SICUREZZA DELLE INFORMAZIONI.

Oggi più che mai il tema strategico più delicato per qualunque impresa, nessuna esclusa.

Il tema della sicurezza delle informazioni è sempre di più vitale importanza in ogni organizzazione.
I dati che gestiamo, le informazioni che ci scambiamo, l'importanza della tutela e della riservatezza dei dati sono temi sempre più comuni e di sempre maggior criticità per ogni sistema aziendale. Oggi poi non esiste più la separazione tra dati digitali e dati "fisici": qualunque dato, ovunque, è gestito al 100% digitalmente. Le informazioni vitali per le aziende di ogni settore e dimensione, sono quindi sempre più frequentemente esposte e oggetto di attacchi informatici e violazioni, aumentando il rischio per le imprese, per le istituzioni e anche per i semplici consumatori, con ingenti danni economici in caso di incidenti.
Pensare che queste tematiche non debbano essere presidiate o che non possano portare problematiche se mal gestite non si addice ad imprese che vogliono essere presenti sul mercato, affidabili nei confronti dei loro clienti e attente alle prospettive di sostenibilità nel tempo ed alla business continuity.
Per gestire al meglio questi aspetti esiste un'intera famiglia di norme, la ISO 27000, che è di grande aiuto per garantire una sicura gestione di questi dati. Per famiglia intendiamo una serie di norme che toccando un tema, lo affrontano sotto diverse sfaccettature. Il tutto sotto il cappello di una norma di riferimento, in questo caso la ISO/IEC 27001.

Lo standard ISO/IEC 27001

Lo standard ISO/IEC 27001 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) è una norma internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.
La norma ISO 27002:2013 è una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001:2013 al fine di proteggere le risorse informative; ISO 27001:2013 è il documento normativo di certificazione al quale l'organizzazione deve fare riferimento per costruire un Sistema di Gestione della Sicurezza delle Informazioni che possa essere certificato da un ente indipendente, mentre la norma ISO 27002:2013 non è certificabile in quanto è una semplice raccolta di raccomandazioni.

Le estensioni della ISO 27001: ISO/IEC 27017, ISO/IEC 27018, ISO 27701

Nascono nel 2015 le linee guida ISO/IEC 27017:2015 e nel 2019 le ISO/IEC 27018:2019 e ISO 27701:2019:

- **ISO/IEC 27701** -Estensione a ISO / IEC 27001 e ISO / IEC 27002 per la gestione delle informazioni sulla privacy è l'ultima norma uscita all'interno della famiglia ISO 27000 e definisce le modalità con cui un'organizzazione può gestire i dati personali al suo interno. Partendo sempre

dai requisiti della ISO 27001 vengono inseriti dei forti riferimenti e controlli nel caso in cui l'azienda sia titolare del trattamento dei dati e nel caso in cui sia responsabile del trattamento dei dati. Questa norma permette alle organizzazioni di creare un forte legame con quanto disposto e definito da parte del Reg.679/2016 in materia di protezione dei dati personali.

- **ISO/IEC 27017** è una linea guida che definisce controlli avanzati sia per fornitori, sia per i clienti di servizi cloud. Chiarisce ruoli e responsabilità dei diversi attori in ambito cloud con l'obiettivo di garantire che i dati conservati in cloud computing siano sicuri e protetti.

- **ISO/IEC 27018** - Codice di condotta per la protezione delle PII (Personally Identifiable information) nei servizi di public cloud per i cloud provider- è una linea guida per i fornitori di servizi cloud pubblici che vogliono migliorare la gestione dei dati personali. L'obiettivo di questo standard è quello di fornire una modalità strutturata, basata sul privacy by design, per far fronte alle principali questioni giuridiche, sia di natura legale che contrattuale, legate alla gestione dei dati personali in infrastrutture informatiche distribuite seguendo il modello del cloud pubblico.

Gli obiettivi della norma di riferimento ISO 27001

La norma specifica i requisiti per stabilire, attuare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni nel contesto dell'organizzazione. Inoltre essa include i

requisiti per la valutazione e il trattamento dei rischi per la sicurezza dell'informazione adatti alle esigenze dell'organizzazione. I requisiti presenti nella norma sono generici e destinati ad essere applicati a tutte le organizzazioni, indipendentemente dal tipo, dalla dimensione o dalla loro natura.

Scopo dello standard è quello di proteggere i dati e le informazioni da una vasta gamma di minacce (accesso non autorizzato, distruzione e furto dati, interruzione di servizio, virus informatici) al fine di assicurare la continuità dell'attività aziendale. Avere un corretto sistema di gestione della sicurezza delle informazioni significa dotarsi di tutte le misure di sicurezza, assicurando i dati in termini di:

- Riservatezza: affinché tutte le informazioni siano accessibili solo alle persone autorizzate

- Integrità: per prevenire le modifiche indebite, accidentali o fraudolente alle informazioni

- Disponibilità: per assicurare che gli utenti possano accedere ai dati sulla base dei propri profili specifici di abilitazione in tempi congruenti con le proprie esigenze operative.

La norma ISO 27001 è una norma volontaria, ciò significa che ogni organizzazione può scegliere se intraprendere un percorso di certificazione o meno.

I benefici della certificazione ISO 27001

Riteniamo che garantire la sicurezza delle informazioni che vengono gestite a qualunque titolo sia oggi un vantaggio competitivo di assoluto valore per qualunque tipo di azienda. Solo la certificazione può però garantire tutti gli stakeholder, attraverso la verifica indipendente, l'applicazione del corretto sistema di gestione e di conseguenza generare valore, e di conseguenza:

Aumentare la fiducia dei clienti

Consentirà al mercato di percepire in maniera ancora più accentuata l'impegno aziendale nella sicurezza dei dati e delle informazioni, incrementando conseguentemente la fiducia dei clienti nei confronti dell'azienda quale soggetto in grado di trattare in modo appropriato i dati affidati all'organizzazione.

Proteggere e migliorare la reputazione

Gli attacchi informatici stanno aumentando ogni giorno per volume e forza, e i danni finanziari e di immagine causati da una scarsa sicurezza delle informazioni possono essere fatali.

L'implementazione di un ISMS certificato ISO 27001 aiuta a proteggere la tua organizzazione da tali minacce e dimostra che hai adottato le misure necessarie per proteggere la tua attività.

Rispettare i requisiti aziendali, legali, contrattuali e normativi

Lo Standard è progettato per garantire la selezione di controlli di sicurezza adeguati e proporzionati, che contribuiscono a proteggere le informazioni in linea con i requisiti normativi, come il Regolamento generale sulla protezione dei dati (GDPR) e le altre leggi sulla sicurezza delle informazioni.

Ottenere un giudizio indipendente sul proprio stato di sicurezza

La certificazione ISO 27001 richiede l'esecuzione di revisioni periodiche e audit interni dell'ISMS, per garantirne un miglioramento continuo. Un revisore esterno esaminerà l'ISMS a intervalli specifici, per stabilire se i controlli funzionano come previsto. Con questa valutazione indipendente, si ottiene l'opinione di un esperto in merito al corretto funzionamento dell'ISMS, e si fornisce anche il livello di sicurezza necessario per proteggere le informazioni dell'organizzazione.

Contatto

Il nostro ufficio di Milano è a disposizione per tutte le ulteriori informazioni. Sono direttamente a vostra disposizione anche i nostri Lead Auditor per tutti gli approfondimenti tecnici.

T +39 02 83965115
milano@sqs.it
www.sqs.it

SQS Italian Branch
Sede legale: Piazzale Biancamano, 2 - 20121 Milano (Mi), Italia
Sede operativa: Galleria del Corso, 4 - 20122 Milano (Mi), Italia
C.F. 97571990155, PARTITA IVA 07301570961