Sistemi di gestione della sicurezza delle informazioni

L’esigenza di implementare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS – Information Security Management System) è sempre più avvertita in ambito aziendale, in quanto vi è la consapevolezza dell’aumento dei rischi che derivano dal fatto che la tecnologia dell’informazione è più che mai il pilastro dei processi produttivi aziendali.

Premesso che il SGSI tratta le “informazioni” in qualsiasi formato (digitale, cartaceo, audio, video,…), tre sono gli aspetti che devono essere focalizzati nello sviluppo di un SGSI:

- RISERVATEZZA: le informazioni devono essere rese disponibili solo agli utenti autorizzati che ne necessitano per la loro operatività e l’accesso deve essere sottoposto a controllo. Le informazioni caratterizzate da un elevato livello di riservatezza devono essere protette, sia nel momento della trasmissione, mediante la crittografia, sia quando vengono archiviate, mediante crittografia o utilizzando un controllo degli accessi.
- INTEGRITÀ: le informazioni devono essere gestite con modalità adeguate per impedirne manomissioni e/o modifiche non autorizzate. Soltanto il personale autorizzato può intervenire sulla configurazione di un sistema o sulle informazioni trasmesse attraverso reti aziendali o mediante internet. Un SGSI, al fine di garantire l’integrità delle informazioni, deve essere predisposto in modo che rimanga traccia di ogni eventuale modifica apportata – intenzionalmente o involontariamente – ai dati.
- DISPONIBILITÀ: le informazioni devono essere sempre disponibili agli utenti autorizzati. Il sistema informatico può essere compromesso – in toto o parzialmente – da attacchi nei confronti dei quali possono essere adottate contromisure automatizzate, quali l’autenticazione e la crittografia, o particolari azioni fisiche, anche a carattere preventivo.

La certificazione secondo la norma ISO/IEC 27001:2013 (UNI ISO/IEC 27001:2014) passa attraverso le seguenti fasi:

1. Definizione del perimetro e dei limiti di applicabilità del SGSI
2. Identificazione e censimento degli asset contenenti informazioni
3. Valutazione dei rischi
4. Piano di trattamento dei rischi
5. Identificazione dei controlli (ISO 27002 eventualmente integrati da altri) applicabili e definizione della Dichiarazione di Applicabilità (*Statement of Applicability* o SoA)
6. Progettazione del sistema di gestione (eventuale integrazione con i sistemi di gestione esistenti)
7. Attuazione di procedure e controlli e delle azioni scaturite dal piano di trattamento dei rischi
8. Audit interni
9. Riesame della direzione
10. Certificazione con Organismo accreditato

Il progetto di certificazione ISO 27001 viene assistito dal consulente che ha l'obiettivo di indirizzare l'azienda verso soluzioni finalizzate a prevenire e mitigare i rischi realmente esistenti perseguendo la massima efficienza delle risorse impegnate nel progetto e dell'operatività dei processi di business.

Alcuni link utili sulla sicurezza delle informazioni e la business continuity:

- 27001 Academy
- ISO 27001 security