Sistema RTS 27001 MD-61

Rev. 02
Agg. 29-10-2020

SCOPO

Ottenere un Contratto di consulenza a pacchetto per sviluppare il sistema e conseguire la certificazione UNI EN 27001
Lo scopo operativo quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato
sistema di gestione della sicurezza delle informazioni (SGSI) finalizzato ad una corretta gestione dei
dati sensibili dell'azienda.

CAMPO D'APPLICAZIONE

Tutte le società che effettuato attività che implichino l'utilizzo di sistemi informatici, praticamente qualunque azienda. Ad oggi le aziende interessate sono la media grande azienda oppure la cosietà che opera lei stessa nel mondo informatico.

RIFERIMENTI NORMATIVI

- UNI EN 27001/2017Tecnologie informatiche- Tecniche di Sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti
-

LEVE COMMERCIALI

Come è già successo per altre certificazioni specifiche il requisito di essere certificati 27001:

- Permette accesso a gare d'appalto
- dare un segnale forte verso un mercato sempre più sensibile alla problematica della gestione in sicurezza delle informazioni
- un vantaggio competitivo in ambito commerciale nei confronti della concorrenza;
- dimostrare un elevato livello di sicurezza delle informazioni all'interno dell'azienda minimizzando i rischi di vulnerabilità tecniche: Gestione della posta elettronica, controllo degli accessi Internet esterni, Backup, antivirus, Firewal.
- un controllo continuo sui processi più rischiosi nello scambio di dati con clienti o fornitori, che potrebbero portare a conseguenze legali per l'azienda;

GENERALITÀ

Dalla perdita di dati agli accessi non autorizzati, dagli attacchi virus al commercio elettronico, dalla pirateria informatica al disaster recovery, la ISO 27001 consente di valutare attentamente tutti i rischi per il business e le diverse tipologie di informazioni gestite, evidenziando le aree in cui è necessario un miglioramento.

La protezione delle Informazioni consiste nell'assicurare, attraverso la gestione controllata dei processi aziendali, i desiderati livelli di:

- **Riservatezza** – proteggere le informazioni da accessi non autorizzati
- **Integrità** – salvaguardare l'accuratezza e la completezza delle Informazioni

- **Accessibilità** – assicurarsi che i dati e le informazioni siano accessibili quando richiesto

Le Macro aree di intervento

- **Esterno** – l'accesso informatico al mondo esterno
- **interno** – Uso della posta elettronica, uso di internet da parte dei dipendenti
- **l'architettura informatica dell'azienda** – accessibilità ai software, hardware utilizzato

LA ISO 27001 E GDPR PRIVACY - DIFFERENZE

Trattandosi di dati è giusto definire la principale differenza tra il regolamento sulla Privacy e la norma di certificazione del sistema di gestione per la sicurezza dei dati e delle informazioni secondo la norma di certificazione Iso 27001 in via generale.

La prima tutela i dati personali sensibili, la seconda tutte le tipologie di informazioni, infatti, pur richiedendo che vengano applicati i requisiti di legge applicabili.

La seconda tiene anche in considerazione i dati di business e della proprietà industriale dell'azienda, i quali devono essere salvaguardati per l'interesse dell'organizzazione cliente.

Allo stesso tempo, tuttavia, non esimia l'azienda dal rispetto delle misure minime di sicurezza e dalla produzione della documentazione richiesta dalla legge sulla Privacy GDPR, per la quale esiste lo schema di Iso 27701.

A COSA È VOLTA LA CONSULENZA

La consulenza è mirata a fornire al cliente un quadro della normativa applicabile e ad effettuare una verifica dei requisiti minimi richiesti dalla norma stessa.
Verrà fornito uno strumento che, attraverso la creazione di un sistema personalizzato, permetterà l'ottenimento del certificato senza la necessità di stravolgere le attività quotidiane aziendali ed il modus operandi degli addetti, anzi, fornirà un valido metodo per garantirsi un recupero nel tempo delle informazioni pregresse.