Politica per la Sicurezza delle Informazioni

SGSI

revisione	data	emissione	approvazione
n° 6	15/10/2024	RGSI	DIR

REVISIONI:

CODICE ISIM001		
REV.	**DATA**	**DESCRIZIONE**
1	27/02/12	Prima Emissione
2	08/02/17	Inserimento di riferimenti sull'importanza di garantire la compliance allo standard PCI DSS
3	17/03/2020	Inserimento riferimenti alle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019
4	16/01/23	Eliminazione dei riferimenti ai requisiti PCI-DSS, in quanto non più applicabili, e ai criteri di accettazione del rischio.
5	15/01/2024	Inserimento riferimenti alla nuova versione della norma ISO/IEC 27001:2022
6	15/10/2024	Estensione del documento alla società B2X.

DOCUMENTI DI RIFERIMENTO:

[1] ISIM008 – Riferimenti a normative e standard applicabili.

INDICE DEL DOCUMENTO

Politica per la sicurezza delle informazioni

Obiettivo del Gruppo ISED (composto dalle società ISED S.p.A. e B2X S.r.l.) nell'ambito della sicurezza delle informazioni è garantire:

1. la raccolta, l'interpretazione delle esigenze operative dei Clienti e la definizione di opportune policy per la gestione delle soluzioni IT;
2. la realizzazione ed il governo di infrastrutture tecnologiche complesse intese come fattore abilitante di soluzioni di Business dei Clienti.

Il principale obiettivo dell'Organizzazione è fornire con rapidità e prontezza tutte le risposte che l'utenza richiede attraverso un costante contatto con il Cliente, al fine di garantire:

- qualità e disponibilità del servizio concordato;
- efficacia dei metodi preventivi e reattivi per la verifica dello stato di sicurezza;
- efficacia dei metodi relativi alla gestione e configurazione dei dispositivi di sicurezza;
- efficacia dei metodi preventivi e reattivi per la gestione degli incidenti di sicurezza;
- ascolto attivo dell'utenza per un servizio di qualità;
- trasparenza dei Processi IT;
- miglioramento continuo ed innovazione;
- garanzia della continuità del business attraverso la protezione ed il tempestivo recupero dei processi critici dagli effetti di malfunzionamenti dei Sistemi Informativi o di disastri.

In considerazione dell'importanza strategica della sicurezza delle informazioni, delle reti e dei sistemi IT, Il Gruppo ISED si è dotato di una politica di alto livello per strutturare le linee guida di un percorso volto al miglioramento della gestione della sicurezza delle informazioni.

Enunciato

La gestione della sicurezza delle informazioni costituisce una priorità di alto livello all'interno della **"Mission"** aziendale, ove si attribuisce importanza strategica al trattamento delle informazioni e concretizza la volontà di difendere la riservatezza, l'integrità e la disponibilità dei dati.

Per questo scopo, Il Gruppo ISED riconosce la necessità di sviluppare, mantenere, controllare e migliorare in modo costante un Sistema di Gestione della Sicurezza delle Informazioni (di seguito, per brevità, SGSI), in conformità alla norma ISO 27001:2022, estesa alle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

Gli obiettivi principali del SGSI si concretizzano nell'assicurare:

- la riservatezza del patrimonio informativo gestito: proprietà per cui l'informazione non è resa disponibile o comunicata ad individui, entità o processi non autorizzati;
- l'integrità del patrimonio informativo gestito: proprietà di tutelare l'accuratezza e la completezza degli asset, ossia di qualsiasi informazione o bene attinente a cui il Gruppo ISED attribuisce un valore;
- la disponibilità del patrimonio informativo gestito: proprietà per cui l'informazione deve essere accessibile ed utilizzabile previa richiesta di una entità autorizzata;
- l'ottemperanza ai requisiti cogenti, del quadro normativo di riferimento e contrattuali;
- l'ottemperanza ai requisiti previsti in tema di trattamento dei dati personali, dalla legge (es. GDPR, d.lgs 101/2018, ecc.), dalle norme di riferimento (es. ISO/IEC 27018:2019, ecc) e dai requisiti contrattuali;
- la redazione, l'aggiornamento e il controllo di piani per la continuità dell'attività del Gruppo ISED;
- l'adeguata formazione in tema di sicurezza delle informazioni del personale;
- la corretta gestione di tutte le violazioni della sicurezza delle informazioni, compresi i data breach, e dei possibili punti deboli, al fine di una corretta rilevazione ed indagine;
- la definizione appropriata dei requisiti di sicurezza condivisi con i clienti dei servizi cloud, in conformità alla norma ISO/IEC 27017:2015.

In questa ottica, il Gruppo ISED è consapevole che la sicurezza delle informazioni è un processo culturale complesso che deve coinvolgere tutte le risorse umane ed organizzative.

Applicabilità

La Politica per la Sicurezza delle Informazioni, si applica a tutto il personale del Gruppo ISED, alle aziende Partners, ai Fornitori, Clienti o Terze Parti sotto contratto, coinvolti nel trattamento delle informazioni o che abbiano accesso agli uffici del Gruppo ISED. A titolo esemplificativo, coloro che:

- Operano su sistemi ed asset di proprietà dell'azienda;
- Entrano in possesso di informazioni relative all'organizzazione;
- Entrano negli uffici del Gruppo ISED;
- Si trovino ad operare in aree classificate o sensibili (e.g. aree CED, locali riservati, etc…)

Obiettivo

Il Gruppo ISED si propone il raggiungimento dei seguenti obiettivi:

- identificare una metodologia di valutazione del rischio adeguata al SGSI, ai requisiti di business individuati, a quelli cogenti e normativi;
- identificare attraverso una idonea analisi dei rischi, il valore del patrimonio informativo, all'interno del campo di applicazione del SGSI, al fine di comprendere le vulnerabilità e le possibili minacce che possano esporlo a rischi;
- gestire il rischio ad un livello accettabile ed in modo allineato al più generale contesto di gestione del rischio strategico dell'organizzazione;
- definire e rendere effettive le linee operative per una architettura di sicurezza intesa come l'insieme di regole, funzioni, strumenti, oggetti e controlli, coerentemente disegnati e resi funzionanti, che garantiscano in ogni struttura organizzativa, ambiente informatico, singolo elaboratore, il rispetto degli standard definiti dal Gruppo ISED;
- controllare, cogliendo ogni spunto di miglioramento, il sistema attuato;
- gestire in modo corretto il trattamento dei dati personali sia nei casi in cui le aziende del Gruppo ISED operano come titolare del trattamento sia nei casi in cui operano come responsabile;
- assicurare il rispetto dei requisiti di sicurezza previsti per i servizi cloud concordati con i clienti.

Responsabilità

La presente politica viene emessa e riesaminata dal Responsabile SGSI del Gruppo ISED (RSGSI), che è anche Responsabile della Gestione del Sistema Integrato aziendale (RGSI), per espressa delega del Consiglio di Amministrazione o di un suo rappresentante.
Il Responsabile SGSI designato dall'Organizzazione facilita l'attuazione della presente politica attraverso norme e procedure appropriate. Tutto il personale ed i fornitori devono seguire le procedure stabilite dal Gruppo ISED per la politica della sicurezza delle informazioni.

Tutto il personale, in base alle proprie conoscenze, ha la responsabilità di riferire al Responsabile SGSI qualsiasi punto debole individuato. Qualsiasi azione, che in modo intenzionale o riconducibile a negligenza provocherà un danno al Gruppo ISED, potrà essere perseguita nelle opportune sedi.

Riesame

La presente politica viene riesaminata regolarmente ed all'attuazione di modifiche che la influenzano, per accertarsi che permanga idonea alle finalità del Gruppo ISED, alle aspettative degli utenti e di tutte le parti interessate.

Riferimenti agli aspetti cogenti e ai regolamenti

Per il Gruppo ISED riveste assoluta importanza, l'idoneità ai requisiti cogenti e regolamentari. La presente politica, in questo particolare ambito, si pone i seguenti traguardi:

- assicurare che siano identificati ed aggiornati tutti i requisiti cogenti e regolamentari applicabili;
- assicurare che questi requisiti siano utilizzati come "dati di ingresso ai processi" e che ne sia riscontrata la conformità nell'ambito del monitoraggio sui "dati di uscita dai processi", con particolare riferimento alle attività di audit interno;
- assicurare che l'organizzazione dimostri adeguatamente la conformità ai requisiti cogenti e regolamentari applicabili.