4 MINACCE E TIPOLOGIE DI ATTACCO

4.1 Catalogo delle Minacce

Di seguito viene fornito un catalogo di massima delle minacce correlate alle informazioni e ai servizi erogati. L'elenco è stato costruito seguendo le linee guida dettate dallo standard ISO/IEC 27005:2011 "Information technology — Security techniques — Information security risk management", e più in generale lo standard ISO/IEC 27001:2013.

Le minacce sono state individuate e selezionate in base alla loro effettiva applicabilità nel contesto del presente documento, escludendo quindi quelle ritenute non applicabili.

ID	Minaccia
M01	Abuso di privilegi da parte dell'utente.
M02	Abuso di risorse.
M03	Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.).
M04	Accesso non autorizzato alle informazioni.
M05	Attacchi all'integrità dei sistemi (software e configurazioni).
M06	Attacchi all'integrità delle informazioni.
M07	Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
M08	Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
M09	Compromissione delle comunicazioni.
M10	Crittografia debole o non validata.
M11	Divulgazione di informazioni riservate.
M12	Errori di amministrazione dei sistemi.
M13	Falsificazione di identità.
M14	Furto di credenziali di autenticazione.
M15	Generazione e/o gestione inadeguata delle chiavi crittografiche.
M16	Negazione dei servizi.
M17	Tentativi di frode.
M18	Uso non autorizzato di privilegi.
M19	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.)
M20	Violazione di leggi, di regolamenti, di obblighi contrattuali.
M21	Danneggiamento, perdita o furto di un asset fisico.

Tabella 3 - Catalogo delle Minacce