**Allegato 11 Piano sicurezza**

*1 Obiettivi del Piano di sicurezza Informatica*

Il piano di sicurezza garantisce che:

* i documenti e le informazioni trattati dal Comune di Casorate Sempione siano resi disponibili, integri e riservati;
* i dati personali comuni, sensibili e/ o giudiziari vengano 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, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

*2 Generalità*

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 e sulle direttive strategiche stabilite dal vertice del Comune di Casorate Sempione definisce:

* le politiche generali e particolari di sicurezza da adottare all’interno del Comune;
* le modalità di accesso al Protocollo Informatico e agli archivi;
* gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell’allegato b) del Decreto Legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”, in caso di trattamento di dati personali;
* i piani specifici di formazione degli addetti;
* le modalità con le quali deve essere effettuato il monitoraggio periodico dell’efficacia e dell’efficienza delle misure di sicurezza.

*3 Formazione dei documenti informatici – aspetti di sicurezza*

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 a essere gestiti mediante strumenti informatici e a 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 .

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma digitale o avanzata, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione, come riportato sul sito dell’Agenzia per l’Italia Digitale ([www.agid.gov.it](http://www.agid.gov.it)), al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura. A titolo d’esempio si utilizzano preferibilmente: PDF e PDF/ A.

*4 Gestione delle registrazioni di protocollo e di sicurezza*

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) presenti o transitate nel sistema di Protocollo Informatico 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 (Intrusion Detection System (IDS), sensori di rete e firewall);
* dalle registrazioni del software di Protocollo Informatico;
* dalla politica delle password.

*5 Accesso ai documenti informatici*

Il controllo degli accessi è assicurato utilizzando un sistema di autorizzazione basato sulle credenziali di accesso al proprio computer tramite Active Directory. La profilazione degli utenti avviene in via preventiva e consente di definire le abilitazioni/ autorizzazioni che possono essere effettuate/rilasciate a ogni singolo utente.

Il sistema di protocollo informatico adottato dal Comune di Casorate Sempione:

* consente il controllo differenziato dell’accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
* 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.

Ciascun utente del Protocollo Informatico può accedere solamente ai documenti che sono stati direttamente assegnati. Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall’Amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell’archivio.

*6 Utenti interni alla AOO*

I livelli di autorizzazione per l’accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti con il permesso del Responsabile del servizio Protocollo. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all’inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

*7 Profili utente e responsabilità*

Il sistema garantisce la tutela dei dati personali e dei dati sensibili tramite l'assegnazione differenziata dei diritti di modifica e di visualizzazione dei documenti di protocollo in rapporto alle funzioni e al ruolo svolto dagli utenti.

Il sistema prevede diverse possibilità di combinazione dei profili di accesso al protocollo informatico:

* visibilità: possibilità per un utente abilitato di visualizzare una registrazione di protocollo, con l’esclusione dei documenti riservati;
* inserimento: possibilità per un utente abilitato di inserire i dati e provvedere ad una registrazione di protocollo;
* modifica: possibilità per un utente abilitato di modificare i dati gestionali di una registrazione di protocollo, con l’esclusione dei dati obbligatori;
* annullamento: possibilità per un utente abilitato di annullare una registrazione di protocollo;

Si descrivono di seguito i profili tipo di accesso al sistema:

*Amministratore di sistema*

Soggetto che ha la possibilità di effettuare operazioni straordinarie sul sistema (es.: ripristino a seguito di eventuali interruzioni, monitoraggio delle operazioni compiute, predisposizione delle autorizzazioni di accesso al sistema, ecc.).

*Protocollatore*

Il protocollatore è l'utente che ha l’autorizzazione ad eseguire la registrazione dei documenti, all'acquisizione di immagini da scanner ed alla conseguente associazione al documento di protocollo, e parimenti alla associazione di eventuali allegati informatici (operazione che può essere eseguita anche differita, ma che poi non può più essere più modificata).

Al Protocollatore è tipicamente assegnata anche la possibilità di accedere all'anagrafica per inserire o modificare (ma non cancellare) strutture e persone esterne e comuni.

*Responsabile del procedimento o affare (RPA)*

E’ la persona che ha la responsabilità del documento. Suo compito, nell’ambito della gestione documentale, è quello di inserire il documento in un fascicolo e trattare il procedimento o l’affare a cui quel fascicolo si riferisce.

Il RPA è ovviamente abilitato anche a svolgere le stesse operazioni curate in via ordinaria dal protocollista.

*Utente abilitato alla consultazione*

Gli utenti delle AOO possono essere abilitati all’accesso al sistema informativo nella modalità della sola visione e con le restrizioni formalmente indicate dal RPA.

*8 Conservazione dei documenti informatici*

La conservazione dei documenti informatici avviene a cura del Responsabile della Conservazione in modo conforme a quanto previsto dal D.P.C.M. 3 dicembre 2013 – Regole tecniche in materia di sistema di conservazione, dal D. M.E.F. del 17 giugno 2014, dal D.P.R. 633/ 72, dalla Circolare dell’Agenzia delle Entrate n. 45/ E del 19 ottobre 2005, dalla Circolare dell’Agenzia delle Entrate n. 36/ E del 6 dicembre 2006 e loro successive modificazioni o integrazioni, come specificato nel Manuale della Conservazione.