

ALLEGATO N. 7

PIANO DI SICUREZZA RELATIVO ALLA FORMAZIONE, ALLA GESTIONE, ALLA TRASMISSIONE, ALL'INTERSCAMBIO, ALL'ACCESSO, ALLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Premessa

Il presente piano di sicurezza, adottato ai sensi dell'art. 4, comma 1, lettera c), del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico", garantisce che:

- i documenti e le informazioni trattati dall'Ente siano resi disponibili, integri e riservati;
- i dati personali comuni e particolari siano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

A tali fini, l'art. 7 del suddetto DPCM, individua i requisiti minimi di sicurezza dei sistemi di protocollo informatico a cui il presente piano si conforma.

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno dell'Ente;
- le modalità di accesso al Sistema di Gestione Informatica dei Documenti;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle Misure Minime di Sicurezza per la Pubblica Amministrazione di AgID
- la formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Tale piano di sicurezza è soggetto a revisione con cadenza almeno biennale; a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche, potrà essere modificato anticipatamente.

Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel Sistema di Gestione Informatica dei Documenti

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'ausilio delle tecnologie informatiche sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al SGID o come accesso ai documenti, dati e unità archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati, includendo a tale proposito tutti i dati presenti sul Sistema di Gestione Informatica dei Documenti;
- perdita dei documenti e dei dati contenuti nel Sistema;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, Città di Cantù adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Sicurezza della rete di accesso al servizio

Il Sistema di Gestione Informatica dei Documenti non è esposto all'accesso attraverso la rete internet e non vengono utilizzati sistemi in cloud. Il sistema opera all'interno di un server installato nella rete LAN dell'Ente, ereditando dalla stessa tutti i meccanismi previsti per la sicurezza e la protezione.

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; i profili di abilitazione alle funzionalità del Sistema stesso sono attribuiti a ciascun utente sulla base di quanto stabilito dall'allegato n. 2 al presente manuale. L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi.

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, 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 e non contiene riferimenti agevolmente riconducibili al titolare. La *Password* è modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza mensile.

L'*User-Id* non può essere assegnato ad altri incaricati neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Il Responsabile della sicurezza informatica dell'Ente 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 particolari e politiche di sicurezza espressamente previste

L'accesso ai documenti contenenti dati personali particolari 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; 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, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Il personale autorizzato al trattamento di dati personali particolari non deve lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento degli stessi.

Trattamento dei dati personali senza l'ausilio di strumenti elettronici

Ai fini del trattamento dei dati personali, sono impartite agli incaricati istruzioni scritte da parte del Responsabile per la Protezione dei Dati, 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 dall'allegato n. 8 del 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); 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 avverranno in conformità di quanto sancito dalle regole tecniche contenute nel DPCM 22/02/2013, emanate ai sensi dell'art. 71 del D. Lgs. 82/05.

La sottoscrizione del documento con firma digitale avverrà 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 è consentito soltanto al personale abilitato alla protocollazione.

L'accesso in consultazione al registro di protocollo è consentito sulla base dell'organizzazione dell'Ente; ciascun operatore è abilitato ad accedere esclusivamente ai documenti e ai dati di protocollo dei documenti che ha prodotto, che gli sono stati assegnati o, comunque, di competenza del proprio ufficio 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 e alla data e all'ora della stessa.

Eventuali modifiche, autorizzate ai sensi dell'art. 30 del presente manuale, vengono registrate per mezzo di log di sistema che mantengano 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; in tal caso l'unica possibile modifica è l'annullamento della registrazione stessa di cui, analogamente al caso precedente, il Sistema manterrà traccia. L'annullamento di una registrazione di protocollo deve sempre essere accompagnata da autorizzazione scritta del Responsabile della gestione documentale e il SGID deve

recare, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione.

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 permette, al termine della giornata lavorativa, la produzione del 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, alla struttura di conservazione accreditata di cui l'Ente si serve, secondo quanto previsto dall'articolo 3 del presente manuale.

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 dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici in quanto l'Ufficio SICI, avvalendosi della ditta incaricata della gestione in *outsourcing* del sistema informativo, si impegna a rendere ragionevolmente sicuri gli accessi al Sistema e tutti i documenti e dati in esso contenuti.

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 **Backup e ripristino dell'accesso ai dati**

L'Ufficio SICI, avvalendosi della ditta incaricata della gestione in *outsourcing* del sistema informativo garantisce la corretta esecuzione giornaliera delle copie dati che vengono effettuate automaticamente di notte.

Il Backup dei dati contenuti nel Sistema di Gestione Informatica dei Documenti prevede il salvataggio dei dati e delle configurazioni del server. Il backup viene così effettuato con l'ausilio di procedure automatizzate.

I dati vengono memorizzati su NAS con dischi da 2TB, configurati in RAID1 al fine di garantire l'integrità delle copie di sicurezza. A partire dalla sua attivazione, il dispositivo inizia a memorizzare i dati secondo il seguente schema

- 7 backup giornalieri
- 4 backup settimanali, effettuati di domenica
- 3 backup mensili, effettuati l'ultima domenica del mese.
- Un backup remoto giornaliero dei dati relativi alle procedure Halley
- Backup settimanale su disco esterno usb

L'accesso alle NAS avviene in sola lettura con i protocolli di interscambio dati più diffusi.

Al termine dei backup, tutte le informazioni vengono salvate in un database per permettere ai responsabili delle copie di sicurezza di verificare il corretto funzionamento dei backup anche nei giorni successivi. Tutti i dati dei log sono consultabili dall'interfaccia web, in aree protette, per salvaguardare la privacy e le policy di accesso ai file definite dal cliente.

La visualizzazione dei log mostra, in una sola schermata, l'esito dei backup degli ultimi 7 giorni. E' quindi immediatamente visibile ogni eventuale anomalia (backup con errori, parziale o non

effettuato). Per ogni disco vengono visualizzati:

- Il numero di cartelle del backup
- Il numero di file nuovi o modificati
- Il numero di file cancellati. Vengono eliminati al massimo 500 file al giorno per prevenire eventuali cancellazioni massive dovute ad errori di collegamento tra il dispositivo e la sorgente dati.
- Il numero di errori rilevati durante la copia
- La dimensione del backup e lo spazio occupato sul disco da copiare

Il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici avviene entro 4 ore lavorative in caso di generico malfunzionamento, ed entro 12 ore lavorative in caso di disastro.

Un secondo processo di back Up remota i dati contenuti nel Sistema di Gestione Informatica dei Documenti è effettuata su infrastruttura remota SPC-Cloud mediante il software Simpana.

I back up remoti de dati sono effettui attraverso collegamenti criptati.

Trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno dell'Ente avviene esclusivamente per mezzo del Sistema di Gestione Informatica dei Documenti; nessun'altra modalità è consentita, al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati.

La trasmissione di documenti informatici al di fuori dell'Ente avviene tramite PEC o mediante i meccanismi dell'interoperabilità e della cooperazione applicativa di cui al Sistema Pubblico di Connettività, utilizzando le informazioni contenute nella segnatura di protocollo.

I messaggi di posta elettronica certificata prodotti dall'Ente sono compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni.

Le informazioni relative alla segnatura di protocollo sono strutturate in un file conforme alle specifiche XML, compatibile con un file XML Schema e/o DTD, secondo lo schema previsto nella circolare AgID n. 60 del 23 gennaio 2013.

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 avviene mediante la produzione di pacchetti di versamento, basati su uno schema XML conforme a quanto previsto nel manuale di conservazione.

Sicurezza fisica e infrastrutturale del Sistema

L'Ente ha adottato le Misure Minime di Sicurezza per le PA. I moduli di implementazione sono firmati digitalmente dal Responsabile della Transizione Digitale e dal Sindaco e marcati temporalmente.

Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

In particolare le indicazioni di cui all' ABSC 10 (CSC 10): COPIE DI SICUREZZA prevedono che le copie di sicurezza siano localizzate in un secondo sito, posto comunque all'interno del territorio dell'Unione Europea.

In caso di perdita dei dati al procedura di Disaster Recovery prevede il ripristino degli stessi e dell'accesso ad essi entro 24 ore lavorative.

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, decreto legislativo n. 33 del 2013 e dal decreto legislativo n. 97 del 2016.

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.

Piani formativi del personale

Ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, l'Ente predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del Sistema di Gestione Informatica dei Documenti;
- fascicolazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione in materia di protezione dei dati personali;
- aggiornamento sui temi suddetti.

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

La ditta incaricata della gestione in *outsourcing* del sistema informativo e la software house licenziatarie del software Sistema di Gestione Informatica dei Documenti, mantengono per 6 mesi i log di sistema, ognuna entro i limiti delle proprie competenze, al fine di verificare eventuali violazioni del Sistema.

Il Responsabile della gestione documentale dell'ente 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.