...making excellence a habit.

Gestione della sicurezza e della conformità tramite un SGSI

Approccio olistico alla gestione di ISO/IEC 27001, data protection, privacy e PCI DSS

Introduzione

Lo scopo del presente documento è quello di fornire un approfondimento su come un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) possa essere utilizzato per applicare un approccio olistico alla gestione degli standard di sicurezza e degli obblighi di conformità, come ISO/IEC 27001, PCI DSS e privacy.

Grazie all'utilizzo di un solo sistema per la gestione degli obblighi di conformità normativi e legislativi per la sicurezza delle informazioni, le organizzazioni possono contare sull'identificazione di requisiti comuni, maggiore efficienza, visibilità e fiducia. Per ottenere tutto questo, consigliamo l'adozione del modello riconosciuto a livello internazionale ISO/IEC 27001 – Sistemi di Gestione per la Sicurezza delle Informazioni.

ISO/IEC 27001

ISO/IEC 27001 come SGSI

ISO/IEC 27001 è un sistema di gestione riconosciuto a livello internazionale per la gestione dei rischi legati alla sicurezza delle informazioni.

Lo standard fornisce un framework comune, descrivendo I requisiti chiave per implementare un efficace SGSI.

I requisiti fanno riferimento alla governance e alla buona gestione del sistema e intendono assicurare:

- Conoscenza e comprensione continua del contesto organizzativo e delle necessità delle parti interne ed esterne coinvolte
- Leadership e coinvolgimento da parte del senior management per garantire il rispetto delle policy e la corretta allocazione di risorse e responsabilità
- Pianificazione in linea con il SGSI e con gli obiettivi dell'organizzazione
- Supporto e risorse disponibili per il corretto funzionamento del sistema
- Gestione dei rischi appropriata rispetto al rischio aziendale e ai fattori di rischio interni ed esterni all'organizzazione
- Monitoraggio e miglioramento continuo del sistema

L'Annex A dello standard, contiene 114 controlli che possono essere utilizzati per indirizzare le azioni di gestione dei rischi per la sicurezza delle informazioni.

Utilizzare un SGSI ISO/IEC 27001 per gestire una gamma più ampia di requisiti normativi e legali di settore

In aggiunta ai controlli suggeriti, ISO/IEC 27001 richiede che gli obblighi in materia normativa e legale siano compresi e incorporati nel sistema di gestione. In questo caso, vengono presi in considerazione la data protection e il PCI DSS. Il presente documento contiene un'analisi approfondita rispetto a tale connessione.

Privacy

Il nuovo Regolamento UE in materia di Data Protection (General Data Protection Regulation - GDPR) avrà valore esecutivo entro maggio 2018. La normativa fonda le sue radici nell'attuale direttiva per la protezione dei dati e, sebbene non presenti molte differenze rispetto agli attuali principi di data protection, introduce nuovi concetti che devono essere integrati all'interno dei programmi di conformità delle organizzazioni.

La normativa si applica nello specifico nelle seguenti aree:

- Processi di gestione del rischio rinforzati, che includono la privacy tra le principali preoccupazioni
- Obblighi e responsabilità
- Comunicazione con clienti e personale
- Diritto alla privacy e procedure di supporto
- Richieste di cambiamento degli accessi
- Consenso e basi legali
- Gestione dei dati dei minori
- Notifica di violazione dei dati
- Privacy Impact Assessment (PIA) e "Privacy by design"
- Data Protection Officer (DPO)
- Trasferimento di dati a livello internazionale

È comunemente accettato che il GDPR sia uno strumento complesso e abbia un peso non indifferente date le basi normative su cui si fonda. Non è semplice interpretare il GDPR in azioni concrete.

L'approccio comunemente adottato dalle organizzazioni è allineare il proprio sistema rispetto ad uno standard internazionale per la privacy. Standard come ISO 29001 e BS 10012 forniscono un robusto modello di riferimento per la gestione della privacy*. In questo contesto, affidarsi al SGSI ISO/IEC 27001 incorporando i controlli di riferimento degli standard sopra elencati, può portare ad una maggiore efficienza e a un modello centralizzato di conformità.

** Si tenga in considerazione le eccezioni implicite nelle normative come il GDPR, dove specificato, e che la sola certificazione rispetto ad uno standard non costituisce di per sè evidenza di conformità alla normativa. Sono da considerare ad esempio le tempistiche necessarie per notificare le violazioni dei dati, particolari categorie di dati personali sensibili, ruoli e responsabilità del DPO, sanzioni, ecc.*

Payment Card Industry Data Security Standard (PCI DSS v3.2)

Il Payment Card Industry Data Security Standard, comunemente conosciuto come PCI DSS, fornisce un set di controlli specifici obbligatori per la protezione delle informazioni legate alle carte di credito.

Questo tipo di controlli è allineato a quelli dell' Annex A di ISO/IEC 27001 ma ha un valore maggiormente prescrittivo, includendo requisiti molto dettagliati, opposti all'utilizzo dell'approccio risk based per la selezione dei rischi applicabili. Utilizzare il sistema di gestione ISO/IEC 27001 per la gestione del PCI DSS rappresenta una soluzione relativamente continuativa, grazie alla sovrapposizione dei requisiti dell'Annex A.

Molte organizzazioni conformi al PCI DSS scelgono la certificazione ISO/IEC 27001, dato che l'implementazione dei suoi requisiti non comporta praticamente costi aggiuntivi e può essere gestita insieme al PCI DSS.

Lo scopo è un fattore chiave

Lo scopo è un fattore chiave quando si tratta di certificare un sistema rispetto ad uno standard. In molti casi, le organizzazioni avranno uno specifico servizio, reparto o insieme di sistemi certificati rispetto ad uno standard, piuttosto che l'intera organizzazione. Questo è spesso dovuto ai costi e alle risorse necessarie al mantenimento dei processi di governance, così come ai costi associati ai software e alle licenze dei sistemi di sicurezza. È consigliabile definire un livello minimo di sicurezza per tutta l'organizzazione, però tale livello dovrebbe essere maggiore nel caso di asset/sistemi/servizi in cui i livelli di rischio sono più alti. Questo serve tipicamente in tutti quegli ambiti che:

- Generano revenue
- Sono soggetti a controlli normativi
- Interagiscono con le informazioni personali o le informazioni legate alle carte di credito
- Contengono proprietà intellettuale
- Sono gestiti in internet

Quindi, quando si considera lo scopo del sistema di gestione, le organizzazioni dovrebbero allocare le giuste risorse necessarie al buon funzionamento del sistema. ISO 27001 consente la gestione di tale processo, attraverso il controllo dell'"asset management", dove l'inventario e la classificazione di informazioni e servizi gioca un ruolo fondamentale.
Attraverso la comprensione delle informazioni a disposizione, dove e con che strumenti gestirle, è possibile identificare e classificare i sistemi che hanno un ruolo chiave nell'organizzazione.

L'inventario degli asset diventa la principale fonte per determinare le priorità del sistema di gestione, mentre la classificazione delle policy definisce il modo in cui questi sistemi devono essere protetti. Ad esempio, tutti i sistemi possono avere un livello di sicurezza minimo definito, ma nel caso in cui un sistema immagazzina dati relativi a carte di credito o informazioni sensibili, la policy per la classificazione può stabilire che questo tipo di informazione deve essere crittata. Questo tipo di controllo è presente in numerosi requisiti di conformità, inclusi:

1. **ISO 27001**

- A 8.1.1 Inventory of Assets
- A 8.2.1 Classification of Information

2. **PCI DSS v3.2**

- Executive Summary Section 3, 4.3,
- (2.4) Maintain an inventory of system components that are in scope for PCI DSS.

3. **GDPR**

- Articolo 30

Nello scenario sopra indicato, le policy di classificazione e inventario possono essere utilizzate per soddisfare i requisiti di inventario nelle tre aree di conformità sopra citate. Forniscono:

- Un'unica fonte per l'inventario di sistemi e informazioni
- Un approccio consistente per gestire:
  - La classificazione delle informazioni
  - La gestione delle informazioni
  - Il mantenimento delle informazioni
  - La cancellazione delle informazioni

- La sicurezza delle informazioni
- Le richieste di accesso

Di conseguenza, l'organizzazione sarà in grado di rivedere e mantenere un set documentale legato alla governance, garantire la conformità e dimostrare che gli obblighi normativi sono gestiti in modo appropriato.

Classificiazione e inventario non sono gli unici ambiti che coinvolgono tutte e tre le aree. Consideriamo inoltre:

- Governance, ruoli e responsabilità
- Valutazione del rischio
- User awareness
- Controllo degli accessi
- Logging e monitoring
- Incident response e notifica di violazione dei dati
- Change control (privacy by design e privacy impact assessment)
- Gestione di terza parte

Ci sono molte altre aree che si sovrappongono all'interno dei tre requisiti, che devono essere gestite singolarmente.

Conclusioni

La sicurezza delle informazioni è più funzionale se gestita dal board e dai livelli senior executive dell'azienda, dove i responsabili hanno una visione di insieme e la possibilità di delegare ruoli e responsabilità.
Includendo il senior management nella valutazione di rischi e conformità, possono essere prese decisioni strategiche ragionate per la sicurezza delle informazioni, garantendo una maggiore efficienza del sistema.

Un Sistema di Gestione per la Sicurezza delle Informazioni ti aiuta a identificare le opportunità di integrazione dei diversi requisiti e allocare correttamente ruoli e responsabilità. Fornisce solidità e visibilità rispetto all'approccio alla gestione dei rischi e alla governance dell'organizzazione attraverso una punto di vista centralizzato.

- Effettua decisioni informate e garantisci la conformità rispetto ai requisiti normativi
- Risparmia tempo e risorse grazie alla gestione contemporanea di tre diversi programmi di conformità attraverso un unico sistema di gestione.

References

Data Protection Commissioner: https://www.dataprotection.ie/docs/Home/4.htm

Information Commisioner's Office: https://ico.org.uk/

PCI Security Council: https://www.pcisecuritystandards.org/

Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/

International Organization for Standardization: https://www.iso.org/home.html

European Commission: ec.europa.eu/

Cybersecurity e Information Resilience

I nostri servizi in ambito Cybersecurity e Information Resilience consentono alle organizzazioni di mettere in sicurezza le informazioni dagli attacchi informatici, rafforzare l'Information Governance e mitigare i rischi agendo sulle vulnerabilità dell'infrastruttura critica. Aiutiamo le organizzazioni a gestire le sfide nell'ambito della sicurezza delle informazioni:

Consulenza

Cybersecurity e information resilience, security testing e supporto specialistico

Formazione

Corsi di formazione specialistici per la crescita professionale

Ricerca

Ricerche di mercato e progetti di horizon scanning

Soluzioni tecniche

Soluzioni cloud per supportare la tua organizzazione

Our expertise is supported by:

CREST · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR · CYBER ESSENTIALS · CSA cloud security alliance SM

bsi.

Scopri di più

T: +39 02 6679091

E: marketing.italy@bsigroup.com

W: bsigroup.it