

Documento di Valutazione del Rischio informatico

Questo documento descrive le più comuni tipologie di rischi che la casa filiale di Borgo San Lorenzo delle Povere figlie delle Sacre Stimmate potrebbe dover affrontare e i passi fondamentali che si possono adottare per attenuarli prima che si verifichi un danno.

#	Rischio	Descrizione	Probabilità	Severità	Passi da seguire
1	Disastro naturale	Un grave evento avverso derivante dai processi naturali che trasformano la Terra, come inondazioni, uragani, tornado, eruzioni vulcaniche, terremoti, tsunami e altri processi geologici. Un disastro naturale può causare perdite di vite umane e danni sostanziali alle risorse fisiche, come edifici e attrezzature. Le persone potrebbero non essere in grado di svolgere le proprie mansioni lavorative o, se possibile, potrebbero non essere in grado di operare al massimo dell'efficienza.	● Improbabile	● Catastrofico	
2	Guasto software	Un'applicazione o sistema non fornisce un servizio, come previsto dai propri utenti, a causa di errori nelle specifiche, nella progettazione o nell'implementazione.	● Improbabile	● Rilevante	<ol style="list-style-type: none">1. Identificare potenziali problemi prima che possano causare interruzioni all'operatività quotidiana.2. Scegliere soluzioni software di alta qualità offerte da fornitori con una solida esperienza in termini di affidabilità e assistenza clienti.

3	Guasto Hardware	Un malfunzionamento all'interno dei circuiti elettronici o componenti elettromeccaniche di un sistema informatico. La causa principale dei guasti al disco rigido è il surriscaldamento dell'hardware, che può causare gravi danni alle apparecchiature.	● Moderato	● Rilevante	1. Mantenere i backup più recenti di tutti i sistemi critici.
4	Corruzione dei dati	Errori o deterioramenti dei dati che si verificano durante la scrittura, la lettura, la memorizzazione, la trasmissione o l'elaborazione che introducono modifiche involontarie ai dati originali. Può causare una perdita di dati.	● Moderato	● Rilevante	1. Mantenere backup recenti di file critici. 2. Assicurarsi che ci sia sempre abbastanza spazio libero su disco.
5	Errore di backup dei dati	Errore nel processo di copiatura corretta di file o database, fisici o virtuali, su un sito secondario per la conservazione in caso di guasto dell'apparecchiatura o di altre catastrofi.	● Basso	● Critico	1. Eseguire regolarmente i test di verifica per verificare i backup. 2. Correggere eventuali problemi rilevati durante i test prima che siano necessari i backup.
6	Blackout elettrico	Una interruzione dell'energia elettrica a breve o lungo termine in una determinata area.	● Basso	● Basso	

7	Attacchi esterni (hacker, malware, etc.)	Persone che penetrano illegalmente in una rete di computer di un'azienda al fine di ottenere dati sensibili, o software malevoli progettati per interrompere le operazioni dei computer al fine di chiedere un riscatto o per altri motivi.	● Improbabile	● Critico	
8	Minaccia interna	Uso di credenziali valide da parte dei rispettivi proprietari, o intrusi, per sottrarre dati sensibili, quali generalità dei clienti, per vari scopi, quali la vendita o l'utilizzo ai danni del datore di lavoro.	● Improbabile	● Critico	
9	Errore umano	Comportamento umano che provoca l'introduzione di errori in un sistema, quali l'errata configurazione del sistema, la perdita di un dispositivo con dati sensibili o la divulgazione di informazioni tramite l'indirizzo di posta elettronica personale.	● Improbabile	● Rilevante	1. Sottoporre a backup le configurazioni e i dati critici.