ISO 27001

PRESENTAZIONE SULLA NORMA ISO/IEC 27001:2022 - SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Introduzione

La ISO/IEC 27001:2022 è una norma internazionale che specifica i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS - Information Security Management System). La norma è progettata per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite da un'organizzazione, riducendo il rischio di violazioni e proteggendo i dati da accessi non autorizzati.

La ISO 27001 è particolarmente rilevante in tutti quei contesti nei quali la sicurezza delle informazioni è fondamentale per la fiducia dei clienti e per la conformità alle normative vigenti, come il GDPR in Europa.

Contesto della norma

La ISO 27001 è applicabile a organizzazioni di qualsiasi dimensione e settore, e può essere implementata per proteggere tutti i tipi di informazioni, che siano digitali, cartacee o verbali. La norma richiede un approccio sistematico per la gestione dei rischi legati alla sicurezza delle informazioni, assicurando che siano adottati controlli adeguati per mitigare tali rischi. La norma segue la struttura dell'Allegato SL, che facilita l'integrazione con altri sistemi di gestione ISO come ISO 9001 (qualità) e ISO 14001 (ambiente).

Struttura della norma

La ISO 27001 è strutturata in dieci sezioni principali, che delineano i requisiti per stabilire, implementare, mantenere e migliorare il proprio sistema di gestione e sicurezza delle informazioni:

1. Scopo e campo di applicazione
2. Riferimenti normativi
3. Termini e definizioni
4. Contesto dell’organizzazione
5. Leadership
6. Pianificazione
7. Supporto
8. Attività operative
9. Valutazione delle prestazioni
10. Miglioramento

APPROFONDIMENTO SULLE SEZIONI PRINCIPALI-Contesto dell'organizzazione

La sezione 4 della ISO 27001 richiede alle organizzazioni di determinare i fattori interni ed esterni che influenzano la capacità di raggiungere gli obiettivi di sicurezza delle informazioni. Questo include l'identificazione delle esigenze delle parti interessate e la definizione del campo di applicazione.

"L'organizzazione deve determinare le questioni interne ed esterne che sono pertinenti al suo scopo e che influenzano la capacità di conseguire i risultati attesi del proprio sistema di gestione della sicurezza delle informazioni" (ISO/IEC 27001:2022, Sez. 4.1).

Leadership

La sezione 5 sottolinea l'importanza della leadership nel promuovere la sicurezza delle informazioni e nel garantire che l'ISMS sia integrato nei processi aziendali. La direzione deve dimostrare il proprio impegno, definire una politica per la sicurezza delle informazioni e assicurare che i ruoli e le responsabilità siano chiaramente assegnati.

"L'alta direzione deve dimostrare leadership e impegno rispetto al sistema di gestione della sicurezza delle informazioni assicurando che esso sia integrato nei processi aziendali e promuovendo un approccio basato sul rischio" (ISO/IEC 27001:2022, Sez. 5.1).

Pianificazione

La sezione 6 si concentra sulla pianificazione per affrontare i rischi e le opportunità relative alla sicurezza delle informazioni. Le organizzazioni devono identificare i rischi per la sicurezza delle informazioni, valutare l'impatto di tali rischi e definire piani di trattamento del rischio.

"L'organizzazione deve pianificare azioni per affrontare i rischi e le opportunità, garantendo che il sistema di gestione della sicurezza delle informazioni possa conseguire i risultati attesi" (ISO/IEC 27001:2022, Sez. 6.1).

Supporto

Il capitolo 7 riguarda le risorse necessarie per implementare e mantenere l'ISMS. Questo include la gestione delle competenze, la consapevolezza e la comunicazione all'interno dell'organizzazione. La norma sottolinea l'importanza di garantire che tutto il personale comprenda il ruolo che svolge nella protezione delle informazioni.

"L'organizzazione deve determinare e fornire le risorse necessarie per stabilire, implementare, mantenere e migliorare continuamente il sistema di gestione della sicurezza delle informazioni" (ISO/IEC 27001:2022, Sez. 7.1).

Attività operative

La sezione 8 copre la pianificazione e il controllo operativo, richiedendo che le organizzazioni attuino le misure necessarie per affrontare i rischi per la sicurezza delle informazioni. Questo include la gestione degli asset, il controllo degli accessi, la cifratura dei dati e la preparazione alle emergenze.

"L'organizzazione deve pianificare, implementare e controllare i processi necessari per soddisfare i requisiti di sicurezza delle informazioni, assicurando che siano adottate misure per proteggere le informazioni da accessi non autorizzati" (ISO/IEC 27001:2022, Sez. 8.1).

Valutazione delle prestazioni

La sezione 9 tratta la valutazione delle prestazioni dell'ISMS, che include il monitoraggio, la misurazione, l'analisi e la valutazione dell'efficacia del sistema. La norma richiede la conduzione di audit interni regolari e la revisione della direzione per garantire il miglioramento continuo.

"L'organizzazione deve monitorare e misurare l'efficacia del sistema di gestione della sicurezza delle informazioni e analizzare i dati raccolti per migliorare continuamente la sicurezza delle informazioni" (ISO/IEC 27001:2022, Sez. 9.1).

Miglioramento

L'ultima sezione della norma, la sezione 10, si concentra sul miglioramento continuo del sistema di gestione. Le organizzazioni devono gestire le non conformità e adottare azioni correttive per prevenire il ripetersi di incidenti di sicurezza.

"L'organizzazione deve identificare e attuare opportunità di miglioramento per aumentare l'efficacia del sistema di gestione della sicurezza delle informazioni e garantire che le informazioni siano protette in modo adeguato" (ISO/IEC 27001:2022, Sez. 10.2).

Vantaggi dell'implementazione della ISO 27001

L'adozione della norma ISO 27001 offre numerosi vantaggi alle organizzazioni, tra cui:

-Protezione delle informazioni

-Salvaguardia della riservatezza, integrità e disponibilità delle informazioni.

-Conformità normativa: garantisce la conformità alle leggi e regolamenti in materia di sicurezza delle informazioni, come il GDPR.

-Riduzione dei rischi: minimizza i rischi di violazioni della sicurezza e di perdita di dati.

-Vantaggio competitivo: rafforza la fiducia dei clienti e migliora la reputazione dell'organizzazione.

-Miglioramento della gestione: fornisce un quadro strutturato per la gestione della sicurezza delle informazioni.

Processo di certificazione

Il processo di certificazione ISO 27001 segue diverse fasi chiave:

-Preparazione: comprendere i requisiti della norma e sviluppare un piano per implementare un ISMS.

-Implementazione: stabilire politiche, procedure e controlli per conformarsi alla norma.

-Audit interno: condurre audit interni per verificare l'efficacia dell'ISMS.

-Riesame della direzione: la direzione deve esaminare i risultati degli audit e altre informazioni rilevanti per assicurare l'adeguatezza e l'efficacia dell'ISMS.

-Audit esterno: un organismo di certificazione indipendente valuta la conformità dell'organizzazione alla ISO 27001.

-Certificazione: se i requisiti sono soddisfatti, l'organizzazione ottiene la certificazione ISO 27001.

Conclusione

La ISO/IEC 27001:2022 è uno standard essenziale per qualsiasi organizzazione che gestisce informazioni sensibili. Implementare questa norma non significa solo proteggere i dati aziendali, ma anche dimostrare l'impegno verso la sicurezza delle informazioni e la conformità alle normative. La certificazione ISO 27001 non è solo un mezzo per proteggere le informazioni, ma anche un vantaggio competitivo in un mercato sempre più attento alla sicurezza. Attraverso il miglioramento continuo e l'approccio sistematico alla gestione dei rischi, le organizzazioni possono rafforzare la loro resilienza contro le minacce informatiche e garantire la fiducia dei clienti e dei partner commerciali. In sintesi, l'adozione della ISO 27001 è un passo strategico che consente alle organizzazioni di proteggere le loro informazioni più preziose

In sintesi, l'adozione della ISO/IEC 27001:2022 è un passo strategico fondamentale per le organizzazioni che desiderano proteggere le loro informazioni più preziose in un contesto sempre più digitale e vulnerabile. Implementare questa norma non solo offre una protezione robusta contro le minacce alla sicurezza delle informazioni, ma dimostra anche un impegno

concreto verso la conformità normativa e la protezione dei dati dei clienti e delle parti interessate. La certificazione ISO 27001 può fornire un significativo vantaggio competitivo, rafforzando la fiducia dei clienti e dei partner commerciali, e contribuendo a costruire una reputazione solida e affidabile nel mercato. Tuttavia, è importante considerare l'implementazione dell'ISMS come un processo dinamico, che richiede un miglioramento continuo e un monitoraggio costante per affrontare i nuovi rischi e le sfide emergenti. Investire nella sicurezza delle informazioni attraverso la ISO 27001 non è solo una necessità per proteggere l'organizzazione, ma è anche una scelta strategica per garantirne la resilienza e il successo a lungo termine in un mondo in cui la sicurezza dei dati è sempre più cruciale.

Il nostro corso

PARTE I

0.Introduzione alla struttura del corso (min.3.45)

1°Lezione- INTRODUZIONE ALLA ISO 27001: CONCETTI CHIAVE E SCOPO (min. 22.34)

1. Definizione

2. Origine

3. Scopo

4. Benefici

5. Concetto Di Sistema Di Gestione Della Sicurezza Delle Informazioni (SGSI)

6. La Triade Cia: Riservatezza, Integrità, Disponibilità

7. Principio di Approccio Basato sul Rischio

8. Politiche e Procedure nel Contesto ISO 27001

9. Ciclo PDCA (Plan-Do-Check-Act)

10. Certificazione ISO 27001

2°Lezione- LA STRUTTURA DELLA NORMA ISO 27001 E PANORAMICA DELLE SEZIONI (min. 31.10)

1. Obiettivi
2. Struttura Generale
3. Panoramica Delle Clausole
4. Contesto dell’Organizzazione
5. Leadership
6. Pianificazione
7. Supporto
8. Operatività
9. Valutazione delle Prestazioni
10. Miglioramento
11. Annex A-Controlli di Sicurezza: versione 27001:2013 e 27001:2022
12. Annex A: esempio caso pratico
13. Integrazione con Altri Standard ISO

3°Lezione- IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (SGSI) (min.20.13)

1. Obiettivi
2. Introduzione al Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
3. Componenti chiave di un SGSI
4. Il Ruolo della Leadership nel SGSI
5. Politiche e Procedure nel SGSI
6. La Gestione dei Rischi nel SGSI
7. Operatività del SGSI
8. Monitoraggio e Valutazione delle Prestazioni
9. Miglioramento Continuo del SGSI

4°Lezione- VALUTAZIONE E GESTIONE DEL RISCHIO NELLA ISO 27001 (min.20.17)

1. Obiettivi
2. Introduzione alla Gestione del Rischio
3. Processo di Gestione del Rischio nella ISO 27001

4. Identificazione dei Rischi
5. Valutazione dei Rischi
6. Applicazione dei Controlli di Sicurezza (Annex A)
7. Trattamento dei Rischi
8. Accettazione del Rischio Residuo
9. Monitoraggio e Revisione dei Rischi

5°Lezione- RUOLI E RESPONSABILITA' NELLA SICUREZZA DELLE INFORMAZIONI (min. 26.27)

1. Obiettivi
2. Introduzione ai Ruoli e Responsabilità
3. Il Ruolo della Leadership
4. Responsabile della Sicurezza delle Informazioni (CISO)
5. Responsabilità del Personale IT
6. Coinvolgimento delle Risorse Umane
7. Ruoli Specifici nella Gestione del Rischio
8. Gestione degli Incidenti di Sicurezza
9. Il Ruolo del Team Legale e Conformità
10. Coinvolgimento dei Fornitori
11. Formazione e Consapevolezza del Personale

6°Lezione- ANNEX A- controlli di sicurezza e misure tecniche (min. 22.50)

1. Introduzione all'Annex A della ISO 27001
2. Annex A - le versioni della norma
3. Categorie di Controlli dell’Annex A VERSIONE 2013
4. Categorie di Controlli dell’Annex A VERSIONE 2022
5. Gli 11 NUOVI CONTROLLI
6. 1 – THREAT INTELLIGENCE
7. 2 - SICUREZZA DEI SERVIZI CLOUD
8. 3- DATA MASKING
9. 4-PREVENZIONE DELLE FUGHE DI DATI (DLP)
10. 5-MONITORAGGIO DELLE ATTIVITA’ DI SICUREZZA
11. Come implementare i nuovi controlli
12. Benefici della nuova struttura Annex A

7°Lezione- "Implementazione delle Politiche di Sicurezza delle Informazioni" (min. 23.30)

1. Obiettivi

2. Definizione di Politica di Sicurezza delle Informazioni
3. Requisiti per la Politica di Sicurezza secondo la ISO 27001
4. Struttura di una Politica di Sicurezza delle Informazioni
5. Sviluppo delle Politiche di Sicurezza
6. Comunicazione della Politica di Sicurezza
7. Implementazione delle Politiche di Sicurezza
8. Monitoraggio e Revisione delle Politiche di Sicurezza
9. Miglioramento Continuo delle Politiche di Sicurezza

8°Lezione- "Pianificazione e Monitoraggio del Sistema di Gestione ISO 27001" (min. 13.30)

1. Obiettivi
2. Importanza della Pianificazione nel SGSI
3. Pianificazione della Gestione del Rischio
4. Trattamento dei Rischi Identificati
5. Obiettivi per la Sicurezza delle Informazioni
6. Pianificazione delle Modifiche
7. Risorse per il SGSI
8. Monitoraggio e Misurazione del SGSI
9. Audit Interno del SGSI
10. Riesame della Direzione

11. Azioni Correttive e Miglioramento

9°Lezione- “Audit Interni ed Esterni: Conformità e Verifica” (min. 18.07)

1. Obiettivi
2. Definizione di Audit nel Contesto della ISO 27001
3. Tipi di Audit nella ISO 27001
4. Parti che Compongono un Audit
5. Ruoli e Responsabilità durante un Audit
6. Pianificazione di un Audit
7. Esecuzione dell'Audit
8. Reporting dei Risultati
9. Azioni Correttive
10. Monitoraggio Post-Audit
11. Come si Svolge un Audit (Elenco Puntato)
12. Esempio di Audit Interno - Caso Pratico
13. Esempio di Audit Esterno - Caso Pratico
14. Differenze tra Audit Interno ed Esterno
15. Benefici degli Audit per l’Organizzazione

10°Lezione-"La Gestione delle Incidenze di Sicurezza delle Informazion (Min. 23.07)

1. Obiettivi
2. Definizione di Incidente di Sicurezza
3. Obiettivi della Gestione degli Incidenti
4. Fasi della Gestione degli Incidenti
5. Ruoli e Responsabilità nella Gestione degli Incidenti
6. Strumenti per la Rilevazione degli Incidenti
7. Esempio di Incidente di Sicurezza
8. Azioni Correttive
9. Miglioramento Continuo e Analisi Post-Incidente

PARTE II

Introduzione (min. 2.42)

Appendice: Come ottenere la ISO 27001 (min.23.44)

Appendice II: PDCA (min. 29)

Appendice III: La gestione del rischio (min.22.22)

Appendice IV: Audit (min.51.47)

Appendice V: Annex A (min.19.20)