Allegato

Politica per la gestione dei servizi

Storicità del documento

Major Release	Azione	Funzione Aziendale	Data
1	Redatto	COMP, PROCE	23/01/2025
	Verificato	COMP	24/01/2025
	Pubblicato	PROCE	28/01/2025

Storico delle modifiche

Major Release	Minor Release	Data di pubblicazione	Motivo della revisione
1	0	28/01/2025	Prima emissione

1. Politica per la Gestione dei Servizi

Come Direzione di Kirey Advisory S.r.l. intendiamo proteggere le informazioni da un ampio spettro di minacce allo scopo di assicurare la continuità delle nostre attività, minimizzare i rischi, garantire il ritorno dagli investimenti, le opportunità di business, il rispetto delle leggi, la redditività. Tutti i dati e le relative elaborazioni per la gestione delle nostre attività devono essere protetti per garantire che giungano integre a chi deve utilizzarle,che non vadano disperse o peggio ancora che non finiscano nelle mani di concorrenti o di approfittatori.

L'Informazione è un Asset, e come altri Asset materiali o immateriali è essenziale per l'organizzazione Kirey Advisory; come tale ha anche bisogno di essere protetta. Le protezioni sono tanto più necessarie quanto più l'interconnessione è ampia, la qual cosa espone l'Informazione ad una più larga varietà di rischi e di vulnerabilità: frodi, spionaggio, vandalismi, incidenti.

Noi tutti dobbiamo essere consapevoli del problema e ci impegniamo a condividere gli obiettivi ed i principi della sicurezza delle informazioni. Sulla struttura organizzativa e sui processi in essere in Kirey Advisory è stato integrato il SGS cioè un sistema di operazioni e di controlli per gestire il rischio relativo alle informazioni.

In particolare, con l'implementazione di questo sistema:

- Vengono analizzati i rischi;
- Vengono trattati i rischi sulla base di criteri di accettazione dei rischi stessi, in ogni caso non compromettendo il rispetto delle leggi dello Stato ed i requisiti contrattuali.
- Pertanto:
  - Accettiamo consapevolmente i rischi se soddisfano quei criteri;
  - Evitiamo i rischi non permettendo azioni/attività che potrebbero essere causa dei rischi stessi;
  - Oppure trasferiamo i rischi a terze parti.
- Rendiamo consapevoli tutti noi della necessità di operare responsabilmente mediante formazione a tutti i livelli;
- Introduciamo specifiche attività di controllo e abbiamo preso precauzioni contro i disastri;
- Prenderemo adeguati provvedimenti ogni qualvolta si verificheranno delle violazioni;
- Questo sistema include:
  - Il monitoraggio di tutti gli eventi con la verifica dell'efficacia dei controlli prescritti ed il successivo riesame;
  - L'attivazione di azioni di miglioramento;
  - La gestione della documentazione e delle registrazioni di sistema;
  - L'addestramento di tutto il personale per conseguire competenza e consapevolezza sulle problematiche della sicurezza delle informazioni;
  - Audit interni per verificare che i controlli sono efficaci, gli obiettivi dei controlli vengono raggiunti e che le procedure vengono applicate: in sintesi che il SGS sia conforme alla norma di riferimento ISO/IEC 27001 ed alla ISO/IEC 20000-1:2018;
  - Il Riesame della Direzione;
  - Il miglioramento con Azioni Correttive e di Miglioramento.

Nell'ambito di questo sistema sono assegnate le seguenti responsabilità:

- Alla Direzione, per definire il Dominio degli Asset da proteggere;

- Al Responsabile SGS per valutare i rischi cui possono essere esposti i vari Asset;
- Al Responsabile SGS per impostare i controlli, di implementarli e monitorarli;

- Al Responsabile SGSI di registrare tutte le minacce verificate, pianificare e implementare nuovi controlli;
- Ad ogni Dipendente, perché si attenga alle autorizzazioni prescritte e segnali al Responsabile SGSI eventuali minacce riscontrate;
- Alla Direzione, di riesaminare periodicamente lo stato di sicurezza delle informazioni e l'efficacia della presente politica;
- Al Responsabile SGSI di intraprendere azioni di miglioramento.