



# COMUNE DI PINEROLO

**MANUALE  
DI GESTIONE E CONSERVAZIONE  
DEI DOCUMENTI**

**ALLEGATO N. 6**

**PIANO DI SICUREZZA  
DEI  
DOCUMENTI INFORMATICI**

# PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

## Articolo 1 – Sicurezza fisica

1. Il ruolo della sicurezza fisica è quello di proteggere le persone che operano sui sistemi, le aree e le componenti del sistema informativo: essa può essere suddivisa in due parti:
  - a. SICUREZZA DI AREA  
La parte del sistema informativo del comune di Pinerolo in cui risiedono le apparecchiature dedicate alla gestione dei documenti informatici è completamente contenuto in un unico sito. Il locale, sito al secondo piano del palazzo comunale, possiede un unico ingresso dotato di sistema di controllo degli accessi a chiave di identificazione biometrica (impronta digitale).  
Questo sistema di identificazione è attualmente in fase avanzata di test, e sarà presto messo in esercizio definitivamente, si presume che saranno autorizzati all'accesso oltre al personale ed al dirigente del servizio informatico anche le seguenti figure:
    - q Personale della polizia municipale e addetti alla sicurezza ed alla prevenzione incendi;
    - q Custode del palazzo comunale;
    - q Personale addetto alle pulizie.Il locale dispone, altresì, di un sistema di rilevazione di incendio e dei fumi collegato all'impianto di rilevazione generale del comune con dispositivo di allarme, di un sistema di rilevazione dei fumi che si potrebbero sviluppare sotto il pavimento, e, limitatamente alla sala macchine, di un sistema di condizionamento.
  - b. SICUREZZA DEI SERVERS E DELLE PRINCIPALI APPARECCHIATURE DI RETE  
L'isolamento della sala computer, che ospita anche le principali apparecchiature di rete, garantisce la protezione delle risorse da danneggiamenti accidentali.  
Il suo impianto di alimentazione è protetto da un gruppo di continuità con dispositivo di allarme, i servers che gestiscono basi dati sono dotati di un gruppo di continuità secondario in grado di gestirne lo spegnimento automatico in caso di prolungamento della mancanza di corrente.
2. Tutti gli elaboratori classificati di “**Sistema**” sono coperti da servizi di manutenzione software, hardware e sistemistica che garantiscono tempi rapidi di intervento per diagnostica, riparazione e ripristino dei sistemi operativi, DBMS e delle basi dati eventualmente danneggiate tramite i salvataggi meglio descritti nella parte riguardante la sicurezza logica.

## Articolo 2 – Sicurezza logica

1. Il ruolo della sicurezza logica è quello finalizzato alla implementazione dei requisiti di sicurezza nelle architetture informatiche, dotato quindi di meccanismi opportuni e di specifiche funzioni di gestione e controllo.

L'architettura si basa sulla realizzazione di servizi di sicurezza, ovvero su funzioni garantite dal sistema utilizzato sulle piattaforme del sistema informatico comunale.

I servizi attivi sono:

- q Controllo degli accessi
- q Autenticazione
- q Sistema anti-intrusione
- q Confidenzialità
- q Integrità
- q Meccanismi di salvataggio dati.

I meccanismi di sicurezza utilizzati, ovvero le modalità tecniche attraverso le quali è possibile realizzare i servizi di sicurezza sono sostanzialmente:

- q Meccanismi per il controllo degli accessi
- q Meccanismi per l'autenticazione
- q Cifratura
- q Meccanismi di salvataggio dati
- q Antivirus
- q Firewall.

2. Nel seguente comma verranno descritti i principali servizi e strumenti utilizzati:

- a) **Controllo degli accessi** il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informatico avvengano esclusivamente secondo modalità prestabilite. Il controllo accessi viene visto come un sistema caratterizzato da soggetti (utenti, processi) che accedono a oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione).

Funzionalmente è costituito da:

- q Un insieme di politiche e di regole di accesso che stabiliscono le modalità (lettura, modifica, cancellazione, esecuzione) secondo le quali i vari soggetti possono accedere agli oggetti;
- q Un insieme di procedure di controllo (meccanismi di sicurezza) che controllano se la richiesta di accesso è consentita o negata, in base alle suddette regole (validazione della richiesta).

- b) **Autenticazione** per garantire quanto sopra esposto, il sistema informatico comunale è basato su un meccanismo che costringe ogni utente ad autenticarsi, anche più volte, (dimostrare, cioè, la propria identità) prima di poter accedere ad una risorsa.

Ogni nome utente è associato ad una sola password per l'accesso ad una determinata risorsa o ad un insieme di queste, che viene disabilitata dagli amministratori di sistema quando l'accesso non sia più autorizzato o quando l'utente non può accedere per un determinato periodo di tempo.

L'autenticazione è necessaria per accedere alla procedura di gestione del protocollo informatico, come meglio descritto all'art. 33 del manuale di gestione, di cui il presente documento costituisce l'allegato n. 6.

In un prossimo futuro il comune di Pinerolo doterà alcuni utenti di firma digitale che potrà modificare il sistema di autenticazione attualmente in essere e darà la possibilità di gestire documenti informatici con validità giuridica.

c) **Confidenzialità** Ogni utente autorizzato può accedere ad un'area di lavoro riservata per il settore di appartenenza a cui hanno diritto di accesso i soli componenti del gruppo di appartenenza. Egli può inoltre impostare particolari restrizioni di accesso ai file.

d) **Integrità fisica** L'integrità fisica dei dati viene garantita con un duplice meccanismo. Tutti i dati dei sistemi informativi ed i files utente presenti sul server centralizzato sono residenti su architetture di dischi mantenute in configurazione di tipo "mirror" o "raid".

La garanzia di integrità viene estesa da una politica di backup a ciclo periodico su base giornaliera con controllo dell'avvenuto salvataggio da parte del personale preposto anche mediante invio automatico di messaggi e analisi dei reports relativi.

Le letture dei supporti di backup avvengono in occasione delle richieste di ripristino dei dati. I supporti contenenti l'ultimo Backup vengono conservati in cassaforte posta presso il comando di polizia municipale.

e) **Integrità logica** L'integrità logica si ottiene con il meccanismo di verifica dei privilegi di accesso ai file, garantito dal sistema operativo e con il sistema antivirus.

Ogni utente, superata la fase di autenticazione ha accesso ai propri dati residenti nella propria area di lavoro e non può accedere alle altre aree né agli altri applicativi se privo di autorizzazione.

Il sistema antivirus risiede sia sui servers principali, sia sulle postazioni di lavoro utente. Esso controlla tutti i file in entrata ed in uscita da ciascuna macchina ivi compresi gli allegati dei messaggi di posta elettronica ed i files scaricati da internet. Un contratto consente di scaricare, via internet, gli aggiornamenti del sistema antivirus. Essi sono distribuiti sulla rete ad ogni postazione di lavoro in modo trasparente all'utente.

La rete interna del comune di Pinerolo costituisce un segmento della rete Regionale della Pubblica Amministrazione Piemontese (RUPAR Piemonte). La rete comunale (LAN) in questione, oltre ad essere protetta dal sistema anti-intrusione adottato dalla RUPAR Piemonte è provvisto di un ulteriore sistema perimetrale con l'utilizzo di Firewall fisico, la cui gestione è demandata al gestore della sicurezza dell'intera rete regionale.

### **Articolo 3 - Sicurezza organizzativa**

1. Gli aspetti organizzativi riguardano principalmente la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo sicurezza e l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecniche adottate.

All'interno del Settore Istruzione Informativo è stata definita l'unità operativa preposta sia alla gestione dei sistemi informativi che al servizio di gestione dei sistemi di elaborazione dati.

Un ulteriore aspetto inerente la sicurezza organizzativa è quello concernente i controlli sulla funzionalità e sulla affidabilità degli apparati.

E' stata creata una banca dati di tutte le dotazione HW, SW e trasmissione dati; mediante la tenuta di schede informative aggiornate con le sostituzioni, riparazioni delle apparecchiature.

Questa banca dati fornisce una visione del patrimonio arricchita di informazioni sul grado di affidabilità uso ed obsolescenza dei sistemi; è di aiuto nei processi di acquisto ed in quelli di pianificazione degli investimenti e delle scorte e materiali di consumo.