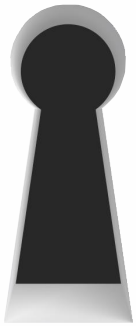
PERRY JOHNSON REGISTRARS, INC.



Componenti chiave della ISO 27001

La ISO 27001 non è un dispositivo o un pacchetto software che possa impedire il verificarsi di eventuali violazioni dei dati, perché una cosa del genere non esiste; in realtà, occorre attenersi ad una norma formalizzata a livello internazionale, che richiede alla vostra organizzazione di scrivere e implementare procedure basate su una norma scritta.

Formazione, sensibilizzazione, processi formalizzati, riesame e miglioramento continuo, e impegno da parte di tutti i membri di un'organizzazione sono gli elementi chiave di un sistema ISMS efficace. Il numero di attacchi e la vulnerabilità dei sistemi informatici e dei software sono tali da rendere difficile la sicurezza delle informazioni affidandosi solo ad un pacchetto software o ad un hardware.

- Unica norma, riconosciuta e accreditata a livello internazionale, per la gestione della sicurezza delle informazioni, che può essere certificata da una parte terza. Lo strumento migliore per promuovere il proprio impegno e il raggiungimento di un sistema di sicurezza delle informazioni. Sempre più richiesta da molte organizzazioni, anche solo per poter partecipare alle gare d'appalto.
- Per la sicurezza delle informazioni, sono le persone a rappresentare un fattore critico; la norma ISO 27001 richiede che gli individui coinvolti nell'ambito della sicurezza delle informazioni acquisiscano una maggiore comprensione del problema, e fornisce un quadro di riferimento per la creazione di una cultura che renda la sicurezza delle informazioni una priorità assoluta. Il personale dipendente rappresenta sempre l'anello più debole nella sicurezza delle informazioni, ed è difficile impedire la divulgazione di dati sensibili, poiché non è necessario portarli via dall'edificio dentro una scatola. Le violazioni possono essere semplici quanto una conversazione casuale con gli amici dopo il lavoro, ascoltata dalla persona sbagliata.
- Gli attacchi alla sicurezza informatica si evolvono e cambiano a una velocità incredibile, e le nuove vulnerabilità sono in genere identificate perché utilizzate per violare la sicurezza. Disporre di un piano di risposta formalizzato in caso di violazione, come richiesto dalla norma ISO 27001, permetterà di ridurre notevolmente i danni subiti e la durata di un attacco. La mancanza di un piano equivale alla pianificazione del fallimento.
- Una volta implementato il vostro sistema ISMS (sistema di gestione per la sicurezza delle informazioni) secondo le linee guida della ISO 27001, saprete individuare e dare priorità alle principali minacce basandovi sui potenziali danni all'organizzazione, compresi quelli finanziari, legali, contrattuali, di reputazione o qualsiasi altro fattore importante per la vostra organizzazione. Tali informazioni verranno comunicate e riesaminate costantemente dalla direzione, ai vari livelli, così che vengano predisposte le risorse e le azioni necessarie per controllare i livelli di rischio che risultano più elevati di quelli che si è disposti ad accettare. In tribunale o per l'opinione pubblica, la mancata conoscenza non esonera dalla responsabilità.

BENEFICI

La direzione può far leva sulla certificazione per ottenere nuovi contratti. Ottenere la certificazione ISO 27001 permetterà alla vostra organizzazione di entrare in contatto con settori in cui la sicurezza delle informazioni è fondamentale, e in cui è richiesta la protezione delle informazioni visualizzate e trattate nel corso delle attività. Grazie alla promozione della certificazione ai sensi di una norma, riconosciuta a livello internazionale in materia di sicurezza delle informazioni, la vostra organizzazione risulterà ancora più interessante per potenziali clienti e stakeholder.