PIANO PER LA SICUREZZA INFORMATICA

ANNO 2016

Sommario

1. Introduzione

Il presente documento si propone di descrivere gli accorgimenti organizzativi e tecnici che il Comune di Monteforte d'Alpone mette in atto per applicare correttamente le misure di sicurezza previste dalla normativa.

Lo scopo di questo è di garantire la protezione del patrimonio informativo da accessi, modifiche, cancellazioni non autorizzate per cause accidentali o intenzionali e ridurne 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 server è situato al primo piano della sede municipale ed è dotato di un apposito armadio server e il locale è dotato di condizionatore.
Considerata la posizione al primo piano e la posizione dell’edificio il rischio di allagamento è praticamente nullo.
L’armadio-server è chiuso a chiave e la sede municipale è dotata di antifurto.

2.2 Connettività

- Accesso ad Internet principale via radio
- Sistemi di sicurezza perimetrale (firewall)

2.3 Server

I server sono situati in apposito locale, dotato di condizionatore, situato all’interno del Municipio.
I server:

- Sono dotati di UPS
- Possono funzionare con 1 alimentatore guasto e con 1 hard disk guasto
- Sono dotati di assistenza hardware per il ripristino in caso di guasto.

2.4 Backup

- Il backup giornaliero viene effettuato su cassette estraibili
- I backup giornalieri vengono effettuati dal lunedì al venerdì. L’armadio rack che contiene l’unità di backup è dotato di serratura.
- I backup giornalieri vengono conservati in un locale ubicato sullo stesso piano di quello che contiene l’armadio server. Tale locale è chiuso a chiave quando non presidiato.

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 all’Ufficio di Polizia Locale.
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		SI/NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Comportamenti degli operatori	**Sottrazione di credenziali di autenticazione**	**sì**	**alto**
	Carenza di consapevolezza, disattenzione o incuria	**sì**	**medio**
	Comportamenti sleali o fraudolenti	**sì**	**alto**
	Errore materiale	**sì**	**medio**
Eventi relativi agli strumenti	**Azioni di *virus informatici o di programmi suscettibili di recare danno***	**sì**	**medio**
	Spamming o tecniche di sabotaggio	**sì**	**basso**
	Malfunzionamento, indisponibilità o degrado degli strumenti	**sì**	**basso**
	Accessi esterni non autorizzati	**sì**	**medio**
Eventi relativi al contesto	**Accessi non autorizzati a locali/reparti ad accesso ristretto**	**sì**	**medio**
	Sottrazione di strumenti contenenti dati	**sì**	**medio**
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	**sì**	**alto**
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	**sì**	**basso**
	Errori umani nella gestione della sicurezza fisica	**sì**	**medio**

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:

- 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.

- Antivirus con aggiornamento automatico;
- Aggiornamenti software
- Backup: vedere 2.4 Backup
- Separazione della rete interna dalle reti esterne con firewall
- Non sono consentite connessioni fra reti interne e reti esterne non gestite dall'amministratore di sistema
- Protezione fisica: l'armadio che contiene il server è chiuso a chiave.

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, già indicate in precedenza:

5.1 Server

Vedere: 2.3 Server

5.2 Backup

Vedere: 2.4 Backup

5.3 Connessioni ad Internet

Per consentire la continuità delle operazioni che necessitano di collegamenti ad internet, fra le quali albo pretorio, conservazione del registro di protocollo, invio e ricezione delle PEC ecc., la sede municipale è dotata di una connessione via radio.

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.