Allegato

Politica per la gestione dei servizi

Storicità del documento

Major Release	Azione	Nominativo	Data
1	Redatto	Antonio Moscato, Lisa Vaccarino	09/06/2021
	Verificato	Antonio Moscato	28/07/2021
	Approvato	Antonio Moscato	30/08/2021
	Pubblicato	Compliance	30/08/2021
2	Redatto	Marco Cassaro, Paola Calabrese	13/12/2022
	Verificato	Vincenzo Biase, Marco Cassaro	12/01/2023
	Approvato	Vincenzo Biase, Marco Cassaro	20/01/2023
	Pubblicato	ORG	20/01/2023

Storico delle modifiche

Major Release	Minor Release	Data di pubblicazione	Motivo della revisione
1	0	30/08/2021	Prima emissione
2	0	20/01/2023	Revisione interna

Lista di distribuzione

Data	Versione	Aziende	Persone
30/08/2021	1	Insirio Srl	Direzione e Dipendenti
20/01/2023	2	Insirio Srl	Direzione e Dipendenti

Politica per la Gestione dei Servizi

Come Direzione di Insirio srl 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 Insirio srl; 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 Insirio srl è stato integrato il SGSI 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 SGSI sia conforme alla norma di riferimento ISO/IEC 27001:2013 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 SGSI, per valutare i rischi cui possono essere esposti i vari Asset;
- Al Responsabile SGSI 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.