LA NORMA ISO 27001 PER LA CYBERSECURITY

Una norma che fornisce un approccio strutturato e sistemico per la gestione della sicurezza delle informazioni. Perché la sicurezza dei sistemi critici non deve e non può essere affidata unicamente a misure tecnologiche di protezione ma va gestita attraverso politiche organizzative, ad esempio con lo standard ISO 27001.

Gli impianti critici industriali – ad esempio nei settori Oil&Gas, fornitura di acqua e energia, infrastrutture e altri - non possono subire interruzioni di servizio: l'impatto di un'interruzione della produzione e dei servizi associati possono infatti portare a conseguenze catastrofiche. E la sicurezza passa anche attraverso le informazioni generate, utilizzate e conservate nei sistemi: pertanto ogni rischio in quest'ambito deve essere valutato e gestito adeguatamente. L'obiettivo generale della sicurezza delle informazioni consiste nella protezione di tre caratteristiche: ***Riservatezza, Integrità*** *e* ***Disponibilità***.

QUALI MINACCE INCOMBONO SUI SISTEMI?

L'**Internet Security threat report 2012** di Symantec riporta che gli attacchi dovuti a malware (virus, worms e trojan horse) bloccati da Symantec nel 2011 sono stati più di 5,5 miliardi con un incremento rispetto al 2010 dell'81%.

SOLUZIONI TECNOLOGICHE, MA NON SOLO

Le organizzazioni si affidano agli amministratori dei sistemi per trovare le soluzioni più adeguate per proteggersi. Spesso però queste figure professionali si limitano a considerare come soluzioni l'installazione di software per la sicurezza.

Ma la sicurezza dei sistemi critici non può essere affidata unicamente a soluzioni tecnologiche, deve essere **gestita attraverso le Policies per la Sicurezza**. Proteggersi efficacemente significa adottare un approccio strutturato e sistemico per la gestione della sicurezza delle informazioni e dei sistemi. Questo approccio viene fornito dalla norma **ISO 27001:2013.**

INFORMATION SECURITY MANAGEMENT SYSTEM ISO 27001:2013

La ISO 27001:2013 è **la norma che stabilisce i requisiti di un Sistema di Gestione per la Sicurezza delle Informazioni** ed introduce due domini: il dominio preventivo attraverso il **Risk Management** e il dominio correttivo attraverso la **Business Continuity** per ridurre le perdite al minimo nel caso si verifichi un incidente distruttivo.

La norma ISO 27001:2013 è suddivisa in due parti:

- la prima parte contiene i requisiti per il Sistema di Gestione per la Sicurezza delle Informazioni (Contesto dell'organizzazione, Leadership e committment, Pianificazione degli obiettivi, Risk assessment e Risk treatment, Attività di supporto, Operation, Valutazione delle prestazioni e miglioramento).
- La seconda parte contiene gli argomenti prevalentemente organizzativi e tecnologici per la sicurezza delle informazioni con gli obiettivi e i controlli che devono essere applicati nei processi dell'organizzazione.

TÜV Rheinland Italia propone **corsi di formazione e servizi di certificazione** in riferimento allo standard ISO 27001. Per maggior informazioni, venite ad incontrare i nostri esperti durante **i seminari gratuiti di introduzione** a questa norma:

- Presentazione della norma **ISO 27001 – Sicurezza delle Informazioni**: **24 luglio a Pogliano Milanese (MI) e 25 luglio a Cittadella (PD)**

Per maggiori informazioni visitate il nostro sito www.tuv.com/it.