

MANUALE DI GESTIONE DOCUMENTALE

Art. 5 DPCM 3/12/2013 ed s.m.i.

Linee Guida AgID

“Regole tecniche per il protocollo informatico”

Comune di Verzegnis

Provincia di Udine



Approvato con delibera di Giunta Comunale n. 112 del 29-12-2025

INDICE

SEZIONE I - Disposizioni generali.....	5
Articolo 1 - Ambito di applicazione	5
Articolo 2 - AOO e modello di protocollazione adottato.....	5
Articolo 3 - Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.....	5
Articolo 4 - Sistema di Gestione Informatica dei Documenti.....	6
Articolo 5 - Piano di sicurezza	7
 SEZIONE II - Formazione dei documenti	 8
Articolo 6 - Disposizioni generali sulla produzione dei documenti	8
Articolo 7 - Informazioni minime del documento cartaceo prodotto dal Comune	8
Articolo 8 - Produzione dei documenti informatici	8
Articolo 9 - Sottoscrizione dei documenti informatici	9
Articolo 10 - Firma elettronica.....	10
Articolo 11 - Firma elettronica avanzata.....	10
Articolo 12 - Firma elettronica qualificata	11
Articolo 13 - Firma digitale	11
Articolo 14 - Validazione temporale dei documenti sottoscritti con firma digitale.....	12
Articolo 15 - Copie informatiche di documenti analogici.....	12
Articolo 16 - Copie analogiche di documenti informatici.....	13
Articolo 17 - Duplicati e copie informatiche di documenti informatici	13
 SEZIONE III - Ricezione dei documenti.....	 14
Articolo 18 - Ricezione di documenti cartacei	14
Articolo 19 - Ricezione di documenti informatici.....	14
 SEZIONE IV - Registrazione dei documenti	 16
Articolo 20 - Eliminazione dei protocolli diversi alternativi al SGID.....	16
Articolo 21 - Documenti soggetti obbligatoriamente alla registrazione di protocollo	16

Articolo 22 - Documenti non soggetti all'obbligo della registrazione di protocollo	16
Articolo 23 - Registrazione di protocollo.....	16
Articolo 24 - Registrazione di protocollo dei documenti informatici.....	17
Articolo 25 - Segnatura di protocollo dei documenti cartacei.....	18
Articolo 26 - Segnatura di protocollo dei documenti informatici.....	18
Articolo 27 - Riservatezza delle registrazioni di protocollo	19
Articolo 28 - Annullamento o modifica delle registrazioni di protocollo	19
Articolo 29 - Registro giornaliero delle registrazioni di protocollo	20
Articolo 30 - Differimento dei termini di registrazione	20
Articolo 31 - Registro di emergenza.....	20

SEZIONE V - Classificazione e fascicolazione dei documenti 22

Articolo 32 - Titolario di classificazione e piano di conservazione dell'archivio.....	22
Articolo 33 - Classificazione dei documenti.....	22
Articolo 34 - Formazione e identificazione dei fascicoli	23

SEZIONE VI - Gestione della corrispondenza in entrata..... 25

Articolo 35 - Ricezione.....	25
Articolo 36 - Gestione della corrispondenza cartacea	25
Articolo 37 - Gestione della corrispondenza informatica	26
Articolo 38 - Registrazione di protocollo e classificazione	26
Articolo 39 - Assegnazione	26
Articolo 40 - Scansione.....	26
Articolo 41 - Recapito e presa in carico della corrispondenza informatica.....	27
Articolo 42 - Sub assegnazione	27
Articolo 43 – Fascicolazione	27

SEZIONE VII - Gestione dei documenti interni, dei flussi documentali e dei procedimenti amministrativi..... 28

Articolo 44 - Produzione dei documenti della AOO	28
Articolo 45 - Gestione dei flussi documentali interni.....	28
Articolo 46 - Gestione dei procedimenti amministrativi.....	28

SEZIONE VIII - Gestione della corrispondenza in uscita	29
Articolo 47 - Spedizione dei documenti su supporto cartaceo	29
Articolo 48 - Spedizione dei documenti informatici	29
 SEZIONE IX - Archiviazione dei documenti.....	 31
Articolo 49 - Archivio dell'amministrazione.....	31
Articolo 50 - Archivio corrente.....	31
Articolo 51 - Archivio di deposito.....	31
Articolo 52 - Archivio digitale	32
Articolo 53 - Archivio ibrido	32
 SEZIONE X - Approvazione ed aggiornamento	 33
Articolo 54 - Approvazione, aggiornamento e pubblicità del manuale	33
 GLOSSARIO	 34
 ELENCO ALLEGATI.....	 41

SEZIONE I - DISPOSIZIONI GENERALI

Articolo 1 – Ambito di applicazione

Il presente Manuale di Gestione, adottato ai sensi degli articoli 3 e 5 del DPCM 3/12/2013 “Regole tecniche per il protocollo informatico”, descrive il sistema di gestione documentale e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi del Comune di Verzegnis.

Articolo 2 – AOO e modello di protocollazione adottato

Ai fini della gestione documentale il Comune di Verzegnis (d'ora in poi denominato anche Comune o Ente) è costituito in un'unica Area Organizzativa Omogenea (AOO) (Allegato 1 al presente manuale)

Ai sensi dell'art. 50, comma 4, del DPR 445/00, per AOO si intende un insieme di uffici da considerare ai fini della gestione unica e coordinata dei documenti, che assicuri uniformità di classificazione, archiviazione e comunicazione interna.

Nell'ambito dell'AOO è predisposto un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, secondo le modalità previste dall'art. 3 del presente manuale. Il Sistema di protocollo informatico o Sistema di Gestione Informatica dei Documenti (SGID), utilizzato per la registrazione dei documenti, è unico nell'ambito dell'AOO.

Il modello di protocollazione adottato dal Comune di Verzegnis è parzialmente decentrato, in quanto la protocollazione in arrivo è svolta dall'Ufficio Protocollo, mentre la protocollazione in partenza e la registrazione dei protocolli interni sono svolte da ciascun ufficio dell'Ente.

Il Responsabile della gestione documentale (RGD) provvede ad assegnare le abilitazioni all'accesso e all'utilizzo delle funzioni del Sistema di Gestione Informatica dei Documenti del Comune di Verzegnis.

Articolo 3 – Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

Nell'ambito del Comune di Verzegnis, ai sensi dell'art. 61, comma 1, del DPR 445/00, è stato individuato un Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, denominato Area Affari Generali-Servizio Protocollo Generale, cui è demandata la gestione dell'Ufficio Protocollo e dell'Archivio.

Al Responsabile della gestione documentale sono affidati i compiti di cui all'art. 61, comma 3, del DPR 445/00 e all'art. 4 del DPCM 3/12/2013 “Regole tecniche per il protocollo informatico”; in particolare:

- attribuisce i livelli di autorizzazione per l'accesso alle funzioni del Sistema di Gestione Informatica dei Documenti;
- garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
- cura che le funzionalità del Sistema, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- autorizza l'utilizzo del registro di emergenza per le registrazioni di protocollo, nei casi e secondo le modalità previste dall'art. 63 del DPR 445/00;
- autorizza l'annullamento delle registrazioni di protocollo secondo quanto disposto dall'art. 54 del DPR 445/00;

- garantisce il buon funzionamento del Sistema di Gestione Informatica dei Documenti, la formazione e la gestione dell'archivio digitale dell'Ente, nonché la corretta conservazione degli archivi cartacei;
- predispone l'aggiornamento del Manuale di gestione, seguendo le modalità di revisione previste dall'articolo 53 del presente manuale;
- cura la pubblicazione del Manuale di gestione sul sito internet istituzionale del Comune;
- predispone e aggiorna, d'intesa con il Responsabile per la sicurezza informatica e il Responsabile per il trattamento dei dati personali, il piano per la sicurezza informatica, di cui all'articolo 5 del presente manuale, secondo quanto disposto dall'art. 4, comma 1, lettera c), del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico";
- assicura la corretta produzione del registro giornaliero di protocollo e la sua trasmissione al sistema di conservazione entro la giornata lavorativa successiva, garantendone, inoltre, l'immodificabilità del contenuto secondo quanto disposto dall'art. 7, comma 5, del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico";
- predispone il pacchetto di versamento e ne assicura la trasmissione al sistema di conservazione ai sensi dell'art. 6, comma 3, del DPCM 3/12/2013 "Regole tecniche in materia di sistema di conservazione" e degli articoli 11 e 15 del DPCM 13/11/2014 "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", stabilendo i tempi entro cui i documenti, i fascicoli e le aggregazioni documentali informatiche debbano essere versati in conservazione; verifica, infine, il buon esito dell'operazione di versamento.

Articolo 4 – Sistema di Gestione Informatica dei Documenti

Il Sistema di Gestione Informatica dei Documenti (SGID) è costituito dall'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti, come specificato dall'art. 1, comma 1, lett. r), del DPR 445/00.

Il Sistema di Gestione Informatica dei Documenti adottato dal Comune di Verzegnis è integrato funzionalmente con le caselle di posta elettronica certificata (PEC) attivate dall'Ente.

Conformemente ai disposti degli articoli 52 del DPR 445/00 e 6 e 7 del DPCM 3/12/2013 e s.m.i. "Regole tecniche per il protocollo informatico" il Sistema SGID:

- garantisce la "funzionalità minima" del protocollo informatico che, ai sensi dell'art. 56 del DPR 445/00, comprende le operazioni di registrazione, segnatura di protocollo e classificazione dei documenti;
- è dotato delle funzionalità necessarie a garantirne la sicurezza e l'integrità;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali (fascicolazione);
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- assicura l'univoca identificazione ed autenticazione degli utenti;
- assicura la registrazione delle attività rilevanti ai fini della sicurezza e consente il tracciamento di qualsiasi evento di modifica delle informazioni trattate, individuandone l'autore, la data, l'ora e impedendo che tali registrazioni possano essere modificate senza autorizzazione;
- consente l'accesso al sistema, ai documenti e alle informazioni contenute, in condizioni di

sicurezza, mediante la definizione di specifici livelli di abilitazione per gli utenti interessati, nel rispetto della normativa vigente in materia di trattamento dei dati personali;

- rispetta le misure di sicurezza previste al decreto legislativo n. 196/03 (come aggiornato ed integrato dal GDPR (Regolamento UE 2016/679);

Il Sistema di Gestione Informatica dei Documenti consente inoltre:

- la produzione del registro giornaliero di protocollo conformemente a quanto disposto dall'art. 53, comma 2, del DPR 445/00 e dall'art. 7, comma 5, del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico";
- la registrazione e la trasmissione tra gli uffici dei documenti amministrativi prodotti internamente con i relativi metadati, permettendo il tracciamento di tutte le attività svolte;
- lo scambio di documenti tra le pubbliche amministrazioni secondo i meccanismi di interoperabilità e cooperazione applicativa.

Articolo 5 – Piano di sicurezza

Il piano di sicurezza relativo alla formazione, gestione, trasmissione, accesso, interscambio e conservazione dei documenti informatici è adottato ai sensi del DPCM 3/12/2023 ed è conforme alle vigenti disposizioni di legge.

Conformemente a quanto previsto dal D.Lgs 82/05, il piano adotta misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito e non conforme alle finalità della raccolta dei dati contenuti all'interno del sistema.

Per quanto specificatamente previsto nel suddetto piano di sicurezza si rimanda all'allegato n. 2 al presente manuale.

SEZIONE II – FORMAZIONE DEI DOCUMENTI

Articolo 6 – Disposizioni generali sulla produzione dei documenti

Ai sensi dell'art. 22, comma 1, lettera d), della L. 241/90 per documento amministrativo si intende ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, formati dalle pubbliche amministrazioni o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa. Ai sensi dell'art. 1, comma 1, lettera p), del D. Lgs. 82/05 per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Ai sensi dell'art. 23-ter del D. Lgs. 82/05 per documenti amministrativi informatici si intendono, gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse.

Il Comune, conformemente a quanto previsto, dal Codice dell'Amministrazione Digitale (CAD), nello svolgimento delle proprie attività, predispone i propri atti utilizzando sistemi informativi automatizzati. I documenti prodotti dal Comune, i cui originali siano su supporto informatico, sono prodotti nel rispetto delle regole tecniche emanate ai sensi dell'art. 71 del D. Lgs. 82/05, conformemente alle modalità previste dal presente manuale.

Ciascun documento formato dal Comune, sia esso interno o da trasmettere all'esterno, tratta un unico argomento.

Articolo 7 – Informazioni minime del documento cartaceo prodotto dal Comune

Le informazioni minime presenti nei documenti cartacei prodotti dal Comune di Verzegnis sono le seguenti:

- denominazione e stemma ufficiale del Comune;
- indicazione dell'AOO e dell'ufficio che ha prodotto il documento;
- indirizzo completo del Comune comprensivo di numero di telefono e casella di posta elettronica istituzionale;
- indicazione di luogo, giorno, mese e anno di formazione;
- numero e data di protocollo, se soggetto a registrazione;
- oggetto;
- riferimenti ad eventuali documenti precedenti;
- sottoscrizione a cura del responsabile, o dei responsabili, del procedimento;
- indicazione del destinatario qualora si tratti di documento in uscita.

Articolo 8 – Produzione dei documenti informatici

I documenti informatici sono prodotti dal Comune di Verzegnis attraverso l'utilizzo di appositi strumenti software o mediante estrazione e raggruppamento di dati provenienti dalle basi dati gestite dall'Ente.

I documenti informatici prodotti dal Comune contengono le informazioni minime elencate nel precedente art. 6; il Sistema SGID manterrà il collegamento tra il documento e i dati inseriti in fase di protocollazione, ivi incluso il numero di protocollo assegnato.

I formati elettronici utilizzati dal Comune di Verzegnis per la produzione dei documenti informatici, anche ai fini della conservazione:

- sono conformi a quanto disposto dall'allegato n. 2 al DPCM 3/12/2013;
- sono aperti, completamente documentati e preferibilmente riconosciuti come standard

da organismi internazionali;

- sono indipendenti da specifiche piattaforme tecnologiche hardware e software;
- non possono contenere macroistruzioni o codice eseguibile;
- sono ampiamente adottati;
- sono preferibilmente stabili e non soggetti a continue modificazioni nel tempo;
- sono preferibilmente utilizzabili con versioni precedenti e successive dell'applicativo software che li ha prodotti;
- sono privi di meccanismi tecnici di protezione che possano impedirne la replica del contenuto su nuovi supporti o la possibilità di effettuare migrazioni, pregiudicandone la fruibilità nel lungo periodo a causa dell'obsolescenza tecnologica;
- permettono la fruizione anche ad utenti diversamente abili.

I formati elettronici utilizzati dal Comune sono:

TIPOLOGIA DI DOCUMENTI - FORMATI UTILIZZABILI	ESTENSIONE
Documenti di testo Pdf, Pdf/A	.pdf
Documenti di testo Office Open XML (OOXML)	.docx, .xlsx, .pptx
Documenti di testo Open Document Format	.odt, .ods, .odp, .odg
Immagini raster TIFF	.tif
Immagini JPEG	.jpeg, .jpg
File non binari "in chiaro" XML e i suoi derivati	.XML I
TXT con specifica della codifica del carattere adottata (Character Encoding)	.tXt
Messaggi di posta elettronica Eml e tutti i formati conformi allo standard RFC 2822/MIME	.eml
Messaggi di posta elettronica Msg e tutti i formati conformi allo standard RFC 2822/MIME	.msg
Formato di archiviazione dei dati pensato per il salvataggio di pagine web e i documenti ipertestuali.	.mht

I documenti sottoscritti digitalmente e la marcatura temporale sono accettati nei formati (verificare formati) P7M, M7M, PDF e P7S.

Il documento informatico presenta la caratteristica di immodificabilità in modo tale che forma e contenuto dello stesso non siano alterabili durante le fasi di tenuta, accesso e conservazione.

Articolo 9 – Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici prodotti dal Comune avviene in conformità di quanto previsto dal D. Lgs. 82/05 e dal DPCM 22/02/2013 “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”.

Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle suddette regole tecniche, emanate ai sensi dell’art. 20, comma 3 e dell’art. 71 del D. Lgs. 82/05, che garantisce, pertanto, l’identificabilità dell’autore, l’integrità e l’immodificabilità del documento, ha l’efficacia della scrittura privata prevista dall’articolo 2702 del Codice Civile.

Il dispositivo per la generazione della firma digitale è usato esclusivamente dal titolare designato dal Comune; ai sensi della normativa vigente tale utilizzo si presume comunque riconducibile al titolare, salvo che questi dia prova contraria.

L’utilizzo da parte del Comune delle varie tipologie di sottoscrizioni elettroniche avviene nei casi e con le modalità disposte dagli articoli 9, 10, 11 e 12 del presente manuale.

Articolo 10 – Firma elettronica

Per firma elettronica si intende, ai sensi dell’art. 1, comma 1, lettera q), del D. Lgs. 82/05, l’insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

Ai sensi dell’art. 21, comma 1, del D. Lgs. 82/05 e Regolamento eIDAS, il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Come firma elettronica (c. d. firma elettronica “debole”) il Comune di Verzegnis adotta la *User-Id* e la *Password* per l’accesso al Sistema da parte degli utenti interni.

Le credenziali di identificazione (*User-Id* e *Password*) utilizzate per accedere al Sistema di Gestione Informatica dei Documenti del Comune costituiscono una firma elettronica e devono essere utilizzate esclusivamente dal soggetto cui sono state assegnate; tale tipologia di sottoscrizione è abilitata solo nelle comunicazioni e nelle registrazioni dove è sufficiente l’identificazione informatica del soggetto che le esegue.

Richiamati il DPCM 24/10/2014 e il DL 76/2020, per quanto concerne l’identificazione degli utenti esterni, il Comune di Verzegnis sta terminando l’adeguamento, al fine di permettere l’identificazione degli utenti esterni che accedano a servizi erogati direttamente on-line, mediante l’utilizzo del Sistema pubblico dell’Identità digitale di cittadini ed imprese (SPID) e della Carta di Identità Elettronica (CIE).

Articolo 11 – Firma elettronica avanzata

Per firma elettronica avanzata si intende, ai sensi dell’art. 1, comma 1, lettera q-bis), del D. Lgs. 82/05, l’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 può 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 documenti sottoscritti con firma elettronica avanzata hanno l’efficacia prevista dall’art. 2702 del Codice Civile se la soluzione di firma, conformemente a quanto disposto dall’art. 56 del DPCM 22/02/2013 garantisce:

- l’identificazione del firmatario del documento;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati

biometrici eventualmente utilizzati per la generazione della firma medesima;

- la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- l'individuazione del soggetto che eroga la soluzione di firma elettronica avanzata;
- l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne il contenuto;
- la connessione univoca della firma al documento sottoscritto.

Ai sensi dell'art. 61, comma 1, del DPCM 22/02/2013, come integrato dal Regolamento europeo eIDAS e dal Codice dell'Amministrazione Digitale (CAD), l'invio di dichiarazioni e istanze da una casella di posta elettronica certificata (PEC), le cui credenziali di accesso siano state rilasciate previa identificazione ai sensi del DPCM 27/09/2012 ed s.m.i. "Regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata", effettuato richiedendo la ricevuta completa di avvenuta consegna, sostituisce nei confronti della Pubblica Amministrazione la firma elettronica avanzata; pertanto i documenti che pervengano al Comune di Verzegnis utilizzando la suddetta modalità, ai sensi dell'art. 65, comma 2, del D. Lgs. 82/05, sono equivalenti a quelli sottoscritti con firma autografa apposta in presenza del dipendente addetto al procedimento.

Articolo 12 – Firma elettronica qualificata

Per firma elettronica qualificata si intende, ai sensi dell'art. 1, comma 1, lettera r), del D. Lgs. 82/05, 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.

La soluzione di firma elettronica qualificata adottata dal Comune di Verzegnis è la firma digitale.

Articolo 13 – Firma digitale

Per firma digitale si intende, ai sensi dell'art. 1, comma 1, lettera s), del D. Lgs. 82/05, quel particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consenta 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. Ai sensi dell'art. 24, comma 2, del D. Lgs. 82/05, l'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

I documenti informatici prodotti dal Comune di Verzegnis nello svolgimento della propria attività istituzionale sono sottoscritti dai responsabili del procedimento con firma digitale conforme alla normativa vigente.

Il titolare del dispositivo di firma digitale, conformemente a quanto previsto dall'art. 8, comma 5, del DPCM 22/02/2013:

- assicura la custodia del dispositivo sicuro per la generazione della firma in suo possesso e adotta le misure di sicurezza fornite dal certificatore al fine di adempiere agli obblighi di cui all'art. 32, comma 1, del D. Lgs. 82/05;
- conserva le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave e segue le indicazioni fornite dal certificatore;
- richiede immediatamente la revoca del certificato qualificato relativo alle chiavi contenute

nel dispositivo sicuro per la generazione della firma digitale inutilizzabile o di cui abbia perduto il possesso o il controllo esclusivo;

- salvo quanto previsto dalle medesime regole tecniche in materia di firma remota, mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma elettronica qualificata o digitale;
- richiede immediatamente la revoca del certificato qualificato relativo alle chiavi contenute nel dispositivo sicuro per la generazione della firma digitale qualora abbia il ragionevole dubbio che possa essere usato da altri.

Articolo 14 – Validazione temporale dei documenti sottoscritti con firma digitale

I documenti informatici, sottoscritti con firma digitale, necessitano di un riferimento temporale che attesti il momento in cui la sottoscrizione è stata apposta; attraverso la validazione temporale (o marcatura temporale), si attribuisce al suddetto documento una data ed un orario certi opponibili ai terzi.

Detto riferimento temporale viene attribuito al documento per mezzo della generazione e dell'applicazione di una marca temporale conforme a quanto previsto dal titolo IV del DPCM 22/02/2013; ai sensi dell'art. 41, comma 4, dello stesso DPCM costituiscono, inoltre, validazione temporale:

- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- il riferimento temporale ottenuto attraverso l'utilizzo della posta elettronica certificata;
- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica.

Articolo 15 – Copie informatiche di documenti analogici

Le copie su supporto informatico di documenti formati dalla Pubblica Amministrazione in origine su supporto analogico ovvero da essa detenuti hanno, ai sensi dell'articolo 23-ter, comma 3, del D. Lgs. 82/05, il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto di quanto stabilito dagli articoli 4 e 10 del DPCM 13/11/2014; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico, salvo il caso di documenti analogici originali unici individuati ai sensi del DPCM 21/03/2013 "Individuazione di particolari tipologie di documenti analogici originali unici"; il Comune di Verzegnis conserva comunque l'originale cartaceo nel proprio archivio.

Le copie per immagine, su supporto informatico, di documenti in origine formati su supporto analogico nonché le copie e gli estratti informatici di documenti originariamente analogici, vengono prodotti dal Comune di Verzegnis utilizzando i formati idonei alla conservazione previsti dalle Linee Guida AgID sul documento informatico.

Ai sensi dell'articolo 4, comma 1, del DPCM 13/11/2014 e s.m.i., le suddette copie per immagine sono prodotte per mezzo di processi e strumenti che assicurino il mantenimento di contenuto e forma identici a quelli del documento analogico da cui sono tratte. L'efficacia probatoria delle stesse è la medesima degli originali da cui provengono se la conformità ad essi non è espressamente disconosciuta.

Nell'ambito del Comune, le copie per immagine su supporto informatico di documenti

originariamente analogici vengono sottoscritti con firma digitale dal pubblico ufficiale preposto a rilasciare le copie.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento originariamente analogico, sarà inserita nello stesso documento informatico contenente la copia per immagine; il documento in tal modo prodotto sarà sottoscritto con firma digitale del pubblico ufficiale a ciò autorizzato.

Gli estratti e le copie informatiche, non per immagine, di documenti amministrativi analogici devono garantire, previo raffronto, la corrispondenza del contenuto a quello dell'originale. Il pubblico ufficiale preposto al rilascio della copia inserisce la dichiarazione di conformità nel documento contenente la copia informatica, sottoscrivendolo con firma digitale.

Articolo 16 – Copie analogiche di documenti informatici

Ai sensi dell'art. 23 del D. Lgs. 82/05, le copie analogiche di documenti informatici hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue parti è attestata da un pubblico ufficiale a ciò autorizzato e non è espressamente disconosciuta.

Ai fini della conservazione il Comune di Verzegnis procede al mantenimento dell'originale informatico.

Articolo 17 – Duplicati e copie informatiche di documenti informatici

Ai sensi dell'art. 23-bis del D. Lgs. 82/05, i duplicati informatici, se prodotti in conformità di quanto previsto dal successivo comma, hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti.

Il duplicato, ai sensi dell'articolo 5 del DPCM 13/11/2014 come integrato dalle Linee Guida AGID sul documento informatico, è prodotto mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine.

Ai sensi dell'articolo 6, comma 1, del DPCM 13/11/2014, come aggiornato e dettagliato dalle Linee Guida AGID, le copie e gli estratti informatici di un documento informatico, prodotti utilizzando i formati previsti e mediante processi e strumenti che assicurino la corrispondenza del contenuto della copia o dell'estratto informatico a quello del documento informatico da cui sono tratti, hanno la stessa efficacia probatoria dell'originale, se sottoscritti con firma digitale da parte di chi li ha prodotti, salvo che la conformità all'originale non sia espressamente disconosciuta.

Ai sensi dell'articolo 6, comma 3, del DPCM 13/11/2014, come integrato ed aggiornato dalle Linee Guida AGID, laddove richiesto dalla natura dell'attività, l'attestazione di conformità della copia o dell'estratto informatico all'originale è inserita nel documento contenente la copia o l'estratto; il documento in tal modo prodotto è sottoscritto con firma digitale da parte del pubblico ufficiale a ciò autorizzato.

Ai fini della conservazione, il Comune di Verzegnis mantiene l'originale informatico.

SEZIONE III – RICEZIONE DEI DOCUMENTI

Articolo 18 – Ricezione di documenti cartacei

I documenti cartacei possono pervenire al Comune di Verzegnis attraverso le seguenti modalità:

- il servizio postale gestito da Poste Italiane Spa o altro gestore autorizzato;
- la consegna diretta, brevi manu, ai vari uffici dell'AOO;
- gli apparecchi telefax, nei casi previsti.

I documenti ricevuti mediante il servizio postale tradizionale vengono consegnati giornalmente all'Ufficio Protocollo.

I documenti consegnati direttamente ai vari uffici della AOO, se soggetti all'obbligo della registrazione di protocollo, vengono presi in carico dal personale che li riceve e da questi fatti pervenire, nell'arco della stessa giornata lavorativa, al suddetto ufficio.

I documenti pervenuti tramite telefax vengono trattati con le stesse modalità degli altri documenti cartacei in arrivo; corre l'obbligo, tuttavia, di sottolineare che, ai sensi dell'art. 47, comma 2, lettera c), del D. Lgs. 82/05 non è ammessa la trasmissione dei documenti a mezzo fax tra le pubbliche amministrazioni.

Qualora all'atto della consegna diretta di un documento cartaceo venga richiesto il rilascio di una ricevuta, l'ufficio a cui è stato presentato il documento rilascia una fotocopia del primo foglio su cui è apposta la sigla dell'addetto a cui tale documento è stato consegnato e un timbro che attesti la data di arrivo. Se la consegna è effettuata direttamente all'ufficio che esegue la protocollazione, l'addetto rilascerà, invece, la fotocopia del primo foglio con apposto il timbro contenente i dati di protocollo.

La protocollazione dei documenti cartacei in arrivo viene eseguita con le modalità descritte dall'art. 22 del presente manuale, mentre la scansione del documento per l'acquisizione dell'immagine da allegare a detta registrazione avverrà secondo le modalità descritte dal successivo art. 39.

Articolo 19 – Ricezione di documenti informatici

Ai sensi dell'art. 45, comma 1, del D. Lgs. 82/05, i documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

Al fine di soddisfare il suddetto requisito, i documenti informatici sono, di norma, acquisiti dal Sistema di Gestione Informatica dei Documenti del Comune di Verzegnis mediante le caselle di posta elettronica certificata attivate dall'Ente ed indicate nell'allegato

n. 1 del presente manuale di gestione.

La posta elettronica certificata garantisce la certezza della provenienza e l'integrità dei documenti ricevuti.

Le caselle PEC attivate dal Comune di Verzegnis sono comunicate all'Agenzia per l'Italia digitale (AgID) al fine di essere inserite nell'Indice delle Pubbliche Amministrazioni (IPA), avendo cura di comunicare tempestivamente e almeno con cadenza semestrale le variazioni.

Le caselle di posta elettronica certificata attivate dal Comune di Verzegnis sono integrate funzionalmente con il Sistema di Gestione Informatica dei Documenti, in modo tale che si formi una "coda" della corrispondenza in arrivo che permetta la registrazione di protocollo e l'acquisizione sul Sistema di tutti i documenti ricevuti; tale "coda" sarà resa accessibile al personale dell'Ufficio Protocollo, abilitato ad eseguire la registrazione di protocollo dei documenti in arrivo.

Qualora i documenti pervenuti tramite PEC siano le ricevute di avvenuta consegna rilasciate dal gestore del servizio di posta elettronica certificata relative a documenti spediti dall'AOO o i messaggi di ritorno generati automaticamente dai sistemi di gestione documentale delle amministrazioni destinatarie di una spedizione, il Sistema procede automaticamente alla loro archiviazione, collegandoli alla registrazione di protocollo cui si riferiscono. Se le ricevute di posta elettronica certificata si riferiscono a situazioni di anomalia come, ad esempio, il mancato recapito di una spedizione, il SGID notifica l'evento al personale responsabile.

I documenti che dovessero pervenire al Comune di Verzegnis attraverso il fax server vengono protocollati dall'Ufficio Protocollo direttamente in modalità informatica e gestiti come gli altri documenti informatici in arrivo.

I documenti informatici provenienti da altre pubbliche amministrazioni possono essere recapitati al Comune di Verzegnis sia attraverso le suddette caselle PEC, sia utilizzando i meccanismi dell'interoperabilità e della cooperazione applicativa di cui al Sistema Pubblico di Connettività (SPC), utilizzando le informazioni contenute nella segnatura di protocollo, nel rispetto di quanto previsto dalla normativa vigente.

Qualora si verifichi il caso in cui un documento informatico, soggetto alla registrazione di protocollo, pervenga agli uffici del Comune utilizzando una modalità diversa da quelle esposte precedentemente, ad esempio la consegna diretta del documento memorizzato su un supporto rimovibile o l'inoltro tramite una casella di posta elettronica convenzionale, il personale che riceve tale documento procede alla sua valutazione e, accertatane la provenienza, lo inoltra all'Ufficio Protocollo, che provvederà alla registrazione. Tali eventualità devono comunque essere disincentivate e costituire un'eccezione rispetto all'utilizzo del canale istituzionale appositamente predisposto che è la posta elettronica certificata.

Per la registrazione di protocollo dei documenti informatici ricevuti dal Comune di Verzegnis si procede secondo le modalità descritte nel successivo art. 23.

SEZIONE IV – REGISTRAZIONE DEI DOCUMENTI

Articolo 20 – Eliminazione dei protocolli diversi alternativi al SGID

Nell'ambito dell'AOO, secondo quanto disposto dall'art. 3, comma 1, lettera e), del DPCM 3/12/2013 (come aggiornato dalle più recenti linee guida AgID) "Regole tecniche per il protocollo informatico", qualsiasi protocollo interno, diverso o alternativo al Sistema di Gestione Informatica dei Documenti, è abolito.

Articolo 21 – Documenti soggetti obbligatoriamente alla registrazione di protocollo

Ai sensi dell'art. 53, comma 5, del DPR 445/00, sono oggetto di registrazione di protocollo obbligatoria i documenti ricevuti e spediti dall'AOO, indipendentemente dalla tipologia di supporto su cui sono formati e tutti i documenti informatici prodotti dall'Ente, anche quelli con valenza esclusivamente interna, ma utilizzati ai fini amministrativi.

Sono esclusi dalla registrazione obbligatoria i documenti elencati nel successivo articolo del presente manuale.

Articolo 22 – Documenti non soggetti all'obbligo della registrazione di protocollo

Ai sensi dell'art. 53, comma 5, del DPR 445/00, sono esclusi dalla registrazione di protocollo le seguenti tipologie di documenti: le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'Amministrazione.

I documenti soggetti a registrazione particolare, i cui originali siano informatici, sono comunque soggetti a registrazione sul Sistema di Gestione Informatica dei Documenti; tale registrazione avverrà tramite l'assegnazione a ciascun documento di un codice identificativo univoco e persistente.

Articolo 23 – Registrazione di protocollo

Per ciascuna delle tipologie di documenti descritte al precedente art. 20 viene effettuata una registrazione di protocollo attraverso il Sistema di Gestione Informatica dei Documenti descritto nell'art. 4 del presente manuale. Tale registrazione, ai sensi dell'articolo 53, comma 3, del DPR 445/00, consiste nella memorizzazione dei dati obbligatori riferiti al documento stesso ed è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

La numerazione delle registrazioni di protocollo dei documenti del Comune di Verzegnis è unica e progressiva; corrisponde all'anno solare, chiudendosi il 31 dicembre di ogni anno e ricominciando dal 1° gennaio dell'anno successivo. Il numero di protocollo è composto da almeno sette cifre numeriche.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il Sistema di Gestione Informatica dei Documenti abbia già attribuito ad altri documenti, anche qualora questi ultimi fossero strettamente correlati tra loro.

Ad ogni registrazione di protocollo vengono associati al documento almeno i seguenti dati, conformi a quanto sancito dall'art. 53, comma 1, del DPR 445/00:

- il numero di protocollo, generato automaticamente dal Sistema e registrato in forma non

modificabile;

- la data di registrazione, generata automaticamente dal Sistema e registrata in forma non modificabile;
- l'indice di classificazione;
- il mittente o il destinatario del documento, registrati in forma non modificabile;
- l'oggetto del documento, contenente una sintetica, ma esaustiva descrizione del contenuto, registrato in forma non modificabile;
- la data e il protocollo del documento ricevuto, se disponibili.

Le registrazioni di protocollo del Comune di Verzegnis, inoltre, contengono i seguenti dati opzionali:

- la data di arrivo per i documenti in entrata (se diversa dalla data di registrazione a protocollo);
- la descrizione sintetica degli allegati;
- il mezzo di ricezione o di spedizione;
- l'ufficio di competenza;
- le copie per conoscenza.

I documenti per cui venga differita la registrazione di protocollo, secondo quanto previsto dall'articolo 29 del presente manuale, devono inoltre riportare gli estremi dell'autorizzazione al differimento dei termini di registrazione.

Ulteriori informazioni che l'Ente intendesse valorizzare in sede di protocollazione del documento, sono inserite nel campo "note al protocollo"; nel Comune di Verzegnis, nel suddetto campo è, di norma, indicato se un documento è stato inserito per errore, se trattasi di un'integrazione, ovvero la motivazione di un eventuale annullamento di protocollo.

Articolo 24 – Registrazione di protocollo dei documenti informatici

La registrazione di protocollo dei documenti informatici viene eseguita dopo aver accertato che gli stessi siano leggibili attraverso i sistemi utilizzati dal Comune di Verzegnis; dovranno essere altresì verificate la provenienza e l'integrità dei documenti, nonché il formato utilizzato, se leggibile e conforme a quelli adottati dal Comune, l'assenza di macroistruzioni o codici eseguibili tali da modificare il contenuto del documento medesimo e la validità temporale dell'eventuale firma digitale. Qualora gli accertamenti di cui al comma precedente dovessero concludersi con un esito negativo:

- laddove sottoscritto con firma digitale scaduta, il documento sarà comunque oggetto della registrazione di protocollo e verrà acquisito sul Sistema; sarà compito del Responsabile del procedimento incaricato della trattazione eseguire le opportune verifiche e valutare il trattamento da riservare a tale documento;

in tutti gli altri casi:

- verrà notificata al mittente, laddove identificabile, la condizione di eccezione, affinché provveda al rinvio del documento secondo i criteri dettati dal Comune;
- il documento oggetto di eccezione sarà mantenuto fino alla ricezione del documento corretto o, comunque, quanto necessario ai fini di un controllo successivo e, trascorso tale termine, si procederà alla sua eliminazione.

La registrazione di protocollo dei documenti informatici comporta la memorizzazione sul SGID delle stesse informazioni indicate dal precedente articolo del manuale, aggiungendo, tra i dati obbligatori, l'impronta del documento informatico, costituita dalla sequenza di simboli binari in grado di

identificarne univocamente il contenuto, ex. 53, comma 1, lettera f), del DPR 445/00 e L. 183/2011. Eseguita l'operazione di registrazione, i documenti informatici memorizzati nel Sistema di Gestione Informatica dei Documenti sono immutabili e collegati logicamente ai rispettivi dati identificativi. La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo tale che, ad ogni messaggio, corrisponda una registrazione, a seguito della quale il Sistema di Gestione Informatica dei Documenti memorizzerà:

- l'intero messaggio;
- il testo del messaggio unitamente ai dati identificativi;
- gli allegati al messaggio insieme ai relativi dati identificativi.

Articolo 25 – Segnatura di protocollo dei documenti cartacei

La segnatura di protocollo è effettuata contemporaneamente all'operazione della registrazione di protocollo; essa consiste nell'apposizione o nell'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile.

La segnatura di protocollo di un documento cartaceo avviene mediante l'apposizione su di esso di un timbro sul quale siano riportate le seguenti informazioni:

- denominazione dell'AOO;
- data e numero di protocollo del documento;
- indice di classificazione e numero del fascicolo, ove disponibili.

Sul documento da segnare potrà, alternativamente, essere apposta un'etichetta adesiva, non rimovibile né modificabile, prodotta dal Sistema di Gestione Informatica dei Documenti all'atto dell'operazione di registrazione di protocollo; su di essa andranno riportati i dati precedentemente specificati.

Articolo 26 – Segnatura di protocollo dei documenti informatici

L'operazione di segnatura di protocollo dei documenti informatici è effettuata contemporaneamente all'operazione di registrazione di protocollo e persegue il fine di favorire l'interoperabilità tra diversi sistemi di gestione documentale, riportando le informazioni archivistiche fondamentali, in modo da facilitare il trattamento dei documenti da parte del ricevente.

I dati relativi alla segnatura di protocollo di un documento trasmesso dal Comune sono associati al documento stesso e contenuti in un file XML conforme alle specifiche di cui alle più recenti linee guida per la gestione documentale e la conservazione. Tali dati sono i seguenti:

- codice identificativo dell'Amministrazione;
- codice identificativo dell'AOO;
- codice identificativo del registro;
- data di protocollo;
- numero di protocollo;
- oggetto;
- mittente;
- destinatario o destinatari.

Per quanto riguarda i documenti protocollati in uscita, nella segnatura di protocollo possono altresì essere specificate una o più delle seguenti informazioni incluse anch'esse nello stesso file XML:

- indice di classificazione;
- identificazione degli allegati;
- informazioni sul procedimento a cui si riferisce e sul trattamento da applicare al documento.

L'Amministrazione che riceve il suddetto file XML utilizzerà le informazioni in esso contenute per eseguire, eventualmente anche in forma automatizzata, la registrazione di protocollo del documento in entrata e per avviarlo alla Unità Organizzativa Responsabile competente del trattamento.

Articolo 27 – Riservatezza delle registrazioni di protocollo

Il Sistema di Gestione Informatica dei Documenti, conformemente a quanto stabilito nell'art. 4 del presente manuale, consente l'accesso ai documenti e alle informazioni nel rispetto della normativa vigente in materia di riservatezza dei dati personali, per mezzo di uno specifico livello di accesso stabilito per ciascun documento che venga registrato sul Sistema stesso.

Tale livello di riservatezza è attribuito al documento nel momento della sua registrazione sul SGID e serve a determinare, attraverso la creazione di specifiche o predefinite Access Control List (ACL), quali utenti o gruppi di utenti possono avere accesso al documento medesimo.

Di norma, ciascun utente può accedere esclusivamente ai documenti che ha prodotto, che gli sono stati assegnati o di competenza del proprio ufficio e alle informazioni ad essi collegate; viceversa, il Sistema non rende disponibili né visualizza i documenti e i dati delle relative registrazioni di protocollo per cui gli utenti non siano autorizzati.

Le tipologie documentarie riservate e le modalità di trattamento delle stesse, ivi compresi i livelli di riservatezza da associare a ciascuna, sono individuate dal Responsabile della gestione documentale d'intesa con il Responsabile per il trattamento dei dati personali.

Secondo i medesimi criteri vengono definiti anche i livelli di riservatezza dei fascicoli informatici; tale operazione viene eseguita al momento dell'apertura degli stessi sul Sistema. Per quanto concerne le caselle di posta elettronica integrate con il protocollo informatico, il Sistema di Gestione Informatica dei Documenti consente l'accesso a ciascuna di esse esclusivamente al personale autorizzato sulla base dell'organizzazione dell'Ente.

Articolo 28 – Annullamento o modifica delle registrazioni di protocollo

L'eventuale annullamento delle registrazioni di protocollo deve essere autorizzato dal Responsabile della gestione documentale.

Le informazioni relative alle registrazioni annullate rimangono memorizzate nel Sistema di Gestione Informatica dei Documenti e, conformemente a quanto disposto dall'art. 54 del DPR 445/00, recano una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento di autorizzazione.

Ai sensi dell'art. 8, comma 1, del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico", come aggiornato dalle più recenti Linee Guida AGID sul Documento Informatico, l'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile (la data e il numero di protocollo) comporta l'automatico e contestuale annullamento dell'intera registrazione di protocollo.

L'annullamento anche di un solo campo delle altre informazioni registrate in maniera immodificabile, con particolare riferimento al mittente, al destinatario e all'oggetto, che fosse necessario per correggere eventuali errori intercorsi in sede di immissione di dati, ai sensi dell'art. 8, comma 2, del suddetto DPCM, 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, all'ora e all'autore della modifica; tale disposizione si applica per lo stesso campo o per ogni altro che dovesse, in seguito, risultare errato.

Articolo 29 – Registro giornaliero delle registrazioni di protocollo

Il Responsabile della gestione documentale provvede alla produzione, in modalità informatica, 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 quelle modificate e annullate in quella medesima data.

Al fine di garantire l'immodificabilità del contenuto, il Responsabile della gestione documentale trasmette il registro giornaliero di protocollo al sistema di conservazione entro la giornata lavorativa successiva;

Articolo 30 – Differimento dei termini di registrazione

Di norma le registrazioni di protocollo dei documenti ricevuti dal Comune sono effettuate entro la giornata lavorativa successiva a quella di ricezione.

Eccezionalmente, in presenza di situazioni che lo rendano necessario, come un imprevisto carico di lavoro che non permetta di effettuare le registrazioni di protocollo nella stessa giornata lavorativa e qualora, a causa di tale condizione, possa venir meno un diritto di terzi, il Responsabile della gestione documentale può autorizzare il differimento della registrazione di protocollo dei documenti ricevuti, fissando comunque un limite di tempo entro cui le registrazioni dovranno essere effettuate e conferendo valore, nel caso di scadenze predeterminate, alla data di arrivo dei documenti.

Tutte le registrazioni di protocollo che vengono differite devono riportare gli estremi del suddetto provvedimento di autorizzazione.

Articolo 31 – Registro di emergenza

Qualora, per cause tecniche, non sia possibile usufruire del Sistema di Gestione Informatica dei Documenti, il Responsabile della gestione documentale autorizza l'Ufficio Protocollo all'effettuazione delle registrazioni di protocollo su un registro, anche cartaceo, di emergenza.

Le registrazioni di emergenza, in partenza, in arrivo o interne, vengono tutte eseguite dall'Ufficio Protocollo.

Le informazioni da inserire nel registro di emergenza, ovvero i campi obbligatori da compilare, sono gli stessi previsti dal protocollo generale.

Le modalità con cui vengono eseguite le registrazioni di protocollo sul registro di emergenza sono quelle sancite dall'art. 63 del DPR 445/00, in particolare:

- sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora del ripristino della funzionalità del Sistema;
- qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile della gestione documentale può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione;
- per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate;
- la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati

nell'ambito del sistema documentale del Comune;

- le informazioni relative ai documenti protocollati in emergenza sono inserite nel Sistema di Gestione Informatica dei Documenti al ripristino delle funzionalità dello stesso, prima che sia eseguita qualsiasi ulteriore operazione di registrazione di protocollo. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario; si avrà cura, tuttavia, di inserire nel Sistema anche il numero utilizzato in emergenza, in modo che sia mantenuta stabilmente la correlazione tra questo e il numero di protocollo attribuito al ripristino.

Il modello del registro di emergenza è indicato all'allegato 4 del presente manuale.

SEZIONE V – CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

Articolo 32 – Titolario di classificazione e piano di conservazione dell'archivio

Il titolare di classificazione e il piano di conservazione sono gli strumenti archivistici utilizzati dall'Ente per l'organizzazione, la gestione e la conservazione del proprio archivio.

Il titolare di classificazione consiste in un sistema precostituito di partizioni astratte, ordinate gerarchicamente, definito sulla base dell'organizzazione funzionale del Comune ed è lo strumento utilizzato dall'Ente per organizzare in maniera razionale e ordinata la sedimentazione dei documenti del proprio archivio, secondo un ordine logico che rispecchi lo sviluppo storico dell'attività svolta.

Il piano di conservazione, integrato con il titolare suddetto, è lo strumento che stabilisce i criteri e i tempi di selezione del materiale archivistico, al fine di distinguere la documentazione da destinare alla conservazione permanente da quella proposta periodicamente per lo scarto.

Qualora, a seguito di modifiche legislative, risulti necessario aggiornare tali strumenti ovvero si presenti la necessità di apportare variazioni o revisioni, queste vengono predisposte dal Responsabile della gestione documentale.

L'applicazione del detto titolare e delle sue eventuali modifiche, non è mai retroattiva, in considerazione del fatto che deve essere mantenuto nel tempo il legame dei fascicoli e dei documenti dell'archivio con la struttura del titolare vigente al momento della produzione degli stessi e, dunque, il corretto vincolo archivistico che lega la produzione documentaria del Comune all'attività e alle funzioni dello stesso; a tal fine viene garantita la storicizzazione delle variazioni del titolare e la possibilità di ricostruire le diverse voci nel tempo.

Le modifiche del titolare impediscono di aprire nuovi fascicoli nelle partizioni eventualmente eliminate ma non precludono la possibilità di inserire i documenti in fascicoli precedentemente aperti all'interno di tali voci, fino alla chiusura degli stessi.

Le suddette variazioni del titolare di classificazione sono, di norma, introdotte a partire dal 1° gennaio dell'anno successivo.

Il titolare unico di classificazione è riportato all'allegato 3 del presente manuale.

Articolo 33 – Classificazione dei documenti

La classificazione è l'operazione che viene eseguita a partire dal titolare ed è finalizzata ad organizzare logicamente, in relazione alle funzioni dell'Ente, tutti i documenti ricevuti e prodotti dal Comune di Verzegnis, siano essi cartacei o informatici, successivamente alla loro registrazione nel Sistema di Gestione Informatica dei Documenti.

Tale operazione consiste nell'assegnazione a ciascun documento di un codice, detto indice di classificazione che, in base all'oggetto del documento medesimo, lo associa alla voce del titolare relativa alla corrispondente funzione dell'Ente; sulla base dell'indice di classificazione risulta indicata la posizione logica del documento all'interno dell'archivio ed è possibile l'inserimento nel fascicolo appropriato.

A ciascun documento è associato un unico indice di classificazione, anche qualora attenga a più procedimenti, facenti riferimento a fascicoli di classifiche diverse; in tal caso l'indice di classificazione sarà quello relativo alla collocazione che, in base all'oggetto, venga ritenuta prevalente.

La classificazione dei documenti è eseguita dal personale che ne effettua la relativa registrazione al protocollo.

Nel caso siano presenti errori nell'indice di classificazione di un documento protocollato in arrivo, il personale dell'ufficio che riceve il documento lo comunica all'Ufficio Protocollo che procede a

correggere, sul Sistema, la classificazione errata; il Sistema di Gestione Informatica dei Documenti manterrà traccia delle operazioni svolte, registrandone l'autore, la data e l'ora.

Nel caso di documenti cartacei, l'operatore che procede alla classificazione provvede a riportare l'indice di classificazione nell'apposito spazio previsto nella segnatura di protocollo o ad apporre l'etichetta di cui all'articolo 24 del presente manuale.

Nell'ambito del Comune di Verzegnis, tutti i soggetti abilitati all'operazione di classificazione devono conoscere e saper correttamente utilizzare il titolario di classificazione; è compito del Responsabile della gestione documentale provvedere affinché detto personale sia adeguatamente formato sul corretto utilizzo dello strumento e debitamente istruito sulle variazioni eventualmente apportate ad esso.

Articolo 34 – Formazione e identificazione dei fascicoli

Il Sistema di Gestione Informatica dei Documenti consente la formazione di fascicoli cartacei, informatici, ibridi e di aggregazioni documentali informatiche.

Per fascicolo si intende un insieme di documenti, ordinati cronologicamente, relativi ad un medesimo procedimento amministrativo o affare oppure alla medesima persona fisica o giuridica, classificati in maniera omogenea; il fascicolo costituisce l'unità di base, indivisibile, di un archivio.

Ai sensi dell'allegato n. 1 del DPCM 3/12/2013, e secondo le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate da AgID, per fascicolo informatico si intende un'aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella Pubblica Amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del D. Lgs. 82/05.

Per aggregazione documentale informatica si intende un'aggregazione di documenti informatici o di fascicoli informatici, riuniti per 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.

Per fascicolo ibrido si intende un fascicolo o un'aggregazione documentale composta al tempo stesso da documenti cartacei e documenti informatici.

Tutti i documenti registrati nel SGID del Comune di Verzegnis, indipendentemente dal supporto sul quale sono prodotti, sono riuniti in fascicoli sulla base dell'oggetto, dell'attività, del procedimento amministrativo, della persona fisica o giuridica cui si riferiscono.

L'operazione di fascicolazione consiste nell'inserire ciascun documento nel fascicolo di riferimento, costituito all'interno della corrispondente partizione logica prevista dal titolario di classificazione del Comune.

La fascicolazione, fondamentale per la gestione e l'uso dell'archivio, consente di collegare i singoli documenti a quelli precedenti e successivi prodotti o ricevuti dal Comune nell'ambito di uno stesso procedimento, affare o attività, in modo da riflettere il concreto espletamento delle funzioni dell'Ente; tale operazione sarà di tipo logico per i documenti informatici e di tipo fisico per quelli cartacei.

I documenti sono collocati all'interno del fascicolo secondo l'ordine cronologico di registrazione nel Sistema di Gestione Informatica dei Documenti; ogni fascicolo all'interno dell'archivio del Comune va ad occupare un posto specifico, tale posizione è di natura logica, nel caso di fascicoli informatici, o fisica, nel caso di fascicoli cartacei o per quanto riguarda la parte cartacea dei fascicoli ibridi.

La formazione dei fascicoli è competenza dei responsabili dei procedimenti amministrativi, individuati all'interno delle singoli uffici incaricati della trattazione dei relativi affari.

L'apertura di un nuovo fascicolo o di una nuova aggregazione documentale comporta la registrazione nel Sistema di Gestione Informatica dei Documenti almeno delle seguenti informazioni che li identificano all'interno dell'archivio del Comune:

- oggetto del procedimento (denominazione del fascicolo);
- responsabile del procedimento;
- data di apertura;
- indice di classificazione;
- numero del fascicolo (un numero progressivo, immutabile, attribuito automaticamente dal Sistema al momento dell'apertura nell'ambito della voce di classificazione di appartenenza).

E' infine possibile inserire, in un apposito campo, l'indicazione dei tempi di conservazione previsti per ciascun fascicolo.

Anche i fascicoli composti esclusivamente da documenti cartacei devono essere formati sul sistema di Gestione Informatica dei Documenti, collegando tra loro le registrazioni di protocollo relative ai documenti cartacei contenuti nel fascicolo; tale operazione è fondamentale al fine di mantenere la corretta numerazione univoca di tutti i fascicoli presenti nell'archivio dell'Ente, a prescindere dal supporto su cui sono formati.

Al termine di ciascun procedimento amministrativo si procede alla chiusura del relativo fascicolo, integrando le suddette informazioni con la data di chiusura che fa riferimento alla registrazione nel Sistema dell'ultimo documento prodotto nel corso della trattazione dell'affare medesimo.

Nel caso di fascicoli cartacei o componenti cartacei di fascicoli ibridi, nel Sistema di Gestione Informatica dei Documenti va associata a detti fascicoli un'ulteriore informazione, inserita nel campo "note", relativa alla posizione fisica che questi occupano nell'archivio dell'Ente, al fine di consentire un agile reperimento, avendo cura, in particolar modo nel caso di fascicoli ibridi, che sia chiaro il collegamento con la parte informatica della stessa unità archivistica, in modo che l'unità logica del fascicolo medesimo sia salvaguardata e il recupero della documentazione necessaria a svolgere le consuete attività del Comune sia quanto più semplice e funzionale possibile. I fascicoli cartacei o le porzioni cartacee dei fascicoli ibridi devono riportare tutte le suddette informazioni sul proprio frontespizio.

I fascicoli, qualora se ne avverta l'esigenza ai fini operativi o in considerazione dell'eccessiva mole di documenti contenuti, possono essere al loro interno articolati in sottofascicoli e questi ultimi, a loro volta, in inserti.

Nel caso le esigenze operative imponessero di creare aggregazioni di fascicoli per gestire procedimenti amministrativi particolarmente complessi e articolati, tali collegamenti tra i fascicoli saranno gestiti attraverso l'inserimento sul Sistema di un'ulteriore informazione che indichi tale collegamento, inserita nel campo denominato "numero manuale".

I fascicoli cartacei e i fascicoli ibridi devono recare sul frontespizio, in aggiunta alle informazioni sopra elencate i sottofascicoli e inserti cartacei eventualmente contenuti al proprio interno.

Ad ogni fascicolo corrisponde nel Sistema di Gestione Informatica dei Documenti uno specifico livello di riservatezza, sulla base di quanto disposto dall'art. 26 del presente manuale, in modo da stabilire quali utenti o gruppi di utenti possano accedere a ciascun fascicolo; tali livelli di riservatezza possono essere diversificati per i documenti contenuti all'interno dello stesso fascicolo, potendo prevedere per essi un livello di riservatezza superiore a quello del fascicolo di cui sono parte.

I fascicoli e le serie documentarie cartacee, relativi a procedimenti e affari conclusi, sono trasferiti nell'archivio di deposito del Comune, secondo quanto disposto dall'art. 67 del DPR 445/00.

Per quanto concerne i fascicoli informatici e le aggregazioni documentali informatici è compito del Responsabile della gestione documentale predisporre il pacchetto di versamento per il trasferimento dei medesimi presso il conservatore accreditato, nel rispetto delle modalità operative previste nel manuale di conservazione e nell'articolo 3 del presente manuale.

SEZIONE VI – GESTIONE DELLA CORRISPONDENZA IN ENTRATA

Articolo 35 – Ricezione

Le modalità operative attraverso le quali vengono trattati i documenti in entrata sono descritte nella sezione III del presente manuale.

Articolo 36 – Gestione della corrispondenza cartacea

La corrispondenza cartacea indirizzata nominativamente al personale del Comune di Verzegnis viene regolarmente aperta e registrata al protocollo, a meno che sulla busta non sia riportata la dicitura “riservata”, “personale”, “confidenziale”, “S.P.M.” *et similia*. In quest’ultimo caso viene recapitata in busta chiusa al destinatario il quale, dopo averla aperta e preso visione del contenuto, qualora valuti che il documento ricevuto non sia riservato ai sensi della normativa vigente sulla privacy, lo deve riconsegnare celermente all’ufficio preposto per le attività di protocollazione.

Le lettere anonime devono essere protocollate ed identificate come tali, con la dicitura “mittente sconosciuto” o “mittente anonimo”. I documenti anonimi il cui contenuto sia giuridicamente irrilevante o inequivocabilmente da ricondurre a scherzi o situazioni simili, vengono distrutti; se, invece, si ritiene che contengano dati o informazioni rilevanti, dopo la registrazione di protocollo, si provvede ad inviarli agli uffici competenti per ulteriori eventuali determinazioni.

I documenti sottoscritti, di cui non sia identificabile l’autore, vengono protocollati indicando nel campo mittente la dicitura “mittente non identificabile” e sono inoltrati al responsabile competente; quest’ultimo, ricevuto il documento, valuterà la possibilità nonché la necessità di acquisire gli elementi mancanti per perfezionare l’atto, provvedendo altresì affinché venga integrata la registrazione di protocollo.

I documenti ricevuti privi di firma, ma il cui mittente sia comunque identificabile, vengono protocollati e inoltrati al responsabile del procedimento, che valuterà la necessità di acquisire la dovuta sottoscrizione per il perfezionamento degli atti.

La corrispondenza cartacea riportante l’indicazione “offerta”, “gara d’appalto”, “preventivo” o simili, o dal cui involucro sia possibile evincere che si riferisca alla partecipazione ad una gara, non deve essere aperta, ma protocollata in base agli elementi rilevabili dal plico o dal bando dell’Amministrazione, apponendo numero di protocollo e data di registrazione direttamente sulla busta. Sull’esterno della busta, accanto alla segnatura di protocollo, viene annotato l’orario di arrivo unicamente nei casi in cui il documento venga consegnato *brevi manu* oltre il limite orario stabilito nel bando o nell’avviso pubblico: la specifica oraria viene pertanto a contrassegnare soltanto le offerte pervenute oltre la prevista scadenza. L’ufficio competente allo svolgimento della procedura di gara provvede alla custodia della busta o dei contenitori così protocollati, sino all’espletamento della gara; lo stesso ufficio, successivamente alla fase di apertura delle buste, riporterà gli estremi di protocollo presenti sulle buste su ogni documento che le stesse contengano.

Qualora il Comune di Verzegnis dovesse ricevere un documento cartaceo di competenza di altro ente, altra AOO, altra persona fisica o giuridica, lo stesso verrà trasmesso a chi di competenza, se individuabile, altrimenti sarà restituito al mittente. Nel caso in cui un documento della fattispecie sopra indicata venga erroneamente registrato al protocollo, verrà spedito a chi di competenza, oppure restituito al mittente unitamente ad una lettera di trasmissione opportunamente protocollata; il documento erroneamente protocollato sarà soggetto alla procedura di annullamento del protocollo.

Articolo 37 – Gestione della corrispondenza informatica

In tutti i casi in cui la corrispondenza in arrivo dovesse contenere file non leggibili, presentare sottoscrizioni digitali scadute, macroistruzioni o codici eseguibili, ovvero, dovesse essere prodotta utilizzando formati digitali non conformi a quelli adottati dal Comune, si seguiranno le indicazioni previste dall'art. 23 del presente manuale.

Per quanto concerne la ricezione, da parte del Comune, della corrispondenza in formato elettronico di competenza di altro ente, altra AOO, altra persona fisica o giuridica, le modalità da seguire, nel trattamento, sono le stesse previste per gli analoghi casi che abbiano ad oggetto la corrispondenza cartacea.

Articolo 38 – Registrazione di protocollo e classificazione

Le operazioni di registrazione di protocollo e di classificazione della corrispondenza in entrata, sia essa cartacea o informatica, vengono eseguite secondo le regole specificate nelle sezioni IV e V del presente manuale; per eventuali casi particolari si seguiranno le indicazioni previste nell'articolo 35, per quanto attiene la corrispondenza cartacea e 36 per quel che riguarda quella informatica.

I documenti ricevuti via fax, i cui mittenti siano soggetti diversi dalle pubbliche amministrazioni, vengono registrati al protocollo generale; ai sensi dell'art. 45 del D. Lgs. 82/05, infatti, i documenti trasmessi con qualunque mezzo telematico o informatico idoneo ad accertarne la fonte di provenienza soddisfano il requisito della forma scritta e non devono essere seguiti dalla trasmissione dell'originale. Tuttavia, qualora in seguito pervengano gli originali, ad essi saranno attribuiti numero e data di protocollo assegnati ai relativi fax.

Per quanto concerne le comunicazioni tra pubbliche amministrazioni, si ribadisce che, ai sensi dell'art. 47, comma 2, lettera c), del D. Lgs. 82/05, è esclusa la trasmissione dei documenti tramite fax.

Articolo 39 – Assegnazione

L'operazione di assegnazione è finalizzata all'individuazione dell'ufficio cui compete la trattazione del relativo affare o procedimento amministrativo, nonché degli eventuali altri uffici interessati per conoscenza. L'assegnazione dei documenti ricevuti dal Comune di Verzegnis è effettuata dall'operatore che esegue la registrazione di protocollo dei documenti in arrivo.

L'assegnazione è effettuata contestualmente alla registrazione di protocollo; nel caso di dubbi sull'individuazione degli uffici cui trasmettere i documenti ricevuti, l'assegnazione può essere eseguita anche in un momento successivo.

Nel caso di una assegnazione errata, l'ufficio che riceve il documento lo rimanderà indietro all'unità di protocollazione, comunicando l'errore. L'Ufficio Protocollo procederà ad una nuova assegnazione, correggendo le informazioni inserite nel Sistema di Gestione Informatica dei Documenti.

Il SGID tiene traccia di ogni passaggio, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua le operazioni sopra descritte, con la data e l'ora di esecuzione.

Articolo 40 – Scansione

I documenti su supporto cartaceo soggetti a registrazione di protocollo, dopo le operazioni di registrazione, classificazione e segnatura, sono digitalizzati in formato immagine attraverso un processo di scansione manuale.

Il processo di scansione si articola nelle seguenti fasi:

- acquisizione delle immagini in modo che ad ogni documento, anche composto da più fogli, corrisponda un file unico in un formato idoneo alla conservazione,

- verifica della leggibilità e della qualità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- collegamento delle rispettive immagini alla relativa registrazione di protocollo;
- memorizzazione delle immagini nel Sistema di Gestione Informatica dei documenti, in modo non modificabile.

L'operazione di scansione viene eseguita esclusivamente nei casi in cui non vi sia la possibilità di acquisire i documenti direttamente in formato elettronico.

I documenti ricevuti dal Comune su supporto cartaceo, ancorché digitalizzati, una volta registrati a protocollo, classificati ed assegnati, sono comunque consegnati anche in originale cartaceo all'ufficio competente.

Articolo 41 – Recapito e presa in carico della corrispondenza informatica

I documenti informatici in entrata, una volta protocollati e classificati, sono assegnati agli uffici competenti e resi disponibili attraverso il Sistema di Gestione Informatica dei Documenti; la loro "presa in carico" è pertanto automatica e avviene contestualmente all'assegnazione.

Qualora dovesse verificarsi un'assegnazione errata, si procederà secondo quanto descritto nell'art. 38 del presente manuale.

Articolo 42 – Sub assegnazione

Nell'ambito di ciascun ufficio, il Responsabile cui sono stati assegnati i documenti ricevuti, già protocollati e classificati, esegue per ognuno di essi l'operazione di sub assegnazione.

La sub assegnazione può essere effettuata anche più volte per ciascun documento ed è finalizzata ad individuare i soggetti incaricati della trattazione dei suddetti documenti.

Articolo 43 – Fascicolazione

Nell'ambito degli uffici cui sono assegnati i documenti in entrata viene eseguita, a cura dei vari Responsabili dei procedimenti amministrativi, l'operazione di fascicolazione così come descritta nella sezione V del presente manuale.

SEZIONE VII – GESTIONE DEI DOCUMENTI INTERNI, DEI FLUSSI DOCUMENTALI E DEI PROCEDIMENTI AMMINISTRATIVI

Articolo 44 – Produzione dei documenti dell'AOO

Il Comune di Verzegnis, per quanto riguarda i flussi documentali interni, ha provveduto ad una progressiva dematerializzazione, in modo che gli originali di tutti i documenti siano esclusivamente informatici, salvo in casi eccezionali.

I documenti i cui originali siano informatici, sono formati nel rispetto delle regole definite nella sezione II del presente manuale e, all'interno degli uffici dell'Ente, circolano esclusivamente in modalità digitale.

Le operazioni di registrazione, classificazione e fascicolazione dei documenti interni aventi valenza amministrativa sono eseguite dai vari uffici che li hanno formati e sono svolte secondo quanto disposto nelle precedenti sezioni IV e V del presente manuale di gestione.

Articolo 45 – Gestione dei flussi documentali interni

La circolazione dei documenti amministrativi informatici all'interno degli uffici del Comune di Verzegnis avviene esclusivamente utilizzando le funzionalità del Sistema di Gestione Informatica dei Documenti, tramite l'assegnazione ai vari uffici destinatari, la sub assegnazione e per mezzo delle comunicazioni interne Halley.

Non è consentito, per tali comunicazioni, l'uso di mezzi di trasmissione alternativi a quanto sopra descritto, ivi compreso l'utilizzo di e-mail.

Analogamente la trasmissione di fascicoli o di parti di essi tra i vari uffici interni al Comune avviene utilizzando il Sistema di Gestione Informatica dei Documenti.

Articolo 46 – Gestione dei procedimenti amministrativi

Il Sistema di Gestione Informatica dei Documenti realizza le condizioni operative per una gestione efficace dei flussi documentali dell'Ente anche ai fini dello snellimento delle procedure, della trasparenza e dell'efficacia dell'azione amministrativa ai sensi degli articoli 64 e seguenti del DPR 445/00.

Il Sistema, anche alla luce di quanto previsto dall'articolo 24, comma 3-bis, del D.L. 90/14 "Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari", tenderà gradualmente a realizzare la gestione integrata dei procedimenti amministrativi, permettendo così agli uffici ed agli utenti di controllare gli stati di avanzamento delle loro pratiche e le responsabilità connesse ai procedimenti stessi.

La gestione dei procedimenti amministrativi avrà il fine di consentire:

- l'elencazione dei vari step del procedimento, specificandone le varie fasi, i sub-procedimenti, i possibili percorsi alternativi cui la pratica potrà giungere;
- le comunicazioni interne circa gli stati di avanzamento dei procedimenti amministrativi;
- il controllo dei tempi di svolgimento delle attività connesse al procedimento amministrativo e la segnalazione delle scadenze;
- il tracciamento di ogni operazione effettuata;
- la ricerca e la visualizzazione dello stato di avanzamento delle pratiche attive.

SEZIONE VIII – GESTIONE DELLA CORRISPONDENZA IN USCITA

Articolo 47 – Spedizione dei documenti su supporto cartaceo

La spedizione di documenti prodotti o comunque trattati dal Comune di Verzegnis avviene, di norma, in modalità informatica, secondo le indicazioni definite nell'articolo 47 del presente manuale; l'invio di documenti cartacei avviene esclusivamente nei casi in cui risulti impossibile procedere in modalità digitale.

I documenti da spedire su supporto cartaceo, una volta registrati, classificati e fascicolati, vengono imbustati e convogliati agli uffici preposti alle operazioni di affrancatura, contabilizzazione delle spese e spedizione.

Nel caso di spedizioni che utilizzino posta raccomandata con ricevuta di ritorno, posta celere, corriere od altro mezzo di spedizione che richieda di allegare altra documentazione alla busta, la relativa modulistica verrà compilata a cura degli uffici mittenti.

La minuta (fotocopia) del documento cartaceo spedito verrà conservata all'interno del relativo fascicolo.

Nel caso in cui l'Ente si trovi ad interagire con utenti sprovvisti di adeguati strumenti informatici o impossibilitati al loro utilizzo si procede, qualora si tratti di documenti originali informatici, alla produzione e alla consegna della copia conforme, in formato analogico, prodotta secondo le modalità previste dall'articolo 15 del presente manuale.

Articolo 48 – Spedizione dei documenti informatici

La spedizione dei documenti informatici avviene, di norma, per mezzo delle caselle di posta elettronica certificata di cui all'articolo 18 del presente manuale, attraverso il Sistema di Gestione Informatica dei Documenti; quest'ultimo, una volta composto il messaggio da spedire, lo inoltra al destinatario o ai destinatari, utilizzando il servizio di PEC del Comune.

I documenti informatici vengono trasmessi agli indirizzi di posta elettronica certificata dichiarati dai destinatari ovvero reperibili in indici ed elenchi ufficiali di pubblica consultazione (es.: <http://www.indicepa.gov.it> per le pubbliche amministrazioni).

La trasmissione di documenti informatici tra pubbliche amministrazioni avviene mediante posta elettronica certificata o mediante i meccanismi di interoperabilità e cooperazione applicativa di cui al Sistema Pubblico di Connettività (SPC), utilizzando le informazioni contenute nella segnatura di protocollo.

La spedizione di un documento informatico viene eseguita dal Sistema al completamento delle operazioni di registrazione di protocollo, classificazione e fascicolazione, conformemente a quanto descritto nelle Sezioni IV e V del presente manuale.

L'integrazione funzionale tra il servizio di posta elettronica certificata e il SGID ovvero i meccanismi di interoperabilità e cooperazione applicativa consentono la produzione del messaggio da parte del Sistema stesso e il suo invio in automatico.

Le ricevute rilasciate dai gestori del servizio di posta elettronica certificata e i messaggi di ritorno generati dal SGID del destinatario saranno identificati dal Sistema e da questo automaticamente archiviati, collegandoli alle registrazioni di protocollo dei documenti corrispondenti; nel caso di ricezione di notifiche di eccezione, che segnalino situazioni di anomalia, ivi incluso il mancato recapito del messaggio stesso, il Sistema di Gestione Informatica dei Documenti provvederà a notificare l'evento al personale responsabile.

Al fine di garantire la riservatezza dei dati di cui all'art. 4 del D. Lgs. 196/03 ed s.m.i. (D.Lgs. 101/2018) "Codice in materia di protezione dei dati personali", i documenti informatici trasmessi ad

altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o regolamento che siano indispensabili per il perseguimento delle finalità per le quali sono acquisite.

In ogni caso, sono osservate le disposizioni contenute nei regolamenti adottati dal Comune per il trattamento dei dati personali, sensibili e giudiziari anche con strumenti elettronici.

SEZIONE IX – ARCHIVIAZIONE DEI DOCUMENTI

Articolo 49 – Archivio dell'amministrazione

L'archivio del Comune di Verzegnis consiste nel complesso organico degli atti, cartacei o informatici, prodotti o ricevuti dall'Ente nell'esercizio delle proprie funzioni e per il conseguimento dei propri fini istituzionali.

I documenti facenti parte dell'archivio del Comune sono legati tra loro dal vincolo archivistico: nesso che collega in maniera logica la documentazione posta in essere dal soggetto produttore. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico.

L'archivio dell'Ente costituisce un bene culturale ai sensi dell'art. 10, comma 2, lettera b), del D.Lgs. 42/04 "Codice dei beni culturali e del paesaggio", come tale è inalienabile, non può essere smembrato, danneggiato, distrutto o utilizzato in modo tale da recare pregiudizio alla sua conservazione; è obbligo del Comune, ai sensi dell'art. 30, comma 4, del suddetto decreto conservare il proprio archivio nella sua organicità, provvedendo inoltre ad ordinare e inventariare il proprio archivio storico.

Ai sensi dell'art. 21, commi 1 e 2, del D. Lgs. 42/04 le operazioni di spostamento degli archivi non correnti, l'esecuzione di opere e lavori, nonché lo scarto del materiale archivistico sono soggetti all'autorizzazione della Soprintendenza archivistica competente per territorio.

Le responsabilità del Comune, connesse alla tutela del proprio patrimonio archivistico, si estendono anche agli archivi digitali depositati presso un conservatore accreditato ai sensi della normativa vigente; in tal senso la competenza per la tutela degli archivi pubblici da parte del Ministero dei beni e delle attività culturali e del turismo si esercita anche sui sistemi di conservazione digitale.

L'archivio in senso proprio costituisce un complesso unitario composto, ai fini della gestione documentale, dall'archivio digitale, dall'archivio ibrido e dall'archivio cartaceo; quest'ultimo, per motivi organizzativi e funzionali, si articola in archivio corrente, archivio di deposito e archivio storico.

Articolo 50 – Archivio corrente

Per archivio corrente si intende l'insieme dei documenti e dei fascicoli prodotti, acquisiti e conservati dal Comune di Verzegnis nell'esercizio delle proprie funzioni, relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione e per i quali sussista un interesse attuale.

L'archivio corrente del Comune si forma svolgendo le opportune procedure di classificazione e fascicolazione secondo le modalità previste nella sezione V del presente manuale; tali operazioni permettono la sedimentazione e l'organizzazione dell'archivio in maniera corretta e ordinata, in modo da rendere più semplice il recupero dei documenti.

I fascicoli e le unità archivistiche cartacee che costituiscono l'archivio corrente sono conservate a cura dei Responsabili dei procedimenti amministrativi.

Articolo 51 – Archivio di deposito

Per archivio di deposito si intende l'insieme dei documenti e dei fascicoli cartacei relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulti più necessaria una trattazione inerente le attività amministrative correnti, ma che possono rivelarsi ancora utili per finalità amministrative e giuridiche.

Il Responsabile della gestione documentale procede, al versamento nell'archivio di deposito dell'Ente dei fascicoli relativi a procedimenti o affari conclusi; tali fascicoli sono individuati dai Responsabili dei procedimenti amministrativi che ne hanno curato la formazione, gestione e

trattazione, i quali procedono a verificarne la corretta formazione e la completezza.

Il suddetto versamento delle unità archivistiche nell'archivio di deposito viene registrato nel Sistema di Gestione Informatica dei Documenti, inserendo per ciascun fascicolo l'informazione che specifichi il proprio trasferimento in deposito.

I fascicoli conservati nell'archivio di deposito dell'Ente recano sul frontespizio le informazioni previste dall'art. 33 del presente manuale.

La gestione dell'archivio di deposito è demandata all'Area Affari Generali-Servizio Protocollo; il Responsabile della gestione documentale provvede a:

- conservare la documentazione contenuta nel detto archivio di deposito;
- garantirne la consultazione nel rispetto della normativa vigente sull'accesso ai documenti amministrativi;
- registrare la movimentazione dei fascicoli dati in consultazione;
- selezionare la documentazione da proporre per lo scarto e quella da destinare al versamento nell'archivio storico producendo, in entrambi i casi, i relativi elenchi, secondo quanto descritto nel successivo articolo.

L'archiviazione e la custodia dei documenti che contengano dati personali o dati sensibili avviene nel rispetto della normativa vigente in materia di protezione e tutela dei dati personali.

Articolo 52 – Archivio digitale

L'archivio digitale del Comune di Verzegnis è costituito da documenti, aggregazioni documentali e fascicoli informatici registrati e gestiti per mezzo del Sistema di Gestione Informatica dei Documenti; tale Sistema rappresenta, dunque, il luogo in cui l'archivio digitale ha sede.

La conservazione a lungo termine e quella permanente dell'archivio digitale del Comune di Verzegnis è demandata ad un soggetto conservatore accreditato dall'AgID ed avviene nel rispetto di quanto previsto dalla vigente normativa in materia.

Il trasferimento dei documenti informatici e dei relativi metadati al sistema di conservazione suddetto avviene predisponendo il pacchetto di versamento.

Articolo 53 – Archivio ibrido

Per archivio ibrido si intende il complesso di documenti, fascicoli e aggregazioni documentali, in parte cartacei e in parte digitali, prodotti, acquisiti e conservati dall'Ente nello svolgimento delle proprie attività. I documenti cartacei facenti parte di fascicoli o aggregazioni documentali ibride saranno oggetto di versamento all'archivio di deposito del Comune di Verzegnis, secondo le modalità previste dal precedente art. 50; per quanto riguarda, invece, la documentazione digitale e i metadati relativi al fascicolo o all'aggregazione documentale, essi saranno oggetto di trasferimento al sistema di conservazione accreditato secondo quanto previsto dal precedente art. 51. In ogni caso viene mantenuto il collegamento logico tra la parte cartacea e quella digitale di una stessa unità archivistica; a tal fine, il frontespizio di ciascun fascicolo ibrido, contenente la documentazione cartacea dello stesso, riporterà le informazioni previste dall'art. 33 del presente manuale.

SEZIONE X – APPROVAZIONE E AGGIORNAMENTO

Articolo 54 – Approvazione, aggiornamento e pubblicità del manuale

Il presente Manuale è approvato, integrato e modificato con delibera della Giunta comunale; lo stesso è soggetto a revisione su iniziativa del Responsabile della gestione documentale.

In caso di sopravvenienze normative, introduzione di nuove prassi tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza, evoluzione delle procedure e delle infrastrutture tecnologiche o comunque, ogni qual volta il Responsabile lo riterrà necessario, si potrà procedere a revisione del Manuale anche prima della scadenza sopra prevista.

La modifica o l'aggiornamento di uno o di tutti gli allegati al presente Manuale non comporta la revisione nei modi di cui sopra del Manuale stesso.

Il presente Manuale è pubblicato nel sito internet istituzionale del Comune di Verzegnis, ai sensi dell'art. 5, comma 3, del DPCM 3/12/2013 e s.m.i..

GLOSSARIO

Access Control List (ACL): metodo utilizzato per determinare l'accesso o meno alle risorse del Sistema di Gestione Informatica dei Documenti da parte degli utenti, stabilito sulla base di specifici livelli di riservatezza associati a ciascuna risorsa informatica.

Accesso: operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.

Accreditamento: riconoscimento, da parte dell'Agenzia per l'Italia digitale (AgID), del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione.

Agenzia per l'Italia Digitale (AgID): organismo che svolge attività di progettazione e coordinamento delle iniziative strategiche per la più efficace erogazione di servizi in rete della pubblica amministrazione a cittadini e imprese. Elabora gli indirizzi, le regole tecniche e le linee guida per la piena interoperabilità e cooperazione applicativa tra i sistemi informatici della pubblica amministrazione e tra questi e i sistemi dell'Unione Europea, assicura l'uniformità tecnica dei sistemi informativi pubblici destinati a erogare servizi ai cittadini e alle imprese, garantendo livelli omogenei di qualità e fruibilità sul territorio nazionale, nonché la piena integrazione a livello europeo.

Aggregazione documentale informatica: aggregazione di documenti informatici o di fascicoli informatici, riuniti per 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.

Archivio: complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura, formati, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento della propria attività.

Archivio corrente: complesso dei documenti riferibili ad attività o procedimenti amministrativi in corso di istruttoria e trattazione o da poco conclusi.

Archivio di deposito: complesso di documenti relativi ad attività o procedimenti conclusi, trasferiti dall'archivio corrente in quanto non più necessari alle attività quotidiane.

Archivio storico: complesso dei documenti relativi ad affari esauriti da oltre 40 anni e destinati, previa le operazioni di scarto, alla conservazione permanente.

Archivio ibrido: complesso di documenti, fascicoli e aggregazioni documentali in parte cartacei e in parte digitali.

Archivio informatico: archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche, gestiti e conservati in ambiente informatico.

Area Organizzativa Omogenea (AOO): un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del DPR 445/00.

Assegnazione: individuazione, da parte del personale abilitato alla registrazione di protocollo, della UOR di competenza e/o della persona fisica responsabile della trattazione dell'affare o del documento nella fase corrente.

Autenticità: caratteristica di un documento informatico che garantisce di essere ciò che dichiara

di essere, senza aver subito alterazioni o modifiche.

Casella istituzionale di posta elettronica certificata (PEC): casella di posta elettronica istituita dall'AOO per la ricezione e la spedizione di messaggi/documenti informatici.

Certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche.

Certificato qualificato: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.

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

Chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.

Chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.

Classificazione: attività di organizzazione logica di tutti i documenti secondo il titolare di classificazione, articolato in voci individuate in relazione alle funzioni dell'Ente. Tale operazione consiste nell'assegnazione a ciascun documento, in base all'oggetto, di un indice di classificazione e del numero di repertorio del fascicolo in cui il documento stesso è contenuto.

Codice eseguibile: insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.

Codice identificativo dell'AOO: codice univoco, assegnato alle AOO dall'IPA.

Codice IPA: il codice univoco che viene assegnato all'Ente al termine del processo di accreditamento. Il Codice IPA viene comunicato tramite e-mail dal gestore dell'IPA al referente dell'Ente.

Conservatore accreditato: soggetto, pubblico o privato, che svolge attività di conservazione, al quale sia stato riconosciuto dall'AgID il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Conservazione: insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione.

Coordinatore della Gestione Documentale: responsabile della definizione di criteri uniformi di classificazione ed archiviazione, nonché di comunicazione interna tra le AOO, ai sensi di quanto disposto dall'articolo 50, comma 4, del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.

Copia analogica del documento informatico: documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.

Copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.

Copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto.

Copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento informatico da cui è tratto, ma avente diversa sequenza di valori binari.

Dispositivi sicuri per la generazione della firma elettronica qualificata: mezzi sui quali il firmatario può conservare un controllo esclusivo e la cui conformità è accertata ai sensi dell'art. 12 del DPCM 22/02/2013.

Documento amministrativo: ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.

Documento amministrativo informatico: atto formato dalla pubblica amministrazione con strumenti informatici o comunque da essa detenuto, il cui originale sia in formato digitale.

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

Documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.

Fascicolazione: operazione di riconduzione dei documenti classificati relativi a un medesimo affare o procedimento amministrativo nello stesso fascicolo.

Fascicolo: insieme di documenti, ordinati cronologicamente, relativi ad un medesimo procedimento amministrativo o affare oppure alla medesima persona fisica o giuridica, classificati in maniera omogenea.

Fascicolo ibrido: fascicolo o aggregazione documentale composta da documenti cartacei e documenti informatici.

Fascicolo informatico: aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento.

Fax Server: software o combinazione di software e hardware in grado di elaborare, inviare e ricevere documenti informatici; di solito è installato su di una organizzazione di rete locale (LAN).

Firma digitale: un particolare tipo di firma elettronica avanzata 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.

Firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

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 può

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.

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.

Formato elettronico: modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico.

Funzionalità aggiuntive: le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.

Funzionalità interoperative: le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del DPR 445/00.

Funzionalità minima: la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del DPR 445/00.

Funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.

Gestione dei documenti: insieme delle attività finalizzate alla registrazione di protocollo, alla classificazione, alla fascicolazione, all'assegnazione, al reperimento, alla conservazione e all'accesso dei documenti amministrativi formati o acquisiti dall'AOO.

Gestore di posta elettronica certificata: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata.

Identificativo univoco: sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.

Identificazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.

Immodificabilità: caratteristica che rende il documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e garantisce la staticità ai fini della conservazione del documento stesso.

Impronta di una sequenza di simboli binari (bit): la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.

Indice delle Pubbliche Amministrazioni (IPA): l'Indice delle Pubbliche Amministrazioni consente di reperire le informazioni relative alla Posta Elettronica Certificata (PEC) e alle strutture organizzative, le cosiddette Aree Organizzative Omogenee (AOO), di tutte le pubbliche amministrazioni locali e centrali. L'IPA è una sorta di "rubrica telefonica" evoluta con informazioni dettagliate e certificate. Esso contiene, infatti, la struttura e le competenze degli uffici pubblici con i nominativi dei referenti, l'elenco dei servizi offerti, le informazioni per il loro utilizzo, i numeri di telefono, gli indirizzi di posta elettronica istituzionali afferenti alle AOO e gli indirizzi di posta elettronica certificata attivati dalle Amministrazioni.

Indice di classificazione: codice alfanumerico assegnato a ciascun documento, per mezzo dell'operazione di classificazione, che identifica le partizioni logiche del titolare cui il documento fa riferimento.

Insieme minimo di metadati del documento informatico: complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta e la conservazione.

Integrità: insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.

Interoperabilità: capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.

Leggibilità: insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.

Log di sistema: registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.

Macroistruzione: istruzione o codice in grado di modificare il contenuto di un documento informatico.

Manuale di conservazione: strumento organizzativo che illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Manuale di gestione: strumento organizzativo che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Marca temporale: il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo.

Metadati: insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.

Pacchetto di archiviazione (AIP): pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le modalità riportate nel manuale di conservazione.

Pacchetto di versamento (SIP): pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.

Pacchetto informativo: contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.

Piano della sicurezza del sistema di gestione informatica dei documenti: documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il

Sistema di Gestione Informatica dei Documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza.

Piano di conservazione: strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione.

Piano generale della sicurezza: documento per la pianificazione delle attività volte alla protezione del sistema e di tutte le possibili azioni finalizzate alla gestione del rischio nell'ambito dell'organizzazione di appartenenza.

Processo di conservazione: insieme delle attività finalizzate alla conservazione dei documenti informatici.

Procedimento amministrativo: sequenza di atti e/o fatti tra loro connessi per la definizione di decisioni dell'Amministrazione, nel perseguimento di pubblici interessi, che ha come atto conclusivo la produzione di un atto amministrativo perfetto ed efficace.

Produttore: persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel

sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.

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.

Rapporto di versamento: documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

Registro di protocollo: registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti.

Registro particolare: registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5, del DPR 445/00.

Repertorio informatico: registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano atti e documenti o indici di atti e documenti secondo un criterio che ne garantisca l'identificazione univoca all'atto della immissione cronologica.

Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (RGD): dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del DPR 445/00, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

Responsabile della conservazione: soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione (DPCM 3/12/2013).

Responsabile del trattamento dei dati: la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Responsabile della sicurezza: soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.

Riferimento temporale: evidenza informatica, contenente la data e l'ora, con riferimento al Tempo Universale Coordinato (UTC), che viene associata ad uno o più documenti informatici.

Scarto: operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.

Segnatura di Protocollo: l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso.

Serie archivistica: aggregazione di unità archivistiche con caratteristiche omogenee in relazione alla natura o alla forma delle unità archivistiche medesime, ovvero in funzione dell'oggetto, della materia e delle funzioni del produttore.

Sistema di conservazione: sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice.

Sistema di Gestione Informatica dei Documenti (SGID): nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del DPR 445/00; per i privati è il sistema che consente la tenuta di un documento informatico.

Sistema pubblico di connettività (SPC): l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.

Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID): sistema costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente su richiesta degli interessati.

Staticità: caratteristica che garantisce l'assenza nel documento informatico di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione del documento medesimo.

Titolare: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica.

Titolario o sistema di classificazione: sistema precostituito di partizioni astratte che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.

Unità Organizzativa Responsabile (UOR): l'Unità Organizzativa Responsabile è un sottoinsieme di una AOO, cioè un complesso di risorse umane e strumentali cui è affidata una competenza omogenea.

Utente: persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

Validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

ELENCO ALLEGATI

ALLEGATO 1 - Descrizione AOO

ALLEGATO 2 - Piano di sicurezza

ALLEGATO 3 - Titolare unico di classificazione

ALLEGATO 4 – Modello di registro di protocollo di emergenza

Allegati al Manuale di Gestione
Del Protocollo Informatico

Comune di Verzegnis

Provincia di Udine



Approvato con delibera di Giunta Comunale n. 112 del 29-12-2025

ALLEGATO 1 – DESCRIZIONE AOO

SEZIONE AOO

Denominazione dell'Amministrazione	COMUNE DI VERZEGNIS
Codice identificativo assegnato all'Amministrazione (<i>Codice univoco AOO</i>)	AF9FD8E codice IPA: c_l801
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	Via Udine n. 2 - 33020 Verzegnis (UD)
Nominativo del Responsabile	Baschiera Andrea
Casella di posta elettronica istituzionale dell'AOO	comune.verzegnis@certgov.fvg.it
Data di istituzione della AOO	01/06/2010

SEZIONE UO – UFFICIO PROTOCOLLO

Denominazione dell'UO	UFFICIO PROTOCOLLO
Codice identificativo assegnato All'ufficio	codice univoco: 3DCGHH codice IPA: c_l801
Tipologia	Ufficio per l'erogazione di servizi
Indirizzo dell'UO	Via Udine n. 2 - 33020 Verzegnis (UD)
Nominativo del Responsabile	Scarparo Raffaella
Domicilio digitale	comune.verzegnis@certgov.fvg.it

ALLEGATO 2 – PIANO DI SICUREZZA

POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATICO

1.1 Premessa

1. L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.
2. L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

1.2 Scopo

1. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.
2. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.
3. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

1.3 Ambito di applicazione

1. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, società che prestano servizi specifici) includendo tutto il personale affiliato con terze parti.
2. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

1.4 Politiche – Uso generale e proprietà

1. Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.
2. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.
3. Le singole unità operative, sono responsabili della creazione di linee guida per l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare

il loro Dirigente.

4. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.
5. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

1.5 Politiche Sicurezza e proprietà dell'informazione

1. Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.
2. Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.
3. Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in *stand-by* con un comando specifico.
4. Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.
5. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.
6. Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "new group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.
7. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di competenza dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.
8. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.
9. Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

2 POLITICHE ANTIVIRUS

2.1 Premessa

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.

I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.

I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

2.2 Scopo

Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

2.3 Ambito di applicazione

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

2.4 Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile.
- Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile.
- Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
- Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
- Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
- Non scaricare mai messaggi da siti o sorgenti sospette.
- Evitare lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
- Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
- Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
- Evitare collegamenti diretti ad Internet via modem.
- Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in

condizione di protezione in scrittura.

- Se si utilizza una postazione di lavoro che necessita di un “bootstrap” da supporti di archiviazione rimovibili, usare questo protetto in scrittura.
- Non utilizzare i server di rete come stazioni di lavoro.
- Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.
- Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.

Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno.

- Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.
- Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.
- I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
- Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la “Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico... [omissis]...che prevede la reclusione sino a due anni e la multa sino a lire venti milioni”.
- Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
- È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

2.5 Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

- verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
- verificare se il virus ha diffuso dati;
- identificare il virus;
- attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;

- diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

3 POLITICHE USO NON ACCETTABILE

1. Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).
2. In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.
3. L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

3.1 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
2. Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
5. Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
6. Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
 - a. accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione;
 - b. attività di "sniffing";

- c. disturbo della trasmissione;
 - d. spoofing dei pacchetti;
 - e. negazione del servizio;
 - f. le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
 - g attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
 11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
 12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
 13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
 14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

3.2 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
3. Uso non autorizzato delle informazioni della testata delle e-mail,
4. Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
6. Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

4 LINEE TELEFONICHE COMMUTATE (ANALOGICHE E DIGITALI)

4.1 Scopo

1. Di seguito vengono illustrate le linee guida per un uso corretto delle linee telefoniche commutate (analogiche convenzionali) e digitali (ISDN, ADSL).
2. Queste politiche coprono due diversi usi distinti: linee dedicate esclusivamente ai telefax e linee di collegamento alle risorse elaborative dell'Amministrazione.

4.2 Ambito di applicazione

1. Queste politiche sono relative solo a quelle linee che sono terminate all'interno della/e sede/i dell'Amministrazione. Sono pertanto escluse le eventuali linee collegate con le abitazioni degli

impiegati che operano da casa e le linee usate per gestire situazioni di emergenza.

4.3 Politiche – Scenari di impatto sull'Amministrazione

1. Esistono due importanti scenari che caratterizzano un cattivo uso delle linee di comunicazione che tentiamo di tutelare attraverso queste politiche.
2. Il *primo* è quello di un attaccante esterno che chiama un gruppo di numeri telefonici nella speranza di accedere alle risorse elaborative che hanno un modem collegato. Se il modem è predisposto per la risposta automatica, allora ci sono buone probabilità di accesso illecito al sistema informativo attraverso un server non monitorato. In questo scenario, al minimo possono essere compromesse solo le informazioni contenute sul server.
3. Il *secondo* scenario è la minaccia di una persona esterna che può accedere fisicamente alle risorse dell'Amministrazione e utilizza illecitamente un PC da tavolo o portatile corredato di un modem connesso alla rete. In questo caso l'intruso potrebbe essere capace di connettersi, da un lato, alla rete sicura dell'Amministrazione attraverso la rete locale e, dall'altro, simultaneamente di collegarsi con il modem ad un sito esterno sconosciuto (ma precedentemente predisposto). Potenzialmente potrebbe essere possibile trafugare tutte le informazioni dell'Amministrazione, comprese quelle vitali.

4.4 Politiche – Telefax

1. Dovrebbero essere adottate le seguenti regole:
 - le linee fax dovrebbero essere approvate solo per uso istituzionale;
 - nessuna linea dei telefax dovrebbe essere usata per uso personale;
2. Le postazioni di lavoro che sono capaci di inviare e ricevere fax non devono essere utilizzate per svolgere questa funzione.
3. Eventuali deroghe a queste politiche possono essere valutate ed eventualmente concesse dal Responsabile della sicurezza caso per caso dopo una attenta valutazione delle necessità dell'Amministrazione rispetto ai livelli di sensibilità dei dati.

4.5 Politiche – Collegamento di PC alle linee telefoniche analogiche

1. La politica generale è quella di non approvare i collegamenti diretti dei PC alle linee telefoniche commutate.
2. Le linee commutate rappresentano una significativa minaccia per l'Amministrazione di attacchi esterni. Le eccezioni alle precedenti politiche dovrebbero essere valutate caso per caso dal responsabile della sicurezza.

4.6 Politiche – Richiesta di linee telefoniche analogiche

Una volta approvata la richiesta individuale di linea commutata dal responsabile dell'incaricato all'uso della linea medesima, questa deve essere corredata dalle seguenti informazioni da indirizzare al responsabile della sicurezza di rete:

- una chiara e dettagliata relazione che illustri la necessità di una linea commutata dedicata in alternativa alla disponibilità di rete sicura dell'Amministrazione;

- lo scopo istituzionale per cui si rende necessaria la linea commutata;
- il software e l'hardware che deve essere collegato alla linea e utilizzato dall'incaricato;
- che cosa la connessione esterna richiede per essere acceduta.

5 POLITICHE PER L'INOLTRO AUTOMATICO DI MESSAGGI DI POSTA ELETTRONICA

5.1 Scopo

1. Lo scopo di queste politiche è prevenire rivelazioni non autorizzate o involontarie di informazioni confidenziali o sensitive dell'Amministrazione

5.2 Ambito di applicazione

1. Queste politiche riguardano l'inoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

5.3 Politiche

1. Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio all'esterno dell'Amministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati all'esterno dell'Amministrazione.
2. Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario.

6 POLITICHE PER LE CONNESSIONI IN INGRESSO SU RETE

6.1 Scopo

1. Proteggere le informazioni elettroniche dell'Amministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dall'esterno su rete.

6.2 Ambito di applicazione

1. Lo scopo di queste politiche è definire adeguate modalità di accesso da remoto ed il loro uso da parte di personale autorizzato.

6.3 Politiche

1. È responsabilità del personale con i privilegi di accesso dall'esterno, alla rete dell'Amministrazione, garantire che personale non autorizzato non possa accedere illecitamente alla Intranet dell'Amministrazione ed alle sue informazioni. Tutto il personale che può accedere al sistema informativo dell'Amministrazione dall'esterno deve essere consapevole che tale accesso costituisce "realmente" una estensione del sistema informativo

che potenzialmente può trasferire informazioni sensitive.

2. Il personale e le persone terze devono, di conseguenza, porre in essere tutte le ragionevoli misure di sicurezza in loro possesso per proteggere il patrimonio informativo ed i beni dell'Amministrazione.
3. Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un reinstradamento della connessione.

7 POLITICHE PER L'USO DELLA POSTA ISTITUZIONALE DELL'AMMINISTRAZIONE

7.1 Scopo

1. Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.

7.2 Ambito di applicazione

1. La politica di seguito descritta intende illustrare l'uso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dell'Amministrazione stessa.

7.3 Politiche – Usi proibiti

1. Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

7.4 Politiche – Uso personale

1. È considerato accettabile l'uso personale della posta istituzionale dell'Amministrazione a condizione che:
 - i messaggi personali siano archiviati in cartelle separate da quelle di lavoro;
 - venga utilizzata una ragionevole quantità di risorse pubbliche;
 - non si avviino catene di lettere o messaggi scherzosi, di disturbo o di altro genere.
2. Il personale dell'Amministrazione, nel rispetto dei principi della privacy, non avrà controlli sui dati archiviati a titolo personale, ricevuti o trasmessi.
3. L'Amministrazione può però controllare senza preavviso i messaggi che transitano in rete per verificare il rispetto delle politiche concernenti gli "usi proibiti" di cui sopra.
4. Non è ammesso l'uso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

8.1 Scopo

1. Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura.
2. Solo i sistemi wireless che si adattano a queste politiche o hanno la garanzia di sicurezza certificata dal responsabile della sicurezza, possono essere utilizzati per realizzare i collegamenti all'Amministrazione.

8.2 Ambito di applicazione

1. La politica riguarda tutti i dispositivi di comunicazione dati senza fili collegati (PC e cellulari telefonici) alla Intranet dell'Amministrazione, ovvero qualunque dispositivo di comunicazione wireless capace di trasmettere "pacchetti" di dati.
2. Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

8.3 Politiche – Registrazione delle schede di accesso

1. Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
2. Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing). Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate.

8.4 Politiche – Approvazione delle tecnologie

1. Tutti i dispositivi di accesso alle LAN dell'Amministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.

ALLEGATO 3 – TITOLARIO UNICO DI CLASSIFICAZIONE

1 AMMINISTRAZIONE GENERALE

- 1 1 legislazione e circolari esplicative
- 1 2 denominazione, territorio e confini, toponomastica
- 1 3 statuto
- 1 4 regolamenti
- 1 5 patrocini, stemma, gonfalone
- 1 6 archivio generale
- 1 7 sistema informativo comunale
- 1 8 informazioni e relazioni con il pubblico
- 1 9 politica del personale, ordinamento uffici e servizi
- 1 10 organizzazioni sindacali
- 1 11 controlli esterni
- 1 12 editoria e attività informativo-promozionale
- 1 13 cerimonie, attività di rappresentanza, onorificenze
- 1 14 gemellaggi, interventi umanitari, rapporti istituzionali
- 1 15 forme associative e adesione ad associazioni
- 1 16 associazionismo e partecipazione organi e organismi

2 ORGANI DI GOVERNO

- 2 1 segretario e vice segretario
- 2 2 sindaco
- 2 3 giunta
- 2 4 consiglio comunale
- 2 5 conferenza capigruppo e commissioni consiliari
- 2 6 commissario straordinario
- 2 7 revisori dei conti
- 2 8 organi di controllo interni
- 2 9 consulte frazionali

3 RISORSE UMANE

- 3 1 selezione concorsi
- 3 2 assunzioni e cessazioni
- 3 3 formazione
- 3 4 tutela della salute e sicurezza sul luogo di lavoro
- 3 5 orario di lavoro, presenze e assenze
- 3 6 procedimenti disciplinari
- 3 7 fascicoli del personale finanza e patrimonio

4 RISORSE FINANZIARIE E PATRIMONIALI

- 4 1 bilancio preventivo e piano esecutivo di gestione
- 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 pubblicit  e pubbliche affissioni

5 AFFARI LEGALI

- 5 1 contenzioso
- 5 2 responsabilit  civile e patrimoniale verso terzi e assicurazioni
- 5 3 pareri e consulenze

6 PIANIFICAZIONE E GESTIONE DEL TERRITORIO, LAVORI PUBBLICI

- 6 1 urbanistica
- 6 2 edilizia privata
- 6 3 ambiente
- 6 4 opere pubbliche
- 6 5 protezione civile ed emergenze
- 6 6 catasto
- 6 7 servizio idrico integrato, luce, gas, rifiuti

7 SERVIZI ALLA PERSONA

- 7 1 diritto allo studio e servizi
- 7 2 asili nido e scuola dell'infanzia
- 7 3 promozione e sostegno delle istituzioni di istruzione
- 7 4 istituti culturali (musei, biblioteche, teatri)
- 7 5 attivita' ed eventi culturali
- 7 6 attivita' ed eventi sportivi
- 7 7 pianificazione e accordi strategici con enti e privati e con il volontariato sociale
- 7 8 tutela e curatela di incapaci
- 7 9 assistenza diretta e indiretta, benefici economici
- 7 10 attivita' ricreative e di socializzazione
- 7 11 politiche per la casa
- 7 12 politiche per il sociale

8 ATTIVITA' ECONOMICHE

- 8 1 agricoltura e pesca
- 8 2 artigianato
- 8 3 industria
- 8 4 commercio e suap
- 8 5 fiere e mercati
- 8 6 esercizi turistici e strutture ricettive
- 8 7 promozione e servizi

9 POLIZIA LOCALE E SICUREZZA PUBBLICA

9 1 sicurezza ed ordine pubblico

10 TUTELA DELLA SALUTE

10 1 salute e igiene pubblica

10 2 trattamento sanitario obbligatorio

10 3 zooprofilassi veterinaria

10 4 randagismo animale e ricoveri

11 SERVIZI DEMOGRAFICI

11 1 stato civile

11 2 anagrafe

11 3 censimenti

11 4 polizia mortuaria e cimiteri

12 ELEZIONI E INIZIATIVE POPOLARI

12 1 liste elettorali

12 2 elezioni

12 3 albi elettorali

12 4 referendum

13 LEVA MILITARE

13 1 leva e servizi militari

13 2 ruoli matricolari

14 OGGETTI DIVERSI

14 1 oggetti diversi

ALLEGATO 4



Comune di Verzegnis

Provincia di Udine

Sede municipale: via Udine n. 2 - 33020 VERZEGNIS
P.I. 00505890301 - C.F. 84001410301
tel. 0433 2713

MODELLO DI REGISTRO DI PROTOCOLLO DI EMERGENZA

A. Schema di provvedimento di autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza.

N°	data	Tipo (in uscita, in entrata, interno)	Mittente/destinatario	Oggetto	Classificazione	N. allegati	Mezzo di trasmissione	note
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								

B. Schema di provvedimento di autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza.

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445, preso atto che, per le cause sotto riportate:

- Data interruzione: *[campo da compilare]*
- Ora interruzione: *[campo da compilare]*
- Causa della interruzione: *[campo da compilare]*

non è possibile utilizzare la normale procedura informatica, si autorizza lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza.

Il Responsabile della gestione documentale

[firma autografa del responsabile]

C. Schema di provvedimento di revoca allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza.

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445, considerato che, per le cause sotto riportate:

- Data interruzione: *[campo da compilare]*
- Ora interruzione: *[campo da compilare]*
- Causa della interruzione: *[campo da compilare]*

non è stato possibile utilizzare la normale procedura informatica e, dunque, è stato autorizzato lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;

preso atto che dalla data sotto riportata:

- Data ripristino: *[campo da compilare]*
- Ora ripristino: *[campo da compilare]*

è stato ripristinato il normale funzionamento della procedura informatica, si revoca l'autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza e si dispone il tempestivo inserimento delle informazioni relative ai documenti protocollati in emergenza nel sistema informatico, con automatica attribuzione della numerazione di protocollo ordinaria, mantenendo la correlazione con la numerazione utilizzata in emergenza.

Il Responsabile della gestione documentale

[firma autografa del responsabile]