UNIONE TERRED'ACQUA

Costituita fra i Comuni di:

Anzola dell'Emilia
Calderara di Reno
Crevalcore
Sala Bolognese
San Giovanni in Persiceto
Sant'Agata Bolognese

DELIBERAZIONE DELLA GIUNTA DELL'UNIONE NR. 30 DEL 05/09/2016

OGGETTO: APPROVAZIONE DEL MANUALE DI GESTIONE DEL PROTOCOLLO E DEI FLUSSI DOCUMENTALI E DELL'ARCHIVIO

Il giorno **5 settembre 2016,** alle ore **15:00**, nella sala della Giunta del Comune di San Giovanni in Persiceto, sede dell'Unione, si è riunita la Giunta dell'Unione.

Risultano presenti:

	Componente	Qualifica	Presente
1	BASSI EMANUELE	PRESIDENTE	**SI**
2	FALZONE GIAMPIERO	COMPONENTE	**SI**
3	BROGLIA CLAUDIO	COMPONENTE	**NO**
4	PELLEGATTI LORENZO	COMPONENTE	**SI**
5	VERONESI GIAMPIERO	COMPONENTE	**SI**
6	SERRA MAURIZIO	COMPONENTE	**SI**

Il **Presidente, BASSI EMANUELE**, riconosciuta legale l'adunanza ai sensi dell'art. 25 dello Statuto dell'Unione, invita la Giunta a prendere in esame l'oggetto sopra indicato.

Partecipa il SEGRETARIO DELL'UNIONE, **D.SSA CICCIA ANNA ROSA**, il quale provvede alla redazione del presente verbale.

Unione Terred'Acqua

DELIBERAZIONE DI GIUNTA DELL'UNIONE NR.30 DEL 05/09/2016

OGGETTO:
APPROVAZIONE DEL MANUALE DI GESTIONE DEL PROTOCOLLO E DEI FLUSSI DOCUMENTALI E DELL'ARCHIVIO

LA GIUNTA DELL'UNIONE

Premesso:

- che la gestione dei flussi documentali è un insieme di funzionalità che consentono di gestire e organizzare la documentazione ricevuta e prodotta dalle amministrazioni, attraverso la corretta registrazione di protocollo, l'assegnazione, la classificazione, la fascicolazione, il reperimento e la conservazione dei documenti informatici;
- che ai sensi del DPCM 3 dicembre 2013 le Pubbliche Amministrazioni devono adeguare i loro sistemi di gestione documentale alle Regole tecniche in esso contenute;
- che l'intento del DPCM è quello di introdurre concretamente modificazioni organizzative ed operative e disciplinare la realizzazione di una gestione completamente informatica dei flussi documentali e che lo strumento attraverso cui ottenere tale riforma è il manuale di gestione;

richiamati:

- il DPR 28/12/2000, n.445 recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
- la Direttiva del 9/12/2002 del Ministro per l'innovazione e le tecnologie recante "Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali";
- Il DPCM 14/10/2003 pubblicato sulla G.U. del 25/10/2003, concernente l"Approvazione delle Linee guida per l'adozione del Protocollo informatico e per il trattamento informatico dei procedimenti amministrativi";
- il Codice dell'Amministrazione Digitale – CAD – approvato con D. Lgs. n. 82/2005 e s.m.i.;
- il DPCM 03/12/2013 ad oggetto "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 D.Lgs. n. 82/2005;
- il DPCM 13/11/2014 avente ad oggetto "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71 del Codice dell'amministrazione digitale di cui al D.Lgs. n. 82/2005;

ritenuto opportuno dotarsi del Manuale di gestione del protocollo e dei flussi documentali e dell'archivio, adeguato alle più recenti normative in materia come sopra richiamate, approvando il medesimo come da allegato a) al presente atto;

ritenuto di individuare nel Responsabile del Servizio Segreteria il responsabile per la tenuta del protocollo informatico, della gestione dei flussi documentali e dell'archivio ai sensi dell'art. 61 del D.P.R. n. 445/2000;

acquisito il parere favorevole, firmato digitalmente, espresso sulla proposta di deliberazione n. 87 del 01/09/2016, dal Responsabile del Servizio Segreteria, dott. Luigi Nuvoletto, in ordine alla regolarità tecnica, ai sensi dell'art. 49 del ai sensi dell'art. 49 del D.Lgs. 267/2000;

con voti favorevoli unanimi espressi nei modi di legge,

DELIBERA

per tutto quanto in premessa esposto:

1) di approvare il Manuale di gestione del protocollo, dei flussi documentali e dell’archivio, che si allega al presente atto per formarne parte integrante e sostanziale (allegato A);

2) di dare atto che il Manuale di gestione è strumento di lavoro necessario alla corretta tenuta del protocollo ed alla gestione del flusso documentale e dell’archivio, e pertanto dovrà essere aggiornato quando innovazioni tecnologiche, nuove situazioni organizzative o normative lo richiedano o, comunque, ogni qualvolta si renda necessario alla corretta gestione documentale;

3) di provvedere alla pubblicazione del Manuale sul sito internet dell’Unione;

Attesa l’urgenza di provvedere in merito, il presente provvedimento, col voto favorevole di tutti gli intervenuti, viene dichiarato immediatamente eseguibile, ai sensi dell’art. 134, comma 4, del D.Lgs. 267/2000.

Allegati:

- *Allegato A-Manuale di gestione del protocollo, dei flussi documentali*
    - *Allegato 1) al Manuale – Titolario di classificazione*
    - *Allegato 2) al Manuale – Piano per la sicurezza informatica*

UNIONE TERRED’ACQUA

MANUALE DI GESTIONE DEL PROTOCOLLO, DEI FLUSSI DOCUMENTALI E DELL’ARCHIVIO

Allegato alla deliberazione della Giunta dell’Unione n. 30 del 05/09/2016

SOMMARIO

PREMESSA

Il Manuale di gestione è l'insieme delle norme, direttive e procedure interne che stabiliscono le modalità concrete di formazione, utilizzo e conservazione dei documenti, definiscono le responsabilità di tutte le strutture operative dell'Amministrazione e forniscono le informazioni necessarie ad un efficiente trattamento dei documenti.

La gestione dei documenti non ha più solo funzione di "certificazione" dei documenti ricevuti e spediti e di organizzazione dell'archivio, ma deve essere intesa come un servizio integrato di attività che connettono il sistema documentario con i sistemi di gestione dei processi e dei flussi documentali, con i sistemi di comunicazione dei documenti e le applicazioni di supporto al lavoro cooperativo.

La versione aggiornata del manuale recepisce, inoltre, i contenuti del D.P.C.M. 3.12.2013 recante le "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. 82/2005" con particolare riferimento alla gestione della casella di posta elettronica certificata, del documento informatico e del fascicolo informatico.

Il presente manuale viene integrato con i seguenti allegati:

Allegato 1) – Titolario di classificazione
Allegato 2) – Piano per la Sicurezza informatica approvato con deliberazione di Giunta dell'Unione nr. 64 del 28/12/2015

SEZIONE I – DEFINIZIONI E AMBITO DI APPLICAZIONE

Art. 1. Ambito di applicazione

1. Il presente Manuale è adottato nel rispetto del Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005 n. 82 (di seguito chiamato Codice) e ai sensi degli art. 3 e 5 del D.P.C.M. 03 dicembre 2013 recante le regole tecniche per il protocollo informatico.
   Esso descrive e disciplina le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti amministrativi dell'Unione Terred'acqua.

Art. 2. Definizioni.

1. Ai fini dell'applicazione del presente Manuale si intendono richiamate le definizioni contenute nel DPR 445/2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, in proseguo Testo Unico), nel D.lgs. 82/2005 (Codice) e nel D.lgs. 196/2003 (Codice in materia di protezione dei dati personali, in proseguo Codice della privacy).
2. Salva l'applicazione del comma 1, ai fini del presente Manuale si intende per:

a) **archivio**: complesso dei documenti, comunque formati, prodotti o acquisiti da una persona fisica o giuridica durante lo svolgimento della propria attività e nell'esercizio delle proprie funzioni, legati da un vincolo necessario;

b) **assegnazione**: operazione di individuazione dell'ufficio competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;

c) **documento analogico a preminente carattere giuridico-probatorio**: il documento non informatico redatto nell'esercizio delle funzioni al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative, oppure il documento da cui possono nascere diritti, doveri o legittime aspettative di terzi;

d) **documento informatico**: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti

e) **elenco di consistenza**: strumento che descrive in modo sintetico le unità archivistiche per facilitare la ricerca dei documenti;

f) **fattura elettronica**: documento informatico, non contenente codice eseguibile né macroistruzioni, generato in formato XML (eXtensible Markup Language) secondo lo schema e le regole riportate nelle Specifiche tecniche del formato della FatturaPA, trasmesso in via telematica al Sistema di Interscambio (SdI), e da questo recapitato all'amministrazione

g) **firma elettronica**: insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzti come metodo di identificazione informatica,

h) **firma elettronica avanzata**: insieme di dati in forma elettronica, allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario puo' conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati

i) **firma elettronica qualificata**: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma

j) **firma digitale**: un particolare tipo di firma elettronica qualificata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave

pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

k) **impronta di un documento informatico**: una sequenza di simboli binari di lunghezza predefinita, generata mediante l'applicazione al documento di una funzione matematica di *hash*, in grado di identificare in modo univoco il contenuto;

l) **indice delle amministrazioni pubbliche**: l'indice destinato alla conservazione e alla pubblicazione dei dati relativi alle pubbliche amministrazioni ed alle loro aree organizzative omogenee;

m) **marca da bollo digitale**: il documento informatico che costituisce la ricevuta di versamento dell'imposta di bollo ed attesta associazione dell'Identificativo Univoco di Bollo Digitale (IUBD) all'impronta digitale del documento

n) **piano di classificazione**: sistema precostituito di partizioni astratte gerarchicamente ordinate, individuate sulla base delle competenze del soggetto produttore, al fine di identificare secondo uno schema logico che va dal generale al particolare l'unità archivistica, per consentire la sedimentazione secondo un ordine che rispecchi storicamente lo sviluppo dell'attività svolta;

o) **scarto**: eliminazione fisica e irreversibile di documenti;

p) **serie**: ciascun raggruppamento di documenti o fascicoli con caratteristiche omogenee in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'Ente;

q) **smistamento**: individuazione della unità organizzativa responsabile cui trasmettere il documento;

r) **unità archivistica**: documento o insieme di documenti, rilegati o aggregati secondo un nesso logico di collegamento organico, che li individua come unità indivisibile (es. fascicolo, registro, repertorio);

s) **validazione temporale**: il risultato della procedura informatica con cui si attribuiscono , ad uno o più documenti informatici , una data e un orario opponibili a terzi;

t) **vincolo archivistico**: nesso che collega in maniera logica e necessaria la documentazione che compone l'archivio prodotto da un ente;

u) **Codice dell'Amministrazione Digitale (o Codice)**: il D.Lgs. 7-3-2005 n. 82;

v) **posta elettronica certificata (PEC)**: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi, di cui all'art. 48 del Codice;

w) **Carta di Identità Elettronica (CIE)**: il documento di identità elettronico di cui all'art. 66, comma 1 del Codice;

x) **istanza**: una richiesta in forma scritta indirizzata all'Unione per l'attivazione di una procedura amministrativa, finalizzata all'emanazione di un provvedimento e all'attivazione di un'azione;

y) **comunicazione**: la trasmissione di un documento, di qualunque natura, all'Unione nell'ambito di un procedimento amministrativo o di altre attività proprie dell'ente;

z) **pratica**: insieme di atti e documenti necessari all'avvio, processamento e completamento di una procedura amministrativa nelle materie di competenza dell'ente;

SEZIONE II - DISPOSIZIONI GENERALI

Art. 3. Individuazione dell'Area Organizzativa Omogenea

1. L'Unione Terred'acqua è organizzata in un'unica Area Organizzativa Omogenea (AOO), che coincide con il complesso delle Aree e dei Servizi (unità organizzative responsabili, in proseguo UOR) individuati con la deliberazione di approvazione della macrostruttura dell'Ente.
2. Il codice identificativo nell'Indice delle pubbliche amministrazioni è: **udctd.**

Art. 4. Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi

1. Le funzioni del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi (di seguito Servizio) sono svolte dal Servizio Segreteria. Il Responsabile del Servizio (RSP) è il Responsabile del Servizio Segreteria dell'Unione. Nei casi di vacanza, assenza o impedimento di quest'ultimo le funzioni sono svolte dal soggetto appositamente nominato.

2. In particolare il *Servizio* ha il compito di:

a) predisporre il manuale di gestione;

b) organizzare, di concerto con le strutture interne competenti (responsabili in materia di organizzazione del lavoro, definizione e gestione dei procedimenti amministrativi e in materia di informatica) il sistema di gestione dei flussi, che comprende la registrazione a protocollo e la classificazione dei documenti, l'assegnazione dei documenti ai Servizi di competenza, la costituzione e la repertorazione dei fascicoli, l'individuazione dei responsabili della conservazione dei documenti e dei fascicoli nella fase corrente;

c) attribuire il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni, di concerto con la struttura competente in materia informatica;

d) garantire che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del Testo Unico;

e) stabilire, di concerto con la struttura competente in materia di informatica, i criteri minimi di sicurezza informatica del sistema e delle procedure per garantire la registrazione permanente della gestione dei flussi documentari;

f) garantire, di concerto con la struttura competente in materia di informatica, la conservazione delle copie di sicurezza in luoghi differenti;

g) garantire la corretta produzione e la conservazione del registro giornaliero di protocollo;

h) curare, di concerto con la struttura competente in materia di informatica, che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro 24 ore dal blocco delle attività;

i) garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione a protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzioni di accesso esterno e le attività di gestione degli archivi;

j) autorizzare le operazioni di annullamento e modifica ai sensi dell' art. 54 del Testo Unico;

k) autorizzare l'uso del registro di emergenza ai sensi dell' art. 63 del Testo Unico;

l) vigilare sulla correttezza delle registrazioni anche attraverso controlli a campione;

m) cura la corretta conservazione dei documenti ai sensi della vigente normativa;

n) curare la redazione e l'aggiornamento del piano di classificazione;

Art. 5. Compiti degli addetti alla protocollazione

1. Gli addetti alle operazioni di registrazione a protocollo, all'atto della registrazione, descrivono il documento e i suoi eventuali allegati in maniera sintetica ma esauriente.
2. La verifica della congruità formale e sostanziale della documentazione presentata ai fini del procedimento amministrativo spetta al Responsabile del procedimento amministrativo (RPA), che provvede ai sensi della l. 241/1990.

Art. 6. Unicità del protocollo informatico

1. Il sistema di protocollo informatico è unico. Nell'ambito dell'area organizzativa omogenea la numerazione delle registrazioni di protocollo è quindi unica e rigidamente progressiva. Essa si chiude al 31 dicembre e ricomincia da 1 all'inizio di ogni anno.
   Il sistema di protocollo informatico adottato dall'Unione Terred'acqua comprende la "funzionalità minima" di cui all'articolo 56 del Testo unico.

Art. 7. Modello operativo adottato per la gestione dei documenti

1. Per la gestione dei documenti è adottato un modello operativo di tipo decentrato che prevede la partecipazione attiva di più soggetti ed uffici utenti a cui sono attribuite competenze diverse per la ricezione, registrazione, classificazione, fascicolazione e l'assegnazione dei documenti.

Art. 8. Caselle di Posta elettronica

1. L'AOO è dotata della casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA): unione.terredacqua@cert.provincia.bo.it ; tale casella costituisce l'indirizzo virtuale dell'AOO e di tutti gli uffici che ad essa fanno riferimento ed è accessibile, per l'invio e la ricezione di documenti, solo dall'ufficio protocollo.
2. Nell'ambito dell'organizzazione degli uffici e dei servizi possono essere associate e gestite direttamente dai servizi di riferimento ulteriori caselle di Posta Elettronica Certificata, previa autorizzazione del Responsabile del Protocollo (RSP). Dette caselle di posta elettronica, sono pubblicate sull'Indice delle Pubbliche Amministrazioni (IPA) e gestite tramite il protocollo.
3. Le caselle di Posta Elettronica Certificata sono accessibili, per l'invio e la ricezione di documenti, come sopra detto, mentre per la manutenzione e la gestione tecnica sono accessibili solo dal servizio Informatico (SIAT).

Art. 9. Flusso documentale tra Comuni appartenenti all'Unione e Unione

1. L'Unione provvederà a redigere, di concerto con i comuni, apposite linee operative per la gestione del flusso documentale tra l'Unione e Comuni appartenenti ad essa.

SEZIONE III - FORMAZIONE DEI DOCUMENTI

Art. 10. Tipologia dei documenti

1. I documenti si distinguono in:

a) **documenti in arrivo**: documenti, con rilevanza giuridico-probatoria, prodotti da altri soggetti e acquisiti dall'Ente nell'esercizio delle sue funzioni;

b) **documenti in partenza**: documenti, con rilevanza giuridico-probatoria, prodotti dal personale dell'Ente nell'esercizio delle sue funzioni e spediti a soggetti esterni all'Amministrazione;

c) **documenti interni**: documenti, a preminente carattere informativo o a preminente carattere giuridico-probatorio, scambiati tra le diverse UOR afferenti alla medesima AOO.

2. Ogni documento deve trattare un solo oggetto.

Art. 11. Trattamento delle differenti tipologie di documenti

1. I documenti in arrivo sono registrati nel protocollo informatico e classificati a cura:

a) dell'Ufficio Segreteria, che provvede ad assegnarli al Servizio competente;

b) degli Uffici abilitati per quanto riguarda i propri procedimenti.

2. I documenti in partenza sono registrati nel protocollo informatico e classificati a cura del Servizio competente a trattare l'affare o il procedimento amministrativo.

3. I documenti interni a preminente carattere giuridico-probatorio sono registrati nel protocollo informatico e classificati a cura del Servizio competente alla formazione e gestione del fascicolo relativo all'affare o al procedimento che sta trattando. In fase di registrazione del documento al protocollo informatico, il file va inserito e salvato nella registrazione mediante le operazioni previste dall'applicativo in uso.

4. I documenti interni a preminente carattere informativo, quali ad es. memorie informali, appunti, brevi comunicazioni scambiate tra uffici, non vanno protocollati.

Art. 12. Modalità di formazione dei documenti e contenuti minimi

1. I documenti formati dall'Amministrazione sono prodotti nativamente in formato digitale, come previsto dal DPCM 13 novembre 2014; le regole per la determinazione dei contenuti e della struttura dei documenti sono definite dal presente Manuale di Gestione.
   Al minimo, su di essi sono riportate le seguenti informazioni:
   - denominazione e stemma dell'Amministrazione;
   - indicazione dell'area organizzativa omogenea e dell'ufficio utente che ha prodotto il documento;
   - indirizzo completo con numero di telefono e fax;
   - indirizzo di posta elettronica del Responsabile del Procedimento e di PEC dell'Amministrazione;
   - data completa, luogo, giorno, mese, anno;
   - oggetto del documento;
   - sottoscrizione del Responsabile del Procedimento

Art. 13. Formato dei documenti informatici

1. Con riferimento alle indicazioni contenute nell'art. 10 del DPCM 3.12.2013 e nell'allegato "Formati" del medesimo provvedimento, i documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma elettronica, sono convertiti in formati standard (PDF o PDF/A) in possesso dei requisiti previsti dalla

normativa vigente al fine di garantire la leggibilità per altri sistemi e la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

2. Nel caso di documenti in formato immagine il formato ammesso è TIFF e JPG, mentre per documenti audio e video i formati ammessi sono MP3, AVI, WMV, MPEG)4.
   Altri formati ammessi che consentono una corretta conservazione dei documenti informatici sono: Office Open XML (OOXML), Open Document Format, XML, TXT e, per preservare l'autenticità dei messaggi di posta elettronica, lo standard di riferimento è RFC 2822/MIME.

Art. 14. Sottoscrizione dei documenti informatici

1. La sottoscrizione dei documenti informatici formati dall'Amministrazione è ottenuta con un processo di firma digitale o elettronica conforme alle disposizioni contenute nel Codice.
2. Il documento informatico, cui è apposta una firma elettronica, mediante credenziali di identificazione «user-id e password», sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
3. Il documento informatico sottoscritto con firma elettronica qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, del Codice che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile.
4. Il documento informatico sottoscritto con una firma elettronica qualificata o digitale soddisfa il requisito di immodificabilità previsto dall'art. 21, c. 2, del CAD, se non contiene macroistruzioni, codici eseguibili o altri elementi, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati;
5. Le firme elettroniche qualificate o digitali, ancorché sia scaduto, revocato, o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile a terzi che collochi la generazione della firma in un momento precedente alla sospensione, scadenza o revoca del suddetto certificato.

SEZIONE IV - RICEZIONE DEI DOCUMENTI

Art. 15. Modalità di ricezione dei documenti

1. Le modalità di ricezione dei documenti possono essere:

   a) *brevi manu* (normale o notificata);

   b) servizi postali tradizionali o corrieri autorizzati;

   c) telefax o fax server;

   d) telegramma;

   e) telematica.

Art. 16. Ricezione dei documenti cartacei

1. I documenti cartacei che provengono dal servizio postale tradizionale, da corrieri autorizzati o ricevuti con apparecchi telefax o fax server, sono consegnati all'ufficio protocollo che provvede all'eventuale apertura delle buste ed alla registrazione e successivo inoltro agli uffici.
2. I documenti cartacei consegnati direttamente ad altri uffici sono immediatamente protocollati e consegnati all'ufficio protocollo.
3. Non sono aperte le buste:

   a) riportanti le diciture "riservato", "personale", "confidenziale" o dalla cui confezione si evinca il carattere di corrispondenza privata;

   b) indirizzate nominativamente ai Sindaci senza specificazione della materia delegata

   c) indirizzate nominativamente ai Consiglieri dell'Unione;

   d) riportanti le diciture "offerta", "gara d'appalto", "preventivo-offerta" oppure qualora sia presente la sigillatura con ceralacca e controfirma o comunque la confezione rechi la dicitura "non aprire".
4. Se il destinatario di una busta che riporta la dicitura "riservata" o "personale" reputa che il documento ricevuto debba essere protocollato provvede a trasmetterlo al più vicino Ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.
5. Le buste pervenute tramite raccomandata o tramite posta tradizionale con utilizzo del francobollo vengono consegnate insieme al documento.

Art. 17. Ricezione di documenti informatici

1. I documenti informatici con firma digitale sono ricevuti sulla casella di Posta Elettronica Certificata istituzionale dell'Unione (PEC) oppure sulle altre caselle di PEC dei servizi dell'Unione, integrate con il sistema di protocollo e con la verifica della firma.
2. Sulla casella di PEC possono essere ricevuti messaggi e documenti provenienti da PEC istituzionali, da PEC non istituzionali, da caselle normali, istituzionali o meno. Nel caso in cui un documento informatico con firma digitale sia spedito da PEC e ricevuto nella casella di posta elettronica personale dovrà essere inoltrato alla casella di PEC istituzionale inviando contestualmente un messaggio, per conoscenza, al mittente con l'indicazione della casella di posta corretta.
3. I messaggi e documenti ricevuti sulla PEC istituzionale e sulla pec FATTURA PA sono protocollati e classificati dall'Ufficio Protocollo, che provvede all'assegnazione, mentre i messaggi e documenti ricevuti sulle PEC dedicate a singoli servizi sono protocollati e classificati dal servizio di riferimento;

4. Nel caso in cui pervengano sulla PEC messaggi dal cui contenuto si rilevi che sono stati erroneamente ricevuti, l'operatore rifiuta il messaggio con la dicitura "Messaggio pervenuto per errore".
5. I documenti che pervengono all'Amministrazione attraverso la posta elettronica, ma che sono sprovvisti di firma digitale, vengono ugualmente protocollati quando fanno parte di un procedimento amministrativo; non si protocollano quando contengono delle semplici comunicazioni.
6. La ricezione di istanze o di comunicazioni relative ai procedimenti amministrativi informatici può avvenire mediante l'utilizzo di un servizio dedicato on-line all'indirizzo reperibile sul sito dell'Unione, se disponibile per lo specifico procedimento amministrativo;
7. Del respingimento dell'istanza e/o comunicazione, per difformità alle regole di invio stabilite dal presente regolamento, l'ufficio interessato o l'ufficio protocollo, nel caso di impossibilità assoluta di trasmissione attraverso il protocollo interno, darà opportuna comunicazione all'interessato o al suo procuratore entro un termine congruo, in relazione allo specifico procedimento, nel caso che non vi siano norme specifiche e comunque entro un termine non superiore a 15 gg;

Art. 18. Attestazione di ricezione dei documenti

1. Qualora venga richiesto il rilascio di una ricevuta attestante l'avvenuta consegna diretta di un documento cartaceo l'Ufficio consegna la stampa dell'operazione di registrazione o appone il numero di protocollo sulla copia del documento che si consegna per la protocollazione, oppure rilascia la ricevuta prodotta dal sistema di protocollo informatico con gli estremi della segnatura.
2. Nel caso di ricezione informatica tramite PEC, la notifica di avvenuta ricezione è assicurata dal sistema stesso.

SEZIONE V - REGISTRAZIONE DI PROTOCOLLO E SEGNATURA DEI DOCUMENTI

Art. 19. La registrazione di protocollo dei documenti

1. Per registrazione di protocollo si intende l'operazione di memorizzazione delle informazioni fondamentali relative al contenuto, alla forma, all'autore e alla modalità di trasmissione del documento.
2. Tutti i documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi, indipendentemente dal supporto e ad eccezione di quelli specificatamente indicati nel successivo art., salvo quanto previsto dal successivo art. 23 (Documenti non soggetti a registrazione di protocollo), vanno registrati.

Art. 20. Il registro di protocollo

1. Il registro di protocollo informatico, è atto pubblico di fede privilegiata, che certifica l'effettivo ricevimento e l'effettiva spedizione di un documento ad una certa data, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici a favore o a danno delle parti.
2. Le registrazioni di protocollo non sono modificabili, salvo quanto previsto dal successivo art. 29. La registrazione è eseguita in un'unica operazione, senza possibilità di inserire le informazioni in più fasi successive.

Art. 21. Elementi obbligatori della registrazione di protocollo

1. Per ogni documento ricevuto o spedito è effettuata una registrazione con il sistema di gestione informatica dei documenti.
2. Ciascuna registrazione di protocollo contiene almeno i seguenti dati obbligatori, registrati in forma non modificabile in unica operazione senza possibilità per l'operatore di inserire le informazioni in più fasi successive:

   a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;

   b) data di registrazione, assegnata automaticamente dal sistema e registrato in forma non modificabile;

   c) mittente per il documento in arrivo, destinatario per il documento in partenza e registrato in forma non modificabile;

   d) oggetto del documento registrato in forma non modificabile;

   e) impronta del documento informatico generata impiegando la funzione di hash SHA-1 e registrata in modo non modificabile ;

   3. Sono elementi facoltativi della registrazione di protocollo:

   a) tipo di documento;

   b) numero e descrizione degli allegati;

   c) indicazione del Servizio competente;

   d) classificazione archivistica;

   e) data di arrivo o di partenza;

   f) mezzo di ricezione o di spedizione;

   g) copie per conoscenza.

3. La banca dati (anagrafica) dei soggetti, mittenti e destinatari, va mantenuta da chi effettua registrazioni di protocollo e implementata per i dati ritenuti essenziali, in osservanza del principio di necessità del trattamento dei dati personali ai sensi dell'art. 3 del Codice della privacy. I soggetti vanno inseriti senza duplicazioni, considerando come tale, in caso di persona giuridica, l'Ente nel suo complesso, a prescindere dalle sue articolazioni interne.
4. La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, riferita sia al corpo del messaggio che ai file allegati. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronico ricevuto.

Art. 22. Modalità di registrazione a protocollo dei documenti interni

1. I documenti interni di preminente carattere giuridico-probatorio sono registrati a protocollo dalla UOR mittente e presi in carico dalla UOR ricevente, senza ulteriore protocollazione.
2. Se la UOR ricevente è tenuta, a seguito della richiesta, a fornire un parere, provvede alla registrazione di quest'ultimo sul protocollo informatico come documento interno, avendo cura di collegarlo al documento di richiesta e di mettere il documento nel fascicolo di chi ha scritto. La UOR che riceve il parere non protocolla il documento

Art. 23. Documenti non soggetti a registrazione di protocollo

1. Sono escluse dalla registrazione di protocollo, ai sensi dell'art. 53, c. 5 del dpr 445/2000, le seguenti tipologie documentarie:

   a) atti interni, che non costituiscono fasi obbligatorie e imprescindibili dei procedimenti amministrativi;

   b) certificati anagrafici e di stato civile;

   c) certificazioni varie;

   d) documenti di interesse effimero (ad es., partecipazioni, condoglianze, ringraziamenti, auguri, richieste di appuntamenti);

   e) estratti conto bancari e postali;

   f) gazzette ufficiali, bollettini ufficiali;

   g) inviti a manifestazioni;

   h) materiali pubblicitari;

   i) materiali statistici;

   j) libri, giornali, riviste, pubblicazioni varie;

   k) notiziari della pubblica amministrazione;

   l) documentazione già soggetta a registrazione particolare su appositi registri, quali ad esempio:

      1. deliberazioni di Giunta e Consiglio;
      2. determinazioni;
      3. contratti/convenzioni;
      4. buoni d'ordine;
      5. mandati e reversali;
      6. verbali CDS;
      7. ordinanze e decreti

8. richieste di iscrizione anagrafica.

2. Non sono soggetti a registrazione di protocollo tutti i seguenti documenti interni:

   a) convocazioni ad incontri o riunioni;

   b) memorie informali;

   c) appunti;

   d) richieste di servizi di pulizia;

   e) richieste di forniture di cancelleria;

   f) dismissioni di beni e attrezzature;

   g) trasmissione di documenti e atti già protocollati o repertoriati;

   h) semplici avvertenze di arrivi/scadenze offerte;

   i) comunicazioni relative a corsi di formazione interni;

   j) lettere di trasmissione di copie di leggi e decreti.

3. Non si registrano i documenti pervenuti senza lettera di accompagnamento, quali ad esempio i verbali di gara, di consegna lavori, ecc. Tali documenti sono smistati direttamente all'Ufficio competente.

4. Le risposte agli accertamenti d'ufficio (ad es. controlli sul casellario giudiziale) e ai controlli sulle dichiarazioni sostitutive possono non essere registrate a protocollo nei casi in cui l'esito dell'accertamento consista nell'apposizione da parte dell'Amministrazione certificante di un timbro e di una sottoscrizione sulla richiesta dell'Ente e qualora nel procedimento amministrativo non sia necessaria la data certa di ricevimento. In tal caso, il ricevimento dell'esito è memorizzato nel registro di protocollo, utilizzando il campo "note" con la dicitura "pervenuto esito del…".

Art. 24. Documenti sottoposti a registrazione particolare

1. I documenti indicati all'art. 23, c.1, lett. l) sono sottoposti a registrazione presso registri autonomi.

2. Il registro contiene le seguenti informazioni:

   a) i dati identificativi di ciascun atto (autore, oggetto, data) registrati in modo non modificabile;

   b) i dati di classificazione e fascicolazione;

   c) il numero di registrazione, che è un numero progressivo annuale, registrato in modo non modificabile.

Art. 25. La segnatura di protocollo

1. La segnatura di protocollo consiste nell'apposizione al documento di un segno grafico riportante, in forma permanente non modificabile, le informazioni riguardanti la registrazione di protocollo.

2. La registrazione di protocollo e la segnatura costituiscono un'operazione unica e vanno effettuate contemporaneamente; hanno entrambe natura di atto pubblico.

3. La segnatura di protocollo viene apposta di norma sul recto (il davanti) del primo foglio del documento analogico mediante etichetta autoadesiva corredata di codice "Quick Response" identificativo del documento.

4. L'operazione di acquisizione dell'immagine dei documenti cartacei viene eseguita dopo l'operazione di segnatura, in modo da acquisire con la scansione anche il segno sul

documento. Il software assegna automaticamente l'immagine del documento alla sua registrazione di protocollo.

5. Nel caso di documenti informatici i dati di segnatura di protocollo sono contenuti un'unica volta nell'ambito dello stesso messaggio in un file conforme alle specifiche dell'ExtensibleMarkup Language (XML) e compatibile con il Document Type Definition (DTD).

Art. 26. Elementi della segnatura

1. L'Unione recepisce come elementi obbligatori della segnatura di protocollo sia le informazioni minime, attinenti alla funzione identificativa di carattere giuridico-probatorio ai sensi del comma 1 dell'art. 55 del Testo Unico, sia le informazioni facoltative di carattere gestionale previste dal comma 3 del citato art. 55 (identificazione della AOO e indice di classificazione).

Art. 27. Differimento delle registrazioni

1. Le registrazioni di protocollo dei documenti pervenuti presso l'Amministrazione sono effettuate nella giornata di arrivo e comunque non oltre le 48 ore dal ricevimento di detti documenti.
2. Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza, previo motivato provvedimento del RSP, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.
3. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento sopra citato.

Art. 28. Documenti riservati

1. Sono previste particolari forme di riservatezza e di accesso controllato al protocollo unico per:

   a) documenti contenenti dati sensibili e giudiziari ai sensi del Codice della privacy;

   b) ogni altra tipologia individuata dal RSP, con successivo atto, su indicazione del Segretario dell'Unione e d'intesa con i responsabili delle UOR.
2. Le procedure adottate per la gestione dei documenti e dei procedimenti amministrativi ad accesso riservato, comprese la registrazione, la segnatura, la classificazione e la fascicolazione, sono le stesse adottate per gli altri documenti e procedimenti amministrativi, ma la visibilità del documento è consentita solo alle persone autorizzate.
3. I documenti registrati in modalità riservata divengono integralmente consultabili alla scadenza dei termini indicati dalla normativa vigente. Motivate richieste di consultazione possono essere accolte prima della scadenza dei termini con le procedure previste dalla normativa vigente in tema di accesso agli atti amministrativi.

Art. 29. Modifica e annullamento di una registrazione

1. Ciascun operatore può provvedere direttamente alla modifica degli elementi facoltativi delle registrazioni di protocollo che ha effettuato. Il sistema consente la visualizzazione delle modifiche effettuate .
2. La modifica o l'annullamento di una registrazione di protocollo deve essere richiesto entro 24 ore, con specifica nota indirizzata al RSP, adeguatamente motivata, attraverso il sistema gestionale/applicativo informatico del protocollo all'Ufficio Protocollo.
3. L'annullamento viene effettuato in maniera tale da consentire la lettura delle informazioni registrate in precedenza e da non alterare le informazioni registrate negli elementi obbligatori di protocollo. Nel record di protocollo appaiono in forma ben visibile, oltre alla dicitura "annullato", la data e il nome dell'operatore che ha effettuato l'annullamento, nonché la motivazione dell'annullamento.

4. L’annullamento delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile determina l’automatico e contestuale annullamento della intera registrazione di protocollo
5. L’annullamento anche di un solo campo delle altre informazioni, registrate in forma immodificabile, necessario per correggere errori intercorsi in sede di immissione di dati, deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l’ora e all’autore della modifica.

Art. 30. Registro giornaliero di protocollo

1. Il responsabile provvede alla produzione del registro giornaliero di protocollo, costituito dall’elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell’arco di uno stesso giorno ivi comprese le registrazioni annullate o modificate nella stessa data.
2. Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l’immodificabilità del contenuto.

Art. 31. Registro di protocollo di emergenza

1. Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico, ogni evento deve essere registrato su un supporto alternativo anche cartaceo, denominato *Registro di emergenza* sul quale devono essere riportate la causa, la data e l’ora di inizio dell’interruzione, la data e l’ora di ripristino della piena funzionalità del sistema ed eventuali annotazioni ritenute rilevanti dal RSP.
2. Prima di autorizzare l’avvio della procedura, il RSP deve impostare e verificare la correttezza di data e ora sui rispettivi registri di emergenza.
3. Ogni registro di emergenza inizia il 1° gennaio e termina il 31 dicembre di ogni anno. Il RSP deve annotare nel protocollo informatico unico i periodi di attivazione del registro di emergenza.
4. Nel registro di emergenza ogni documento è individuato da numero e anno di registrazione, dall’UOR di assegnazione e dal numero di protocollo.
5. Una volta ripristinata la piena funzionalità del sistema, il RSP provvede alla chiusura del registro di emergenza, annotando su di esso il numero di registrazioni effettuate e la data e ora di chiusura.
6. Alla ripresa della piena funzionalità del sistema di protocollo informatico, l’incaricato adibito al protocollo attribuisce ad ogni registrazione recuperata dal registro di emergenza un nuovo numero di protocollo informatico, seguendo senza soluzione di continuità la numerazione raggiunta al momento dell’interruzione del servizio. A tale registrazione sono associati anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.
7. Ai fini della individuazione della data di ricevimento del documento si fa riferimento al numero attribuito dal registro di emergenza.

Art. 32. Lettere anonime, prive di firma o con firma illeggibile

1. Le lettere anonime sono protocollate e identificate come tali, con la dicitura “anonimo” nel campo “Mittente”.
2. Le lettere con mittente, prive di firma, vanno protocollate ed identificate come tali, specificando nel campo oggetto “documento privo di firma”. Compete al responsabile del procedimento valutare se il documento privo di firma debba ritenersi valido e come tale trattato dall’Ufficio assegnatario.
3. Sono equiparati ai documenti non firmati quelli pervenuti con firma illeggibile. Nel caso il mittente non sia identificabile, nel campo relativo si indica “non identificato”.

Art. 33. Documenti ricevuti sulle caselle personali di posta elettronica

1. Per le caselle di posta elettronica non certificata è a discrezione del Responsabile del Servizio o del dipendente a cui è affidata la gestione della casella di posta elettronica la trasmissione al protocollo per un'acquisizione formale.
2. I messaggi e i documenti ricevuti sulle caselle personali di posta elettronica e non conformi agli standard indicati dalla normativa vigente devono essere considerati documenti analogici di tipo cartaceo e quindi devono essere stampati con l'apposizione della dicitura "documento ricevuto tramite posta elettronica".
3. Nel caso in cui il documento pervenuto via posta elettronica debba essere acquisito in un procedimento amministrativo per il quale è indispensabile verificare la certezza della provenienza del documento medesimo, deve essere richiesta la trasmissione tramite pec, in caso di impossibilità la consegna, del documento originale, che sarà il solo protocollato.

Art. 34. Ricezione di documenti informatici su supporti rimovibili

1. Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, l'Amministrazione si riserva la facoltà di acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decifrare e interpretare con le tecnologie a sua disposizione; superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.
2. Qualora il documento informatico su supporto rimovibile venga consegnato direttamente all'Amministrazione e sia accompagnato da una lettera di trasmissione, è quest'ultima ad essere protocollata; qualora, invece, manchi la lettera di trasmissione, sarà protocollato previa la compilazione dell'interessato di un documento autografo di presentazione.

Art. 35. Documenti in partenza con il medesimo contenuto indirizzati a più destinatari

1. Nel caso di documenti con contenuto identico indirizzati a molteplici soggetti il sistema informatico di protocollazione prevede la possibilità di duplicare la prima registrazione di protocollo inserita nell'apposito fascicolo attribuendo ad ognuno di essi una propria registrazione e numero di protocollo.
2. È possibile dare un unico numero di protocollo al documento identico indirizzato a molteplici soggetti soltanto qualora si tratti di comunicazioni tali da non implicare alcun impegno giuridico. In tal caso, nella registrazione di protocollo, va riportato il nominativo del primo destinatario seguito dalla indicazione «… ed altri. Vedi elenco allegato alla minuta»; alla registrazione di protocollo va associato il file contenente l'elenco dei destinatari. Tale elenco in formato cartaceo va allegato alla minuta.

Art. 36. Offerte per gare, appalti, concorsi, ecc. in busta chiusa e sigillata

1. La registrazione di offerte per gare, appalti, concorsi, ecc. in busta chiusa e sigillata deve essere effettuata sulla base degli elementi rilevabili dalla busta o involto, elementi che devono essere specificati nei relativi bandi. La segnatura deve essere apposta sulla busta o sull'involto chiusi, tempestivamente e comunque nella giornata di ricevimento. È prevista inoltre l'indicazione dell'ora di ricezione per le offerte giunte l'ultimo giorno utile per la presentazione.
2. Una volta aperte le buste la segnatura deve essere apposta, a cura del responsabile della procedura di gara, anche sui documenti in esse contenuti.

Art. 37. Documenti pervenuti all'Unione per errore

1. I documenti pervenuti per errore all'Unione Terred'acqua non devono essere protocollati e devono essere spediti immediatamente al destinatario con la dicitura «Erroneamente pervenuto all'Unione Terred'acqua il ...».

2. Nel caso in cui un documento pervenuto per errore venga erroneamente registrato al protocollo, si provvede ad apporre sul documento la dicitura “erroneamente pervenuto al all’Unione Terred’acqua il ... e protocollato per errore” e a spedirlo accompagnato da una specifica lettera di trasmissione protocollata con numero diverso rispetto a quello attribuito erroneamente al documento.
3. Qualora il destinatario non sia individuabile, il documento è rimandato al mittente.

Art. 38. Documenti pervenuti senza indicazione esplicita del destinatario

1. I documenti pervenuti tramite il servizio postale e presentati a integrazione o comunque privi di indicazione chiara del destinatario “Unione Terred’acqua**”**, vengono consegnati senza essere protocollati all’Ufficio competente, unitamente alla busta.
2. Se la consegna avviene a mano l’addetto dell’Ufficio ricevente deve far redigere al consegnatario una nota di accompagnamento oppure far apporre una nota esplicativa sul documento («Al Unione Terred’acqua »).

Art. 39. Restituzione di documenti protocollati

1. Se le fasi del procedimento rendono necessaria la restituzione del documento protocollato o di un suo allegato (es: fideiussione a seguito di svincolo, documenti per gare d’appalto contenenti fideiussioni…), si procede a effettuare una copia del documento e ad annotarvi i motivi della restituzione e gli eventuali atti di riferimento.

Art. 40. Procedimenti che prevedono la redazione o l’invio di documenti su web

1. Nell’eventualità di documenti per i quali sia imposto da altre Amministrazioni l’invio telematico tramite specifiche *form* sul web, al fine di rispettare il principio di documentalità, l’invio deve essere sottoposto a registrazione di protocollo attraverso il salvataggio del risultato dell’invio e, ove possibile, del file dei dati trasmessi.
2. Non è soggetto a registrazione di protocollo l’inserimento obbligatorio di dati all’interno di *database* permanentemente *on line*.

SEZIONE VI – CLASSIFICAZIONE, ASSEGNAZIONE DEI DOCUMENTI E SCANSIONE

Art. 41. Classificazione dei documenti

1. Tutti i documenti ricevuti e prodotti dagli uffici dell'area organizzativa omogenea, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al titolario riportato **nell'allegato 1)**.
2. Nel momento in cui è effettuata la segnatura di protocollo deve inoltre essere apposta al documento la classificazione, sia per quanto riguarda la corrispondenza in arrivo che per quella in partenza.
3. La fascicolazione viene invece effettuata dal Servizio Responsabile del procedimento, sia per quanto riguarda l'arrivo e la partenza

Art. 42. Assegnazione dei documenti in originale

1. Al termine delle operazioni di registrazione, segnatura di protocollo e classificazione i documenti ricevuti sono assegnati in originale al Servizio competente.
2. Qualora un documento in arrivo tratti più oggetti/argomenti afferenti a procedimenti diversi, si deve attribuire comunque al documento un unico numero di protocollo, assegnarlo al Servizio competente in base all'oggetto/argomento principale o prevalente o, in assenza, al primo destinatario della lista qualora indirizzato a più destinatari all'interno dell'Unione, e assegnare il documento in copia agli altri Servizi, esclusivamente tramite protocollo informatico.

Art. 43. Assegnazione dei documenti in copia

1. L'Ufficio Protocollo assegna in copia agli altri Uffici il documento qualora ritenga utile o necessario che questi, per la loro competenza, ne vengano informati, o su richiesta degli Uffici stessi. Il Responsabile del procedimento può assegnare in copia ad altri Uffici il documento che ha in carico, qualora lo ritenga utile o necessario.
2. Nel caso di documento che prevede destinatari in copia per conoscenza, dopo la registrazione e l'assegnazione dell'originale, l'Ufficio Protocollo provvede a registrare, mediante l'apposita funzione, a chi sono inviate le copie per conoscenza esclusivamente tramite protocollo informatico.
3. I destinatari delle copie per conoscenza ai sensi dei commi precedenti possono scegliere di non conservarle, una volta acquisita la conoscenza dell'oggetto.

Art. 44. Assegnazione di originali plurimi, per competenza o per conoscenza

1. Il documento in più esemplari originali indirizzato a più destinatari all'interno dell'Unione viene registrato dall'Ufficio ricevente con un unico numero di protocollo, assegnato al Servizio competente in base all'oggetto/argomento principale o prevalente o, in assenza, al primo destinatario della lista, e registrato in copia agli altri destinatari, limitandosi a riportare sugli altri esemplari la stessa segnatura e ad apporre la dicitura "copia".
2. I documenti in più esemplari, identici per contenuto ma con diversi numeri di protocollo, indirizzati a più destinatari all'interno dell'Unione, sono trattati ognuno come documento originale e assegnati ai sensi dell'art. 42, c. 1 (Assegnazione dei documenti in originale).

Art. 45. Correzione di una assegnazione

1. Nel caso di assegnazione errata, il Servizio che riceve il documento, in base alle abilitazioni del sistema, può restituire il documento all'Ufficio che ha effettuato la registrazione, che provvede alla correzione, oppure può trasferirlo direttamente sul carico del Servizio competente nel più breve tempo possibile, provvedendo contestualmente ad inviare il documento cartaceo al Servizio medesimo.

Art. 46. Scansione

1. I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine attraverso un processo di scansione.
2. Le operazioni che costituiscono il processo di scansione sono:

   a) acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico file;

   b) verifica della leggibilità e della qualità delle immagini acquisite;

   c) collegamento delle immagini alle rispettive registrazioni di protocollo in modo non modificabile;

   d) memorizzazione delle immagini su supporto informatico.
3. Gli Uffici che protocollano direttamente i documenti di loro competenza possono eseguirne la scansione in qualsiasi momento utilizzando, , lo scanner collegato al sistema di protocollo informatico.
4. I documenti cartacei dopo l'operazione di riproduzione in formato immagine vengono inviati ai RPA destinatari per le operazioni di fascicolazione e conservazione.
5. I documenti contenenti dati sensibili e giudiziari sono scansionati previa verifica dell'attribuzione del corretto livello di riservatezza in fase di registrazione di protocollo.

Art. 47. Documenti non soggetti a scansione

1. Non sono soggetti a scansione:

   a) il documento cartaceo ricevuto in formato diverso da quello A4 oppure su carta colorata;

   b) il documento cartaceo che supera le 50 pagine, salvo esplicita richiesta del responsabile del procedimento.

Art. 48. Smistamento dei documenti

1. I documenti ricevuti dall'Ufficio Protocollo su supporto cartaceo vengono smistati giornalmente, dopo la loro protocollazione, attraverso il sistema di posta interna.

Art. 49. Trasmissione dei documenti su supporto informatico

1. Fino al completo utilizzo della posta certificata quale canale privilegiato per la trasmissione dei documenti, gli stessi possono essere consegnati all'Amministrazione anche attraverso un supporto digitale (CD, Floppy, ecc.); il formato richiesto è PDF, anche per i progetti e gli elaborati cartografici.
2. Il contenuto del supporto digitale viene poi inserito in allegato all'istanza presentata, attraverso il software applicativo di gestione del protocollo informatico.

SEZIONE VII - SPEDIZIONE DEI DOCUMENTI

Art. 50. Trasmissione dei documenti in partenza

1. La trasmissione dei documenti può avvenire per mezzo di:

   a) posta elettronica certificata (PEC);

   b) posta elettronica personale;

   c) servizio di posta tradizionale (ad es. per raccomandata, posta prioritaria, posta celere, assicurata, corriere). In questo caso i documenti da spedire sono trasmessi a cura dei vari Servizi all'Ufficio abilitato alla spedizione.

   d) telefax;

   e) consegna diretta al cittadino.

2. Nel caso di spedizioni tramite il servizio postale che richiedano una documentazione da allegare alla busta (quali ad es. raccomandata con ricevuta di ritorno, posta celere, corriere, ecc.) la relativa modulistica viene compilata a cura degli Uffici che richiedono tale operazione.
3. I singoli Servizi consegnano la posta cartacea in spedizione all'Ufficio abilitato in busta chiusa e già indirizzata, senza allegare la minuta.
4. L'Ufficio di spedizione esegue le operazioni di pesatura, calcolo delle spese postali e tenuta della relativa contabilità.

Art. 51. Spedizione dei documenti su supporto cartaceo

1. I documenti da spedire su supporto cartaceo sono trasmessi all'ufficio abilitato alla spedizione dopo che sono state eseguite le operazioni di registrazione di protocollo, segnatura di protocollo, classificazione e fascicolazione, a cura dell'ufficio produttore.
2. La copia firmata del documento spedito deve essere conservata all'interno del relativo fascicolo

Art. 52. Spedizione dei documenti informatici

1. I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica.
2. Per la spedizione dei documenti informatici l'Amministrazione si avvale della casella di posta elettronica certificata (PEC) e dei servizi di autenticazione e marcatura temporale offerti da un certificatore iscritto nell'elenco pubblico tenuto dall'Autorità per l'informatica nella pubblica amministrazione (D. Lgs. n. 68/2005 e successive modificazioni).
3. L'operatore invia il documento informatico al destinatario, attraverso la casella di posta certificata istituzionale, utilizzando le funzionalità del software di protocollo, che provvede:

   a. ad effettuare l'invio telematico utilizzando i servizi di autenticazione e marcatura temporale offerti dal certificatore scelto dall'Amministrazione;

   b. a verificare l'avvenuto recapito dei documenti spediti per via telematica;

   c. ad archiviare le ricevute elettroniche collegandole alle registrazioni di protocollo dei rispettivi documenti spediti.

4. L'Amministrazione utilizza la casella di PEC per inviare comunicazioni ad altre Pubbliche Amministrazioni, imprese o soggetti appartenenti ad ordini professionali, cittadini in possesso di un indirizzo PEC, cittadini in possesso di un indirizzo mail normale, per l'invio di comunicazioni che non richiedano la notifica a mezzo posta.

Art. 53. Ricezione e spedizione dei documenti a mezzo telefax

1. I documenti pervenuti tramite telefax o fax server, se soggetti alla registrazione di protocollo, sono consegnati all'Ufficio Protocollo, che provvede alle operazioni di registrazione e segnatura di protocollo, classificazione ed assegnazione.
2. Nel caso in cui ad un documento ricevuto via telefax faccia seguito l'originale, l'addetto alla registrazione di protocollo deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax e apporre la dicitura "già pervenuto via fax il giorno…". E' necessario comunque accertare che si tratti del medesimo documento: qualora si dovesse riscontrare una differenza, anche minima, si deve procedere alla registrazione con un nuovo numero di protocollo.
3. Il documento in partenza trasmesso via telefax reca una delle seguenti diciture:

   a) "Anticipato via telefax", se il documento originale viene successivamente inviato al destinatario;

   b) "La trasmissione via fax del presente documento non prevede l'invio del documento originale" nel caso in cui l'originale non venga spedito. Il RPA è comunque tenuto a spedire l'originale qualora il destinatario ne faccia motivata richiesta.
4. La segnatura viene apposta sul documento e non sulla copertina di trasmissione. La copertina del telefax e il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.

SEZIONE VIII - GESTIONE DEI DOCUMENTI E DEI FLUSSI DOCUMENTALI

Art. 54. Il piano di classificazione

1. Il piano di classificazione viene aggiornato periodicamente su proposta del RSP e le eventuali integrazioni e modifiche entrano in vigore il 1° gennaio dell'anno seguente alla loro approvazione.
2. Il sistema di gestione del protocollo garantisce la storicizzazione del piano di classificazione in relazione alle modificazioni delle funzioni e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del piano vigente al momento della produzione degli stessi.

Art. 55. Formazione e gestione dei fascicoli

1. Il fascicolo è l'unità archivistica indivisibile di base che raccoglie i documenti relativi a un procedimento amministrativo o ad un affare, legati da un vincolo originario e necessario, a prescindere dalla forma e dal supporto.
2. In base ai criteri fissati nell'art. 57 (Criteri per la costituzione dei fascicoli), il responsabile di servizio o altra persona da lui incaricata, è responsabile della corretta fascicolazione e custodia di tutta la documentazione informatica e cartacea di cui risulta assegnatario e pertanto si occupa di:
   a) formare nuovi fascicoli,

   b) gestire fascicoli già formati, inserendo la documentazione sia in entrata che in uscita attraverso le operazioni di classificazione,

   c) chiudere il fascicolo quando la pratica cui si riferisce è conclusa, disponendo la trasmissione al servizio che ne cura l'archiviazione.

3. Per esigenze pratiche, derivanti dalla natura del procedimento, dalla sua durata o anche in funzione della quantità dei documenti da gestire, il fascicolo può essere distinto in sottofascicoli, oppure in più fascicoli fra loro collegati.
4. I documenti, all'interno del fascicolo, vanno conservati secondo l'ordine progressivo di registrazione o, se assente, secondo la propria data.

Art. 56. Identificazione del fascicolo

1. Il fascicolo è individuato dai seguenti elementi:
   a) anno di apertura;

   b) titolo e classe di appartenenza o indice di classificazione;

   c) numero di repertorio, cioè il numero sequenziale attribuito automaticamente dal sistema;

   d) oggetto, cioè un testo sintetico e normalizzato che descrive puntualmente e compiutamente l'affare/attività cui si riferisce.
2. Oltre a questi elementi devono essere indicati la UOR e il RPA, l'eventuale restrizione all'accesso nel rispetto della tutela della riservatezza e dei dati personali, l'indicazione dell'anno di chiusura e il suo status (corrente, deposito, storico).

Art. 57. Criteri per la costituzione dei fascicoli

1. I criteri per la costituzione dei fascicoli sono:
   a) fascicoli relativi ad affari o procedimenti amministrativi;

b) fascicoli relativi a persone fisiche o giuridiche;

c) fascicoli per attività o tipologia di forma del documento.

2. L'Ufficio Protocollo controlla periodicamente la tenuta dei fascicoli e la eventuale presenza di documenti non inseriti in fascicoli.

Art. 58. Fascicoli relativi ad affari o procedimenti amministrativi

1. Qualora un documento dia luogo all'avvio di un autonomo affare o procedimento amministrativo, il RPA assegnatario provvede all'apertura di un nuovo fascicolo.
2. Gli elementi che individuano il fascicolo sono gestiti dal RPA. Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto.

Art. 59. Fascicoli relativi a persone fisiche o giuridiche

1. Per ogni persona fisica o giuridica (ad esempio: personale dipendente, assistiti, associazioni, attività economiche, ecc.) deve essere istruito un fascicolo nominativo. Il fascicolo viene aperto al momento dell'inizio del rapporto con l'Unione Terred'acqua e chiuso al momento della cessazione del rapporto.
2. I fascicoli delle persone fisiche e giuridiche costituiscono una serie archivistica autonoma per ciascuna delle categorie di persone fisiche o giuridiche (serie dei fascicoli dei dipendenti, serie dei fascicoli degli assistiti, ecc.). All'interno di ciascuna serie i fascicoli vanno conservati in ordine cronologico di instaurazione del rapporto.

Art. 60. Fascicoli per attività o tipologia di forma del documento

1. I fascicoli per attività o tipologia di forma del documento comprendono i documenti prodotti nello svolgimento di un'attività amministrativa semplice, ripetitiva e non discrezionale, che si esaurisce in risposte obbligate o meri adempimenti (ad esempio: il fascicolo delle notifiche, delle pubblicazioni all'albo pretorio, ecc).
2. Il fascicolo per attività comprende documenti con destinatari e oggetti diversi, ma con identica classifica; la sua durata è solitamente annuale ma se la massa documentale è eccessiva può articolarsi secondo altre cadenze temporali (ad esempio semestrale o mensile).

Art. 61. Formazione delle serie, dei registri e dei repertori

1. La documentazione dell'Unione forma la serie generale del "Carteggio" raccolta in fascicoli e suddivisa per anni secondo i titoli e le classi.
2. Il piano di classificazione prevede anche la formazione di talune serie all'interno di ciascun titolo e di alcune serie di carattere generale, nonché la enumerazione dei registri.
3. Sono repertori di carattere generale e trasversale:
   a) ordinanze emanate dal Presidente dell'Unione e dai Responsabili;

   b) determinazioni dei Responsabili;

   c) deliberazioni del Consiglio dell'Unione;

   d) deliberazioni della Giunta dell'Unione;

   e) circolari;

   f) contratti e convenzioni;

   g) albo pretorio;

   h) notifiche.

Art. 62. Repertorio dei fascicoli

1. Il repertorio dei fascicoli è lo strumento sul quale si annotano con un numero identificativo progressivo i fascicoli secondo l'ordine cronologico con cui si costituiscono all'interno delle suddivisioni del piano di classificazione. La catena numerica che assegna il numero ai singoli fascicoli è trasversale a tutti i servizi ed è gestita dal sistema di protocollo informatico.
2. Sono elementi costitutivi del repertorio:

   a) anno di istruzione del fascicolo;

   b) classificazione completa;

   c) numero ed eventuali partizioni in sottofascicoli;

   d) anno di chiusura;

   e) oggetto del fascicolo ed eventualmente dei sottofascicoli;

   f) annotazione dello *status* relativo all'età (corrente, deposito, storico, o in alternativa, dell'avvenuto scarto);

3. Ciascun fascicolo è registrato nel repertorio dei fascicoli che ha cadenza annuale, inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

SEZIONE IX - ARCHIVIAZIONE E CONSERVAZIONE DEI DOCUMENTI

Art. 63. Memorizzazione dei documenti informatici e delle rappresentazioni digitali dei documenti cartacei

1. I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo o al momento dell'inserimento negli appositi repertori informatici.
2. Le rappresentazioni digitali dei documenti su supporto cartaceo, acquisite con l'ausilio dello scanner, sono memorizzate nel sistema, in modo non modificabile, al termine del processo di scansione.

Art. 64. Conservazione dei documenti informatici

1. La conservazione dei documenti informatici è affidata tramite apposita convenzione al Polo Archivistico Regionale della Regione Emilia) Romagna, in possesso dei requisiti e delle autorizzazioni previste dalla normativa vigente; le tipologie di documenti da affidare in conservazione saranno definite con appositi atti, unitamente alle relative specifiche tecniche.
2. Il versamento dei documenti in conservazione avviene attraverso un apposito collegamento informatico tra i software gestionali dell'ente e la piattaforma di gestione documentale con la piattaforma di conservazione; il trasferimento è programmato una volta a settimana, in orario notturno, mentre il registro giornaliero di protocollo è versato in conservazione quotidianamente. Il Polo archivistico della Regione Emilia-Romagna ha adottato il Manuale di conservazione previsto dal DPCM 3 dicembre 2013, pubblicato sul sito web istituzionale e sul sito di AGID.

Art. 65. Archiviazione e conservazione dei documenti caratacei

1. L'archivio è il complesso dei documenti prodotti o acquisiti dall'Ente durante lo svolgimento della propria attività. I documenti amministrativi prodotti o detenuti da questo Ente sono oggetto di tutela ai sensi dell'art. 10 del Codice dei beni culturali di cui al decreto legislativo 42/2004.
2. L'Unione Terred'acqua, ai sensi dell'art. 30 del predetto codice, assolve all'obbligo di conservazione e ordinamento degli archivi.
3. Ai fini di un corretto esercizio dell'azione amministrativa, i fascicoli prodotti dagli uffici dell'Unione sono raccolti in archivi che possono essere distinti in:

Archivio corrente – la parte di documentazione relativa agli affari ed ai procedimenti in corso di trattazione
Archivio di deposito – la parte di documentazione di affari esauriti,
Archivio storico – la parte di documentazione relativa agli affari esauriti destinata alla conservazione perenne

La coesistenza, nell'ambito di uno stesso procedimento, di documenti di natura mista (digitali e e cartacei) dà vita al cosiddetto "archivio ibrido".

Per quanto riguarda le procedure di scarto dovrà farsi riferimento previste dalla vigente normativa e dalle procedure della Sovrintendenza archivistica regionale.

SEZIONE X - ACCESSIBILITÀ E SICUREZZA DEL SISTEMA DI GESTIONE DEI DOCUMENTI

Art. 66. Accessibilità da parte degli utenti appartenenti all'AOO

1. La riservatezza delle registrazioni di protocollo è garantita dal sistema attraverso l'uso di profili utente e password.
2. L'operatore che effettua la registrazione di protocollo inserisce il livello di riservatezza richiesto per il documento in esame, se diverso da quello standard applicato automaticamente dal sistema.
3. Il livello di riservatezza applicato ad un fascicolo è ereditato automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. Quelli che invece hanno un livello di riservatezza superiore lo mantengono.
4. Sono previsti particolari livelli di riservatezza e di accesso controllato al protocollo unico per:
   a) i documenti che contengono dati sensibili e giudiziari ai sensi del Codice della privacy;

   b) i documenti sottratti all'accesso in base alla normativa vigente.

5. Sulla base delle richieste avanzate dagli uffici dell'Amministrazione, i diversi livelli di autorizzazione ed i conseguenti differenti profili sono assegnati agli utenti dal Responsabile del Servizio Protocollo il quale, inoltre, provvede all'assegnazione di eventuali nuove autorizzazioni, alla revoca o alla modifica di quelle già assegnate.

Art. 67. Piano per la sicurezza informatica

1. Il Piano per la sicurezza informatica è il documento relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni.
2. Costituisce allegato al presente manuale e viene redatto dal servizio informatico dell'Unione Terred'acqua, d'intesa con il responsabile della conservazione.

SEZIONE XI - ALBO PRETORIO ON LINE

Art. 68. Ambito di applicazione

1. L'albo pretorio on line, ai sensi dell'art. 32, c. 1, della Legge 69 del 18/6/2009, dall'1/1/2011 rappresenta l'unica forma di pubblicità legale degli atti e provvedimenti amministrativi soggetti per legge a obblighi di pubblicazione.

Art. 69 – Principi e finalità

1. L'Albo pretorio informatico è istituito in apposita area individuata nel portale istituzionale dell'Unione al fine di assicurare l'adempimento degli obblighi di pubblicazione di atti e provvedimenti aventi effetto di pubblicità legale.
2. Restano, in ogni caso, salve le ulteriori forme di pubblicità previste da leggi e/o regolamenti per particolari tipi di atti.

Art. 70 – Servizio Albo pretorio

1. La tenuta dell'Albo pretorio on line è a cura del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, ai soli fini di questo atto denominato "Servizio Albo pretorio".
2. Il Servizio Albo pretorio procede alla pubblicazione di tutti gli atti esterni.
3. Le pubblicazioni degli atti dei servizi sono di competenza dei singoli servizi come precisato nell'art. 74, c.1.
4. Il Servizio Albo pretorio individua i responsabili competenti per l'inserimento degli atti all'Albo pretorio.

Art. 71 – Acquisizione dei documenti da parte degli utenti

1. Limitatamente al periodo di pubblicazione, l'acquisizione dei documenti pubblicati da parte dell'utenza avviene gratuitamente e senza formalità, mentre le disposizioni in materia fiscale e di bollo sono applicate solo in caso d'uso.
2. Decorso il termine di pubblicazione legale, trova applicazione la disciplina in materia di diritto di accesso.

Art. 72 – Modalità di pubblicazione dei documenti

1. I documenti soggetti ad obbligo di pubblicazione sono pubblicati in versione integrale e conforme all'originale, compresi gli eventuali allegati informatici.
2. Gli allegati che, per motivi tecnici, non possono essere pubblicati con modalità informatica sono comunque visionabili presso il Servizio Segreteria dell'Unione e sono liberamente consultabili per l'esclusivo periodo di pubblicazione degli atti cui fanno riferimento.
3. I documenti sono pubblicati all'Albo pretorio informatico per il tempo stabilito dalle singole disposizioni di legge o di regolamento e sono rimossi dall'Albo al termine del periodo di pubblicazione.
4. Il periodo di pubblicazione è di quindici giorni consecutivi, salvo termini diversi previsti da norme speciali.

Art. 73 – Annullamento della pubblicazione

1. Dopo la pubblicazione dell'atto, la registrazione di pubblicazione è immodificabile, salva la possibilità di inserire note interne di pubblicazione.
2. Il responsabile del procedimento amministrativo o il soggetto esterno istante possono richiedere l'annullamento della pubblicazione. L'atto rimane pubblicato fino al termine di pubblicazione originario con la dicitura "Annullato in data …". Contestualmente è possibile richiedere la pubblicazione del documento corretto: in tal caso il termine di pubblicazione ricomincia a decorrere dalla data della nuova richiesta.

Art. 74 – Competenze e responsabilità

1. Il programma di pubblicazione dei documenti integrato con il software gestionale del protocollo e degli atti amministrativi permette la gestione decentrata della pubblicazione degli atti all'Albo pretorio *on line*. Ciascun Servizio provvede quindi autonomamente alla pubblicazione degli atti di propria competenza, inserendo i dati richiesti dal sistema.
2. L'atto da pubblicare deve essere allegato alternativamente secondo le seguenti modalità:
   a) in file formato pdf, firmato digitalmente;
   b) in file formato pdf con firma a stampa e richiamo nell'atto all'art. 3, c. 2 del D.lgs. 39/1993;
   c) in file formato pdf ottenuto dalla scansione del documento in formato cartaceo con firma autografa.
3. Spetta al responsabile del procedimento amministrativo o comunque al soggetto esterno richiedente garantire che l'atto da pubblicare sia conforme alle norme sulla tutela della riservatezza previste dal D. lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), nonché di ogni altra disposizione di legge o di regolamento che rilevi ai fini del trattamento di dati personali.
4. Il Responsabile del Servizio Albo pretorio non è responsabile del contenuto degli atti pubblicati.

Art. 75 – Gestione del servizio per la pubblicazione di atti su richiesta di terzi

1. Il Responsabile del Servizio Albo pretorio cura la pubblicazione degli atti su richiesta di soggetti esterni all'Amministrazione.
2. Le richieste di pubblicazione di atti da parte di soggetti esterni possono pervenire in uno qualunque dei modi di trasmissione di documenti previsti dal Manuale di Gestione, almeno il giorno lavorativo precedente la data di inizio della pubblicazione.
3. Il soggetto richiedente indica le date di inizio e fine pubblicazione, allegando, in alternativa:

   - il file dell'atto da pubblicare in formato pdf, firmato digitalmente;

   - il documento in formato cartaceo con firma autografa, che il Servizio Albo pretorio provvederà a scansionare.

Art. 76 – Registro dell'Albo pretorio e attestazione di pubblicazione

1. Il registro informatico dell'Albo pretorio è costituito dai file di report, contenenti i progressivi di registrazione, firmati digitalmente dal Responsabile del Servizio Albo pretorio o da suo delegato.
2. L'attestazione di avvenuta pubblicazione viene rilasciata dal Responsabile del Servizio Albo pretorio o da suo delegato soltanto ai soggetti terzi:
   - tramite invio telematico degli estremi di pubblicazione all'ufficio o al soggetto richiedente, qualora il documento sia stato trasmesso in originale digitale o copia conforme digitale;
   - tramite apposita comunicazione al soggetto esterno degli estremi di pubblicazione, qualora il documento sia stato trasmesso in formato analogico.

SEZIONE XII - DISPOSIZIONI FINALI

Art. 77. Modalità di comunicazione del Manuale

1. In ottemperanza all'art. 5, comma 3 del DPCM 31 ottobre 2000, il presente Manuale di gestione viene reso accessibile mediante pubblicazione sul sito internet dell'Unione Terred'acqua

Art. 78. Modalità di aggiornamento del Manuale

1. Il Manuale di gestione, il titolario di classificazione, il piano di conservazione sono aggiornati ogniqualvolta risulti necessario, a seguito di innovazioni normative o regolamentari, con apposito provvedimento della Giunta dell'Unione.
2. Gli atti di gestione tecnica in attuazione del Manuale sono adottati con successivi provvedimenti del RSP.

ALLEGATO 1

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
1	0	**Amministrazione generale**
1	1	Legislazione e circolari esplicative
1	2	Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica
1	3	Statuto
1	4	Regolamenti
1	5	Stemma, gonfalone, sigillo
1	6	Archivio generale
1	7	Sistema informativo
1	8	Informazioni e relazioni con il pubblico
1	9	Politica del personale; ordinamento degli uffici e dei servizi
1	10	Relazioni con le organizzazioni sindacali e di rappresentanza del personale
1	11	Controlli interni ed esterni
1	12	Editoria e attività informativo-promozionale interna ed esterna
1	13	Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti
1	14	Interventi di carattere politico e umanitario; rapporti istituzionali
1	15	Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni
1	16	Area e città metropolitana
1	17	Associazionismo e partecipazione

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
2	0	**Organi di governo, gestione, controllo, consulenza e garanzia**
2	1	Sindaco
2	2	Vice-Sindaco
2	3	Consiglio
2	4	Presidente del Consiglio
2	5	Conferenza dei capigruppo e Commissioni del Consiglio
2	6	Gruppi consiliari
2	7	Giunta
2	8	Commissario prefettizio e straordinario
2	9	Segretario e Vice-segretario
2	10	Direttore generale e dirigenza
2	11	Revisori dei conti
2	12	Difensore civico
2	13	Commissario ad acta
2	14	Organi di controllo interni
2	15	Organi consultivi
2	16	Consigli circoscrizionali
2	17	Presidente dei Consigli circoscrizionali
2	18	Organi esecutivi circoscrizionali
2	19	Commissioni dei Consigli circoscrizionali
2	20	Segretari delle circoscrizioni
2	21	Commissario ad acta delle circoscrizioni
2	22	Conferenza dei Presidenti di quartiere

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
3	0	**Risorse umane**
3	1	Concorsi, selezioni, colloqui
3	2	Assunzioni e cessazioni
3	3	Comandi e distacchi; mobilità
3	4	Attribuzione di funzioni, ordini di servizio e missioni
3	5	Inquadramenti e applicazione contratti collettivi di lavoro
3	6	Retribuzioni e compensi
3	7	Trattamento fiscale, contributivo e assicurativo
3	8	Tutela della salute e sicurezza sul luogo di lavoro
3	9	Dichiarazioni di infermità ed equo indennizzo
3	10	Indennità premio di servizio e trattamento di fine rapporto, quiescenza
3	11	Servizi al personale su richiesta
3	12	Orario di lavoro, presenze e assenze
3	13	Giudizi, responsabilità e provvedimenti disciplinari
3	14	Formazione e aggiornamento professionale
3	15	Collaboratori esterni

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
4	0	**Risorse finanziarie e patrimonio**
4	1	Bilancio preventivo e Piano esecutivo di gestione (PEG)
4	2	Gestione del bilancio e del PEG (con eventuali variazioni)
4	3	Gestione delle entrate: accertamento, riscossione, versamento
4	4	Gestione della spesa: impegno, liquidazione, ordinazione e pagamento
4	5	Partecipazioni finanziarie
4	6	Rendiconto della gestione; adempimenti e verifiche contabili
4	7	Adempimenti fiscali, contributivi e assicurativi
4	8	Beni immobili
4	9	Beni mobili
4	10	Economato
4	11	Oggetti smarriti e recuperati
4	12	Tesoreria
4	13	Concessionari ed altri incaricati della riscossione delle entrate
4	14	Pubblicità e pubbliche affissioni

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
5	0	**Affari legali**
5	1	Contenzioso
5	2	Responsabilità civile e patrimoniale verso terzi; assicurazioni
5	3	Pareri e consulenze

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
6	0	**Pianificazione e gestione del territorio**
6	1	Urbanistica: piano regolatore generale e varianti
6	2	Urbanistica: strumenti di attuazione del piano regolatore generale
6	3	Edilizia privata
6	4	Edilizia pubblica
6	5	Opere pubbliche
6	6	Catasto
6	7	Viabilità
6	8	Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
6	9	Ambiente: autorizzazioni, monitoraggio e controllo
6	10	Protezione civile ed emergenze

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
7	0	**Servizi alla persona**
7	1	Diritto allo studio e servizi
7	2	Asili nido e scuola materna
7	3	Promozione e sostegno delle istituzioni di istruzione e della loro attività
7	4	Orientamento professionale; educazione degli adulti; mediazione culturale
7	5	Istituti culturali (Musei, Biblioteche, Teatri, Scuola comunale di musica, etc.)
7	6	Attività ed eventi culturali
7	7	Attività ed eventi sportivi
7	8	Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale
7	9	Prevenzione, recupero e reintegrazione dei soggetti a rischio
7	10	Informazione, consulenza ed educazione civica
7	11	Tutela e curatela di incapaci
7	12	Assistenza diretta e indiretta, benefici economici
7	13	Attività ricreativa e di socializzazione
7	14	Politiche per la casa
7	15	Politiche per il sociale

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
8	0	**Attività economiche**
8	1	Agricoltura e pesca
8	2	Artigianato
8	3	Industria
8	4	Commercio
8	5	Fiere e mercati
8	6	Esercizi turistici e strutture ricettive
8	7	Promozione e servizi

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
9	0	**Polizia locale e sicurezza pubblica**
9	1	Prevenzione ed educazione stradale
9	2	Polizia stradale
9	3	Informative
9	4	Sicurezza e ordine pubblico

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
10	0	**Tutela della salute**
10	1	Salute e igiene pubblica
10	2	Trattamento Sanitario Obbligatorio
10	3	Farmacie
10	4	Zooprofilassi veterinaria
10	5	Randagismo animale e ricoveri

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
11	0	**Servizi demografici**
11	1	Stato civile
11	2	Anagrafe e certificazioni
11	3	Censimenti
11	4	Polizia mortuaria e cimiteri

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
12	0	**Elezioni ed iniziative popolari**
12	1	Albi elettorali
12	2	Liste elettorali
12	3	Elezioni
12	4	Referendum
12	5	Istanze, petizioni e iniziative popolari

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
13	0	**Affari militari**
13	1	Leva e servizio civile sostitutivo
13	2	Ruoli matricolari
13	3	Caserme, alloggi e servitù militari
13	4	Requisizioni per utilità militari

UNIONE TERRED'ACQUA

Titolario di classificazione

Titolo	Classe	Descrizione
14	0	**Oggetti diversi**

ALLEGATO 2

Unione Terred'Acqua

PIANO DELLA SICUREZZA INFORMATICA

approvato con delibera della Giunta dell'Unione n. 64 del 28/12/2015

Sommario

1. Struttura del sistema e protezioni

1.1. Architettura della rete

Presso ogni comune dell'Unione c'e' un nodo principale di Lepida denominato PAL (Punto Accesso Lepida). Questi nodi sono collegati al nodo centrale di Persiceto con VPN configurando così una architettura a stella.
La rete Lepida è in fibra ottica Gbit.

Tutte le Sedi comunali sono collegate alla rete aziendale.

Tutti i dipendenti dotati di postazione di PC possono quindi collegarsi alla rete dati ed accedere ad internet. L'accesso ai dati è centralizzato verso la sede del CED SIAT a Persiceto, mentre per l'accesso ad internet, ogni comune "esce" dal proprio PAL di Lepida. Presso ogni PAL comunale è presente un firewall, gestito e configurato dal SIAT, per la protezione della rete stessa.

1.2. Sicurezza della rete

Tendenzialmente e preferibilmente tutte le sedi sono connesse alle sedi comunali dotate di PAL Lepida mediante LAN o MAN (metropolitan area network).
Ove non possibile si è proceduto alla connessione via VPN su linea ADSL oppure HDSL attraverso appositi firewall.
L'accesso alla rete comunale è comunque permesso solo tramite autenticazione con nome utente e password.
Tutti i sistemi elencati afferiscono a un sistema di firewall, che controlla il traffico dati in base a politiche di sicurezza prestabilite.

1.3. Architettura del Sistema Informatico

1.1.1. Banche dati

I dati strutturati delle applicazioni gestionali possono essere memorizzati in:

- banche dati centralizzate, per le applicazioni utilizzate da più utenti
- più raramente, su stazione di lavoro per applicazioni mono-utente o qualora il software non renda possibile l'installazione su server

Le banche dati degli applicativi gestionali ed ulteriori banche dati, nonché archivi documentali non strutturati sono conservati in:

- server e sistemi di memorizzazione centralizzati presso il CED dell'Unione (DB server e file server)
- server e/o sistemi di memorizzazione decentrati presso gli Enti
- server e/o sistemi di memorizzazione ubicati presso Datacenter esterni (es. Lepida, PARER, ecc.)
- Personal Computer distribuiti negli uffici degli enti.

Può quindi accadere che alcune banche dati risiedano esclusivamente sul personal computer dell'utente che le utilizza; ciò può accadere sia per scelta personale (**fortemente sconsigliata**) del singolo utente che volontariamente le mantiene solo sulla propria postazione, sia per le caratteristiche intrinseche del programma utilizzato. L'utente finale diventa quindi il responsabile unico dei documenti e delle banche dati non salvate sui server di rete (e quindi non ricomprese nel sistema centralizzato di backup schedulati). Gli addetti ai S.I. hanno sensibilizzato ed informato gli assegnatari dei P.C. su questa problematica.

1.1.2. Posta elettronica

La posta elettronica viene gestita esternamente; ai dipendenti o amministratori è assegnata una casella individuale nella forma nome.cognome@;
Esistono caselle non nominali corrispondenti a gruppi di lavoro o figure istituzionali ma per le quali è definito un responsabile della casella stessa.

1.1.3. Sistema di autenticazione

Il principale sistema di autenticazione è Microsoft Windows Active Directory, che viene utilizzato per

autenticare gli utenti di risorse condivise sulla rete quali:

- cartelle
- stampanti
- accesso agli applicativi

Alcune procedure applicative sono integrate con Active Directory di Windows e quindi le credenziali di accesso a queste procedure sono le stesse dell'accesso alla rete e al PC.
Altre procedure applicative, invece, non utilizzano questo sistema centralizzato, ma possiedono un proprio sistema di autenticazione.

Per l'accesso ai personal computer ci si avvale esclusivamente delle credenziali di Active Directory

Solo per manutenzione, gli amministratori o incaricati esterni (ditte esterne) possiedono delle apposite credenziali locali della postazione di lavoro stessa.

1.4. Sicurezza dei dati

1.1.4. Banche dati centralizzate

L'accesso ai dati avviene tramite le procedure gestionali che li trattano: all'utente viene richiesta la digitazione di username e password. Queste credenziali sono verificate dall'Active Directory per le procedure già integrate, oppure dalla procedura stessa.
Contestualmente viene verificato se l'utente è autorizzato all'utilizzo della funzionalità richiesta, cioè l'utente può essere abilitato solo ad alcuni moduli o funzionalità del programma applicativo.
Il sistema di autorizzazione è sempre gestito dalla procedura informatica.
La gestione del rilascio delle credenziali di Active Directory compete al servizio informativo Associato (SIAT)
Il rilascio e gestione delle credenziali o delle funzionalità utente all'interno del programma applicativo compete agli Uffici Responsabili dell'Unione e dei singoli Comuni, che agiscono nel rispetto di quanto previsto dal "Codice in materia di protezione dei dati personali", allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", in particolare dei Punti 13 e 14, che vengono riportati di seguito:

"13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione."

1.1.5. Archivi documentali centralizzati

I server contenenti archivi documentali richiedono l'autenticazione e l'autorizzazione dell'utente tramite il dominio Active Directory.
Questa autenticazione avviene in modo trasparente per l'utente (senza la richiesta di ulteriore autenticazioni) se le credenziali di accesso al PC sono le stesse che nel dominio Active Directory.

1.1.6. Banche dati ed archivi documentali residenti su P.C.

I PC che contengono banche dati locali o archivi documentali, contenenti dati personali e/o sensibili sono protetti da credenziali di accesso personali di Active Directory (oltre alla password di amministratore locale del PC utilizzata solo dal SIAT per interventi tecnici).

1.5. Aggiornamenti dei software

I programmi per elaboratore (inclusi i sistemi operativi) vengono tempestivamente aggiornati mediante l'installazione delle nuove versioni degli stessi o delle patches rilasciate dai produttori al fine di prevenirne la vulnerabilità e correggerne i difetti.
La frequenza di aggiornamento non può essere superiore ai 6 mesi.

2. Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni

2.1. Incaricati del trattamento informatico

Sono tutti gli operatori tecnici del servizio SIAT.

2.2. Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica

Il preposto alla gestione delle credenziali provvede a creare un account con password provvisoria da modificarsi obbligatoriamente al primo accesso.

2.3. Assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione consistono in un codice per l'autenticazione dell'incaricato (user-id tipicamente terredacqua\cognome.nome) associato ad una parola chiave riservata (password).

Le credenziali di accesso al sistema e la relativa casella email vengono create dal SIAT a seguito di una richiesta, di norma inoltrata mediante l'apposita procedura informatica, in cui il Dirigente/Responsabile del Settore/Ufficio competente (o suo delegato alla gestione).
Nella richiesta vengono altresì esplicitate le abilitazioni che lo stesso dovrà avere relativamente al sistema gestito mediante Active Directory (cartelle condivise, applicativi e banche dati locali)
L'invio della richiesta al SIAT presuppone che il Dirigente/Responsabile che la inoltra attesti che l'utente abbia titolo ad accedere alla rete e ai dati a cui viene abilitato.
L'incaricato del SIAT crea le relative credenziali Active Directory ed email e comunica, in modo riservato, le password temporanee all'utente, che le dovrà sostituire al primo accesso con quelle definitive.

Può accadere che, per esigenze di servizio, esistano credenziali d'accesso non legate ad un singolo lavoratore e che possono essere condivise da tutto un gruppo di operatori. Queste credenziali non possono consentire l'accesso a banche dati o documenti contenenti dati personali e verranno assegnate unicamente a dipendenti del Comune individuati quali responsabili della gestione della password

2.4. Modalità di gestione delle password

Nel caso un utente abbia dimenticato una password, si dovrà rivolgere al SIAT che, previo riconoscimento, provvederà a resettarla e a comunicarla riservatamente all'utente, che, al primo accesso, dovrà necessariamente modificarla con una nuova di sua scelta.

Eccezionalmente, nel caso in cui si renda indispensabile ed indifferibile, per esclusive necessità **tecniche** di operatività e sicurezza, i tecnici SIAT preposti alla gestione delle credenziali potranno modificare la password degli utenti; in questi casi, giustificandone le ragioni, ne daranno tempestiva comunicazione scritta agli stessi, che quindi provvederanno a sostituirla obbligatoriamente al primo accesso.

Ai sensi di quanto previsto dal punto 10 dell'Allegato B al D. Lgs. 30 giugno 2003, n. 196, gli addetti del SIAT potranno modificare la password degli utenti e comunicare tale nuova password ad un altro utente.
Tale eventualità potrà verificarsi dietro richiesta scritta proveniente dal Responsabile apicale dell'Ufficio/Servizio qualora, in caso di prolungata assenza o impedimento dell'incaricato, sia indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. Qualora si tratti della password di un responsabile apicale di un comune o dell'Unione, la richiesta dovrà pervenire, rispettivamente, dal Sindaco o dal Presidente dell'Unione.
La richiesta dovrà contenere il nome dell'utente di cui va modificata la password, le ragioni che ne rendono indispensabile e indifferibile la modifica e il nome dell'utente a cui la nuova password dovrà essere comunicata.
Il SIAT comunicherà tempestivamente per iscritto all'utente dell'avvenuto cambio password e delle ragioni che lo hanno reso necessario, nonché il nominativo dell'utente a cui la nuova password è stata comunicata.
L'utente dovrà quindi procedere, appena possibile, a modificare la sua password.

2.5. Considerazioni generali sulle password

1.1.7. Sicurezza e limiti nell'uso delle password

L'utilizzatore ha l'obbligo di impostare la password seguendo la procedura di cambio password nel rispetto della normativa vigente
Ogni incaricato che riceve le proprie password ne è direttamente responsabile e non deve in alcun modo comunicare le proprie password a persone diverse od altri incaricati.
Le password sono strettamente personali e non vanno comunicate a nessuno.
Non è tecnicamente possibile ricostruire le password impostate dagli utenti.
Architetture in cui gli utenti non eseguano una validazione (logon) ad un dominio e non implementano complete funzionalità di sicurezza non sono e non dovranno più presenti all'interno della rete aziendale.

1.1.8. Durata e cambio della password

Ogni utente autorizzato ad accedere alle banche dati ha ottenuto dagli addetti al SIAT un codice identificativo (USER-NAME) ed una parola segreta (PASSWORD) che deve immediatamente cambiare.
La durata delle password viene definita a livello centrale; il sistema avviserà l'utente quando la password sta per scadere ed è quindi necessario cambiarla. Alle password di accesso al dominio Windows è dato un periodo di vita massimo di 90 giorni. Trascorso tale periodo se l'utente non l'ha già autonomamente cambiata, il sistema lo costringe ad immetterne una nuova altrimenti il sistema non si attiva.
Per impostare la nuova password è necessario fornire anche quella vecchia; nel caso in cui l'utente l'avesse dimenticata, l'amministratore di sistema, dopo aver riconosciuto l'utente, può forzare la creazione di una nuova password provvisoria.
Un utente che non sia stato disabilitato può modificare la propria password anche prima della scadenza autenticandosi con userid e vecchia password (valida per questa funzione anche se scaduta).
Gli utenti possono modificare la propria password in qualsiasi momento, oppure essere chiamati a cambiarla dal sistema stesso, in risposta a policy aziendali o interventi amministrativi.
Gli utenti sono tenuti a cambiare la password anche nel caso in cui abbiano il sospetto che la stessa non sia più segreta.

1.1.9. Requisiti delle password

Gli utenti sono stati sensibilizzati, informati ed istruiti sull'importanza dell'uso, della segretezza e sulle modalità di modifica delle password.
Le password devono essere significative e conformi ai requisiti di complessità. Ovvero:

- devono essere lunghe almeno 8 caratteri
- devono essere "complesse", cioè contenere almeno 3 delle 4 seguenti tipologie: maiuscole, minuscole, numeri, caratteri speciali.
- si deve evitare di immettere sequenze della stessa lettera
- deve presentare differenze significative rispetto alle password per cui non devono ricordare quelle precedenti (Es: con una minima modifica di un solo carattere).
- non deve contenere il nome, il cognome o l'user-name (account utente)
- non deve trattarsi di una parola o di un nome comune

2.6. Disattivazione credenziali per disuso.

Nel momento in cui un utente perde il diritto ad accedere alla rete aziendale, il dirigente referente o l'ufficio personale ne comunicano tempestivamente la data di perdita dei requisiti.
Almeno semestralmente viene fatta una verifica straordinaria del permanere, in capo agli utenti abilitati, dei requisiti necessari all'abilitazione onde evidenziare eventuali eventi di cessazione non comunicati.

Il mancato uso delle credenziali per almeno sei mesi continuativi determina la loro disattivazione salvo quelle preventivamente autorizzate per i soli scopi di gestione tecnica.
Per riattivare le credenziali, l'utente dovrà rivolgersi al servizio SIAT che, verificatone il diritto, lo riattiverà con le stesse modalità del caso di "dimenticanza di password"
Periodicamente il SIAT controllerà e disattiverà gli account non utilizzati nei sei mesi precedenti

Il codice di identificazione, laddove inutilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

3. Modalità di gestione delle stazioni di lavoro

3.1. Soggetto preposto alla pulizia o recupero delle banche dati su PC

Preposto alla pulizia o recupero delle banche dati su PC è il Responsabile del SIAT che provvederà alla designazione del personale incaricato.

3.2. Programmi antivirus

Un software antivirus è installato su tutti i PC, sui server di posta elettronica, sui file server.
Il software antivirus viene aggiornato in maniera automatica ogni qualvolta la casa produttrice rilascia un aggiornamento riguardante la definizione dei virus o l'aggiornamento del software.

Il software produce report dettagliati sulla natura dei Client in rete LAN (utente collegato, Sistema operativo e stato dell'aggiornamento) e sul loro stato di infezione.

Gli utilizzatori di strumenti informatici sono stati informati sul pericolo che i "virus informatici" attacchino i personal computer e ne danneggino il contenuto oltre a propagarsi su altri computer o sui server di rete. Tutti sono tenuti ad utilizzare i programmi di antivirus presenti nell'ente per verificare che i supporti ottenuti dall'esterno, i files ricevuti via e-mail o scaricati da internet, non siano infetti.

Gli utenti non debbono disattivare la procedura di aggiornamento automatico, e non devono disattivare (anche temporaneamente) la funzione di protezione antivirus.

3.3. Programmi antispam

La protezione da Spam, è ottenuta tramite un fornitore esterno, che ha la gestione dell'intero sistema di posta elettronica.
Tipicamente le e-mail contenenti virus vengono già eliminate da questo antispam; qualora superassero l'antispam, le e-mail vengono anche sottoposte dal sistema del fornitore ad ulteriore controllo antivirus.
In definitiva una email è soggetta a un sistema antispam e due sistemi antivirus, uno del sistema centralizzato di posta ed uno del pc locale.

3.4. Interventi di Manutenzione

Gli interventi di manutenzione sui PC degli utenti vengono di norma effettuati, in remoto o in loco, alla presenza degli assegnatari dei PC stessi.
L'accesso remoto ai PC degli utenti avviene previo consenso espresso da questi ultimi alla richiesta di accesso remoto presentata dal software di controllo.

Nel caso sia necessario inserire la password dell'utente, verrà chiesto a quest'ultimo di digitarla e non dovrà quindi essere comunicata al tecnico.

I tecnici del SIAT o di ditte esterne incaricate della manutenzione dispongono di una password di amministratore del PC che consente l'accesso senza la necessità di conoscere la password dell'utente.

Nel caso il PC debba essere trasferito presso un laboratorio per la sua riparazione, i tecnici incaricati dovranno limitarsi alle sole operazioni tecniche necessarie alla rimozione del guasto e non dovranno accedere in modo generalizzato ai file memorizzati nel disco del PC stesso.

3.5. Società esterne o professionisti per la manutenzione e l'assistenza

Il Responsabile del SIAT nomina la società che effettua la manutenzione dei sistemi hardware o software responsabile del trattamento dei dati utilizzando l'apposito modello il quale andrà integrato con

una specifica assunzione di impegno da parte del responsabile stesso al rispetto delle seguenti disposizioni:

- non effettuare copie né procedere alla eliminazione degli archivi informatici di titolarità dell'ente detenuti.
- informare preventivamente gli interessati del giorno e dell'orario in cui saranno effettuati gli interventi tecnici.
- richiedere preventivamente l'autorizzazione ai tecnici del SIAT nel caso di interventi di assistenza tramite collegamento remoto. Gli stessi tecnici dovranno essere avvisati al termine delle operazioni.
- usare riservatezza su dati ed informazioni addivenuti in loro possesso.
- trasmettere al Responsabile del SIAT l'elenco degli incaricati al trattamento e successive variazioni
- trasmettere al Responsabile del SIAT il nominativo degli amministratori di sistema affinché si possa provvedere al loro incarico

3.6. Dismissione delle stazioni di lavoro

In caso di dismissione di PC, il SIAT comunica al Responsabile apicale del Servizio l'elenco dei PC da dismettere: questi segnala l'eventuale presenza, su dischi locali degli stessi, di banche dati da recuperare.
Il soggetto preposto, una volta recuperate le banche dati, disinstalla i dischi magnetici dalla postazione di lavoro. La postazione potrà essere smaltita mentre i dischi fissi dovranno essere resi illeggibili prima della rottamazione.
I dischi dei PC usati che eventualmente il Comune dovesse cedere in comodato d'uso, prima della consegna vengono riformattati con modalità sicure, impedendo il recupero di banche dati che vi erano contenute.

4. Salvataggio dei dati

Il salvataggio delle banche dati esistenti sui server è in carico all'Ufficio SIAT.
Sui sistemi centralizzati vengono fatte copie quotidiane degli archivi documentali e delle banche dati strutturate allo scopo di fornire almeno una versione aggiornata alla notte precedente.
L'esecuzione dell'operazione di salvataggio è verificata quotidianamente dagli operatori.

In caso di danneggiamento o perdita di dati, gli stessi vengono tempestivamente ripristinati mediante le copie presenti nel sistema di backup.

Ogni singolo lavoratore è invece responsabile dell'effettuazione di copie di sicurezza degli archivi e dei documenti memorizzati unicamente sul proprio PC.

5. Locali

La sala macchine dell'Unione dove risiedono fisicamente i server e le librerie a dischi magnetici su cui sono memorizzati i dati degli Enti, è dotata di impiantistica tale da garantire la sicurezza fisica dell'hardware, sia delle banche dati, in particolare:

- porta d'ingresso REI
- stabilizzatore di temperatura per i locali;
- doppio gruppo di continuità e di stabilizzazione della corrente;
- impianto di rilevamento fumi con invio SMS in caso di allarme;
- impianto antintrusione;

La chiave di accesso ai locali della sede centrale è in carico esclusivo al SIAT.
Solo per gestione delle emergenze, una chiave è consegnata presso il servizio Lavori Pubblici del Comune sede del SIAT

Presso ogni comune è presente un CED secondario periferico ubicato in locali chiusi a chiave. Le chiavi di a questi locali sono in carico al comune stesso.

6. Cautele generali

6.1. Password

Il sistema centralizzato di autenticazione provvede in modo automatico alla scadenza della password
Nel caso in cui le password siano impostate dall'utente in sistemi che non ne prevedano la scadenza temporale, è sua responsabilità provvedere alla loro modifica almeno ogni 90 giorni.

Le password esterne al sistema Active Directory devono rispettare i limiti, la sicurezza e la durata di quelle precedentemente indicate nella sezione "Modalità di gestione delle Password"

6.2. Uso del Computer

Il PC non deve essere lasciato incustodito.
In caso di allontanamento anche temporaneo, l'utente attivo al momento deve essere disconnesso o deve essere attivata la modalità salvaschermo con protezione mediante password
Il Dirigente di Settore/Responsabile delegato può impartire ulteriori istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro.
E' impostata a livello centrale, una policy di sicurezza distribuita su tutte le postazioni informatiche che blocca il PC in caso di inattività per 30 minuti. Il nuovo accesso sarà consentito solo con password di Active Directory

6.3. Custodia dei supporti

Per motivi di sicurezza e al fine di evitare accessi non autorizzati e trattamenti non consentiti, devono essere impartite, da parte del Responsabile apicale del Settore, le istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili (es: CD, DVD, PenDrive) su cui sono memorizzati i dati.

6.4. Supporti ricevuti dall'esterno

Nel caso di supporti ricevuti dall'esterno, come nel caso di allegati ricevuti via e-mail, l'utente deve prestare massima attenzione e sottoporre il supporto a controllo antivirus

7. Divieti

Divieti per l'utente	**Chi può fare questa operazione**	**Operazioni preliminari**	**Conseguenze**	**Responsabile nel caso di non rispetto del divieto**
Vietato installare programmi	Addetti al S.I.	-Sensibilizzazione e formazione sui rischi e responsabilità. -Verifica compatibilità con i sistemi. -Verifica esistenza di virus informatici. -Verifica della regolare licenza d'uso	-Disinstallazione programma. -Eliminazione virus. Ripristino situazione originale. -Segnalazione al direttore di area.	Consegnatario del computer
Vietato disinstallare programmi	Addetti al S.I.	-Sensibilizzazione e formazione sui rischi e responsabilità.	-Ripristino situazione originale. -Segnalazione al direttore di area.	Consegnatario del computer
Vietato utilizzare (anche senza	Addetti al S.I.	-Sensibilizzazione e formazione sui rischi e responsabilità.	-Eliminazione programma non regolari senza preavviso. -Eliminazione virus.	Consegnatario del computer

installazione) di programmi non autorizzati dal S.I.		-Verifica compatibilità con i sistemi. -Verifica esistenza di virus informatici. -Verifica della regolare licenza d'uso	-Ripristino situazione originale. -Segnalazione al direttore di area.	
Vietato utilizzare programmi di intercettazione dati diretti ad altri utenti	Nessuno	Sensibilizzazione e formazione sui rischi e responsabilità.	-Eliminazione del programma. -Ripristino situazione originale. -Segnalazione al direttore di area.	Consegnatario del computer
Vietato modificare o tentare di modificare la configurazione	Addetti al S.I.	-Sensibilizzazione e formazione sui rischi e responsabilità. -Verifica compatibilità con i sistemi.	-Ripristino situazione originale. -Segnalazione al direttore di area.	Consegnatario del computer

Il SIAT, in conformità alle disposizioni di legge, provvede alla descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento nell'ambito del piano di disaster recovery.

Il Responsabile apicale del SIAT provvede con propria determinazione a redigere l'elenco degli amministratori di sistema e a designarli individualmente con successivo atto precisandone le funzioni e specificandone l'ambito di attività.
Gli estremi identificativi delle persone fisiche designate, con l'indicazione delle funzioni ad esse attribuite, è riportato in un elenco agli atti del SIAT stesso. Con cadenza annuale il Responsabile del SIAT verifica l'operato degli amministratori di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle normative vigenti.
Il SIAT ha adottato le misure necessarie a consentire un'attività di verifica dell'operato degli amministratori di sistema alla luce delle normative vigenti in merito al trattamento dei dati personali.

UNIONE TERRED'ACQUA

Costituita fra i Comuni di:

Anzola dell'Emilia
Calderara di Reno
Crevalcore
Sala Bolognese
San Giovanni in Persiceto
Sant'Agata Bolognese

DELIBERA DELLA GIUNTA DELL'UNIONE
N. 30 del 05/09/2016

OGGETTO:

APPROVAZIONE DEL MANUALE DI GESTIONE DEL PROTOCOLLO E DEI FLUSSI DOCUMENTALI E DELL'ARCHIVIO

Letto, approvato e sottoscritto.

FIRMATO	FIRMATO
IL PRESIDENTE	**IL SEGRETARIO DELL'UNIONE**
Emanuele BASSI	**D.Ssa Anna Rosa CICCIA**

Documento prodotto in originale informatico e firmato digitalmente ai sensi dell'art. 20 del "Codice dell'amministrazione digitale" (D.Leg.vo 82/2005).