Analisi dei rischi e misure di sicurezza informatica adottate

1. Ambito dell'analisi dei rischi – identificazione degli asset

Il focus della presente analisi dei rischi attiene ai documenti informatici ed ai rischi che insistono sulla sicurezza degli stessi (riservatezza, disponibilità ed integrità dell'informazione), rispetto ad un set di minacce identificato ed in considerazione del contesto operativo di trattamento nell'ambito delle soluzioni tecnologiche fornite da Insiel s.p.a in qualità di Responsabile del Trattamento ai sensi dell'art.28 del Regolamento UE 2016/679.

Ulteriori considerazioni rispetto ad altre tipologie di rischio possono essere derivate dalle stesse o essere ad esse collegate, in relazione al contesto di trattamento specifico operato dall'Ente in qualità di Titolare dei dati e alla natura delle informazioni presenti nei documenti stessi.

Tale contestualizzazione è in linea con quanto indicato dalla norma ISO/IEC 27005:2018, lo standard che fornisce alle organizzazioni le linee guida per la gestione efficace ed efficiente dei rischi relativi alla sicurezza delle informazioni, al fine di proteggere le proprie informazioni e quelle dei propri clienti.

Asset primario	Asset collegati – relativi ad attività in capo al responsabile INSIEL
Documento informatico	Sito di elaborazione dati – Data Center regionale
	Sistemi di elaborazione dati – HW/SW
	Reti di comunicazione
	Personale – Amministratori di Sistema
	Organizzazione interna - INSIEL
	Dati / file

2. Identificazione delle minacce / agenti di rischio

Gli asset considerati, collegati ai documenti informatici che costituiscono il patrimonio documentale del Titolare, sono sottoposti all'azione di diverse minacce.

Tra queste, le categorie di minacce considerate nella presente analisi del rischio rispetto all'ambito di riferimento identificato riguardano le diverse tipologie di asset considerati e sono di seguito riassunte:

Minaccia	Asset impattati
Danneggiamento fisico	Sito di elaborazione dati – Data Center regionale
	Sistemi di elaborazione dati – HW/SW
Eventi naturali	Sito di elaborazione dati – Data Center regionale
Perdita di servizi essenziali (alimentazione elettrica / connettività)	Sito di elaborazione dati – Data Center regionale
	Reti di comunicazione
Compromissione delle informazioni	Sistemi di elaborazione dati – HW/SW
	Dati / file
Guasti tecnici	Reti di comunicazione
	Sistemi di elaborazione dati – HW/SW
Azioni non autorizzate	Personale – Amministratori di Sistema

	Organizzazione interna - INSIEL
Attacchi informatici	Sistemi di elaborazione dati – HW/SW
	Reti di comunicazione
	Dati / file
Errori	Personale – Amministratori di Sistema
	Organizzazione interna - INSIEL

Tali minacce, nella presente analisi del rischio, sono tutte considerate come aventi alto impatto sull'asset primario oggetto della stessa, ovvero il documento informatico, e il Responsabile del Trattamento prevede quindi di adottare misure di sicurezza che vadano ad indirizzarne la totalità, nella consapevolezza che nessuna contromisura può annullare il rischio connesso ad una qualsiasi minaccia e che la sicurezza sia sempre da considerarsi come un processo continuo ed un percorso.

3. Identificazione delle contromisure

A livello generale, e nella consapevolezza che un qualsiasi rischio informatico connesso ad una specifica minaccia non potrà mai essere annullato, Insiel s.p.a. in qualità di Responsabile del Trattamento si è dotata di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
Scendendo a livello particolare, in considerazione delle minacce identificate al punto precedente, vengono esplicitate le seguenti misure di sicurezza. Tali contromisure sono esplicitate a livello di sintesi, richiamando il livello di dettaglio alla documentazione, ai sistemi tecnologici, alle procedure, nonché ad ogni altra evidenza riscontrabile e gestita da Insiel s.p.a. in qualità di Responsabile del trattamento.

Minaccia	Asset impattati	Misure di sicurezza implementate
Danneggiamento fisico	Sito di elaborazione dati – Data Center regionale	Controllo accessi fisici al data center regionale: sono implementate specifiche procedure per il controllo accessi, accompagnate da idoneo supporto tecnologico in relazione a: sistemi di controllo accessi/badge, servizio di guardiania, sistemi di videosorveglianza, monitoraggio e presidio 7x24.
	Sistemi di elaborazione dati – HW/SW	Controllo accessi fisici al data center regionale: sono implementate specifiche procedure per il controllo accessi, accompagnate da idoneo supporto tecnologico in relazione a: sistemi di controllo accessi/badge, servizio di guardiania, sistemi di videosorveglianza, monitoraggio e presidio 7x24.
Eventi naturali	Sito di elaborazione dati – Data Center regionale	Sistemi di protezione dei locali del data center regionale a fronte di allagamento, incendio
Perdita di servizi essenziali (alimentazione elettrica / connettività)	Sito di elaborazione dati – Data Center regionale	Ridondanza delle componenti di alimentazione nei singoli sistemi tecnologici, ridondanza dei sistemi tecnologici. Presenza di sistemi a garanzia della continuità elettrica, presenza di procedure di emergenza a supporto. Monitoraggio e presidio 7x24.

	Reti di comunicazione	Ridondanza interna delle componenti delle apparecchiature, ridondanza degli apparati e delle linee di comunicazione
Compromissione delle informazioni	Sistemi di elaborazione dati – HW/SW	I sistemi applicativi sono progettati per realizzare i requisiti funzionali richiesti dalla committenza e sono sottoposti a test funzionali specifici. Sono presenti sistemi di backup / restore volti a garantire il ripristino della disponibilità / integrità delle informazioni gestite, in base agli accordi vigenti.
	Dati / file	È presente un servizio di assistenza volto a supportare l'utente nella risoluzione di problematiche specifiche, anche connesse alla qualità del dato. Sono presenti sistemi di backup / restore volti a garantire il ripristino della disponibilità / integrità delle informazioni gestite, in base agli accordi vigenti.
Guasti tecnici	Reti di comunicazione	Ridondanza interna delle componenti delle apparecchiature, ridondanza degli apparati e delle linee di comunicazione Presenza di competenze interne specialistiche e contratti di manutenzione a copertura dei vari layer tecnologici.
	Sistemi di elaborazione dati – HW/SW	Ridondanza delle componenti di alimentazione nei singoli sistemi tecnologici, ridondanza dei sistemi tecnologici. Presenza di competenze interne specialistiche e contratti di manutenzione a copertura dei vari layer tecnologici.
Azioni non autorizzate	Personale – Amministratori di Sistema	Gli Amministratori di Sistema sono identificati e designati formalmente. Le attività ammesse sono definite da apposito regolamento reso disponibile a tutto il personale. È presente un sistema di controllo accessi fisici ai locali di INSIEL. È presente un sistema di controllo degli accessi logici ai sistemi ed alle reti accedute dal personale
	Organizzazione interna -	Le responsabilità ed i compiti nell'ambito dell'azienda

	INSIEL	sono definite ed assegnate.
Attacchi informatici	Sistemi di elaborazione dati – HW/SW	Sono posti in essere sistemi di protezione antimalware, nei contesti previsti. Sono posti in essere apparati di sicurezza come dispositivi di firewalling, di *intrusion prevention (*IPS). Tutti i sistemi sono gestiti da personale specializzato.
	Reti di comunicazione	Le reti sono segmentate per ridurre il rischio di collegamenti non desiderati tra entità diverse. Sono posti in essere apparati di sicurezza come dispositivi di firewalling, di *intrusion prevention (*IPS)
	Dati / file	I contesti applicativi che danno accesso ad informazioni che presentano requisiti di riservatezza sono protetti da sistemi di autenticazione / autorizzazione
Errori	Personale – Amministratori di Sistema	Viene curata la formazione tecnica del personale addetto. Inoltre, nell'ambito del SGSI certificato secondo la norma ISO/IEC 27001, sono previste periodiche sessioni formative specifiche sulla sicurezza delle informazioni
	Organizzazione interna - INSIEL	Sono in atto specifici processi volti a gestire le diverse casistiche di *incident* in ottemperanza agli accordi contrattuali vigenti, nonché è incentivato il processo di miglioramento continuo anche in ossequio ai diversi *sistemi di gestione certificati* presenti in INSIEL. In caso di incidenti che implichino una violazione dei dati personali (*data breach*), INSIEL si è dotata di una specifica procedura di gestione degli stessi, che tiene conto anche dei tempi di segnalazione concordati con i Titolari.

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: CHITTARO MICHELA
CODICE FISCALE: CHTMHL81E65L483T
DATA FIRMA: 02/07/2025 13:16:06
IMPRONTA: 3CF52882C5A92004C493E41EE20E65E5E77DFD60FC03E7F7206687FB2410875B
E77DFD60FC03E7F7206687FB2410875B47583146EA6D98A9733FE53B618A8A77
47583146EA6D98A9733FE53B618A8A771B85836F64D229D35B005407B19EE93C
1B85836F64D229D35B005407B19EE93C42BC72ECDEE2EDB9596A4137555325FD