



PIANO PER LA SICUREZZA INFORMATICA. ANNO 2016

Indice

1. Introduzione	2
2 L'architettura dell'infrastruttura informatica	2
2.1 Caratteristiche dei locali	2
2.2 Connettività	2
2.3 Server.....	2
2.4 Backup.....	3
2.5 Sistema di videosorveglianza del territorio	3
3 Analisi delle minacce e delle vulnerabilità dell'infrastruttura informatica	4
4 Misure adottate per la protezione e la sicurezza dell'infrastruttura informatica	5
5 Misure adottate per la disponibilità dei dati e la continuità del servizio.....	5
5.1 Server.....	5
5.2 Backup.....	5
6 Conservazione a norma	5



1. Introduzione

Il presente documento si propone di descrivere gli accorgimenti organizzativi e tecnici che il Comune di Rogno mette in atto per applicare correttamente le misure di sicurezza previste dalla normativa in particolare per quanto riguarda la gestione documentale e i sistemi informativi.

Lo scopo di questo è di garantire la protezione del patrimonio informativo da accessi, modifiche, cancellazioni non autorizzate per cause accidentali o intenzionali e ridurre gli effetti causati dall'eventuale occorrenza, nonché di consentire la continuità operativa.

Le misure di sicurezza organizzative, fisiche e logiche adottate e da adottare affinché siano rispettati gli obblighi in materia di sicurezza, devono essere conformi al Codice in materia di protezione dei dati personali, approvato con Dlgs. 30 giugno 2003 n.° 196, in particolare all'allegato B, al fine di assicurare la riservatezza e la salvaguardia dei dati personali trattati dall'Ente.

L'obbligo di tenere un aggiornato Documento Programmatico di Sicurezza è stato abrogato dal Decreto Legge n. 5 del 09/02/2012.

2 L'architettura dell'infrastruttura informatica

2.1 Caratteristiche dei locali

Il CED è situato al secondo piano della sede municipale ed è dotato di un apposito locale server con condizionatore. Considerata la posizione dell'edificio il rischio di allagamento è praticamente nullo. Il CED, quando non presidiato, è chiuso a chiave e la sede municipale è dotata di antifurto.

2.2 Connettività

1. Accesso ad Internet principale via ADSL
2. Sistemi di sicurezza perimetrale (*firewall*)

2.3 Server

Tre server sono situati in apposito locale, dotato di condizionatore, situato all'interno del CED. Il primo gestisce i dati del software gestionale Halley, il secondo gestisce i dati e il dominio comunale; il terzo gestisce l'intercambio dati con il distributore dei sacchetti per la raccolta differenziata. Un server infine, è dedicato alla continuità operativa per il software Halley (in allegato), dotato di condizionatore ed è posizionato in Ufficio demografici collocato al Piano terra dell'edificio comunale;

I primi 2 server:

1. Sono dotati di UPS (*Uninterruptible Power Supply*)
2. Possono funzionare con 1 alimentatore guasto e con 1 hard disk guasto.
3. Sono dotati di assistenza hardware per il ripristino in caso di guasto.

I rimanenti server:

1. Sono dotati di UPS (*Uninterruptible Power Supply*)
2. Sono dotati di assistenza hardware per il ripristino in caso di guasto.



2.4 Backup

Il backup per i dati del software Halley:

1. viene effettuato su cassette con caricatore automatico (*autoloader*).
2. I backup giornalieri vengono effettuati dal lunedì al venerdì, le cassette rimangono nell'*autoloader*. Il *rack* che lo contiene è dotato di serratura.

Il backup per i dati di rete di dominio e di interscambio con il distributore dei sacchetti per la raccolta differenziata:

1. Viene effettuato su *hard disk* removibili;
2. I backup giornalieri vengono effettuati dal lunedì al venerdì, il disco rimane nel PC e viene sostituito una volta alla settimana;

Per tutti i server i backup settimanali e mensili vengono conservati in cassetta ignifuga conservata presso l'ufficio dell'incaricato al salvataggio delle copie. Per tutelarsi in caso di perdita contemporanea dei dati e dei backup (ad esempio in caso di incendio, crollo, furto, atti di vandalismo), n. 1 backup del software Halley completo viene conservato fuori dalla sede principale.

2.5 Sistema di videosorveglianza del territorio

Il comune è dotato di un sistema di videosorveglianza del territorio, la gestione tecnica e della sicurezza è affidata a ditte esterne. Per motivi di sicurezza le reti del sistema informativo comunale devono essere separate da *firewall* dalle reti della videosorveglianza, che sono potenzialmente attaccabili dall'esterno.

È consentita la condivisione della connessione ad internet per motivi di assistenza tecnica, ma solo se in presenza di adeguata separazione (*firewall*).



3 Analisi delle minacce e delle vulnerabilità dell'infrastruttura informatica

Rischi		Descrizione dell'impatto sulla sicurezza
<i>Comportamenti degli operatori</i>	Sottrazione di credenziali di autenticazione	alto
	Carenza di consapevolezza, disattenzione, incuria	medio
	Comportamenti sleali o fraudolenti	alto
	Errore materiale	medio
<i>Eventi agli strumenti</i>	Azione di virus informatici o di programmi in grado di recare danno	medio
	<i>Spamming</i> o tecniche di sabotaggio	medio
	Malfunzionamento, indisponibilità o degrado degli strumenti	basso
	Accessi esterni non autorizzati	medio
<i>Eventi al contesto</i>	Accessi non autorizzati a locali/reparti ad accesso ristretto	medio
	Sottrazione di strumenti contenenti dati	medio
	Eventi distruttivi naturali o artificiali (movimenti tellurici, scariche atmosferiche incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	alto
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	basso
	Errori umani nella gestione della sicurezza fisica	medio



Comune di Rogno (Bg)
Manuale di gestione documentale – Allegato 14
Piano per la sicurezza informatica



4 Misure adottate per la protezione e la sicurezza dell'infrastruttura informatica

Vengono adottate delle misure per la protezione e la sicurezza dell'infrastruttura informatica e dei dati, incluse quelle previste dall'Allegato B - Disciplinare tecnico in materia di misure minime di sicurezza – del Codice in materia di protezione dei dati personali:

1. Autenticazione e autorizzazione degli accessi al sistema ed ai dati. In particolare le parole chiave devono avere una lunghezza minima di 8 caratteri ed una durata massima di 90 giorni, salvo che i dati non siano sensibili, in qual caso la durata può essere impostata su 180 giorni.
2. Antivirus con aggiornamento automatico.
3. Aggiornamenti *software*.
4. Backup: vedere 2.4 *Backup*.
5. Separazione della rete interna dalle reti esterne con *firewall*.
6. Non sono consentite connessioni fra reti interne e reti esterne non gestite all'amministratore di sistema.
7. Protezione fisica: quando non presidiato il locale CED/server rimane chiuso a chiave.
8. È consentita esclusivamente l'installazione di *software* per scopi di servizio.

5 Misure adottate per la disponibilità dei dati e la continuità del servizio

Al fine di consentire il ripristino dei dati e della funzionalità dei sistemi in caso di malfunzionamenti hardware, cancellazioni e/o modifiche accidentali dei dati, interruzioni della connessione ad internet, eventi eccezionali quali incendio, crollo, furto, atti di vandalismo, vengono adottate le seguenti misure, alcune delle quali già indicate in precedenza:

5.1 Server

Vedere: 2.3 *Server*

5.2 Backup

Vedere 2.4 *Backup*

6 Conservazione a norma

Viene effettuata la conservazione a norma del registro di protocollo.

Successivamente verrà attivata la conservazione a norma per tutti i dati che lo richiedono.