
Comune di Saint-Vincent

Regione Autonoma Valle d'Aosta

Région Autonome Vallée d'Aoste



MANUALE DI GESTIONE E CONSERVAZIONE DOCUMENTALE

ALLEGATO N.4

Piano per la sicurezza del sistema di gestione
informatica dei documenti

Sommario	
Obiettivi	3
Introduzione	3
Componenti della sicurezza.....	3
1. Componente organizzativa	3
2. Componente logica	3
3. Componente infrastrutturale.....	3
Accesso ai documenti informatici.....	3
Politiche di sicurezza adottate dalla AOO	4
1. Responsabilità	4
2. Postazioni di lavoro degli utenti del servizio	4
Procedura da adottarsi in caso di violazione dei dati personali	4

Obiettivi

Il piano per la sicurezza garantisce che le informazioni siano disponibili, integre, riservate e che per i documenti informatici sia assicurata l'autenticità, la non ripudiabilità, la validità temporale e l'estensione della validità temporale.

I dati, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento, vengono 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.

Introduzione

Relativamente al sistema di protocollo informatico, sono adottate le seguenti misure:

- modalità definite di accesso al servizio di protocollo, di gestione documentale e archivistico, con abilitazioni commisurate alle effettive esigenze di servizio;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo;
- registrazione delle attività di protocollo effettuate da ciascun utente durante l'arco della giornata, comprese le modifiche autorizzate.

Componenti della sicurezza

1. Componente organizzativa

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione.

2. Componente logica

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

3. Componente infrastrutturale

Il sistema informatico utilizza le seguenti tecnologie:

- Uno o più server in SaaS certificato ACN presso il fornitore del software;
- Un'interfaccia web;
- Tutte le postazioni hanno installato un prodotto antivirus al fine di prevenire la diffusione di software malevolo.

Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso e di autorizzazione (profilazione).

La profilazione consente di definire le abilitazioni/autorizzazioni delle attività che possono essere rilasciate ad un utente del servizio di protocollo e gestione documentale, es. consultazione, inserimento, modifica o annullamento.

Il programma di protocollo adottato dal comune:

- 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, se autorizzata, e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dal comune. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal segretario, previa richiesta del Responsabile di servizio e sentito il parere del Responsabile della gestione e conservazione documentale.

La gestione delle utenze rispetta i seguenti criteri operativi:

- tutti gli utenti possono consultare ed inserire documenti in base al ruolo e agli uffici di appartenenza;
- esiste un ruolo specifico per la richiesta di annullamento dei protocolli;
- esiste un ruolo specifico per la validazione degli annullamenti dei protocolli.

Inoltre esistono diversi profili di abilitazione come specificato nel Manuale.

Politiche di sicurezza adottate dalla AOO

1. Responsabilità

La responsabilità delle azioni compiute nella fruizione del servizio di protocollo è dell'utente fruitore del servizio.

Gli utenti autorizzati ad accedere al servizio di protocollo dispongono di una propria credenziale personale.

La richiesta dell'abilitazione per l'accesso al programma di protocollo deve essere effettuata dal segretario o suo delegato, il quale definisce, di concerto con il Responsabile di servizio, il profilo di accesso e le relative autorizzazioni in merito alla visibilità e alla gestione delle informazioni che l'utilizzatore deve avere. Ogni nuovo utente autorizzato viene registrato secondo una specifica procedura con la quale vengono annotate le informazioni relative all'utente e ai ruoli di appartenenza.

2. Postazioni di lavoro degli utenti del servizio

Per la corretta fruizione del servizio di protocollo informatico e di gestione documentale e al fine di tutelarne l'accesso è necessario che l'utente adotti almeno le seguenti buone norme di comportamento relative alla gestione del proprio posto di lavoro:

- la postazione di lavoro non deve essere lasciata incustodita, anche per brevi periodi, con la sessione attiva;
- prima di allontanarsi, anche momentaneamente, devono essere attivati i sistemi di protezione esistenti relativamente alla postazione di lavoro.

In generale, deve essere adottata la politica della cosiddetta "scrivania pulita" che obbliga a non lasciare materiale riservato incustodito al di fuori dell'orario di lavoro e invita a riporre il materiale di lavoro (documenti, supporti) negli appositi armadi, secondo il livello di sicurezza, di disattivare o bloccare la stazione di lavoro, di tenere chiusi i locali.

Procedura da adottarsi in caso di violazione dei dati personali

Qualora si sospetti una violazione dei dati personali, è necessario comunicare immediatamente e senza ingiustificato ritardo la problematica al proprio Responsabile e al Segretario dell'Ente tramite email (segretario@comune.saint-vincent.ao.it), che provvederanno agli adempimenti di propria competenza in condivisione con il fornitore del programma di protocollo e all'invio delle comunicazioni e segnalazioni dovute al DPO ed eventuali altre autorità.