DataVerso

Protezione e governance per il patrimonio delle informazioni

CyberGO

Cybersecurity and Governance to drive your business

SERVIZI DI CONSULENZA PER LA MESSA IN SICUREZZA DEL PATRIMONIO INFORMATIVO

Servizio in collaborazione con

MOTI-F Srl | VIA BENEDETTO CROCE, 34 – 00142 ROMA

T-CONSULTING Srl | VIA LUIGI GALVANI, 27 – 47122 FORLI'

SOLUZIONI S.R.L. | VIA COGNE, 25 - 40026 IMOLA (BO)

INTRODUZIONE

Protezione e governance del patrimonio delle informazioni

Nell'economia basata su innovazione, velocità, globalizzazione e conoscenza, il patrimonio delle informazioni costituisce uno dei principali fattori necessari ad ogni organizzazione per perseguire i propri obiettivi e per produrre valore, costruendo la propria differenziazione di mercato.

Tuttavia, il processo di valorizzazione delle informazioni - quale componente del patrimonio aziendale – richiede un efficace sistema di governo (c.d *data governance*) che includa con modalità correlate:

- la gestione operativa delle informazioni (c.d. *data management*);
- la sicurezza delle informazioni.

In particolare, con *data governance* si fa riferimento alla disciplina che si occupa di definire i ruoli, i processi e le tecnologie necessarie per gestire e proteggere i dati aziendali, creando di fatto un nesso tra la fase puramente strategica e quella operativa.

Il *data management* riguarda le fasi operative di gestione delle informazioni, facendo specifico riferimento ai processi utilizzati per pianificare, definire, abilitare, creare, acquisire, mantenere, utilizzare, archiviare, recuperare, controllare ed eliminare i dati e le informazioni.

In relazione al valore delle informazioni e al loro ruolo chiave per lo sviluppo di ogni organizzazione, la distruzione, la divulgazione illegittima di un'informazione di business o l'accadimento di ogni altro rischio connesso alla gestione delle informazioni aziendali produce sempre e comunque un danno all'organizzazione, per cui diventa indispensabile individuare e adottare le misure per porre in sicurezza il patrimonio delle informazioni aziendali.

> *La valorizzazione del patrimonio delle informazioni - cruciale per il successo sostenibile di ogni impresa - richiede un sistema di data governance che assicuri una gestione integrata di tutte le attività aziendali che riguardano le informazioni, nell'ambito di un'impostazione organizzativa unitaria.*

Ciò consente di disporre – nel modo meno oneroso – di vantaggi fondamentali per la creazione di valore in ogni organizzazione, tra cui si possono segnalare: supporto informato al processo decisionale (tra cui la pianificazione, la programmazione e il controllo, strumenti necessari per la prevenzione della crisi e dell'insolvenza d'impresa), semplificazione ed efficacia organizzativa, *stakeholder engagement* (fondamentale per ogni percorso di sostenibilità d'impresa).

> *Per poter offrire una risposta unitaria a queste esigenze - rilevanti per ogni organizzazione – è stata definita la suite **DataVerso** - protezione e governance del patrimonio delle informazioni.*

È una linea di servizi integrati di consulenza e formazione dedicati alla tutela e alla valorizzazione delle informazioni aziendali, inclusi gli adempimenti normativi correlati.

Tutti i servizi DataVerso sono fondati su una visione d'insieme della gestione delle informazioni, caratterizzati dall'approccio unitario aziendale e coordinabili in base alle specifiche esigenze di ogni organizzazione, grazie alle esperienze e alle competenze multidisciplinari dei consulenti.

> ***DataVerso** consente alle aziende di evitare di ripetere interventi in ambiti simili, in risposta a singole necessità di performance e/o di compliance, potendo attuare – in relazione al governo e la tutela del patrimonio informativo - le scelte più funzionali per coniugare in modo unitario il supporto al raggiungimento degli obiettivi di performance e l'assolvimento degli obblighi normativi (tra i quali si evidenziano le prescrizioni imposte dalla Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione – Direttiva NIS 2 –, dalla Legge del 28/06/2024 n. 90 – Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, nonché le segnalazioni previste dalla norma sul Whistleblowing).*

TERMINOLOGIA

Sicurezza delle informazioni (Information security)

Riguarda la sicurezza del patrimonio informativo nel suo complesso, facendo riferimento alla protezione dei dati in qualsiasi forma, anche non digitale, includendo anche aspetti organizzativi e di sicurezza fisica.

La sicurezza delle informazioni è caratterizzata dalla salvaguardia della riservatezza, integrità e disponibilità delle informazioni gestite dall'azienda, tenendo conto che la salvaguardia non è riferita solo ad attacchi informatici, ma a qualsiasi tipo di evento che possa compromettere la fruizione, in modo consentito, delle informazioni.

Sicurezza informatica (ICT security)

L'insieme delle misure tecniche e organizzative (prodotti, servizi, regole organizzative e comportamenti individuali) volte alla protezione dei sistemi informatici in termini di salvaguardia della riservatezza, integrità e disponibilità.

La sicurezza informatica risulta essere un sottoinsieme della sicurezza delle informazioni, in quanto riferita ad un ambito più limitato costituito dai sistemi informatici e dai dati nella sola forma digitale.

Cybersicurezza (Cybersecurity)

La cybersecurity è la sicurezza nel preservare l'interazione tra persone, applicazioni e servizi internet nel cyberspazio.

Si occupa di proteggere o difendere l'uso del cyberspazio da attacchi intenzionali, violazioni o incidenti, e dalle loro conseguenze, perseguendo tale obiettivo attraverso l'uso di tecnologie selezionate in termini di resilienza, robustezza, reattività.

La Cybersicurezza rappresenta una sottoclasse della sicurezza informatica, poiché si riferisce, in particolare, alla protezione di infrastrutture, sistemi e dati contro minacce provenienti dal cyberspazio (difesa di computer, server, dispositivi mobili, sistemi elettronici, reti e dati).

INQUADRAMENTO

CyberGO: soluzione per un approccio incisivo e integrato alla protezione delle informazioni

Ogni organizzazione è potenzialmente esposta a numerosi rischi connessi alla gestione delle informazioni.

A titolo esemplificativo, si possono citare: perdita o danneggiamento di informazioni, accesso da parte di persone non autorizzate, alterazione delle informazioni da parte di persone non autorizzate, sopravvenuta impossibilità ad accedere alle informazioni da parte di persone autorizzate causa eventi catastrofali o calamità naturali, fermo di processi aziendali a causa di indisponibilità di informazioni, sottrazione di informazioni riservate (know-how) da parte di dipendenti e/o da soggetti esterni, fuga di informazioni d'interesse commerciale per la concorrenza, fuga di informazioni che possono essere causa di danno al business, impedire l'adempimento agli obblighi di legge, ledere l'immagine o la reputazione dell'organizzazione.

Necessità di governance del rischio cyber

CyberGo
Cybersecurity and Governance to drive your business

Sebbene, in generale, sia riconosciuto che non si possa annullare il rischio, tanto meno quello cyber, gli eventi passati mostrano che spesso il problema è dovuto a misure di sicurezza inadeguate, più che a cause esterne imprevedibili. Questa inadeguatezza è dovuta principalmente al fatto che tali rischi sono maggiormente percepiti come una mancata comprensione dell'importanza dei rischi cyber, trattati come problemi tecnici a carico del dipartimento IT, invece che come rischi aziendali.

Per risolvere definitivamente questa inadeguatezza, diventa fondamentale coinvolgere direttamente l'organo amministrativo (il consiglio d'amministrazione o l'amministratore unico, nella struttura prevalente delle imprese) nella governance del rischio di cybersecurity, con l'assunzione di un ruolo attivo nella governance del rischio connesso alla gestione delle informazioni e l'attribuzione di responsabilità specifiche ben definite.

> *Diventa cruciale che **l'organo amministrativo eserciti una supervisione accurata** su queste questioni e, se necessario, intraprenda percorsi formativi specifici per acquisire le conoscenze necessarie per comprendere i rischi e la loro influenza sui servizi o prodotti forniti ai clienti, oltre a valutare l'efficacia delle contromisure tecniche e organizzative di mitigazione da attuare.*

L'importanza dell'analisi del contesto nella governance del rischio cyber

In un periodo di crescente globalizzazione che incide sempre più sui servizi e prodotti disponibili, è fondamentale esaminare attentamente il contesto e la catena di fornitura per sviluppare una gestione dei rischi su misura, che si integri nelle attività quotidiane dell'organizzazione, assicurando una risposta dinamica ed efficiente ai cambiamenti del mercato. Questo processo deve essere calibrato adeguatamente sotto l'aspetto tecnico, operativo e organizzativo, considerando sia il contesto interno che esterno dell'impresa, oltre agli obiettivi strategici aziendali.

> *In sintesi, una governance del rischio cibernetico realmente efficace non può ignorare le potenziali ripercussioni economiche e sociali che potrebbero derivare dalla realizzazione di un evento dannoso.*

Le segnalazioni degli incidenti di sicurezza delle informazioni

Un importante segno di responsabilizzazione consiste nella pronta notifica degli incidenti informatici alle autorità competenti e, a seconda della gravità del danno, agli stakeholder che potrebbero essere influenzate negativamente. Ci sono diversi obblighi imposti da varie norme cogenti, quali il Regolamento

(UE) 2016/679 e la Direttiva (UE) 2022/2555, quindi **è decisamente importante realizzare una policy unificata integrata che allinei tutti i requisiti imposti dalle singole normative correlate**.

La protezione efficace con l'approccio coordinato tra i diversi ambiti

La sicurezza non riguarda solo tenere lontane le minacce esterne contro i sistemi aziendali, quanto piuttosto proteggere le persone, i processi aziendali e le informazioni durante tutto il relativo ciclo di vita.

L'informazione circola nell'organizzazione secondo molteplici modalità, ognuna delle quali presenta rischi specifici anche non tecnologici: smarrire una chiavetta USB, subire il furto di un portatile o di un documento cartaceo sono solo alcune delle minacce di cui la sicurezza delle informazioni si occupa.

In secondo luogo, molti incidenti hanno come causa primaria l'errore umano, cioè una minaccia non tecnologica e di matrice non volontaria.

Ne consegue che la sicurezza non può essere focalizzata solo sugli aspetti tecnologici, a scapito degli altri fattori di rischio.

Infatti, vanno adottate e tra loro modulate - in relazione allo specifico contesto aziendale - tre diverse tipologie di misure di sicurezza:

- **Sicurezza fisica**, il cui scopo è impedire a un intruso, un estraneo o una persona non autorizzata, l'accesso ai luoghi fisici in cui i dati aziendali sono custoditi, con l'ausilio anche della tecnologia;
- **Sicurezza logica**, il cui scopo è quello di impedire l'accesso ai luoghi digitali (come server, database e computer) dell'organizzazione da parte di persone non autorizzate, con l'ausilio della tecnologia;
- **Sicurezza organizzativa**, il cui scopo è individuare le modalità necessarie per l'implementazione, gestione e controllo delle misure di sicurezza adottate (quali l'identificazione di ruoli, funzioni e responsabilità, lo sviluppo e il mantenimento dell'efficacia del sistema di autoregolamentazione).

Un'efficace protezione delle informazioni - per evitare costi determinati da misure tra loro non allineate, duplicate o in conflitto - richiede per ogni organizzazione:

- un presidio continuo in grado di coordinare la protezione dei sistemi (il "contenitore") e la sicurezza delle informazioni (il "contenuto");
- un insieme di interventi correlati (visione olistica e approccio sistemico) che concilino i diversi ambiti - tra loro complementari - cui rispettivamente si riferiscono Sicurezza delle informazioni, Sicurezza informatica e Cybersecurity;
- una gestione integrata di tutte le attività aziendali che riguardano le informazioni, nell'ambito di un'impostazione organizzativa unitaria e con un approccio multidisciplinare (gestione integrata della sicurezza delle informazioni), coordinata con l'uso della tecnologia.

INTERVENTO

Metodologia applicata per la consulenza sulla sicurezza delle informazioni

La metodologia **CyberGo prende spunto dai principali framework e standard ISO relativi alla sicurezza delle informazioni e alla cybersecurity**, come il NIST e l'ISO 27001, per individuare i requisiti necessari alla creazione di un "Sistema di Gestione" che consenta di monitorare efficacemente tutte le attività connesse alla sicurezza delle informazioni. Questo sistema comprende la definizione di ruoli e responsabilità, il supporto tecnologico e l'elaborazione di procedure formali, sia per le operazioni aziendali quotidiane sia per la gestione delle emergenze, **garantendo così un approccio integrato, sistematico e continuo**.

Il servizio di consulenza CyberGo prevede diverse fasi per creare un sistema di gestione della sicurezza delle informazioni che sia adeguato al contesto aziendale e risponda alle effettive necessità. In particolare, sono incluse:

- Una fase preliminare opzionale, preparatoria in quanto finalizzata alla definizione dello stato dell'arte sulla sicurezza delle informazioni, composta da:
  - Assessment relativo alla sicurezza delle informazioni;
- Una Gap analysis, in riferimento al contesto oggetto dell'intervento, quale l'adeguamento alla direttiva (UE) 2022/2555 (NIS 2) o altre normative applicabili in materia, o la certificazione alla norma ISO 27001.
- Una fase di progettazione del sistema di gestione della sicurezza, composto da:
  - Analisi del contesto interno ed esterno;
  - Valutazione dei rischi;
- Definizione di un piano di adeguamento dei controlli e delle misure di sicurezza necessarie per il trattamento dei rischi rilevati.
- Una fase di sviluppo del sistema di gestione della sicurezza, composto da:
  - Realizzazione del piano di controlli, con la definizione della politica di gestione della sicurezza collegata all'assegnazione dei ruoli e responsabilità nonché la creazione delle procedure e degli altri strumenti di regolamentazione.
- Una fase di attuazione del piano di monitoraggio del sistema di gestione della sicurezza, che include l'identificazione e la configurazione dei servizi e degli strumenti tecnologici necessari per supportare l'applicazione delle misure di controllo.

Soluzioni s.r.l.

via Cogne, 25 - 40026 Imola BO

tel. e fax: 0542 640084

P.IVA, Cod. Fisc. e n. iscrizione al Reg. Imprese BO: 02996441206

R.E.A. BO 483301 - Capitale sociale 16.000,00 € i.v.