di Informatica Trentina S.p.A. che gestisce direttamente il sistema informatico P.I.Tre. nelle componenti organizzative, fisiche, logiche e infrastrutturali. Il Sistema P.I.Tre è erogato nei confronti della Comunità nella forma ASP (Application Service Provider)

- Componente organizzativa della sicurezza
- Componente fisica della sicurezza
- Componente logica della sicurezza
- Componente infrastrutturale della sicurezza
- Gestione delle registrazioni di protocollo e di sicurezza.

## 4.5.3 Trasmissioni e interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

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

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

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

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

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

### 4.5.3.1 All'esterno dell'AOO (Interoperabilità)

P.I.Tre. implementa le regole di interoperabilità descritte dalla normativa in vigore, consentendo la protocollazione semiautomatica (operazione con richiesta di conferma) per i documenti elettronici in arrivo sulla casella di posta istituzionale. Per una descrizione esaustiva dell'interoperabilità del sistema P.I.Tre si rimanda al Manuale Utente di P.I.Tre in allegato 9.

#### 4.5.3.2 All'interno dell'AOO

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

#### 4.5.4 Accesso ai documenti informatici

L'accesso al sistema avviene a seguito del superamento di una procedura di autenticazione che è posta in essere mediante la richiesta all'utente di credenziali di identificazione (**username**, o codice di accesso, e **password**, o parola chiave).

Se un utente deve accedere al sistema con ruoli diversi (es. come Responsabile del Servizio A o come Responsabile del Servizio B) può utilizzare le stesse credenziali di autenticazione (stessi username e password), e una volta effettuato l'accesso al sistema dovrà selezionare con quale ruolo andare accedere ai documenti. Le credenziali, al contrario, non possono essere attribuite a più persone (lo stesso username e la relativa password non possono essere assegnate a persone diverse neppure in tempi diversi).

Le credenziali sono verificate in tempo reale dal sistema di autenticazione.

Il sistema di autenticazione, se le credenziali sono corrette, apre una porta di comunicazione ed una **sessione cifrata** tra il client dell'utente (un browser standard) e il server applicativo (application server) comunicando a quest'ultimo solamente il codice di accesso (username). In questo modo le password non sono a conoscenza del server applicativo che è comunque in grado di individuare in modo univoco l'utente. Il sistema impedisce l'utilizzo contemporaneo delle stesse credenziali di autenticazione da più postazioni di lavoro.

#### 4.5.5 Conservazione di documenti informatici

##### 4.5.5.1 Archivio di deposito

I fascicoli e le serie che si riferiscono a procedimenti ancora in atto o che comunque hanno ancora utilità ai fini dello svolgimento delle attività amministrative costituiscono l'archivio corrente dell'Amministrazione. La documentazione è conservata presso gli uffici di competenza a cura dei Responsabili fino al trasferimento nell'archivio di deposito.

L'archivio di deposito ha la funzione di concentrare e conservare in modo temporaneo tutti i documenti dell'Amministrazione comunale relativi a procedimenti, affari ed attività conclusi e per i quali non risulti più necessaria la trattazione o la consultazione, se non sporadicamente.

Tale archivio accoglie la documentazione relativa ad affari conclusi da meno di 40 anni.

##### 4.5.5.1.1 Collocazione organizzativa

L'archivio di deposito si configura come un servizio funzionalmente distinto rispetto al **Servizio**, unito funzionalmente all'Archivio storico. Il Responsabile dell'Archivio di deposito si coordina con il Responsabile del **Servizio** per le operazioni di trasferimento dei documenti non più occorrenti alle necessità di ufficio.

Tra i compiti primari del Responsabile vi è quello di valutare, di concerto con gli organi tecnici dell'amministrazione, l'idoneità dei locali adibiti ad archivio di deposito, verificando i fattori di rischio (temperatura, umidità, luce, carichi di solai, rischio incendio, impianto elettrico) e predisponendo, nel caso, le opportune modalità di intervento.

##### 4.5.5.1.2 Il trasferimento dei fascicoli relativi ad affari esauriti in archivio di deposito

Ogni settore dell'Amministrazione è tenuto a trasferire all'archivio di deposito i fascicoli delle pratiche concluse e non più di uso corrente. Preliminarmente al trasferimento ciascun RPA che ha in carico i fascicoli procede a verificare l'effettiva conclusione degli affari o dei procedimenti cui i fascicoli si riferiscono e a eliminare tutta la documentazione di natura non archivistica contenuta (ad esempio: copie di lavoro utilizzate a meri fini informativi, materiale pubblicitario, copie gazzette ufficiali, ecc.).

I fascicoli del personale devono essere conferiti all'archivio di deposito l'anno successivo alla data di cessazione dal servizio, qualora siano concluse tutte le pendenze con il dipendente.

##### 4.5.5.1.3 Ordinamento archivistico

L'ordinamento delle unità archivistiche (fascicoli e serie) nell'archivio di deposito è quello stabilito dal Titolare.

#### 4.5.5.1.4 La movimentazione dei fascicoli dall'archivio di deposito

Il responsabile dell'Archivio deve essere a conoscenza della collocazione del materiale archivistico. Per questo motivo annota i movimenti delle singole unità archivistiche (nominativo del richiedente, motivazione, data della richiesta, data della restituzione ed eventuali note sullo stato della documentazione).

L'affidamento temporaneo è consentito mediante richiesta vistata dal responsabile dell'Archivio in duplice esemplare, contenente i motivi e la firma del richiedente. Un esemplare della richiesta è conservato all'interno del medesimo fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio di deposito (cfr. il modello di richiesta di consultazione interna riportato in allegato al presente Manuale, n. 7). Non è prevista l'estrazione di singoli documenti dal fascicolo.

#### 4.5.5.1.5 Consultabilità e accesso ai documenti dell'archivio corrente e dell'archivio di deposito

Al fine di assicurare la trasparenza dell'attività amministrativa e di favorirne lo svolgimento imparziale è riconosciuto a chiunque vi abbia interesse per la tutela di situazioni giuridicamente rilevanti il diritto di accesso ai documenti amministrativi, ovvero "il diritto degli interessati di prendere visione ed estrarre copia dei documenti amministrativi".

In ordine alla necessità di disciplinare le modalità di esercizio del diritto di accesso e i casi di esclusione dal diritto di accesso in relazione all'esigenza di salvaguardare "la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni", garantendo peraltro agli interessati "l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici", l'Amministrazione individua con specifico regolamento le categorie di documenti da essa formati o comunque rientranti nella sua disponibilità sottratti all'accesso o relativamente ai quali l'accesso è differito.

#### 4.5.5.2 La selezione dei documenti

Il Responsabile dell'Archivio provvede, prima del trasferimento nell'archivio di deposito dei nuovi fascicoli, alla selezione della documentazione da proporre per lo scarto sulla scorta del massimario di selezione, previa concessione del nulla osta della competente Soprintendenza ai beni archivistici.

#### 4.5.5.3 La conservazione dei documenti

Il Responsabile dell'Archivio attua tutte le iniziative connesse alla strategia della conservazione. In particolare, nei depositi di archivio sono assicurati i criteri per la corretta conservazione dei documenti, mediante la sicurezza dei locali con sistemi antincendio e antintrusione; il controllo della temperatura e dell'umidità relativa; la prevenzione dell'intrusione di agenti patogeni; l'ordinaria manutenzione e pulizia dei depositi, compresa la periodica spolveratura del materiale documentario unita a periodici interventi di disinfestazione.

#### 4.5.5.4 La conservazione dei documenti informatici

Il Responsabile del Servizio provvede, in collaborazione con le altre figure preposte alla gestione del sistema informatico dell'Amministrazione, a conservare i documenti informatici secondo quanto stabilito dall'apposito manuale di conservazione.

#### 4.5.5.5 Archivio storico

L'archivio storico conserva la documentazione che fa riferimento ad affari esauriti da oltre quarant'anni. Le modalità di gestione ed organizzazione dell'archivio storico sono previste da apposito regolamento.

##### 4.5.5.5.1 Consultabilità e accesso ai documenti dell'archivio storico

I documenti che sono conservati nell'archivio storico dell'Amministrazione, sono liberamente consultabili, ad eccezione di quelli contenenti dati sensibili nonché dati relativi a provvedimenti di natura penale espressamente indicati dalla normativa in materia di trattamento dei dati personali, che diventano consultabili quaranta anni dopo la loro data. Il termine è di settanta anni se i dati sono idonei a rivelare lo stato di salute, la vita sessuale o i rapporti riservati di tipo familiare. Anteriormente al decorso dei termini sopra indicati i documenti restano accessibili ai sensi della disciplina sull'accesso ai documenti amministrativi.

#### 4.5.6 Backup dei dati

La soluzione software P.I.Tre (Protocollo Informatico Trentino) che implementa il sistema di protocollo informatico è erogata in modalità ASP (Application Service Provider) da Informatica Trentina S.p.A. a cui

spetta l'onere di provvedere al backup del sistema completo (front end, back end, database). La frequenza di backup è giornaliera e la sua esecuzione operativa avviene in orario notturno.

## **4.5.7 Politiche di sicurezza adottate dall'AOO**

### **4.5.7.1 Politiche di uso accettabile del Sistema Informativo**

Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.

Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.

L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

#### **4.5.7.1.1 Ambito di applicazione**

Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ecc), includendo tutto il personale affiliato con terze parti.

Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

#### **4.5.7.1.2 Politiche – Uso generale e proprietà**

Gli utenti del sistema informativo devono essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.

Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.

Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.

Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

#### **4.5.7.1.3 Politiche - Sicurezza e proprietà dell'informazione**

Il personale dell'Amministrazione deve porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.

Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati a utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password devono essere cambiate con il primo accesso al sistema informativo e, in seguito, al minimo ogni quattro mesi, a eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.

Tutte le postazioni di lavoro (PC da tavolo e portatili) devono essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico.

Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.

Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.

Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus aggiornato.

Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.

Non si deve permettere ai colleghi, né tanto meno ad esterni, di operare sulla propria postazione di lavoro con le proprie credenziali.

### **4.5.7.2 Politiche di uso non accettabile del Sistema Informativo**

In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.

**4.5.7.2.1 Attività di rete e di sistema**

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.

Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.

È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.

Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.

Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.

Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.

Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.

Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.

Realizzare brecche nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecche della sicurezza si intendono, in modo riduttivo:

- accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
- attività di "sniffing";
- disturbo della trasmissione;
- spoofing dei pacchetti;
- negazione del servizio;
- le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
- attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.

Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.

Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.

Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.

Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.

Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

**4.5.7.2.2 Attività di messaggistica e comunicazione**

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).

Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.

Uso non autorizzato delle informazioni della testata delle e-mail,

Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.

Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.

Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di newsgroup (newsgroup spam).

## 4.6 MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI

### 4.7 REGISTRAZIONE DEI DOCUMENTI

#### 4.7.1 Registrazione di protocollo e altre forme di Registrazione

Tutti i documenti, per poter essere gestiti all'interno del sistema di gestione documentaria, devono essere registrati.

Sono previsti due tipi di registrazione, aventi entrambe validità giuridico-probatoria:

- a registrazione di protocollo
- tutte le altre forme di registrazione previste dall'art. 53 del DPR 445/2000, ritenute alternative alla registrazione di protocollo.

Il protocollo informatico Pi-Tre consente anche la registrazione a sistema dei "documenti non protocollati" (documenti grigi), che sono scannerizzati e classificati come un qualsiasi altro documento e contraddistinti da un numero di identificativo (ID) univoco.

Tale forma di registrazione permette di gestire all'interno del sistema documentario tipologie di documenti altrimenti non attestabili (es. documenti preparatori, memorie informali, fatture elettroniche, scritture provate, atti pubblici digitali, deliberazioni, determinazioni, decreti, ecc.)

##### 4.7.1.1 Registrazione di protocollo

La registrazione di protocollo è la memorizzazione delle informazioni relative al contenuto, alla forma, al mittente/destinatario e alla modalità di trasmissione di un documento. Tale operazione serve ad identificare in modo univoco un documento ricevuto, spedito o prodotto all'interno di un complesso documentario a prescindere dal supporto sul quale è formato, individuandone data, forma e provenienza/destinazione. La registrazione di protocollo è un atto pubblico di fede privilegiata.

##### 4.7.1.1.1 Elementi della registrazione di protocollo

La registrazione di protocollo è costituita da elementi obbligatori, alcuni dei quali solo se disponibili. Alcuni elementi della registrazione sono modificabili, altri non modificabili.

##### Elementi obbligatori

Numero di protocollo	non modificabile
Data di registrazione	non modificabile
Mittente (per i documenti ricevuti) o Destinatario (per quelli spediti)	su Pitre modificabili
Oggetto	su Pitre modificabile
Numero degli allegati	su Pi-Tre elenco allegati modificabile
Descrizione degli allegati	su Pitre modificabile
Tipologia documento	su Pitre modificabile

##### Elementi non obbligatori

Data del documento ricevuto	su Pitre modificabile
Numero di protocollo del documento ricevuto	su Pitre modificabile
Data arrivo	modificabile
Classificazione archivistica	modificabile
Assegnatario per competenza	modificabile
Impronta del documento informatico	non modificabile
Firmatario del documento	non modificabile

Collegamento a documenti precedenti e susseguenti	modificabile
Mezzo di ricezione o spedizione	modificabile
Ufficio mittente	modificabile

NB: sia per gli elementi obbligatori che per gli elementi non obbligatori "MODIFICABILI", il sistema di protocollo informatico Pitre conserva traccia sia della modifica eseguita che della versione originale, conformemente al disposto dell'art. 8 comma 2 del D.M. 3.12.2013.

Per i criteri di inserimento degli elementi della registrazione di protocollo si rimanda a quanto descritto nelle "Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico e per la compilazione della banca/che dati anagrafiche" riportate in allegato al presente Manuale (Allegato 3).

#### 4.7.1.2 Segnatura (timbro) di protocollo

La segnatura di protocollo è l'apposizione mediante timbro o con etichetta adesiva o l'associazione (nel caso di documenti informatici) all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile. Questa operazione è effettuata contestualmente all'operazione di registrazione di protocollo.

La normativa vigente individua quali elementi obbligatori della segnatura di protocollo:

- a) Identificazione dell'amministrazione
- b) Identificazione dell'AOO
- c) Numero progressivo di protocollo
- d) Data di protocollo

Oltre a questi elementi obbligatori, la segnatura può contenere altri elementi che hanno lo scopo di associare al documento elementi di natura gestionale connessi al trattamento dei procedimenti amministrativi (workflow management) e alla gestione archivistica, ed in particolare:

- e) classificazione (titolo e classe)
- f) fascicolo
- g) indicazione della UOR destinataria del documento per competenza
- h) indicazione del RPA assegnatario del documento
- i) indicazione dei destinatari delle copie per conoscenza.

La segnatura di protocollo dell'Ente è posta sui documenti cartacei in arrivo e in partenza sul primo foglio ed ha le seguenti caratteristiche:

- <Nome Ente>
- *numero di registrazione protocollo*
- *giorno, mese, anno della registrazione di protocollo (nella forma gg/mm/aaaa)*

Alcune informazioni possono essere inserite contestualmente all'operazione di protocollazione (quelle indicate come obbligatorie), mentre altre (di natura gestionale) devono essere inserite successivamente, se disponibili.

Per quanto riguarda i documenti informatici, il software assegna automaticamente la segnatura, riportando gli stessi elementi per la segnatura del documento cartaceo.

#### 4.7.1.3 Documenti soggetti a protocollazione

Sono soggetti a registrazione di protocollo i documenti acquisiti o spediti dall'Ente nell'esercizio delle proprie funzioni amministrative. I documenti interni aventi preminente carattere giuridico-probatorio o costituenti comunque un elemento necessario al corretto svolgimento dell'attività amministrativa devono essere protocollati così come tutti i documenti informatici acquisiti o prodotti.

#### 4.7.1.4 Annullamento o modifica di una registrazione di protocollo

L'annullamento di una registrazione di protocollo è consentito **solo per motivate e verificate ragioni**.



La **richiesta di annullamento**, contenente il numero di protocollo da annullare e la motivazione, va inoltrata in **forma scritta** (anche via e-mail) al **Segretario**.

Dopo la autorizzazione del Segretario, la UOP inserisce nell'apposito campo il motivo dell'annullamento e il relativo provvedimento. Il sistema provvederà a registrare l'autore e la data della modifica. Sul documento è apposta la dicitura "annullato", in obliquo sul testo ed in modo da far rimanere comunque leggibile il contenuto. Sul registro di protocollo accanto all'oggetto appare la dicitura "registrazione annullata".

Il Segretario, **sempre su richiesta motivata**, ha inoltre la possibilità di procedere ad un "annullamento parziale" della registrazione, che consiste nella modifica di uno o più elementi obbligatori definiti "non modificabili". In questo caso sul registro di protocollo appaiono solo le modifiche apportate, mentre nel profilo del documento si tiene traccia della data, dell'autore e dei dati precedenti alla modifica (che sono barrati e scritti in rosso).

#### 4.7.1.5 Registrazioni differite (protocollo differito)

Qualora il **Protocollo centrale** o le **UOP abilitate** si trovino nell'impossibilità di procedere entro il giorno della loro ricezione alla registrazione dei documenti pervenuti e qualora ciò potesse pregiudicare un diritto di terzi, il **Segretario** può autorizzare, con un provvedimento scritto, il differimento dei termini di registrazione. Con tale provvedimento si individuano i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione deve essere comunque effettuata. Questo si può verificare, ad esempio, nel caso di un consistente numero di domande di partecipazione ad un concorso in scadenza o ad una gara di appalto.

#### 4.7.1.6 Registrazione con differimento dei termini di visibilità (riservatezza temporanea delle registrazioni di protocollo)

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza temporanea delle informazioni contenute nelle registrazioni di protocollo (ad esempio in occasione di gare e appalti, concorsi ecc.) è prevista la possibilità di differimento della libera visione delle registrazioni di protocollo.

#### 4.7.1.7 Registrazione di protocollo riservata

Alcuni documenti che contengono informazioni di natura particolare che devono essere trattate in forma riservata sono registrati sul protocollo generale con modalità che garantiscano la visione delle registrazioni limitata a particolari soggetti.

#### 4.7.1.8 Operazioni particolari di registrazione di protocollo

##### 4.7.1.8.1 Registrazioni di documenti relativi a gare d'appalto e concorsi

La registrazione deve essere effettuata sulla base degli elementi rilevabili sulla busta o involto (tali elementi sono specificati nei relativi bandi di gara o di concorso). Chi procede alla segnatura appone il timbro sulla busta o sull'involto chiusi (**in nessun caso deve procedere all'apertura**), riportando anche l'ora di consegna della busta o involto, e la propria firma.

Una volta che si sia proceduto all'apertura delle buste si dovranno riportare i dati relativi alla segnatura di protocollo, riportata sulla busta, sulla domanda di partecipazione alla gara o al concorso e sugli allegati eventualmente presenti, e provvedere all'acquisizione dei documenti prodotti.

Per evitare ritardi e garantire una più efficiente gestione delle procedure relative allo svolgimento delle gare, i vari settori ed uffici provvedono a comunicare all'UOP l'indizione e la scadenza di gare e concorsi.

##### 4.7.1.8.2 Rilascio di ricevuta di un documento in arrivo

Qualora un documento sia consegnato personalmente dal mittente al personale del **Protocollo Centrale** o delle altre UOP eventualmente abilitate, questo è tenuto, nel caso di gare d'appalto o concorsi, o comunque quando ne venga fatta esplicita richiesta, a rilasciare una ricevuta attestante l'avvenuta ricezione. Il rilascio della ricevuta può avvenire nei modi seguenti:

- fotocopia della busta protocollata, che riporta anche l'ora di consegna e la firma dell'Utente protocollista che ha effettuato la registrazione.
- ricevuta dell'avvenuta protocollazione dal sistema informatico.

Nel caso di temporaneo ed eccezionale carico di lavoro (ad esempio la consistente registrazione di domande di partecipazione a gare d'appalto nel giorno della scadenza del bando) il personale del **Protocollo Centrale**, o delle UOP abilitate, rilascia la ricevuta su un modulo riportante nome del mittente, data ed ora di ricezione, firma dell'Utente protocollista che ne trattiene copia.

**4.7.1.8.3 Lettere anonime**

Le lettere anonime **sono soggette a registrazione di protocollo**. Qualora si ritenga opportuno, si prevede in alcuni casi l'utilizzo del protocollo riservato (cfr. §§ 4.7.1.6 e 4.7.1.7). Nel campo mittente si indicherà la dicitura "anonimo".

**4.7.1.8.4 Lettere prive di firma o con firma illeggibile.**

Le lettere prive di firma o con firma illeggibile **sono soggette a registrazione di protocollo**. E' demandata alla UOR destinataria o al RPA assegnatario la valutazione della loro efficacia e l'eventuale richiesta del documento firmato o con firma leggibile.

**4.7.1.8.5 Allegati pervenuti senza lettera di accompagnamento**

Nel caso in cui pervengano allegati senza lettera di accompagnamento, questi **vanno protocollati**, o, nel caso, sottoposti ad altre forme di registrazione.

**4.7.1.8.6 Telefax**

I documenti ricevuti o trasmessi tramite telefax **vanno protocollati**.

Il documento trasmesso tramite telefax soddisfa il requisito della forma scritta e la sua trasmissione, a norma di legge, non deve essere seguita dalla trasmissione dell'originale [11]

Al documento originale che segue il telefax deve essere attribuito lo stesso numero di protocollo del telefax, in quanto ogni documento va individuato in base al suo contenuto, indipendentemente dal mezzo di trasmissione (si tratta in sostanza dello stesso documento). Se il telefax riporta annotazioni o appunti che non sono presenti sull'originale va conservato assieme all'originale.

Il documento originale che riporta **integrazioni o modifiche** rispetto al telefax precedentemente pervenuto, dovrà invece essere trattato alla stregua di un nuovo documento con la conseguente attribuzione di un **nuovo numero di protocollo**.

L'Amministrazione riceve generalmente i telefax direttamente sul PC del Protocollo Centrale. Provvede quindi:

- a smistare tramite posta elettronica interna i telefax che non vanno protocollati direttamente ai destinatari;
- ad acquisire i telefax nel sistema di protocollo informatico Pi-Tre per la protocollazione e a smistarli agli interessati con il medesimo sistema.

**4.7.1.8.7 Documenti originali plurimi**

Al documento originale plurimo indirizzato **per competenza** a più destinatari **deve essere assegnato un solo ed unico numero di protocollo**.

**4.7.1.8.8 Corrispondenza personale/riservata**

Ordinariamente la corrispondenza personale/riservata **non è protocollata**. Qualora il destinatario ritenga che tale corrispondenza afferisca ad un procedimento amministrativo (e quindi rientri in un fascicolo), è tenuto a trasmetterla al **Protocollo Centrale** e alle UOP abilitate per le consuete operazioni di registrazione, indicando il grado di riservatezza ritenuto necessario.

**4.7.1.8.9 Documenti con oggetto plurimo**

Alcuni documenti in entrata possono riguardare più argomenti e, in quanto tali, possono potenzialmente essere assegnati per competenza a più RPA in quanto riferibili a procedimenti o a affari diversi. Si tratta dei cosiddetti documenti "ad oggetto plurimo" ai quali deve essere attribuito un unico numero di protocollo, ma classificazione diversificata in relazione agli argomenti trattati, in modo da consentirne la collocazione nei rispettivi fascicoli. In questi casi l'operatore di protocollo:

- registra il documento una sola volta (ogni documento deve essere individuato da un unico numero di protocollo)
- smista il documento a tutti gli interessati i quali provvederanno in relazione ai diversi oggetti a collocarlo nei rispettivi fascicoli.

Non deve presentarsi il caso di documenti in partenza riferiti a più argomenti. E' compito dei RPA verificare che i documenti prodotti e trasmessi trattino una sola materia, chiaramente indicata nell'oggetto del documento stesso.

**4.7.1.8.10 Documenti in partenza con più destinatari**

Nel caso si renda necessario l'invio di uno stesso documento a più di un destinatario è autorizzata la spedizione di copie dell'originale.

Nella registrazione di protocollo va riportato il nominativo di tutti i destinatari, allegando la lista al documento, nel caso in cui gli stessi non siano indicati nel documento. Nel caso di convocazione delle

sedute di organi collegiali, nel campo destinatario va inserita la dicitura "ai componenti del <denominazione organo collegiale>".

#### 4.7.1.8.11 Documenti pervenuti per errore

I documenti pervenuti per errore **non vanno protocollati** e devono essere spediti immediatamente al destinatario. Qualora il destinatario non sia individuabile il documento va rispedito al mittente.

#### 4.7.1.8.12 Documenti smistati e assegnati erroneamente

I documenti smistati e/o assegnati per errore vanno restituiti al **Protocollo Centrale** o all'unità di Smistamento competente che provvederà ad un nuovo smistamento. Non vanno in nessun caso trasmessi direttamente all'Ufficio competente a cura della persona che ha erroneamente la documentazione, in quanto si perderebbe traccia dell'effettiva assegnazione.

Nel sistema informatico i casi di smistamento e/o assegnazione errati vanno gestiti con la funzione di "rifiuto" (inserendo nell'apposito campo la motivazione es. "assegnazione errata"). Tale funzione consente al **Protocollo Centrale** di procedere ad una nuova assegnazione.

#### 4.7.1.8.13 Registrazione a fronte (protocollo)

Ogni numero di protocollo individua un unico documento. Non è pertanto consentita la registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per identificare più documenti collegati tra loro (ad esempio: documento in entrata e relativa risposta in uscita, nemmeno nel caso in cui il procedimento si esaurisca con tale risposta).

## 4.8 DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Per gestione del flusso documentario s'intendono tutti i modi operativi adottati al fine di attuare una corretta acquisizione, produzione, gestione e conservazione dei documenti, comunque formati, afferenti al complesso documentario dell'Amministrazione.

### 4.8.1 Documenti in arrivo

#### 4.8.1.1 Documenti cartacei

##### 4.8.1.1.1 Canali di Acquisizione

I documenti cartacei possono essere acquisiti tramite i seguenti canali:

- Servizio postale o servizio di corriere
- Telefax
- Consegna diretta agli uffici, ai funzionari o agli sportelli dell'Amministrazione/Ente abilitati al ricevimento di documenti
- E-mail

Di seguito si riportano alcune specificità legate al mezzo di trasmissione.

- **Servizio postale o servizio di corriere**

I documenti indirizzati all'Ente e pervenuti agli uffici postali sono ritirati dal personale incaricato e consegnati al **Protocollo Centrale**.

I documenti pervenuti a mezzo corriere direttamente presso le UOR dell'Ente sono consegnati al **Protocollo Centrale**.

- **Telefax**

I documenti trasmessi via telefax sono considerati a tutti gli effetti documenti cartacei. Per legge soddisfano il requisito della forma scritta e la loro trasmissione può non essere seguita da quella del documento originale. Tutti i fax in ingresso devono arrivare direttamente al **Protocollo Centrale**.

- **Consegna diretta**

I documenti possono pervenire direttamente al **Protocollo Centrale**, ovvero arrivare alla struttura interessata che provvede a consegnarli al **Protocollo Centrale** che ne cura la protocollazione, e l'inoltro alla struttura competente.

#### 4.8.1.1.2 Apertura e cernita della corrispondenza in arrivo

Una volta pervenuta al **Protocollo Centrale**, la corrispondenza è suddivisa distinguendo preliminarmente tra:

**a) corrispondenza da non protocollare**

Cfr. §§ 4.7.1.3 e 4.11.1.

**b) corrispondenza personale/riservata**

Se il carattere riservato/personale della corrispondenza è desumibile prima dell'apertura della busta, sulla busta stessa è apposta la dicitura "personale" (se non già presente), e la comunicazione è riconsegnata al destinatario. Qualora invece il carattere personale/riservato emerga dopo l'apertura, la comunicazione è posta in una nuova busta sulla quale si riporta la dicitura "personale" e il destinatario. Successivamente la comunicazione è trasmessa al destinatario.

**c) corrispondenza da protocollare**

I documenti da protocollare sono presi in carico dal **Protocollo Centrale** che provvede, prima della protocollazione, ad individuare la corrispondenza che ha carattere di urgenza.

#### 4.8.1.1.3 Registrazione di protocollo, segnatura e classificazione

I documenti in entrata sono registrati sul registro di protocollo dal personale del **Protocollo Centrale**.

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. Le rappresentazioni digitali dei documenti cartacei, una volta verificate la leggibilità e la qualità, sono archiviate secondo le regole correnti su supporti di memorizzazione in modo non modificabile al termine del processo di scansione.

#### 4.8.1.1.4 Smistamento dei documenti

Una volta protocollati i documenti sono consegnati dal **Protocollo Centrale** ai responsabili di settore. Sono possibili due tipologie di smistamento:

- **per competenza**
  - Viene individuato l'UOR o la persona responsabile del procedimento o dell'attività cui il documento si riferisce
- **per conoscenza**
  - Sono individuate le UOR o le persone interessate, a meri fini informativi, al contenuto del documento

Alla **classificazione** provvederanno gli assegnatari per competenza.

#### 4.8.1.2 Documenti informatici in arrivo

Si rammenta che ai sensi della normativa vigente un documento informatico per avere validità e rilevanza agli effetti di legge deve essere dotato di firma digitale (ex D.lgs. 82/2005, art. 20, comma 1); **tutti** i documenti informatici in questa accezione **devono** essere sottoposti a registrazione di protocollo (ex DPR 445/2000, art. 53, comma 5).

La Comunità utilizza le "**Direttive**" approvate da ultimo (rinvio dinamico) con **delibera Giunta Prov.le n. 1594 del 02.08.2013** (Allegato 8) relativamente a:

- comunicazioni telematiche con altre pubbliche amministrazioni;
- comunicazioni telematiche tra l'amministrazione e società, imprese, professionisti;
- comunicazioni telematiche tra l'amministrazione e privati;
- presentazione di istanze e dichiarazioni all'amministrazione per via telematica.

#### 4.8.1.2.1 Acquisizione e formato dei documenti informatici

I documenti acquisiti dall'Amministrazione, indipendentemente dal software utilizzato, se ricevuti in formato diverso da quelli previsti dalla normativa vigente in materia di conservazione (ad esempio XML, PDF, Tiff), al fine di garantire la loro non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo, **sono recepiti dal sistema e convertiti in uno dei formati standard previsti** (PDF, XML, TIFF).

#### 4.8.1.2.2 Ricezione sulla casella di posta istituzionale

La ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale dell'Ente (cfr. § 3.11.1) e accessibile solo all'ufficio/postazioni preposto/e alla registrazione di protocollo.

Le UOP abilitate, nel caso in cui i documenti così pervenuti:

- Rivelino un destinatario errato, provvedono a rinviarli al mittente;
- Siano dotati di firma digitale, una volta verificata la validità, li acquisiscono a sistema in formato digitale e provvedono alla registrazione di protocollo;
- Siano privi di firma digitale o se la firma non risulti valida, li acquisiscono a sistema in formato digitale e provvedono a sottoporli a registrazione di protocollo indicandoli come "documenti ricevuti via posta elettronica". La valenza giuridica-probatoria di documenti così ricevuti è assimilabile a quella dei documenti non sottoscritti con firma autografa.

Qualora il documento sia inutile (SPAM) o addirittura dannoso (contenente virus) si provvede ad eliminarlo.

#### 4.8.1.2.3 Ricezione sulla casella di posta elettronica non istituzionale

I documenti informatici eventualmente pervenuti alle UOR, non abilitate alla ricezione, devono essere, immediatamente, inoltrati all'indirizzo di posta elettronica istituzionale dell'ente per la verifica della firma e la successiva registrazione.

La richiesta di protocollazione (testo della e-mail) è allegata al documento.

#### 4.8.1.2.4 Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere ricevuti dall'Ente su supporto rimovibile (Hard-disks; CD-Rom; Floppy disk; Pen-drive ecc.), che sia possibile decodificare ed interpretare con le tecnologie a sua disposizione. Una volta verificate tali condizioni, il personale del **Protocollo Centrale** verifica l'autenticità, la provenienza e l'integrità della firma digitale, se disponibile, dei files contenuti sul supporto rimovibile. Nel caso in cui la firma non risulti valida o sia assente, si procede comunque alla protocollazione decidendone l'acquisizione in formato digitale o in formato cartaceo mediante stampa. In entrambi i casi il documento è trattato alla stregua di un documento privo di firma (cfr. § 4.8.1.2.1).

#### 4.8.1.2.5 Registrazione di protocollo, segnatrice e classificazione

I documenti informatici in entrata sono registrati sul registro di protocollo dal personale del **Protocollo Centrale**. Una volta registrati i documenti sono smistati alla UOR competente.

#### 4.8.1.2.6 Smistamento

Lo smistamento effettuato tramite sistema informatico P.I.Tre. genera una notifica (messaggio di posta elettronica) che inserisce nell'elenco delle cose da fare del destinatario il documento trasmesso.

La trasmissione del documento informatico ai destinatari (per competenza o conoscenza) avviene esclusivamente tramite sistema informatico.

### 4.8.2 Documenti in partenza

#### 4.8.2.1 Redazione dei documenti

Ogni documento in uscita va redatto in un unico esemplare originale, che va spedito al destinatario.

L'ufficio proponente, che riceve sulla scrivania copia del documento per competenza, provvederà a classificarlo e stamparlo per l'inserimento nel fascicolo cartaceo.

I documenti prodotti, a prescindere dal supporto sul quale sono formati, devono riportare almeno le seguenti informazioni, destinate ad identificare l'amministrazione mittente:

- Denominazione e stemma dell'Amministrazione
- Indicazione completa dell'AOO e dell'UOR che ha prodotto il documento
- Indirizzo completo dell'Amministrazione (via, numero, CAP, città, provincia)
- Numero di telefono
- Numero di telefax
- Indirizzo istituzionale di posta elettronica
- Codice fiscale dell'Amministrazione
- Data completa (luogo, giorno, mese, anno)
- Numero di protocollo

- Numero di repertorio generale qualora si tratti di documentazione sottoposta ad altre forme di registrazione
- Oggetto del documento
- Sigla del RPA nonché del responsabile della composizione del testo.

#### 4.8.2.2 Documenti cartacei

##### 4.8.2.2.1 Registrazione di protocollo dei documenti cartacei in partenza.

I documenti cartacei da spedire (originale cartaceo firmato e timbrato unitamente a tutti gli allegati), sono protocollati direttamente dall'UOR che provvede all'acquisizione del documento in Pitre ed alla sua classificazione nel fascicolo di competenza.

Le lettere in partenza dovranno contenere l'indirizzo esteso di tutti i destinatari, inseriti con le modalità di cui alle Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico e per la compilazione della banca/che dati anagrafiche. Dovrà essere indicata la tipologia di invio.

##### 4.8.2.2.2 Trasmissione dei documenti cartacei in partenza

Una volta registrato, il documento cartaceo è trasmesso al destinatario direttamente dall'utente protocollista in base alle indicazioni del mittente (posta prioritaria, raccomandata, raccomandata a.r., consegna a mano, e-mail, ecc.). E' opportuno che gli invii per e-mail vengano eseguiti direttamente dall'interessato.

###### 4.8.2.2.2.1 Trasmissione di documenti cartacei a mezzo posta

L'addetto provvede:

- a ritirare la posta in partenza dall'ufficio Protocollo Centrale,
- alle operazioni di spedizione della corrispondenza in partenza comprensive di affrancatura ed eventuale pesatura, ricezione e verifica delle distinte di raccomandate compilate dagli uffici.

#### 4.8.2.3 Documenti informatici in partenza

##### 4.8.2.3.1 Formato dei documenti informatici

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione, al fine di garantire la loro non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

##### 4.8.2.3.2 Registrazione di protocollo dei documenti informatici in partenza

Il documento è girato dal RPA all'utente protocollista della UOP, il quale provvederà alla sua protocollazione. La ricevuta del sistema di posta certificata utilizzata per lo scambio di documenti digitali è rimessa al RPA che provvede a inserirla nel fascicolo competente.

Contestualmente l'utente protocollista inserisce nel sistema di gestione documentaria il documento informatico che corrisponde a quello che è inserito nel fascicolo elettronico.

##### 4.8.2.3.3 Trasmissione dei documenti informatici in partenza

Il documento informatico, prodotto conformemente alle norme di legge, dopo essere stato sottoposto a registrazione di protocollo, può essere trasmesso al destinatario finale via posta elettronica (certificata o no) o su supporto rimovibile.

#### 4.8.3 Documenti interni

##### 4.8.3.1 Registrazione di protocollo dei documenti interni

I documenti interni di preminente **carattere informativo** (memorie informali, appunti, foglio di calcolo, ecc.) **non vanno sottoposti a registrazione di protocollo.**

I documenti interni **rilevanti** ai fini del corretto svolgimento del procedimento cui si riferiscono, **vanno protocollati.**

Solitamente il documento interno è di tipo informatico e segue i modi di redazione e trasmissione sopra indicati al § 4.8.2.1. In via provvisoria, nella fase transitoria verso l'integrale digitalizzazione dei processi documentari della Pubblica Amministrazione, i documenti interni possono essere anche di tipo analogico.

Una volta prodotto il documento, il RPA valuta se lo stesso debba essere o no registrato a protocollo. I documenti da protocollare sono consegnati direttamente all'utente protocollista della UOP di competenza, che provvede alla loro protocollazione. Il RPA provvederà quindi alla sua classificazione ed inserimento nel fascicolo competente.

#### **4.8.3.2 Trasmissione**

Una volta registrato il documento cartaceo è trasmesso al Responsabile di settore. Il documento informatico sia protocollato che non protocollato, inserito a sistema (Pi-Tre), è trasmesso (per competenza, conoscenza, ecc.) ai Responsabili di Settore i quali provvedono allo smistamento/assegnazione dei documenti. Per il solo Servizio Affari Generali provvede direttamente il protocollista.

#### **4.8.4 Flusso documentario tra Amministrazioni comunali aderenti a forme associative intercomunali per l'esercizio di funzioni e servizi**

I flussi documentari che coinvolgono funzioni e servizi per i quali siano state predisposte forme di gestione intercomunale (ad esempio i corpi intercomunali di polizia locale, sportelli unici per le attività produttive, ecc..) presentano alcune particolarità che necessitano di attenzioni specifiche nella definizione di un sistema di gestione documentaria.

In questo caso, la corrispondenza giunge direttamente alla gestione intercomunale, che provvede a registrarla nel registro di protocollo generale.

#### **4.8.5 Assegnazione e presa in carico dei documenti**

##### **4.8.5.1 Assegnazione dei documenti ricevuti in formato cartaceo o digitale**

I documenti ricevuti dall'Amministrazione in formato cartaceo, *anche se successivamente acquisiti in formato immagine con l'ausilio di scanner*, al termine delle operazioni di registrazione, sono smistati alla UOR competente. Qui, il responsabile di settore assegna il documento al RPA di competenza sia in originale che per via informatica attraverso la rete interna dell'Amministrazione/AOO.

L'UOR di competenza ha notizia della posta in arrivo aprendo il programma di protocollo informatico (Pi-Tre) e nelle "cose da fare" (scrivania) troverà i documenti a lui indirizzati.

Il Responsabile di Settore smisterà la documentazione ai RPA specifici, per fare questo dovrà innanzitutto accettare i documenti (se trasmessi per competenza) e poi provvedere a trasmetterli;

La "presa in carico" dei documenti informatici è registrata dal sistema in modo automatico e la data di ingresso dei documenti nelle UOR di competenza coincide con la data di accettazione (se per competenza) o di presa visione (se per conoscenza) degli stessi.

##### **4.8.5.2 Modifica delle assegnazioni**

Nel caso di assegnazione errata, l'UOR che riceve il documento, lo rifiuta. In automatico il documento torna all'UOP che provvederà alla sua corretta riassegnazione.

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

#### **4.9 REGOLE DI SMISTAMENTO E ASSEGNAZIONE DEI DOCUMENTI RICEVUTI**

Si rinvia a quanto descritto nel precedente paragrafo 4.8.1

#### **4.10 UNITÀ ORGANIZZATIVE RESPONSABILI DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI**

Denominazione dell'Amministrazione : **COMUNITA' TERRITORIALE DELLA VAL DI Fiemme**

Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale : **VIA ALBERTI, 4 38033 CAVALESE (TN)**

Codice identificativo assegnato all'Amministrazione: **ctvf\_tn**

Casella di posta elettronica certificata: **comunita@pec.comunitavaldifiemme.tn.it**

Unità organizzative: **SERVIZIO AFFARI GENERALI; SERVIZIO PERSONALE, SERVIZIO FINANZIARIO; SERVIZIO TECNICO; SERVIZIO ATTIVITA' SOCIO-ASSISTENZIALI;**

Numero di telefono **+39 0462 241311**

Numero FAX **+39 0462 241322**

Nominativo del Responsabile del Servizio di Protocollo informatico, gestione documentale e archivistica:  
**dott. Mario Andretta**

L'ORGANIGRAMMA generale del personale della Comunità è inserito nel sito internet dell'ente – Sez. Amministrazione trasparente.

Per quanto riguarda la gestione dei documenti, la Comunità è organizzata in **un'unica AOO** con **5 UOR** (Unità Organizzative Responsabile) (vedi § 3.6.1).

## **4.11 ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE**

### **4.11.1 Documenti esclusi dalla protocollazione**

Secondo quanto prescrive il DPR 445/2000 all'art. 53, comma 5, sono esclusi dalla registrazione di protocollo i seguenti documenti:

- le gazzette ufficiali;
- i bollettini ufficiali ed i notiziari della pubblica amministrazione;
- i materiali statistici;
- i giornali, le riviste e i libri;
- il materiale pubblicitario non richiesto (se la documentazione fa parte come allegato di un procedimento, o della richiesta di iscrizione all'albo fornitori, deve essere trattato come allegato al documento);
- gli inviti a manifestazioni;
- la documentazione già soggetta a registrazione particolare da parte dell'Amministrazione (cfr. § 4.11.2.)
- i documenti di occasione (ringraziamenti, biglietti augurali, condoglianze, congratulazioni ecc.)

Documenti **in arrivo** non soggetti a protocollazione:

- bolle di accompagnamento
- documentazione statistica (non si protocolla la modulistica, sia in entrata che in uscita; si protocolla l'eventuale lettera di accompagnamento)
- ricevute di ritorno delle raccomandate A.R.
- avvisi di pagamento – comunicazioni di bonifici bancari
- documentazione bancaria di routine (contabili, estratti conto, ecc.)
- giustificativi di assenza del personale come previsti dal C.C.L.
- restituzioni dei buoni mensa da parte dei ristoratori o ditte convenzionate

Documenti **in partenza** non soggetti a protocollazione:

- cedolini stipendio
- certificati situazioni retributive e contributive personale strutturato e non strutturato
- modello CUD
- report delle presenze

Le comunicazioni e gli ordini di servizio **interni** sono protocollati in partenza dall'Ufficio Protocollo centrale.



### 4.11.2 Documenti soggetti a registrazione particolare

I documenti già sottoposti “ad altre forme di registrazione” ai sensi dell'art. 53 del DPR 445/2000 non devono essere protocollati. Essi sono sottoposti a registrazione particolare presso repertori informatici o analogici autonomi.

- *Deliberazioni del Comitato Esecutivo e del Consiglio;*
- *Determinazioni dei Responsabili di Settore/Servizio;*
- *Atti rogati dal segretario (contratti e atti unilaterali in forma pubblica amministrativa);*
- *Verbalì delle adunanze del Consiglio;*
- *Verbalì delle adunanze della Giunta;*
- *Contratti in forma di scrittura privata e convenzioni stipulate dai Responsabili di Settore/Servizio;*
- *Fatture elettroniche;*

## 4.12 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

### 4.12.1 Classificazione

La classificazione è l'attività di organizzazione logica di tutti i documenti che entrano a far parte del sistema documentario dell'Ente, 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. La classificazione si effettua sulla scorta del Titolario di classificazione.

#### 4.12.1.1 Titolario di classificazione

Il Titolario di classificazione si articola, secondo uno schema che va dal generale al particolare, in titoli, classi o serie.

Tale schema rappresenta un sistema logico che suddivide i documenti secondo le funzioni istituzionali esercitate dall'Ente, indipendentemente dagli uffici che le esercitano, dato che l'organizzazione di questi ultimi può variare nel tempo, mentre le funzioni dell'Ente si mantengono costanti. Il Titolario di classificazione è riportato in allegato al presente Manuale (Allegato 1).

Il Titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

#### 4.12.1.2 Modifica del Titolario di classificazione

Il Titolario di classificazione è uno strumento tendenzialmente stabile nel tempo, ma non statico. Esso può essere modificato o integrato dalla Giunta Provinciale di Trento, a seguito di assegnazioni di nuove funzioni, ovvero di sviluppo o modifica di funzioni istituzionali già possedute.

Le eventuali modifiche o integrazioni entrano in vigore il primo gennaio dell'anno seguente alla loro approvazione.

### 4.12.2 Massimario di selezione

Il massimario di selezione è lo strumento che consente di coordinare razionalmente l'eliminazione dei documenti non destinati a conservazione perenne. Il massimario riproduce l'elenco delle partizioni del Titolario (titolo, classe o serie), indicando per ciascuna di esse quali documenti debbano essere conservati permanentemente e quali invece debbono essere destinati al macero dopo cinque anni, dopo sette anni, dopo dieci anni, dopo venti anni ecc..

Il massimario è riportato in allegato al presente Manuale (Allegato 2).

Lo scarto degli atti potrà essere fatto solo dopo acquisita la autorizzazione della Soprintendenza per i beni culturali della Provincia Autonoma di Trento – Ufficio beni archivistici, librari e archivio provinciale.

### 4.12.3 FASCICOLI

#### 4.12.3.1 Fascicolo e fascicolazione

Di norma il documento si collega naturalmente e logicamente ad uno o più precedenti e ad uno o più susseguenti, relativi ad un medesimo affare, attività o persona, dando luogo alla formazione di un fascicolo.

Il fascicolo è quindi l'insieme ordinato di documenti relativi ad un medesimo affare, attività o ad una medesima persona fisica. 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 a 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.

Per esigenze pratiche, il fascicolo può essere a sua volta suddiviso in sottofascicoli, in inserti ed ulteriormente in annessi.

La fascicolazione è obbligatoria per tutti i documenti, anche per quelli non protocollati.

#### **4.12.3.2 Tipologie di fascicolo**

I fascicoli si suddividono nelle seguenti tipologie:

- fascicoli relativi a procedimenti ed affari;
- fascicoli relativi ad attività o personale.

#### **4.12.3.3 Fascicoli relativi a procedimenti, affari ed attività amministrative**

I fascicoli relativi a procedimenti, affari o attività amministrative contengono soltanto documenti identificati con la medesima classificazione. La durata del fascicolo è strettamente connessa alla natura dell'affare, procedimento o dell'attività trattata. La durata del fascicolo è determinata dalla tipologia di provvedimento. Pur considerando di norma la durata annuale, a seconda del procedimento la stessa può avere scadenza pluriennale.

La data di chiusura del fascicolo deve coincidere con quella dell'ultimo documento inserito.

#### **4.12.3.4 Fascicoli del personale**

Per ciascun dipendente è istituito 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 (ad esempio: pratica di assunzione, inquadramenti, giustificazioni di assenza, malattie, trasferimenti, valutazioni, partecipazioni a iniziative formative, ecc.).

Il fascicolo personale è chiuso all'atto della cessazione del rapporto di lavoro.

### **4.12.4 Formazione e gestione dei fascicoli**

#### **4.12.5 Apertura e repertoriazione del fascicolo**

Ogni documento, a prescindere dal supporto sul quale è formato, dopo la sua classificazione, smistamento e conseguente assegnazione al RPA, va necessariamente inserito nel fascicolo di competenza (ed eventualmente sottofascicolo ed inserto, qualora se ne ravveda utilità pratica ai fini della conservazione e/o reperimento).

L'apertura del **nuovo fascicolo** avviene in concomitanza con la classificazione. Prima di procedere all'apertura dello stesso è essenziale verificare che non esista già apposito fascicolo, in modo da evitare duplicati.

#### **4.12.6 Gestione periodica dei fascicoli**

I fascicoli di durata annua andranno chiusi con data 31.12. Il sistema proporrà, l'elenco dei fascicoli annuali ricorrenti, che verranno riaperti in automatico in data 01.01 dell'anno di riferimento.

Si precisa che non è corretto l'uso di creare fascicoli destinati a contenere tutta la documentazione proveniente da un determinato ente a prescindere dall'oggetto (ad esempio fascicolo della corrispondenza con la Provincia Autonoma di Trento, con il Comune X).

##### **4.12.6.1 Copertina ("camicia") del fascicolo**

I documenti cartacei che costituiscono il fascicolo sono raccolti all'interno di una copertina (detta anche camicia), che riporta sul frontespizio le informazioni di identificazione (cfr. § 4.12.6):

anno di apertura/titolo\_classe (eventuale serie)/numero di repertorio del fascicolo – descrizione dell'oggetto

- a) anno di apertura;
- b) titolo e classe (desunti dal documento che dà avvio alla pratica), numero di repertorio del fascicolo;
- c) oggetto del fascicolo, ovvero breve descrizione in termini normalizzati dell'oggetto (si raccomanda omogeneità nell'intitolazione di fascicoli che si riferiscono ad affari di uguale natura);
- d) responsabile del procedimento, affare o attività.

#### 4.12.7 Inserimento dei documenti nel fascicolo

I documenti sono conservati all'interno di ciascun fascicolo, sottofascicolo e inserto secondo l'ordine cronologico di registrazione, ovvero in base al numero di protocollo ad essi attribuito o, se assente in base alla propria data.

L'inserimento nel fascicolo di documenti non soggetti a protocollazione avviene con le stesse modalità suindicate. Si rammenta che tutti i documenti devono essere comunque classificati (cfr. 4.12.1.1).

#### 4.12.8 Trasferimento del fascicolo

Qualora le esigenze di trattazione dell'affare lo prevedano, il fascicolo può essere trasferito ad altro ufficio (UOR) mediante riassegnazione. Tale riassegnazione è effettuata dal Responsabile che ha in carico il fascicolo, il quale provvede ad aggiornare le informazioni sul sistema informatico e a modificare il nome del RPA sulla copertina del fascicolo.

Il fascicolo informatico è trasferito automaticamente al nuovo responsabile, mentre il fascicolo cartaceo deve essere trasferito al nuovo RPA competente a cura del primo responsabile.

#### 4.12.9 Chiusura del fascicolo

Il fascicolo, informatico e cartaceo, è chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare/attività. La data di chiusura si riferisce alla data dell'ultimo documento inserito nel fascicolo. Esso va archiviato nell'anno di apertura, rispettando l'ordine di classificazione e codifica del fascicolo.

### 4.13 FORMAZIONE E GESTIONE DELLE SERIE DI UNITA' DOCUMENTARIE E FASCICOLI – Nozioni di serie archivistica

Il Titolare di classificazione prevede che i documenti acquisiti o prodotti in un sistema documentario siano riconducibili all'interno delle sue partizioni (titoli e in subordine classi) in base al proprio oggetto. All'interno di ciascuna classe i documenti, eterogenei per forma ma non per contenuto (verbali, prospetti, lettere, ecc.) sono ripartiti a loro volta in fascicoli in base al comune riferirsi ad una medesima attività o ad un medesimo affare o procedimento (cfr. § 4.12.3.2).

Non sempre però le aggregazioni dei documenti sono state fatte in base all'oggetto o all'affare trattato. In alcuni casi infatti i documenti sono inseriti nei fascicoli di competenza e anche riuniti in base all'identità di forma, di provenienza o di tipologia di atto (rispettivamente ad esempio i contratti, le deliberazioni della Giunta): in tal caso si dice che i documenti sono aggregati in **serie**.

Il concetto di serie in senso stretto trova quindi evidente applicazione nel caso della documentazione organizzata in forma di registro o di volume (ad esempio la serie dei registri dei contratti).

Come si è visto in precedenza (cfr. § 4.12.6) ciascun fascicolo deve essere collocato all'interno di una classe ed individuato mediante il Titolare di classificazione, che, attraverso l'indicazione di alcuni elementi prestabiliti, ne rende possibile la gestione e il reperimento.

### 4.14 MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

Il sistema P.I.Tre è configurato in modo tale che la produzione del registro giornaliero di protocollo sia effettuata in modo automatico alla conclusione di ciascuna giornata lavorativa. Il registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è salvato su file in formato non alterabile, conservato a cura di Informatica Trentina e reso disponibile al Responsabile del Protocollo dell'Amministrazione.

Per la produzione e la conservazione delle registrazioni di protocollo annuali si rimanda al Cap. 4.1 di questo Manuale di Gestione dove l'argomento è ampiamente trattato.

### 4.15 DESCRIZIONE FUNZIONALE E OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO

Il sistema di protocollo informatico utilizzato prende il nome di P.I.Tre (Protocollo Informatico Trentino) ed è reso disponibile all'Amministrazione in modalità ASPX dalla società Informatica Trentina S.p.A.

L'architettura logica del sistema ha le caratteristiche di seguito riportate:

- Il client è costituito da un web browser che colloquia con la componente di front-end, utilizzando il protocollo http (e anche https) per accedere alle funzioni disponibili sull'interfaccia utente (user interface).
- La soluzione applicativa è realizzata secondo una architettura a 3 livelli (Back end, Middle tier, Front tier), garantendo la massima flessibilità e adattabilità rispetto ai diversi servizi erogabili e al carico di lavoro da sostenere
- La soluzione applicativa è realizzata utilizzando tecnologie Web-Oriented
- Il sistema eroga servizi in modalità ASP
- Le funzioni presenti sul front-end si appoggiano ai servizi offerti dalla piattaforma di gestione documentale e dal motore di workflow. Tali piattaforme specializzate di livello "Enterprise" sono basati sul prodotto standard di mercato EMC – Documentum che presenta un comprovato livello di robustezza, solidità, scalabile.
- La soluzione è integrata con le componenti, esterne al sistema, di posta elettronica, di posta elettronica certificata e con il sistema dell'indice delle Pubbliche Amministrazioni, per le funzioni di interoperabilità fra sistemi di protocollo, la gestione delle caselle di posta istituzionale e per altre funzionalità (ad es. notifiche per il workflow).

#### 4.15.1 Identificazione

L'accesso al sistema avviene a seguito del superamento di una procedura di autenticazione che è posta in essere mediante la richiesta all'utente di credenziali di identificazione (username, o codice di accesso, e password, o parola chiave).

Se un utente deve accedere al sistema con ruoli diversi (es. come Capo del Servizio A o come Capo del Servizio B) può utilizzare le stesse credenziali di autenticazione (stessi username e password), e una volta effettuato l'accesso al sistema dovrà selezionare con quale ruolo andare accedere ai documenti. Le credenziali, al contrario, non possono essere attribuite a più persone (lo stesso username e la relativa password non possono essere assegnate a persone diverse neppure in tempi diversi).

Le credenziali sono verificate in tempo reale da un apposito sistema di autenticazione.

Il sistema di autenticazione, se le credenziali sono corrette, apre una porta di comunicazione ed una sessione cifrata tra il client dell'utente (un browser standard) e il server applicativo, comunicando a quest'ultimo solamente il codice di accesso (username). In questo modo le password non sono a conoscenza del server applicativo che è comunque in grado di individuare in modo univoco l'utente. Il sistema impedisce, inoltre, l'utilizzo contemporaneo delle stesse credenziali di autenticazione da più postazioni di lavoro.

#### 4.15.2 Cambio password e blocco delle credenziali

Ogni utente può, in ogni momento, cambiare la propria password. Il sistema controlla che la password sia composta da almeno otto caratteri alfanumerici e che non contenga il nome o il cognome dell'utente. La data in cui la password è cambiata è registrata dal sistema nel record relativo all'utente. Il sistema, ad ogni richiesta di autenticazione, verifica la data dell'ultimo accesso e la data dell'ultimo cambio password. Nel caso in cui l'ultimo cambio password sia anteriore ai **tre mesi**, il sistema obbliga l'utente a cambiare la password. Nel caso in cui l'ultimo accesso al sistema sia anteriore ai sei mesi le credenziali sono disattivate e possono essere ripristinate solo dal responsabile dell'applicativo.

In ogni caso di modifica della password l'utente dovrà provvedere a registrare le modifiche nell'apposito modulo conservato in busta chiusa (personale) presso il Protocollo Centrale.

#### 4.15.3 Firma dei documenti e impronta informatica

I documenti possono essere sottoscritti con firma digitale secondo quanto previsto dalla normativa in vigore. I documenti possono essere sottoscritti sia prima della registrazione sul sistema di protocollo sia durante la fase di registrazione. Nel secondo caso, attivabile da una casella di spunta, il sistema richiede, una volta che l'utente abbia identificato su disco locale i file da firmare, l'utilizzo di un dispositivo sicuro per la creazione della sottoscrizione (es. una smart card, un token usb, etc.). I documenti informatici allegati alla registrazione (siano essi firmati digitalmente o no) sono automaticamente trasferiti sul sistema centrale in un apposito direttorio protetto (accessibile all'applicativo di protocollo e all'amministratore di sistema). Nel record della registrazione è salvata l'impronta (una sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile) dei

documenti informatici allegati. Questa operazione permette, in ogni momento, di evidenziare eventuali modifiche o sostituzioni dei documenti informatici allegati alle registrazioni

#### 4.16 RILASCIO DELLE ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

Le **abilitazioni** di accesso alle informazioni documentali sono rilasciate dall'Amministratore di Sistema sulla base delle indicazioni date dal Segretario, Responsabile del Servizio di Protocollo.

#### 4.17 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Ogni qualvolta non sia possibile utilizzare il protocollo informatico il responsabile del **Servizio di Protocollo** può autorizzare lo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza.

Si tratta di un registro omologo a quello di protocollo, sul quale sono riportate le stesse informazioni. Ogni documento è individuato dal numero assegnato dal registro di emergenza.

Sul *Registro di emergenza* devono essere riportate, a cura del responsabile del **Servizio protocollo**:

- la causa,
- la data e l'ora di inizio dell'interruzione,
- la data e l'ora del ripristino della piena funzionalità del sistema,
- eventuali annotazioni rilevanti.

La procedura di attivazione del Registro di emergenza consiste nell'utilizzare il software *del protocollo informatico* su computer *stand alone*, cioè non collegati alla rete, identificato dal responsabile del **Servizio protocollo**. Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il 1° gennaio e termina il 31 dicembre di ogni anno. Qualora nel corso di un anno non si sia fatto ricorso al registro di emergenza, deve annotarne anche il mancato uso sul registro stesso.

Una volta ripristinata la piena funzionalità del sistema, il responsabile del **Servizio** provvede alla chiusura del registro di emergenza, annotando il numero delle registrazioni effettuate e la data e ora di chiusura. Egli poi provvede senza ritardo alla connessione dei registri di emergenza con il protocollo unico, inserendo le registrazioni effettuate. Verificato lo "scarico" delle registrazioni, autorizza il ripristino del protocollo unico.

Il registro di emergenza è sostanzialmente a configurarsi come un repertorio del protocollo unico: ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo senza soluzioni di continuità la numerazione del protocollo unico raggiunta al momento dell'interruzione del servizio. A tale registrazione sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo unico recheranno, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo unico. L'efficacia della registrazione è dunque garantita dal numero attribuito dal registro di emergenza e a quel numero deve farsi riferimento per l'avvio dei termini del procedimento amministrativo; l'efficienza, invece, verrà garantita dall'unicità della catena documentale e dalla normalizzazione dei dati gestionali, comprese la classificazione e la fascicolazione archivistica.

Per garantire in ogni caso la protocollazione dei documenti è necessario dotarsi del Registro Emergenza.

#### 4.18 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

L'amministrazione adotta con delibera del Comitato Esecutivo il presente "Manuale di gestione", su proposta del responsabile del servizio di protocollo informatico (RSP).

Il presente Manuale potrà essere aggiornato a seguito di:

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

#### 4.18.1 REGOLAMENTI ABROGATI

Con l'entrata in vigore del presente Manuale sono annullati tutti i regolamenti interni all'amministrazione/AOO nelle parti contrastanti con lo stesso.

#### 4.18.2 PUBBLICITÀ DEL PRESENTE MANUALE

Il presente Manuale, a norma dell'art. 22 della legge 7 agosto 1990, n. 241, è reso disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.

Inoltre copia del presente Manuale è:

- fornita a tutto il personale dell'Aoo e se possibile resa disponibile mediante la rete intranet;
- pubblicata sul sito internet dell'amministrazione.

#### 4.18.3 OPERATIVITÀ DEL PRESENTE MANUALE

Il presente regolamento è operativo dalla data di esecutività della deliberazione di approvazione dello stesso.

#### 4.19 ALLEGATI

1	Titolario di classificazione
2	Massimario di selezione
3	Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico e per la compilazione della banca/he dati anagrafiche
4	Fac-simile provvedimento autorizzativo di annullamento numero di protocollo
5	Fac-simile verbale di differimento termini di registrazione di protocollo
6	Modello di elenco di versamento archivio corrente-archivio di deposito
7	Fac-simile di richiesta di consultazione interno fascicolo versato nell'archivio di deposito
8	Direttive sulle comunicazioni telematiche: delibera G.ta Prov.le n. 1594 del 02.08.2013 (rinvio dinamico)
9	Manuale operativo del sistema informatico PITre: <a href="https://www.pi3.it/portal/server.pt/directory/manualistica_pitre/1020?DirMode=1">https://www.pi3.it/portal/server.pt/directory/manualistica_pitre/1020?DirMode=1</a>