

Allegato 4

Piano di sicurezza dei documenti informatici

Aspetti fondamentali della sicurezza

Sommario

Allegato 4.....	1
Piano di sicurezza dei documenti informatici Aspetti fondamentali della sicurezza.....	1
1. Protezione fisica delle risorse.....	3
1.1. Premessa.....	3
2. Protezione logica delle informazioni.....	3
3. Norme per il personale.....	4
3.1. Politiche accettabili di uso del sistema informativo.....	4
3.1.1. Premessa.....	4
3.1.2. Scopo.....	5
3.1.3. Ambito di applicazione.....	5
3.1.4. Politiche – Uso generale e proprietà.....	5
3.1.5. Politiche - Sicurezza e proprietà dell'informazione.....	5
3.2. Politiche, antivirus.....	6
3.2.1. Scopo.....	7
3.2.2. Ambito di applicazione.....	7
3.2.3. Politiche per le azioni preventive.....	7
3.2.4. Politiche per le azioni consuntive.....	8
3.3. Politiche, uso non accettabile del sistema informativo.....	8
3.3.1. Attività di rete e di sistema.....	8
3.3.2. Attività di messaggistica e comunicazione.....	10
3.4. Politiche per l'inoltro automatico di messaggi di posta elettronica.....	10
3.4.1. Premessa.....	10
3.4.2. Scopo.....	10
3.4.3. Ambito di applicazione.....	10
3.4.4. Politiche.....	10
3.5. Politiche per le connessioni in ingresso su rete internet.....	11
3.5.1. Scopo.....	11
3.5.2. Ambito di applicazione.....	11
3.5.3. Politiche.....	11
3.6. Politiche per l'uso della posta istituzionale dell'amministrazione.....	11
3.6.1. Scopo.....	11
3.6.2. Ambito di applicazione.....	11
3.6.3. Politiche – Usi proibiti.....	11
3.6.4. Politiche – Uso personale.....	12
3.7. Politiche per le comunicazioni wireless.....	12
3.7.1. Scopo.....	12

3.7.2.	Ambito di applicazione	12
3.7.3.	Politiche	12
3.8.	Accessibilità dei documenti	12
4.	Aspetti di sicurezza informatica per la formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici	13
4.1.	Formazione dei documenti.....	13
4.2.	Gestione dei documenti e tracciabilità	14
4.3.	Trasmissione e interscambio dei documenti informatici	15
4.3.1.	Scambio dei documenti all'esterno dell'amministrazione (interoperabilità dei sistemi di protocollo informatico)	15
4.3.2.	Scambio dei documenti all'interno dell'amministrazione.....	16
4.4.	Accesso ai documenti informatici	16
4.5.	Accesso al registro di protocollo per utenti interni all'amministrazione	16
4.6.	Conservazione dei documenti informatici	17

1. Protezione fisica delle risorse

1.1. Premessa

L'obiettivo della protezione fisica delle risorse è quello di proteggere le aree e le componenti del sistema informativo.

Il piano è redatto in conformità al Regolamento UE 2016/679 (GDPR) e alle "Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici" (maggio 2021) e la Circolare AgID n. 2/2017 sulle misure minime di sicurezza ICT.

Generalmente le contromisure di sicurezza fisica possono essere ricondotte a sicurezza dell'area e sicurezza delle apparecchiature.

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi informatici. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle sale computer rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

La sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione e di condizionamento. Anche la manutenzione dell'hardware rientra in questa area, come anche la protezione da manomissione o furti.

Le contromisure adottate sono le seguenti:

- I locali dove trovano alloggio i server sono chiusi a chiave, dotati di impianto di condizionamento e dispositivo di accesso con badge.
- Le chiavi di accesso ai locali sono distribuite ai soli dipendenti dell'ufficio Sistemi Informativi gli accessi con badge sono stati assegnati ai soli dipendenti dell'ufficio Sistemi Informativi ed ai servizi di pulizia e ufficio demografici.
- Le apparecchiature sono altresì protette da sbalzi di tensione elettrica tramite UPS.

Per le definizioni tecniche e i termini utilizzati si rimanda all'Allegato 01 – Definizioni.

2. Protezione logica delle informazioni

In Gli obiettivi della protezione logica delle informazioni sono:

- il controllo degli accessi alle informazioni
- il mantenimento della loro integrità e riservatezza
- la sicurezza nella trasmissione e nelle comunicazioni all'interno dell'Amministrazione e con l'esterno (Internet, altre Amministrazioni etc.)
- la sicurezza delle stazioni di lavoro e dei personal computer
- la tempestiva rilevazione di eventuali incidenti di sicurezza.

Il campo di applicazione della Sicurezza Logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.

Le contromisure adottate sono le seguenti:

- Sistema operativo del PdP utilizzato dall'amministrazione, conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi);
- uso di sistemi RAID (si tratta di hard disk multipli visti però dal sistema operativo come un singolo disco. La principale proprietà di questi dispositivi è quella di garantire la disponibilità e l'integrità dei dati anche nel caso di guasto hardware di uno dei dischi;
- protezione dei sistemi di accesso e conservazione delle informazioni con assegnazione ad ogni utente del sistema di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno semestrale durante la fase di esercizio;
- sistemi di backup giornalieri;
- conservazione, a cura dell'ufficio Sistemi Informativi delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- firewall perimetrale che protegge la LAN da intrusioni esterne e web/mail server collocato in DMZ per non compromettere la sicurezza della LAN;
- server accessibili dall'esterno solo tramite vpn o tramite attivazione all'interno della LAN di software per il controllo remoto;
- software anti-virus, con gestione centralizzata, su ogni PC e server;
- manutenzione dei gestionali in uso e gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo costituito dal personale in dotazione all'ufficio Sistemi Informatici;
- Piano di Continuità Operativa necessario a garantire la continuità del servizio informatico e la disponibilità delle informazioni (aggiornate), evitando o limitando i danni al patrimonio informativo a fronte di una emergenza. Il sistema informativo deve essere ripristinato entro sette giorni coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti

3. Norme per il personale

3.1. Politiche accettabili di uso del sistema informativo

3.1.1. Premessa

E' necessario stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale.

Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di

memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc.

Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.

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.

3.1.2. Scopo

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

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

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

3.1.3. Ambito di applicazione

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

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

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

3.1.4. Politiche – Uso generale e proprietà

- Gli utenti del sistema informativo devono essere informati che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.
- Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.
- Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.

3.1.5. Politiche - Sicurezza e proprietà dell'informazione

- Il personale dell'Amministrazione deve porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.
- Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password devono essere cambiate con il primo accesso al sistema informativo e 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.
- Tutte le postazioni di lavoro (PC da tavolo e portatili) devono essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico.
- Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi devono essere esercitate particolari attenzioni.
- Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "news group" che utilizzano il sistema di posta elettronica dell'Amministrazione devono 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.
- Il personale deve considerare lo spazio virtuale dei social network come spazio pubblico. È vietato divulgare attraverso account privati informazioni riservate, corrispondenza interna o documenti di cui si è a conoscenza per ragioni d'ufficio. L'uso dei loghi dell'ente su profili personali non è consentito.
- Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.
- È essenziale che il personale utilizzi la massima attenzione nella gestione degli allegati a email provenienti da fonti sconosciute, poiché potrebbero contenere virus, malware e cavalli di Troia.
- Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla propria postazione di lavoro o con le proprie credenziali.

3.2. Politiche, antivirus

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.

3.2.1. 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.

3.2.2. 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.

3.2.3. Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornato.
- Su ciascuna postazione deve essere sempre attiva la versione dell'antivirus corrente e aggiornata con la più recente versione.
- Non aprire mai file o macro ricevuti con messaggi da 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.
- Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione 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.
- 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.

3.2.4. 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.

3.3. Politiche, uso non accettabile del sistema informativo

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).

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

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.

3.3.1. Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione:

- Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
- Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
- È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
- Introduzione di programmi non autorizzati nella rete o nei sistemi dell'Amministrazione.
- Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
- Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
- Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
- Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
- Realizzare 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.
- Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
- Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
- Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.

- Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
- Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

3.3.2. Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione:

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

3.4. Politiche per l'inoltro automatico di messaggi di posta elettronica

3.4.1. Premessa

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

3.4.2. Scopo

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

3.4.3. Ambito di applicazione

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.

3.4.4. Politiche

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.

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.

3.5. Politiche per le connessioni in ingresso su rete internet

3.5.1. Scopo

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

3.5.2. Ambito di applicazione

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

3.5.3. Politiche

Il personale dell'Amministrazione e le persone terze autorizzate come indicato nell'allegato 5-01 (disciplinare sulle politiche di sicurezza informatica del Comune di Borgomanero) possono utilizzare la linea internet per guadagnare l'ingresso alla Intranet dell'Amministrazione. L'accesso alla rete comunale da remoto è consentito esclusivamente tramite VPN o portale specifico, utilizzando sistemi di autenticazione forte (es. One Time Password). È vietato l'utilizzo di dispositivi personali e la memorizzazione automatica delle credenziali su postazioni non fornite dall'Ente.

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. 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.

3.6. Politiche per l'uso della posta istituzionale dell'amministrazione

3.6.1. Scopo

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.

3.6.2. Ambito di applicazione

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.

3.6.3. Politiche – Usi proibiti

Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di messaggi distruttivi od offensivi, includendo come offensivi i commenti su razza, genere, caratteristiche fisiche, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. I dipendenti che ricevono messaggi con questi contenuti da colleghi devono riportare questi eventi ai diretti superiori immediatamente.

3.6.4. Politiche – Uso personale

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.

3.7. Politiche per le comunicazioni wireless

3.7.1. Scopo

Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura.

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.

3.7.2. Ambito di applicazione

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.

Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

3.7.3. Politiche

Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.

Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing).

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

3.8. Accessibilità dei documenti

In conformità alla Legge 4/2004, al D.Lgs. 106/2018 e alla Circolare AgID n. 1/2016, l'Amministrazione garantisce che ogni atto, modulo o provvedimento sia fruibile indipendentemente da eventuali disabilità personali. Il personale incaricato è tenuto ad attenersi alle seguenti istruzioni sin dalla fase di redazione:

- **Divieto di "Documenti-Immagine":** È vietata la pubblicazione di scansioni digitali di documenti cartacei (scansioni semplici) prive di testo digitale decodificabile, in quanto non leggibili dalle tecnologie assistite.
- **Utilizzo dei Font Istituzionali:** Per tutti gli atti ufficiali (lettere, delibere, ordinanze) deve essere utilizzato esclusivamente il font "Liberation Sans" o "Arial". La dimensione del carattere per il corpo del testo non deve essere inferiore a 12pt.
- **Intestazioni e Loghi:** Ogni documento deve recare esclusivamente i logotipi previsti dal "Manuale d'uso del logo comunale". Per le lettere in uscita, deve essere utilizzato il file specifico.

- **Struttura dei Contenuti:** I documenti devono essere organizzati gerarchicamente utilizzando gli Stili dell'editor di testo (Titolo 1, Titolo 2, Corpo del testo). Questo permette ai lettori di schermo di generare automaticamente indici e segnalibri per la navigazione.
- **Alternative Testuali:** Ogni elemento grafico (immagini, stemmi, grafici) deve essere accompagnato da una descrizione testuale alternativa che ne spieghi il contenuto.
- **Linguaggio e Formattazione:**
 - Utilizzare un linguaggio semplice ed evitare abbreviazioni inusuali o termini tecnici non spiegati.
 - Garantire un contrasto cromatico elevato (testo nero su sfondo bianco).
 - Preferire l'allineamento a sinistra ed evitare il testo giustificato o sottolineato, per non affaticare la vista e non confondere il testo con i link ipertestuali.
- **Conversione in PDF Accessibile:** Il salvataggio finale deve avvenire nel formato PDF/A, assicurandosi di attivare nelle opzioni dell'editor le caselle "Crea segnalibri utilizzando: Intestazioni" e "Tag per la struttura del documento per l'accessibilità".

4. Aspetti di sicurezza informatica per la formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici

4.1. Formazione dei documenti

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

Si adottano preferibilmente i formati PDF/A (nelle versioni 1.4 o superiori), XML e TIFF. I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF/A, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

L'amministrazione adotta come standard i formati previsti dall'Allegato 2 delle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" emanate dall'AgID.

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

Per attribuire una data certa a un documento informatico prodotto all'interno dell'AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 novembre 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 ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.).

L'amministrazione effettua con cadenza almeno annuale una valutazione dell'interoperabilità dei formati utilizzati per mitigare il rischio di obsolescenza tecnologica. Tale attività di censimento e analisi è finalizzata a individuare tempestivamente formati in via di obsolescenza o che comportino rischi di vendor lock-in.

4.2. Gestione dei documenti e tracciabilità

Il sistema di protocollo informatico assicura:

- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Il sistema di protocollo informatico consente:

- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
- il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul PI - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (firewall);
- dalle registrazioni del PI.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RGD e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

Storicizzazione delle Rettifiche e Annullamenti: In conformità al paragrafo 3.1.5 delle Linee Guida AgID, il sistema di protocollo informatico deve garantire la storicizzazione di ogni operazione di annullamento o rettifica. Qualora sia necessario correggere errori materiali nei campi definiti immutabili (mittente, destinatario, oggetto), la procedura deve assicurare che il valore originario e quello rettificato restino entrambi memorizzati, visibili e comparabili all'interno del sistema. Ogni evento di modifica deve essere associato in modo permanente all'identificativo dell'operatore, alla data e all'ora dell'intervento.

4.3. Trasmissione e interscambio dei documenti informatici

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

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

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

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

4.3.1. Scambio dei documenti all'esterno dell'amministrazione (interoperabilità dei sistemi di protocollo informatico)

Per **interoperabilità** dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni.

Ogni messaggio protocollato deve riportare alcune informazioni archivistiche fondamentali, per facilitare il trattamento dei documenti da parte del ricevente. Tali informazioni sono incluse nella segnatura informatica di ciascun messaggio protocollato e sono codificate in formato XML.

Con provvedimento dell'Agenzia per l'Italia Digitale, vengono indicati le modalità di trasmissione dei documenti informatici, il tipo ed il formato delle informazioni archivistiche di protocollo minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai messaggi protocollati.

4.3.2. Scambio dei documenti all'interno dell'amministrazione

Le Unità Organizzative (UO) si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente l'impiego della posta elettronica nelle pubbliche amministrazioni.

4.4. Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale. Il PI adottato dall'amministrazione:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

4.5. Accesso al registro di protocollo per utenti interni all'amministrazione

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

Ciascun utente del PI può accedere solamente ai documenti che sono stati assegnati alla sua UO.

Un utente può avere la visibilità completa sul registro di protocollo solo a seguito di abilitazione.

Il personale dell'ufficio protocollo generale e dell'ufficio sistemi informatici sono abilitati alla visualizzazione completa sul registro protocollo.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. Nel caso in cui sia effettuata la registrazione di un documento riservato, la visibilità completa sul documento stesso è possibile solo alla persona destinataria del documento.

Di norma tutti gli utenti che devono protocollare sono abilitati alla consultazione, inserimento e modifica, ma è possibile abilitare un utente anche alla sola consultazione.

Solo il personale dell'ufficio Sistemi Informatici è invece abilitato all'annullamento.

4.6. Conservazione dei documenti informatici

Per la conservazione dei documenti informatici si applicano le 'Linee Guida sulla formazione, gestione e conservazione dei documenti informatici' emanate dall'AgID (maggio 2021) e i relativi allegati tecnici. Il sistema di conservazione garantisce nel tempo le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici e delle aggregazioni documentali.

Ai sensi dell'art. 44 del Codice, la conservazione può essere svolta all'interno della struttura organizzativa del soggetto produttore dei documenti o affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

L'amministrazione è da tempo impegnata nella progressiva digitalizzazione dei documenti e intende organizzare in modo efficace e a lungo termine la loro conservazione, ma ritiene non economico dotarsi autonomamente delle complesse strutture per una conservazione a lungo termine dei documenti informatici.

L'Amministrazione affida la conservazione digitale in modalità outsourcing a conservatori esterni che offrono idonee garanzie organizzative e tecnologiche. Nello specifico:

- Per il flusso documentale generale e l'archivio del protocollo informatico: Regione Emilia-Romagna tramite il servizio ParER (Polo Archivistico Regionale).
- Per gli ordinativi finanziari (mandati e reversali): intermediario NV Group (Nexi Payments S.p.A. - piattaforma E-DK)."

Tali soggetti sono in grado di fornire idonee garanzie di sicurezza ed efficacia e dispone della strumentazione tecnica necessaria e di personale adeguato allo scopo.

Per le modalità operative di trasmissione del contenuto del pacchetto di versamento al sistema di conservazione si rimanda al manuale di conservazione.

Il manuale di conservazione inoltre 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.

Il Registro giornaliero di protocollo deve essere trasmesso al sistema di conservazione entro la giornata lavorativa successiva alla sua chiusura, per garantirne l'immodificabilità del contenuto e la validità legale nel tempo

Ruoli:

- **Responsabilità:** Il processo è coordinato dal Responsabile della conservazione del Comune, che opera d'intesa con il Responsabile della transizione digitale e il Responsabile della protezione dei dati personali.
- **Procedure Operative:** Per la descrizione analitica delle infrastrutture, delle misure di sicurezza fisica dei server e dei processi di generazione dei pacchetti di archiviazione (AIP), si rimanda esplicitamente ai Manuali di Conservazione dei conservatori esterni

(ParER e Nexi Payments), che formano parte integrante della documentazione di sicurezza dell'ente.

- **Gestione dei Formati:** Il trasferimento al sistema di conservazione avviene esclusivamente per i formati classificati dal Conservatore come Idonei o Gestiti (es. PDF/A, XML, TIFF), monitorando costantemente il rischio di obsolescenza tecnologica.