Certificati.Pro
Quality Management System

ISO 27001

«Sicurezza delle informazioni»

La **ISO 27001** (Tecnologia dell'informazione – Tecniche di sicurezza – Sistemi di gestione per la sicurezza delle informazioni – Requisiti) è lo standard internazionale di riferimento per la gestione della sicurezza delle informazioni.
È pubblicata congiuntamente dall'International Organization for Standardization (ISO) e dalla International Electrotechnical Commission (IEC), due tra le principali organizzazioni internazionali che definiscono norme riconosciute a livello globale.
Questa norma fa parte della serie ISO/IEC 27000, un insieme di standard dedicati alla protezione delle informazioni e alla gestione della sicurezza, sviluppati per aiutare le organizzazioni a ridurre i rischi informatici e migliorare la resilienza dei propri sistemi.

Cos'è la ISO 27001 e qual è il suo scopo
La ISO 27001 stabilisce i requisiti per implementare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS – Information Security Management System).
Questo sistema rappresenta un insieme strutturato di politiche, procedure e controlli che consentono alle organizzazioni di proteggere in modo sistematico ed efficiente le proprie informazioni, siano esse digitali o cartacee.
Lo scopo principale della ISO 27001 è tutelare tre elementi fondamentali delle informazioni:

- Riservatezza – garantire che solo le persone autorizzate possano accedere ai dati.
- Integrità – assicurare che le informazioni siano accurate e non modificate in modo improprio.
- Disponibilità – rendere i dati accessibili alle persone autorizzate quando necessario.

Perché è importante adottare la ISO 27001
Implementare un sistema conforme alla ISO 27001 offre numerosi vantaggi strategici, organizzativi e operativi.

Tra i principali benefici troviamo:

- **Conformità legale e regolamentare**
  La norma consente di soddisfare i requisiti di legge, i regolamenti e gli obblighi contrattuali in materia di sicurezza delle informazioni e protezione dei dati personali.
- **Vantaggio competitivo**
  Ottenere la certificazione ISO 27001 dimostra ai clienti, partner e stakeholder l'impegno dell'organizzazione nella tutela dei dati, rafforzando la fiducia e migliorando la reputazione aziendale.

- **Riduzione dei costi**
  Prevenire incidenti di sicurezza informatica evita danni economici e di immagine. L'adozione della norma riduce la probabilità di violazioni, errori o interruzioni operative.
- **Miglioramento dei processi interni**
  La ISO 27001 favorisce un approccio organizzato e documentato alla gestione dei processi aziendali, promuovendo chiarezza nei ruoli, responsabilità e procedure.

La certificazione ISO 27001
Una azienda può richiedere la certificazione ISO 27001 a un ente di certificazione accreditato, che condurrà un audit per verificare la conformità del sistema di gestione ai requisiti della norma.
In caso di esito positivo, l'organizzazione riceve un certificato ISO 27001 valido generalmente per tre anni, soggetto a verifiche periodiche.
Anche i professionisti individuali possono ottenere la certificazione frequentando corsi di formazione ufficiali e superando un esame, dimostrando così le proprie competenze nella gestione della sicurezza delle informazioni.

I 14 domini di sicurezza della ISO 27001
L'Allegato A della norma elenca 114 controlli di sicurezza, suddivisi in 14 domini tematici. Queste aree coprono tutti gli aspetti della sicurezza delle informazioni, tra cui:

1. Politiche per la sicurezza delle informazioni
2. Organizzazione della sicurezza delle informazioni
3. Sicurezza delle risorse umane
4. Gestione delle risorse e classificazione delle informazioni
5. Controllo degli accessi
6. Crittografia
7. Sicurezza fisica e ambientale
8. Sicurezza operativa
9. Sicurezza delle comunicazioni
10. Acquisizione, sviluppo e manutenzione dei sistemi
11. Rapporti con i fornitori
12. Gestione degli incidenti di sicurezza
13. Continuità operativa e disaster recovery
14. Conformità normativa e contrattuale

Questa struttura dimostra come la ISO 27001 non si limiti alla sola sicurezza informatica, ma abbracci anche aspetti organizzativi, legali, fisici e umani.

ISO 27001

«Sicurezza delle informazioni»

Documentazione richiesta
Per ottenere la conformità alla norma, è necessario predisporre un insieme di documenti obbligatori, tra cui:

- Campo di applicazione dell'SGSI
- Politica e obiettivi per la sicurezza delle informazioni
- Metodologia di valutazione e trattamento del rischio
- Dichiarazione di applicabilità (Statement of Applicability)
- Piano di trattamento del rischio
- Ruoli e responsabilità in materia di sicurezza
- Procedure operative, di gestione degli incidenti e di continuità operativa
- Inventario delle risorse e politiche di controllo accessi

In aggiunta, l'organizzazione deve mantenere registrazioni come: risultati di audit, formazione del personale, azioni correttive e riesami della direzione.

Obbligatorietà e applicabilità
L'adozione della ISO 27001 non è obbligatoria per legge nella maggior parte dei Paesi, ma può diventarlo in specifici settori o in base a requisiti contrattuali.
Molte organizzazioni, tuttavia, scelgono di implementarla volontariamente per dimostrare il proprio impegno nella protezione dei dati e nella gestione della sicurezza informatica.

Conclusione
In un contesto in cui la sicurezza delle informazioni è una priorità assoluta, la certificazione ISO/IEC 27001 rappresenta una garanzia di affidabilità, trasparenza e gestione consapevole dei rischi.
Implementare un sistema di gestione conforme alla norma significa proteggere i dati, rafforzare la fiducia di clienti e partner, e migliorare l'efficienza organizzativa.
È un investimento strategico per qualsiasi organizzazione che voglia crescere in modo sicuro e sostenibile nel mondo digitale.

Certificati.Pro
Quality Management System
375.6866312
www.certificati.pro
info@certificati.pro