DataVerso

Protezione e governance per il patrimonio delle informazioni

Sicurezza delle Informazioni

SERVIZI DI CONSULENZA PER LA MESSA IN SICUREZZA DI ASSET INFORMATIVI E PER LA RELATIVA CERTIFICAZIONE ISO-27001

Servizio in collaborazione con

PACTA AVVOCATI ASSOCIATI | VIA BATTAGLIONE VAL CHIESE, 10 – 36100 VICENZA

SOLUZIONI S.R.L. | VIA UGO LAMBERTINI, 6 - 40026 IMOLA (BO)

–

INTRODUZIONE

Il valore delle informazioni per la gestione dell'azienda

Imprenditori e responsabili aziendali, nell'esercizio quotidiano dell'impresa, ricevono una grande quantità di informazioni che provengono dall'universo dei rapporti necessari per le attività: clienti, fornitori, dipendenti, potenziali clienti, enti pubblici e altri portatori d'interesse.

Il lavoro è svolto in base a conoscenze tecnico-industriali e/o commerciali, sviluppate e continuamente affinate, che determinano le caratteristiche distintive dei prodotti e/o servizi offerti e i vantaggi competitivi dell'azienda stessa. Tale patrimonio di conoscenze, il know-how aziendale, è fruibile ai collaboratori coinvolti nelle rispettive attività, mediante l'accesso a flussi informativi specifici.

Di fatto, **le informazioni sono indispensabili per la gestione aziendale**: aspetti quali definire e capire il mercato, progettare, realizzare e gestire i prodotti, conoscere e fidelizzare i clienti, gestire l'amministrazione, effettuare l'assistenza tecnica, fissare gli obiettivi e controllare i risultati non possono essere efficacemente svolti senza un'adeguata gestione delle informazioni.

Solo una gestione adeguata delle informazioni in tutte le fasi (acquisizione ed elaborazione dei dati, organizzazione e classificazione dei flussi informativi, diffusione selettiva delle informazioni ai destinatari interessati, flussi informativi per l'attuazione efficace delle scelte effettuate) consente ai decisori aziendali di poter concretizzare il processo decisionale con le caratteristiche richieste e di orientare conseguentemente la gestione aziendale.

È per questo motivo che le informazioni sono un bene da valorizzare, proteggere e conservare nel tempo. La gestione del patrimonio informativo aziendale, pertanto, non rappresenta più un semplice costo, ma una reale opportunità di crescita. **Non è quindi più sufficiente proteggere e gestire ordinariamente un patrimonio informativo; diventa un obbligo sfruttarlo, valorizzarlo, farlo evolvere sempre con un occhio di attenzione agli aspetti di protezione e sicurezza**.

Sviluppo e sicurezza debbono quindi viaggiare sempre in parallelo e in continuo equilibrio unendo esigenze considerate sino a poco tempo fa erroneamente in contrasto, quali lo sviluppo del business, lo sfruttamento dell'informazione e il rispetto delle normative etiche, legali e di mercato.

> *Ai fini di conseguire tale vantaggio competitivo e di mantenerlo nel tempo è quindi cruciale la tutela e la messa in sicurezza del patrimonio informativo formatosi in azienda.*

INQUADRAMENTO

Rischi per inadeguata protezione delle informazioni

Ogni azienda 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, 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 danneggiare il business, impedire l'adempimento agli obblighi di legge e ledere l'immagine o la reputazione dell'azienda.

Necessità di protezione delle informazioni

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

Possedere e proteggere un'informazione significa principalmente fare in modo che siano salvaguardati tre requisiti principali – Modello R.I.D.:

- **Riservatezza** (*confidentiality*) – Le informazioni devono essere accessibili direttamente e indirettamente solo alle persone che ne hanno diritto e che sono espressamente autorizzate a conoscerle. Tutelare la riservatezza significa ridurre ad un livello accettabile il rischio che persone non autorizzate possano accedere alle informazioni;
- **Integrità** (*integrity*) – Le informazioni devono essere protette da alterazioni, quali modifiche danneggiamenti o cancellazioni improprie, anche accidentali. Tutelare l'integrità significa ridurre ad un livello accettabile il rischio che le informazioni vengano alterate da persone non autorizzate;
- **Disponibilità** (*availability*) – Le informazioni devono essere sempre accessibili agli utilizzatori che ne hanno diritto nei tempi e nei modi previsti. La disponibilità delle informazioni va assicurata in base a un livello di servizio concordato. Tutelare la disponibilità significa ridurre ad un livello accettabile il rischio di non poter accedere alle informazioni da parte di persone autorizzate.

In una visione di integrazione che considera tutti gli aspetti di compliance legale rilevanti per lo sviluppo di un Sistema per la Gestione della Sicurezza delle Informazioni, Soluzioni propone di analizzare l'ulteriore dimensione:

- della **Compliance** – La Complicance Normativa è un elemento imprescindibile nella gestione della sicurezza delle informazioni. Esistono già diverse leggi nazionali ed internazionali (quali il GDPR, il D.lgs. 196/2003 e s.m.i., il D.lgs. 231/2001) che implicitamente od esplicitamente fanno diretto richiamo ad una gestione in sicurezza dell'informazione. Gli elementi di rispetto legislativo devono quindi entrare come requisiti cogenti nella progettazione della sicurezza dei dati, integrandosi e rinforzando le Politiche di sicurezza dell'azienda e supportando le necessità di business della stessa.

In tal modo, per tutte le fasi dell'intervento è possibile:

a) individuare i requisiti di compliance legale da considerare

b) definire le misure e gli strumenti per soddisfare tali requisiti, con le modalità più funzionali alle specifiche della singola azienda e con caratteristiche armonizzate rispetto alle misure tecniche da attuare per la gestione in sicurezza delle informazioni.

Altri obiettivi fondamentali per assicurare la sicurezza delle informazioni, passano:

- dall'autenticazione – la certificazione dell'identità di un utente deve essere garantita attraverso un processo di riconoscimento del soggetto che esegue determinate operazioni.
- dall'autorizzazione – l'utente, una volta autenticato per l'accesso al sistema, deve poter agire, accedere, consultare e modificare risorse e dati secondo determinati permessi e autorizzazioni;
- dal non ripudio – ogni documento, messaggio o firma prodotti devono essere associati ad un soggetto autenticato ed autorizzato, senza possibilità di ripudio della paternità.

Le scelte di sicurezza delle informazioni per essere efficaci devono riguardare tutto il Sistema informativo aziendale e non il solo Sistema informatico. In altri termini, fino a quando Sistema informativo e Sistema informatico non sono coincidenti, la sicurezza delle informazioni non si deve riferire esclusivamente alla salvaguardia delle informazioni gestite da elaboratori, ma deve avere come oggetto la salvaguardia di tutte le informazioni trattate e distribuite con ogni mezzo.

Sicurezza delle informazioni, Sicurezza informatica e Cybersecurity

In tema di sicurezza si fa riferimento a diversi termini spesso utilizzati erroneamente come sinonimi. In realtà, Sicurezza delle informazioni, Sicurezza informatica e Cybersecurity hanno significati distinti, anche se tra loro complementari. Tutti trattano la protezione dei dati, ma con ambiti di riferimento diversi.

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 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 al solo ambito tecnologico (difesa di computer, server, dispositivi mobili, sistemi elettronici, reti e dati; in generale, di tutti gli oggetti vulnerabili attraverso l'informatica).

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'azienda 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 e che sono fuori dal dominio della Ict security e cybersecurity.

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;
- **Sicurezza logica**, il cui scopo è quello di impedire l'accesso ai luoghi digitali (come server, database e computer) dell'azienda da parte di persone non autorizzate;
- **Sicurezza organizzativa**, il cui scopo è individuare le modalità necessarie per l'implementazione, gestione e controllo delle misure di sicurezza adottate (attraverso l'identificazione di ruoli, funzioni e responsabilità e di un 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 azienda:

- 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 (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).

La governance della sicurezza delle informazioni

La governance della sicurezza delle informazioni riguarda l'uso di asset per garantire un'implementazione efficace della sicurezza delle informazioni e fornisce la garanzia che:

- vengano rispettate le direttive in materia di sicurezza delle informazioni;
- l'organo direttivo riceva una reportistica affidabile e pertinente in merito alle attività inerenti alla sicurezza delle informazioni.

L'implementazione di controlli di sicurezza, in assenza di una precisa strategia e di obiettivi chiari può renderli inefficaci e persino dannosi per l'azienda. Per questo motivo, la governance aziendale è essenziale. La governance IT, che indirizza l'implementazione delle tecnologie dell'informazione e della comunicazione, e la governance della sicurezza delle informazioni, che guida la gestione delle informazioni, fanno entrambe parte della governance aziendale.

Metodologia applicata per la consulenza sulla sicurezza delle informazioni

Lo standard ISO 27001 introduce il concetto di "Sistema di Gestione": uno strumento che permette di **tenere sotto controllo in modo sistematico e continuativo tutti i processi legati alla sicurezza delle informazioni tramite la definizione di ruoli, responsabilità e procedure formali** sia per l'operatività aziendale, che per la gestione delle emergenze.

Lo standard ISO 27001 prevede due macro-fasi distinte:

- La **prima fase** prevede **l'analisi del rischio**, che ha come scopo quello di fornire una serie di raccomandazioni riguardanti la gestione della sicurezza dell'informazione (**ISMS-Information Security Management System**) per garantire la possibilità di organizzare tale gestione su una base comune e soprattutto la più possibile oggettiva e condivisa.

  In sintesi, in questa fase SOLUZIONI definisce dei modelli per l'associazione del rischio a ciascuna classe di informazione.

- La **seconda fase** descrive dettagliatamente il processo di **costruzione di un sistema per la gestione del rischio**, mettendo a disposizione le specifiche per progettare, attuare, gestire, monitorare, revisionare ed aggiornare un ISMS correttamente documentato e orientato ai rischi di Business dell'azienda.

  Sempre, in sintesi, SOLUZIONI identifica le decisioni che l'azienda deve intraprendere in funzione del rispetto dei requisiti della sicurezza (modello R.I.D. implementato con la dimensione C).

> *Anche nel caso in cui un'azienda non intenda certificarsi immediatamente, ma in prima battuta miri esclusivamente ad una protezione informativa, l'approccio di SOLUZIONI è comunque quello di sviluppare un piano di progetto e le successive fasi realizzative basandosi sulla norma ISO 27001.*

Tale scelta non deriva solo dalla volontà di adottare una metodologia e norme internazionali, ma principalmente dalla possibilità di impostare un sistema di sicurezza che su specifiche necessità di mercato e/o legislative, o su richiesta della Direzione, sia certificabile con minimi interventi.

Struttura dell'intervento

Prima fase: analisi del rischio

La gestione del rischio consta di due elementi principali: la **valutazione del rischio** (spesso chiamata analisi del rischio) e il **trattamento del rischio**.

In particolare, la *valutazione del rischio* è un processo durante il quale un'organizzazione deve identificare i rischi per la sicurezza delle informazioni e determinarne la probabilità e l'impatto. In parole povere, l'organizzazione deve riconoscere tutti i potenziali problemi con le relative informazioni, quanto è probabile che si verifichino e quali potrebbero essere le conseguenze.

Invece, lo scopo del *trattamento del rischio* è scoprire quali controlli di sicurezza (cioè misure di protezione) sono necessari per evitare quei potenziali incidenti: la selezione dei controlli è chiamata processo di trattamento del rischio e nella ISO 27001 sono scelti dall'allegato A, che specifica 114 controlli diversi.

LE FASI PRINCIPALI NELLA VALUTAZIONE E NEL TRATTAMENTO DEL RISCHIO		
N.RO	AMBITO	DESCRIZIONE
1	Metodologia di gestione del rischio	Definizione delle regole condivise, su come effettuare la gestione del rischio.
2	Valutazione del rischio	Definizione degli asset e individuazione delle corrispondenti minacce e vulnerabilità. Valutazione dell'impatto e la probabilità di accadimento per ciascuna combinazione di risorse / minacce / vulnerabilità e calcolo del livello di rischio.
3	Trattamento del rischio	Selezionare ed attuare le opzioni per affrontare il rischio. Tale azione implica un processo interattivo per: • Formulare e selezionare le opzioni di trattamento del rischio; • Pianificare ed attuare il trattamento del rischio • Valutare l'efficacia del trattamento • Decidere se il rischio residuo sia accettabile • Intraprendere un ulteriore trattamento, nel caso in cui il rischio risulti non accettabile
4	Rapporto di valutazione e trattamento del rischio	La scelta delle opzioni di trattamento del rischio implica il bilanciamento dei potenziali benefici, che ne deriverebbero in relazione al conseguimento degli obiettivi, rispetto a costi, impegni o svantaggi di attuazione. Le opzioni per il trattamento del rischio possono implicare una o più possibilità: • Evitare il rischio decidendo di non avviare o di non continuare l'attività che genera il rischio • Assumere o aumentare il rischio al fine di cogliere un'opportunità • Rimuovere la fonte di rischio • Modificare la probabilità • Modificare le conseguenze • Condividere il rischio (ad esempio tramite contratti, stipulando un'assicurazione) • Ritenere il rischio con una decisione informata
5	Dichiarazione di applicabilità	Predisposizione del documento che descrive il profilo della sicurezza in cui sono implementati i controlli in relazione ai risultati sul trattamento dei rischi
6	Piano di trattamento del rischio	Predisposizione del documento che descrive come i controlli scelti devono essere attuati, in modo che le disposizioni siano comprese da coloro che saranno coinvolti e i progressi, rispetto al piano, possano essere monitorati. Il piano di trattamento dovrebbe identificare chiaramente l'ordine in cui il trattamento del rischio dovrebbe essere attuato.

Seconda fase: implementazione di un sistema per la gestione della sicurezza dell'informazione (ISMS-Information Security Management System)

Il sistema di gestione per la sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità delle informazioni mediante l'applicazione di un processo di gestione del rischio aumentando la fiducia da parte degli stakeholder sull'adeguatezza della gestione dei rischi.

È importante che il sistema di gestione per la sicurezza delle informazioni sia parte integrante dei processi e della struttura gestionale complessiva dell'organizzazione e che la sicurezza delle informazioni sia considerata nella progettazione dei processi, dei sistemi informativi e dei controlli, tenendo conto delle effettive necessità dell'organizzazione.

LE FASI PRINCIPALI DELL'IMPLEMENTAZIONE DI UN ISMS		
N.RO	AMBITO	DESCRIZIONE
1	**Stabilire il contesto dell'organizzazione**	
	Comprendere l'organizzazione e il suo contesto	L'organizzazione deve comprendere i fattori esterni ed interni pertinenti alle sue finalità e che possono influenzare la capacità di conseguire gli esiti previsti dal sistema di gestione per la sicurezza delle informazioni. In particolare: • Comprendere le necessità e le aspettative degli stakeholder; • Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni; • Attuare un processo continuo di controllo e miglioramento del sistema di gestione per la sicurezza delle informazioni;
	Leadership e impegno	L'alta direzione deve dimostrare interesse e impegno nel raggiungimento degli obiettivi definiti dall'implementazione del sistema di gestione per la sicurezza delle informazioni. In particolare: • la politica per la sicurezza delle informazioni deve essere comunicata e condivisa all'interno dell'organizzazione; • le responsabilità e le autorità per i ruoli, pertinenti la sicurezza delle informazioni, siano assegnate e comunicate;
2	**Capire cosa deve essere protetto**	
	Identificare le informazioni importanti da proteggere	Identificare le informazioni e gli asset (i beni considerati strategici per la sicurezza delle informazioni) è la prima fase da attuare, in quanto strategica per definire le relazioni tra gli asset e le responsabilità. Dall'identificazione delle tipologie delle informazioni si può stabilire meglio la gravità provocata da una possibile violazione, causata da una minaccia.

LE FASI PRINCIPALI DELL'IMPLEMENTAZIONE DI UN ISMS		
N.RO	AMBITO	DESCRIZIONE
	Identificare l'asset model, contenente gli asset strategici per la sicurezza delle informazioni	L'identificazione degli asset permette di determinare le tipologie di minacce e vulnerabilità a cui le informazioni possono essere sottoposte. Le principali categorie di asset sono: • *Siti*, che comprende i luoghi fisici, quali sedi e locali, e gli elementi ausiliari, quali gruppi di continuità, impianti antincendio, sistemi antintrusione; • *Strumenti digitali*, che comprende il network, i server e sistemi operativi, i software o applicazioni, il cloud computing, le postazioni di lavoro e lo storage; • *Strumenti analogici*, quali armadi, cassettiere, scaffalature; • *Organizzazione*, che comprende il personale dipendente e i fornitori di servizi strategici per la sicurezza delle informazioni
	Identificare le relazioni tra le informazioni e gli asset	La correlazione tra gli asset e le informazioni permette di inquadrare meglio il livello di protezione rilevato e necessario per un miglioramento della sicurezza stessa delle informazioni
3	**Valutare i rischi collegati alla sicurezza delle informazioni**	
	Comprendere il valore degli Asset	La valutazione del rischio sulla sicurezza delle informazioni si concentra nell'individuazione preventiva delle minacce che possono provocare un danno al business, agli obblighi legali o alla reputazione di una organizzazione. Questa fase si collega con quanto riscontrato nella valutazione e trattamento del rischio visto nel paragrafo "Prima fase: analisi del rischio"
	Valutare il tipo di contesto in cui opera l'organizzazione	
	Valutare i controlli attuati	
4	**Progettazione, applicazione e monitoraggio dei controlli per la sicurezza delle informazioni**	
	Identificare i controlli da implementare e impostare un Piano di sicurezza delle informazioni	In seguito alla valutazione dei rischi rilevati, l'organizzazione è consapevole del livello di protezione riscontrato e delle azioni, in ordine di priorità, da attuare per mitigare i rischi con livello non accettabile. In questo modo il top management / comitato direttivo per la sicurezza delle informazioni deve valutare ciò che deve essere fatto per affrontare ogni particolare rischio, in relazione alle priorità, ai tempi e ai costi per ogni soluzione proposta.
	Gestire il piano di sicurezza delle informazioni	
	Controllo della sicurezza delle informazioni	
	Monitoraggio della sicurezza delle informazioni	

Tempi di realizzazione dell'intervento

L'intervento sarà svolto indicativamente in circa 4 mesi complessivi. I tempi possono subire variazioni in riferimento alle disponibilità del referente aziendale di progetto.

Le attività saranno iniziate entro circa 1 mese dalla data di ricezione della proposta siglata per accettazione.

Gli interventi saranno definiti in base ad un piano di lavoro concordato con il referente aziendale di progetto e formalizzato durante la prima attività di consulenza.

Personale e competenze impiegate

L'intervento verrà svolto attraverso un Gruppo di Progetto multidisciplinare.

La scelta dei professionisti che compongono il Gruppo di Progetto è finalizzata a garantire la copertura delle diverse professionalità necessarie.

DataVerso

Protezione e governance per il patrimonio delle informazioni

Servizio in collaborazione con

PACTA AVVOCATI ASSOCIATI

PACTA Avvocati Associati

via Battaglione Val Chiese, 10 – 36100 Vicenza

tel. +39 0444 564365

P.IVA, Cod. Fisc.: 03791420247

info@pactavvocati.it www.pactavvocati.it

Soluzioni CONSULENZA MANAGERIALE

Soluzioni s.r.l.

via Ugo Lambertini, 6 - 40026 Imola BO

tel. e fax: +39 0542 640084

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

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