CITTÀ DI PORTO TORRES

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Piano di Sicurezza dei Documenti Informatici

Comune di Porto Torres

CITTÀ DI PORTO TORRES

Indice generale

CITTÀ DI PORTO TORRES

Introduzione

Le Pubbliche Amministrazioni, ai sensi dell'art. 4, comma 1, lett. c del DPCM 3 dicembre 2013, nell'ottica di sviluppare concretamente il Sistema di gestione informatica dei documenti, devono predisporre:
Il Piano per la sicurezza informatica relativo alla formazione, gestione, trasmissione, interscambio, ‟ accesso e conservazione dei documenti informatici, nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del D.Lgs. 196/2003 «Codice della Privacy»″.
Il suddetto Piano deve essere predisposto dal Responsabile della gestione documentale, d'intesa con il Responsabile della conservazione, il Responsabile dei sistemi informativi e il Responsabile del trattamento dei dati personali.

La sicurezza di un sistema informativo è da intendersi come:

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

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

Gli aspetti principali:

- L'analisi dei rischi, cioè la valutazione dello stato attuale della sicurezza del sistema informativo, al fine di individuare le vulnerabilità del sistema, stimare l'esposizione al rischio e individuare le possibili misure di protezione.
- Le politiche di sicurezza, che specificano gli obiettivi, individuano le responsabilità e dichiarano l'impegno dell'Ente relativamente alla messa in sicurezza del sistema informativo.
- La gestione del rischio, cioè la ricerca dell'equilibrio tra i costi dei controlli individuati e il valore dei beni da proteggere (analisi costi/benefici), al fine di determinare il giusto livello di sicurezza da perseguire.

Normativa di riferimento

La fonte normativa di riferimento è il D.P.C.M. 3-12-2013. "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" che all'Articolo 4 definisce nel seguente modo i compiti del Responsabile della gestione documentale e i contenuti del piano di sicurezza per i documenti informatici:

“Art. 4. Compiti del responsabile della gestione documentale”

1. In attuazione dell'art. 61 del testo unico, le pubbliche amministrazioni di cui all'art. 2, comma 2, del Codice definiscono le attribuzioni del responsabile della gestione documentale ovvero, ove nominato, del coordinatore della gestione documentale. In particolare, al responsabile della gestione è assegnato il compito di:
    a. predisporre lo schema del manuale di gestione di cui all'art. 5;
    b. proporre i tempi, le modalità e le misure organizzative e tecniche di cui all'art. 3, comma 1, lettera e);
    c. predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi o, nel caso delle pubbliche amministrazioni centrali, il responsabile dell'ufficio di cui all'art. 17 del Codice e con il responsabile del trattamento dei dati personali di cui al suddetto decreto.
2. Il coordinatore della gestione documentale definisce e assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna tra le aree organizzative omogenee, ai sensi dell'art. 50 , comma 4, del testo unico.”

Architettura delle Infrastrutture e gestione della Sicurezza

Sicurezza della rete di accesso al servizio

Misure adottate per la protezione della rete Comune di Porto Torres

La rete comunale

Le principali sedi e uffici del Comune sono collegate tra loro tramite fibra ottica secondo uno schema logico ad anello e costituiscono una MAN.

All'interno della MAN sono presenti due datacenter: uno principale presso la sede di Via Ponte Romano e uno secondario nel sito di disaster recovery presso la sede di Viale delle Vigne.

La MAN si interfaccia alla rete Internet tramite una connessione in fibra ottica di tipo FTTH da 100mbps.

E' presente un firewall che agisce come sistema di sicurezza perimetrale relativo alla messa in sicurezza delle comunicazioni Untrusted che avvengono tra l'esterno della rete (tipicamente Internet/Extranet) ed il resto dell'infrastruttura.

Fornisce inoltre un sistema di autenticazione per l'accesso ai servizi della rete comunale dall'esterno, tramite tunnel VPN.

E' presente un sistema di autenticazione basato su Active Directory per l'autenticazione degli utenti alle postazioni di lavoro interne alla rete e per la gestione dei permessi e degli accessi alle risorse condivise.

E' presente un sistema Antivirus gestito in maniera centralizzata per la protezione dei terminali e dei server Windows connessi alla rete.

WIFI cittadina

Presso la Piazza Umberto I e presso il Parco di S. Gavino è presente una connessione Wi-fi alla quale possono avere libero accesso tutti coloro che hanno richiesto apposite credenziali secondo quanto disposto dall'art. 7 D.L. 27 luglio 2005, n. 144 (c.d. decreto Pisanu) convertito con Legge n. 155 del 31 luglio 2005.
Anche presso il Parco di Balai, è presente una connessione Wi-fi alla quale possono avere libero accesso tutti coloro che sono in prossimità, la navigazione è controllata e limitata a tutti i siti istituzionali ad eccezione esclusivamente di alcuni social, quali ad esempio facebook ed instagram.

Gestione utenti e Credenziali di accesso

Il rilascio delle credenziali è gestito dagli operatori del Servizio Sistemi informativi e innovazione tecnologica su richiesta del Dirigente in ragione dell'immissione in servizio di un dipendente o di un collaboratore esterno. Le credenziali d'accesso sono nominative e strettamente personali e sono valide per l'accesso alle risorse e ai vari servizi della rete comunale, compresi gli applicativi gestionali.

La password di accesso rispondono ai requisiti di complessità e di sicurezza imposta

dalle normative vigenti.

L'accesso al computer, alle risorse di rete e agli applicativi gestionali è quindi autorizzato solo per i soggetti che superano un processo di autenticazione e riconoscimento dell'utente, da cui ne consegue il riconoscimento dell'identità dell'utilizzatore dichiarata.

Disaster Recovery, copie di sicurezza e backup

Per prevenire il rischio di perdita dei dati e di potenziale indisponibilità degli applicativi gestionali sono attivi diversi sistemi tra i quali abbiamo backup periodici e replica delle macchine virtuali server. Abbiamo inoltre ridondanza di server per l'esecuzione di macchine virtuali in caso di eventi disastrosi e calamitosi.

Le copie vengono archiviate in appositi dispositivi, situati in entrambi i datacenter.

Protezione dei dati

Protezione da virus e malware e controllo delle intrusioni

Il rischio di intrusione o di accesso indesiderato dall'esterno è garantito da un firewall che, come già detto, governa e controlla gli accessi ed impedisce anche l'accesso dall'esterno. Il firewall ha attivo un sistema di Intrusion prevention system (IPS) con politiche che permettono di prevenire e bloccare attacchi interni o esterni. Queste politiche vengono aggiornate automaticamente in modo che tengano conto delle ultime vulnerabilità rese note.
All'interno della rete, sia a protezione dei server che delle postazioni utente interne (che possono essere a loro volta un mezzo anche inconsapevole di intrusione), sono attivi due antivirus di tecnologie diverse e l'antispam. L'uso di tecnologie diverse e/o produttori diversi aumenta il grado di protezione poiché una minaccia può essere intercettata di un sistema ma non da un altro.

Software di protocollazione e conservazione

Il sistema di Conservazione consente di gestire in sicurezza e nel rispetto della normativa vigente l'intero processo di conservazione digitale di documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini delle disposizioni tributarie.
Come definito dall'art. 44 del CAD, infatti, il sistema di conservazione dei documenti informatici assicura:

- l'identificazione certa del soggetto che ha prodotto il documento (autenticità),
- l'integrità del documento (immodificabilità),
- la leggibilità e l'agevole reperibilità di documenti e relative informazioni identificative,
- il rispetto delle misure di sicurezza.

Con la conservazione digitale a norma dei documenti, nel Comune di Porto Torres si ha una gestione basata sul documento informatico di cui ne viene mantenuta la validità legale nel tempo, garantendone l'integrità e l'autenticità.

Accesso al Sistema di Gestione Informatica dei Documenti e ai documenti e dati in esso contenuti da parte di utenti interni all'AOO

L'accesso al Sistema di Gestione Informatica dei Documenti, da parte degli utenti interni all'AOO, avviene attraverso l'utilizzo di credenziali di autenticazione.
L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi ed alla struttura organizzativa.
Le credenziali di autenticazione consistono in un codice (User-Id), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (Password), conosciuta solamente dal medesimo; tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione/autenticazione, il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente, memorizzando, ai fini di controllo, l'User-Id corrispondente, ma non la Password dello stesso.
Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della Password; quest'ultima è composta da almeno otto caratteri, tra cui almeno un numero e un carattere speciale . La Password deve essere modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza trimestrale.
L'User-Id non può essere assegnato a nessun altro incaricato per nessuna motivazione. Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità (intesa come efficacia sulla sicurezza) che consente all'incaricato l'accesso ai dati personali.
Il Responsabile della sicurezza informatica del Comune di Porto Torres non è in grado di conoscere la Password dell'utente; qualora l'utente medesimo dimenticasse la propria Password si procederà all'assegnazione di una nuova chiave di accesso.

Accesso al trattamento di dati personali sensibili o giudiziari e politiche di sicurezza espressamente previste

L’accesso ai documenti contenenti dati personali, sensibili o giudiziari e ai dati medesimi avviene per mezzo dell’individuazione di specifici profili di autorizzazione, stabiliti sulla base del livello di riservatezza di ciascun documento, fascicolo, sottofascicolo o inserto, secondo quanto stabilito nel Manuale di Gestione;
tali profili, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all’inizio del trattamento.
Periodicamente, e comunque con cadenza almeno annuale, deve essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Gli incaricati del trattamento di dati personali, sensibili o giudiziari non devono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento degli stessi.

Gestione di credenziali di accesso a servizi esterni

L’accesso a servizi esterni all’ente possono, in rari casi, essere gestiti con credenziali che vengono fornite da enti o servizi esterni.
Queste credenziali di autenticazione devono essere consegnate in busta chiusa e sigillata al Responsabile del Settore/Area di riferimento; in caso di prolungata assenza o impedimento del soggetto incaricato, qualora si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Responsabile di settore è autorizzato ad utilizzare le credenziali contenute nella suddetta busta per procedere al trattamento, comunicandolo al titolare.
Il soggetto titolare delle credenziali provvederà, al momento del proprio rientro in servizio, alla sostituzione della Password, provvedendo all’inserimento della stessa in altra busta sigillata da riconsegnare al suddetto Responsabile.
Questo per garantire che l’accesso ai servizi sia sempre possibile da parte del Responsabile del Servizio anche in caso di assenza prolungata o impedimento del soggetto incaricato.

Trattamento dei dati personali, sensibili o giudiziari senza l’ausilio di strumenti elettronici

Ai fini del trattamento dei dati personali, sensibili o giudiziari, devono essere impartite agli incaricati istruzioni scritte da parte del Responsabile per il trattamento dei dati personali, relative alle modalità delle operazioni, del controllo e della custodia di atti e documenti.

Analogamente al trattamento dei medesimi dati svolto per mezzo di strumenti elettronici, sarà verificato il sussistere delle condizioni per l’accesso e il trattamento dei suddetti dati, da parte di ciascun utente o gruppo di utenti, con cadenza almeno annuale.

I suddetti documenti, sono controllati e custoditi dagli incaricati del trattamento per tutto il tempo di svolgimento dei relativi compiti, trascorso il quale provvederanno alla restituzione; nell'arco di tale periodo gli incaricati medesimi si assicureranno che a tali documenti non accedano persone prive di autorizzazione.
L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solo previa autorizzazione; le persone ammesse sono identificate e registrate.

Formazione dei documenti

I documenti dell'AOO sono prodotti utilizzando i formati previsti dal DPCM 3/12/2013 e dal presente Manuale.
L'apposizione della firma digitale, volta a garantire l'attribuzione certa della titolarità del documento e la sua integrità, avviene previa conversione in un formato, tra quelli previsti dal suddetto DPCM, che garantisca la leggibilità, l'interscambiabilità, la non alterabilità, l'immutabilità nel tempo del contenuto e della struttura del documento medesimo (ad esempio il formato PDF/A); l'acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati avente le medesime caratteristiche.
L'apposizione delle varie tipologie di sottoscrizioni elettroniche, l'apposizione della firma digitale, nonché la validazione temporale del documento sottoscritto digitalmente deve avvenire in conformità a quanto sancito dalle regole tecniche contenute nel DPCM 22/02/2013, emanate ai sensi dell'art. 71 del D. Lgs. 82/05.
L'eventuale sottoscrizione del documento con firma digitale deve avvenire prima dell'effettuazione della registrazione di protocollo.

Sicurezza delle registrazioni di protocollo

L'accesso al registro di protocollo al fine di effettuare le registrazioni o di apportare modifiche (nessuno può apportare modifiche se non il responsabile) è consentito soltanto al personale abilitato alla protocollazione (vedi Manuale di Gestione) .

L'accesso in consultazione al registro di protocollo è consentito sulla base dell'organizzazione del Comune di Porto Torres: di norma, ciascun operatore è abilitato ad accedere esclusivamente ai documenti e ai dati di protocollo dei documenti che ha prodotto l'Area Funzionale di appartenenza, assegnati alla scrivania da altri corrispondenti o, comunque, di competenza della U.O. di riferimento.

Ogni registrazione di protocollo viene memorizzata dal Sistema di Gestione Informatica dei Documenti, unitamente all'identificativo univoco dell'autore che l'ha

eseguita insieme alla data e l'ora della stessa.
Eventuali modifiche vengono registrate per mezzo di log di sistema e mantengono traccia dell'autore, della modifica effettuata, nonché della data e dell'ora;

il Sistema mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione.

Il Sistema non consente la modifica del numero e della data di protocollo;

L'annullamento delle informazioni non modificabili di una registrazione di protocollo può essere autorizzato unicamente dal Responsabile del servizio di protocollo informatico, a seguito di richiesta scritta (trasmessa anche via e-mail) indicante il numero di protocollo da annullare e i motivi dell'annullamento. il Sistema di Gestione informatica dei Documenti (SGID) deve recare, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione , generalmente il numero del verbale con allegato il verbale sottoscritto.

L'impronta digitale del documento informatico, associata alla registrazione di protocollo del medesimo è generata utilizzando una funzione di hash, conforme a quanto previsto dalla normativa vigente.

Al fine di garantire l'immodificabilità delle registrazioni di protocollo, il Sistema produce, al termine della giornata lavorativa, un registro giornaliero delle registrazioni di protocollo, in formato digitale; tale registro, formato nel rispetto di quanto previsto nel Manuale di conservazione, sarà trasferito, nell'arco della giornata lavorativa successiva, al conservatore affidatario del servizio di conservazione sostitutiva.

Gestione dei documenti e sicurezza logica del Sistema

I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano immodificabili e non eliminabili; l'accesso ad essi, da parte degli utenti interni all'AOO, avviene soltanto attraverso il Sistema medesimo, previa la suddetta procedura di identificazione informatica e nel rispetto dei profili di autorizzazione di ciascun utente.
Il Sistema consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività;
il Sistema effettua, inoltre, il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il Sistema e tutti i documenti e/o dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici dannosi in quanto il Comune di Porto Torres si impegna a rendere ragionevolmente sicuri gli accessi al Sistema e tutti i documenti e dati in esso contenuti tramite collegamento criptato, inoltre si impegna ad aprire le porte in uscita (LAN to WAN) del firewall esclusivamente verso gli indirizzi preventivamente individuati dal titolare del trattamento o dal responsabile all'uopo
incaricato.
I sistemi di sicurezza sopra elencati sono gestiti giornalmente da personale tecnico del Comune di Porto Torres e ottemperano al D.Lgs. 196/03 e ss.mm.ii.
Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dall'AOO e il Sistema di Gestione Informatica dei Documenti, vengono costantemente tenuti aggiornati, per mezzo dell'installazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Conservazione dei documenti

I documenti registrati sul SGID sono conformi ai requisiti e contengono i metadati previsti ai fini della conservazione permanente. Il trasferimento in conservazione avverrà mediante la produzione di pacchetti di versamento, basati su uno schema XML conforme a quanto previsto nel Manuale di Conservazione.

Accesso di Utenti esterni al Sistema

L'esercizio del diritto di accesso da parte di utenti esterni al Sistema viene effettuato nel rispetto di quanto sancito dalla legge 241/90 e del D. Lgs. 196/03.
Qualora l'utente esterno decida di esercitare il proprio diritto di accesso rivolgendosi direttamente all'URP o ad altro sportello allo scopo predisposto, la consultazione deve avvenire in modo che siano resi visibili soltanto dati o notizie che riguardino il soggetto interessato ed adottando gli opportuni accorgimenti (ad es. il posizionamento del monitor) volti ad evitare la diffusione di informazioni di carattere personale.

Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

L'amministratore di Sistema (non nominato dal Comune di Porto Torres in conformità al Provvedimento Generale dell'Autorità Garante per la Protezione dei dati personali:

“Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”, del 27 novembre 2008) controlla periodicamente i log di sistema e li mantiene per 6 mesi, al fine di verificare eventuali violazioni del Sistema.
Il Responsabile della gestione documentale del Comune effettua periodiche verifiche sul corretto funzionamento del Sistema di Gestione Informatica dei Documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale.

Misure di tutela e garanzia

Qualora Il Comune adotti misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere all’esecuzione, riceverà dall’installatore una descrizione scritta dell’intervento che ne attesti la conformità alle disposizioni del disciplinare tecnico di cui all’allegato b) del D. Lgs. 196/03.
In base al disposto dell’articolo 34, comma 1, del D. Lgs. 196/03 il trattamento dei dati personali effettuato mediante l’utilizzo di strumenti elettronici è subordinato al rispetto delle misure minime previste nell’allegato b) al Codice in materia di protezione dei dati personali “Disciplinare tecnico in materia di misure minime di sicurezza”.