Città
metropolitana
di Milano

Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi della Città Metropolitana di Milano

Allegato n. 16

Piano per la sicurezza informatica relativo alla formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici

Sommario

1. Premessa

Il presente Piano della Sicurezza (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) inerente alla gestione, trasmissione, interscambio, accesso e conservazione dei documenti che transitano attraverso il protocollo informatico di Città Metropolitana di Milano.

Lo scopo del documento è quello di poter stabilire, attuare, mantenere e migliorare in modo continuo il sistema di gestione per la sicurezza delle informazioni.
Il sistema di gestione della sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità delle informazioni mediante l'applicazione di un processo di gestione del rischio e dà fiducia alle parti interessate sull'adeguatezza della gestione dei rischi.

2. Riferimenti normativi

- DPR 20 ottobre 1998, n. 428 - Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD) e in particolare art. 50 bis;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale ex al Decreto Legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

3. Il piano di sicurezza

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 informatico 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 toccati dal documento sono:

- Componenti e configurazioni - la descrizione delle risorse e delle configurazioni del sistema, in particolare in riferimento al protocollo informatico, attraverso il quale l'ente effettua la gestione, interscambio, archiviazione e conservazione dei dati e politiche di sicurezza in essere.
- Analisi dei rischi - la valutazione delle minacce, e delle vulnerabilità che incombono o possono incombere sulle risorse e configurazioni del sistema.
- Gestione del rischio - le azioni adottate o da adottare al fine di determinare il giusto livello di sicurezza da perseguire.

3.1 Revisione e modifica del piano di sicurezza

A fronte di cambiamenti significativi del sistema, l'Ente effettua la revisione del piano sicurezza al fine di assicurarne la continua idoneità, adeguatezza ed efficacia e, in ogni caso, le modifiche vengono approvate dall'Ente stesso.

3.2 Revisione e modifica delle politiche di sicurezza

Tutta la documentazione, ed in particolare le politiche di sicurezza, vengono riesaminate periodicamente mediante un'apposita pianificazione o quando al verificarsi di cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.
Il riesame comprende una valutazione delle opportunità di miglioramento delle politiche dell'organizzazione e dell'approccio alla gestione della sicurezza delle informazioni in risposta ai cambiamenti dell'ambiente organizzativo, dei servizi erogati, delle clausole legali o dell'ambiente tecnico.

Revisioni delle politiche estemporanee vengono effettuate nei seguenti casi:

- verificarsi di incidenti di sicurezza;
- variazioni tecnologiche significative;
- modifiche all'architettura informatica;
- aggiornamenti delle prescrizioni normative;
- risultati delle eventuali attività di audit interni.

4. Componenti e configurazioni – Protocollo Informatico

4.1 Sedi di Città Metropolitana e Protocollo Informatico

Città Metropolitana di Milano è composta da una sede principale e da due sedi decentrate.
Esiste un unico registro di protocollo informatico. La protocollazione viene gestita in maniera decentrata, ovvero ogni Unità organizzativa registra i propri documenti in ingresso, in uscita all'Ente e quelli interni.

Il software di gestione del protocollo informatico è composto da un'applicazione web che risiede presso un'infrastruttura dedicata in cloud.
L'Ente, attraverso la collaborazione dei responsabili di Settore interessati ed il servizio informatico, definisce e aggiorna a livello contrattuale con i diversi fornitori dei servizi cloud e applicativi, le politiche di sicurezza in merito alla protezione dei dati, controllandone periodicamente lo stato, al fine garantire i corretti livelli di sicurezza atti a rispettare i principi di riservatezza, integrità e disponibilità.

4.2 Connettività

La gestione delle linee dati svolge un ruolo fondamentale nell'utilizzo di software web, residenti presso piattaforme cloud.
La gestione delle linee dati è affidata al servizio informatico, che ne tiene costantemente monitorato lo stato e ne tiene aggiornato l'elenco.
Tale elenco contiene la descrizione e le caratteristiche di ogni linea, le informazioni riguardo il fornitore che ne cura la manutenzione e gli eventuali dettagli contrattuali rilevanti, insieme alle eventuali specifiche di sicurezza.

4.3 Archivi

Gli archivi del protocollo informatico risiedono presso un db server su di una piattaforma in cloud. E' compito dell'ente tenere ed aggiornare l'elenco di ogni banca dati, insieme alle informazioni rilevanti e caratteristiche, quali: funzione, fornitore, ubicazione, metodologie di backup, effettuando quindi verifiche di attendibilità e correttezza dell'elenco attraverso controlli a campione o verifiche complete.
Le informazioni vengono richieste, se necessarie, direttamente alle ditte fornitrici dei servizi cloud e dell'applicativo su cui poggia il db.

4.4 Posta elettronica

Anche le caselle di posta elettronica vengono gestite attraverso un servizio in Cloud.
Gli aspetti di gestione e manutenzione dell'infrastruttura, di backup e di continuità di servizio sono in carico al fornitore del servizio cloud, con il quale l'Ente gestisce le politiche di sicurezza a livello contrattuale.

L'Ente cura internamente la parte di gestione amministrativa delle caselle attraverso delle prassi formalizzate. La creazione di una nuova casella avviene tramite apposita richiesta, in seguito

alla compilazione di modulistica concordata o attraverso comunicazione ufficiale su altri canali (cartacea, email).
Per le persone fisiche, le caselle sono composte da indirizzi nominali, del tipo:
<iniziale_nome>.<cognome>@cittametropolitana.milano.it

Al protocollo informatico, oltre alla PEC, è stato associato l'indirizzo di posta:
protocollo@cittametropolitana.milano.it.

4.5 Posta elettronica certificata

Le caselle di PEC attive sono gestite tramite un servizio di fornitura esterno e rilasciate da fornitori accreditati.
La casella istituzionale è direttamente integrata al softwaredi protocollo informatico, quindi, il backup dei messaggi avviene seguendo il naturale percorso di integrazione con le procedure dell'Ente.
La continuità operativa e la manutenzione del servizio sono gestite a livello contrattuale con il fornitore.
La casella PEC associata al protocollo informatico il cui indirizzo è protocollo@pec.cittametropolitana.mi.it è di tipo chiuso.

4.6 Sicurezza perimetrale

La gestione della sicurezza perimetrale avviene su due diversi livelli:
- a livello di infrastruttura cloud e software applicativo web, dove viene gestita a livello contrattuale con i fornitori dei vari servizi; è compito dell'ente assicurarsi che i fornitori adottino le adeguate misure di sicurezza perimetrale.
- a livello interno, dove viene gestita dall'ente attraverso il servizio informatico che ne mantiene le configurazioni, ne effettua una copia prima di ogni modifica; pianifica ed effettua gli aggiornamenti e ne tiene monitorato il corretto funzionamento.

4.7 Sistemi di protezione da malware

Presso le postazioni di lavoro e i server dell'Ente è installato e attivo un sistema antivirus.
Tale software viene gestito a livello centralizzato dal servizio informatico che ne cura gli aggiornamenti, le installazioni sulle postazioni ed il monitoring delle segnalazioni e dei risultati delle scansioni.
In occasione di criticità relativa a virus o malware il servizio informatico adotta le azioni opportune ed effettua le comunicazioni del caso, sia a livello di formazione e consapevolezza.

4.8 Sistemi e politiche di backup

La gestione dei backup riguardante l'infrastruttura cloud su cui poggia l'applicativo del protocollo informatico, viene effettuata anch'essa da un servizio cloud dedicato.
L'ente quindi gestisce anche i sistemi e le politiche di backup contrattualmente, direttamente con i fornitori del servizio, in modo da adempire alle misure minime di sicurezza Agid.

L'Ente, in collaborazione con il fornitore,mantiene l'elenco delle risorse sottoposte a backup e delle relative procedure adottate per l'esecuzione delle copie di salvataggio, oltre ad effettuare verifiche giornaliere della corretta esecuzione dei processi di backup ed effettuare una verifica

periodica della correttezza delle impostazioni dei sistemi di backup e della adeguatezza dei processi di backup.
Periodicamente viene effettuato un riesame delle risorse sottoposte a backup, in modo da assicurare che venga salvata la totalità dei dati facenti parte del sistema informatico.

E' in fase di valutazione infine l'applicazione di modalità di backup offline.

4.9 Log e tracciamento delle attività

L'applicativo web di gestione del protocollo permette il tracciamento dei log inerente alle attività effettuate sull'applicativo stesso.
L'Ente, a livello contrattuale, disciplina con i fornitori, attraverso una specifiche politiche di sicurezza, le modalità di creazione, gestione, eliminazione salvataggio e conservazione dei log di tracciamento delle attività.

4.10 Accesso logico alle reti e ai sistemi

L'accesso alla rete ed ai sistemi, in particolare al protocollo informatico, può avvenire esclusivamente tramite un processo di autenticazione che prevede un nome utente ed una password.
La gestione delle password ed i livelli di complessità sono centralizzati.
La password deve essere composta da almeno otto caratteri alfanumerici essa non deve contenere riferimenti agevolmente riconducibili all'assegnatario.
L'Ente gestisce internamente l'assegnazione delle password di accesso al sistema.

Nome utente e password sono strettamente personali. L'utente è tenuto a:

- Non comunicare a terzi la password
- A non annotare la password su supporti posti in vicinanza della propria postazione di lavoro o comunque incustoditi.

La password di accesso alla rete viene cambiata autonomamente secondo quanto stabilito dalla normativa vigente.
In caso di assenza, anche temporanea, del personale incaricato dei trattamenti dei dati, sui P.C. devono essere chiuse le procedure di accesso ai dati o attivato il blocco attraverso lo screen saver con password.

Le credenziali di accesso ai sistemi informatici sono rilasciate su richiesta che avviene tramite la compilazione di moduli specifici a seconda dei servizi per i quali si richiede l'accesso. I processi di autorizzazione e di revoca sono illustrati ai paragrafi successivi.

4.11 Sistemi di autenticazione e gestione privilegi utenze

Gli utenti autorizzati accedono alle risorse tramite diversi livelli di autenticazione, a seconda dei privilegi autorizzativi che vengono loro rilasciati.
In generale, l'accesso alle postazioni di lavoro, ai sistemi di navigazione Internet, all'applicativo del protocollo informatico e ai documenti residenti sul file server (cartelle di rete condivise), viene disciplinato in fase di rilascio delle credenziali da parte dell'ente, previa apposita richiesta fatta pervenire dal responsabile di settore, nella quale vengono specificate, anche in maniera implicita, le funzioni dell'utente.
Le utenze ed i privilegi agli utenti vengono gestiti e assegnati a seconda delle effettive necessità e competenze, concordate con gli appositi responsabili di settore.

4.12 Modalità di accesso remoto

La gestione ed il controllo degli accessi al sistema effettuati da parte di terzi (es. manutentori esterni, istruttori applicativo, sistemisti, etc..) è in capo al servizio informatico.
Le autorizzazioni di accesso vengono definite in sede contrattuale e vengono effettuate le apposite nomine in caso di accesso con profili di amministrazione.
Di volta in volta, in base alle specifiche attività da effettuare il servizio informatico autorizza l'accesso alle risorse, fisiche e logiche con credenziali identificate e con livelli di autorizzazione minimi per l'attività che deve essere effettuata

4.13 Telelavoro e lavoro agile

La modalità del telelavoro è abilitata in casi di emergenza o a seguito dell'attivazione di particolari progetti, per il periodo di tempo stabilito dall'emergenza o dai progetti stessi. Il servizio informatico, nei casi di telelavoro adibito per scopi non riguardanti il fronteggiamento di particolari emergenze, ma per l'attivazione di progetti concordati, fornisce gli strumenti necessari per permettere agli utenti di effettuare connessioni sicure con il sistema dell'Ente (es. connessioni VPN debitamente configurate).

4.14 Inventario degli asset – protocollo informatico

L'Ente, in sede contrattuale, insieme al fornitore dei servizi cloud, mantiene aggiornato l'elenco delle risorse presenti presso la piattaforma cloud che ospita i servizi del protocollo informatico,
Internamente, tiene un inventario delle risorse hardware e software presenti presso l'Ente per l'utilizzo e la gestione del protocollo informatico.

4.15 Notebook, smartphone e altri supporti mobili

Agli utenti possono essere forniti dispositivi mobili, quali: notebook, supporti di memorizzazione esterna mobili quali chiavette USB, dischi esterni, e altro.
L'Ente tiene aggiornato l'elenco degli strumenti di supporto mobile o memorizzazione esterna forniti in dotazione.
La corretta gestione di questi strumenti, la custodia e le metodologie di protezione delle informazioni in esse contenute sono gestite dai responsabili di settore, attraverso adeguate azioni di informazione agli utenti finali sui rischi che corrono utilizzando tali strumenti.
Inoltre vengono effettuati periodicamente delle analisi sui dati presenti nei dispositivi mobili, anche potenziali, al fine di decidere l'applicazione o meno della crittografia dei dati a porzioni delle memorie analizzate sui dispositivi mobili.

Tutti i supporti mobili, nel momento del non utilizzo, devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in un armadio/cassetto chiuso a chiave.

4.16 Responsabilità degli utenti e formazione

E' obiettivo dell'Ente definire nel piano formativo annuale, delle sessioni periodiche relative all'utilizzo sicuro delle risorse informatiche, nonché sui temi di protezione dei dati personali.

5. Analisi delle minacce e delle vulnerabilità dell'infrastruttura informatica

Sulla base delle componenti del sistema e delle politiche di sicurezza descritte al punto 4, viene effettuata un'analisi circa l'impatto che hanno, o possono avere, una serie di minacce e vulnerabilità, sulle risorse che fanno parte del sistema di gestione del protocollo informatico

Rischi		Impatto sulla sicurezza: alto/medio/basso
Minacce derivanti dal comportamento degli utenti e amministratori	Sottrazione di credenziali di autenticazione	Basso
	Carenza di consapevolezza, disattenzione o incuria	Medio
	Comportamenti sleali o fraudolenti	Basso
	Errore materiale nell'utilizzo delle risorse	Basso
Minacce derivanti da terze parti	Minacce apportate da virus informatici, programmi suscettibili a recare danno	Basso
	Tentativi di fishing o spamming	Basso
	Accessi non autorizzati a locali o risorse	Basso
Minacce derivanti da altre cause	Eventi distruttivi o limitanti per l'accesso o la fruizione delle risorse di cause naturali o artificiali	Basso
	Guasti a sistemi complementari (impianto elettrico, climatizzazione, etc.)	Basso
	Errori umani nella gestione della sicurezza fisica	Medio
	Malfunzionamento, indisponibilità o degrado degli strumenti	Basso
	Sottrazione di risorse e strumenti contenenti dati	Basso

6. Misure adottate per la protezione e la sicurezza del sistema informatico, sulla base dei rischi considerati e del loro livello di impatto

Sulla base delle caratteristiche del sistema informatico e dei servizi con esso erogati, e delle minacce analizzate al par.5, vengono descritte qui le misure adottate per la protezione e la sicurezza dell'infrastruttura informatica e dei dati:

- Migrazione del sistema di protocollo informatico in cloud con relativa gestione delle politiche di sicurezza a livello contrattuale.
- Presenza di antifurto presso la sede. Presidio in orario di lavoro dei locali e uffici. Tutti gli uffici vengono chiusi quando non presidiati.
- Autenticazione e autorizzazione degli accessi al sistema ed ai dati, attraverso l'utilizzo di profili nominali e credenziali adeguatamente complesse (in base alla rilevanza dei dati trattati).
- Gestione adeguata e controllata dei profili di amministratore, secondo effettive necessità e competenze.
- Antivirus gestito e a livello centralizzato con aggiornamento automatico delle minacce, da parte del Servizio Informatico.
- Aggiornamenti software e applicazione delle patch periodiche e amministrate a livello centrale da parte del fornitore. (gestito a livello contrattuale)
- Backup dei dati dell'intero sistema gestito attraverso infrastruttura cloud dedicata, gestione politiche di sicurezza a livello contrattuale.
- Sicurezza perimetrale e content filtering gestiti attraverso la gestione e configurazione di firewall di rete.
- Gestione controllata di connessioni sicure fra rete interna ed esterni: es. collegamento dei fornitori esterni per manutenzione o helpdesk o degli utenti interni per telelavoro.