ISO 27001:2013 - Certificato dello standard internazionale per il sistema di gestione della sicurezza delle informazioni

Introduzione

Questo standard internazionale è stato preparato per fornire i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni. L'adozione di un sistema di gestione della sicurezza delle informazioni è una decisione strategica per un'organizzazione. L'istituzione e l'implementazione del sistema di gestione della sicurezza delle informazioni di un'organizzazione è influenzata dalle esigenze e dagli obiettivi dell'organizzazione, dai requisiti di sicurezza, dai processi organizzativi utilizzati e dalle dimensioni e dalla struttura dell'organizzazione. Tutti questi fattori di influenza dovrebbero cambiare nel tempo.

Il sistema di gestione della sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità delle informazioni applicando un processo di gestione del rischio e dà fiducia alle parti interessate che i rischi sono adeguatamente gestiti.

È importante che il sistema di gestione della sicurezza delle informazioni sia parte integrante e integrato con i processi dell'organizzazione e la struttura di gestione complessiva e che la sicurezza delle informazioni sia considerata nella progettazione di processi, sistemi informativi e controlli. Si prevede che l'implementazione di un sistema di gestione della sicurezza delle informazioni sarà ridimensionata in base alle esigenze dell'organizzazione.

Questo standard internazionale può essere utilizzato da parti interne ed esterne per valutare la capacità dell'organizzazione di soddisfare i requisiti di sicurezza delle informazioni dell'organizzazione.

L'ordine in cui i requisiti sono presentati nella presente norma internazionale non riflette la loro importanza né implica l'ordine in cui devono essere attuati. Gli elementi dell'elenco sono enumerati solo a scopo di riferimento.

ISO/IEC 27000 descrive la panoramica e il vocabolario dei sistemi di gestione della sicurezza delle informazioni, facendo riferimento alla famiglia di standard dei sistemi di gestione della sicurezza delle informazioni (inclusi ISO/IEC 27003[2], ISO/IEC 27004[3] e ISO/IEC 27005[4]), con relativi termini e definizioni.

Scopo

La presente norma internazionale specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni nel contesto dell'organizzazione. Questa norma internazionale include anche requisiti per la valutazione e il trattamento dei rischi per la sicurezza delle informazioni adattati alle esigenze dell'organizzazione. I requisiti stabiliti nella presente norma internazionale sono generici e si intendono applicabili a tutte le organizzazioni, indipendentemente dal tipo, dalle dimensioni o dalla natura. L'esclusione di uno qualsiasi dei requisiti specificati nelle clausole da 4 a 10 non è accettabile quando un'organizzazione dichiara la conformità alla presente norma internazionale.