

## Sistemi di Gestione Sicurezza Informazioni (SGSI) ISO/IEC 27001

La norma ISO/IEC 27001 è uno standard internazionale, promosso dalla ISO (International organization for standardization) e dalla IEC (International electrotechnical commission), per la gestione della sicurezza delle informazioni, che un'organizzazione adotta per:

- pianificare
- attuare
- operare
- monitorare
- riesaminare
- mantenere
- migliorare

il sistema di gestione per la sicurezza delle informazioni delle aziende.

La ISO/IEC 27001 è la capogruppo della famiglia di norme SGSI serie ISO/IEC 27000 che:

- definiscono i requisiti per creare un SGSI
- forniscono una guida per progettare, attuare, mantenere e migliorare un SGSI
- esprimono le linee guida nei vari ambiti di utilizzo di un SGSI
- valutano la conformità di un SGSI

Oltre alla ISO/IEC 27001 la certificazione permette di attuare delle estensioni ad altre norme che descrivono le linee guida negli specifici ambiti/settori come a titolo di esempio

- ISO/IEC 27017, Codice di condotta per i controlli di sicurezza delle informazioni su servizi in cloud
- ISO/IEC 27018, Codice di condotta per la protezione delle informazioni di identificazione personale (PII) in cloud pubblici che agiscono come processori PII
- ISO/IEC 27701 - Standard internazionale per la gestione delle informazioni sulla privacy
- ISO 27799 - Gestione della sicurezza delle informazioni in materia di salute utilizzando ISO/IEC 27002

**BRESCIA**  
Le Tre Torri - Via Flero, 46  
25125 Brescia (BS)

**TORINO**  
Corso Vinzaglio, 12  
10121 Torino (TO)

**MILANO**  
Via Vittor Pisani, 8  
20124 Milano (MI)

**CAMPIONE D'ITALIA**  
Via Belvedere, 14  
22060 Campione d'Italia (CO)

**SOFIA**  
Ul. Georgi Benkovski, 14  
1000 Sofia Center

Tel. +39 030 447 51  
info@q-aid.it  
www.q-aid.it

## PERCHÉ CERTIFICARSI ISO/IEC 27001

Con l'applicazione delle indicazioni contenute nello standard ISO/IEC 27001, un'organizzazione può analizzare e verificare i propri rischi ed individuare le minacce che possono intaccare la propria azienda. Lo standard consente un approccio complessivo alla sicurezza delle informazioni in tutti gli ambiti interessati: dai documenti in formato digitale a quelli in formato cartaceo, dalle strumentazioni hardware (computer e reti) alle competenze del personale.

Il vantaggio reale della certificazione ISO/IEC 27001 è permettere di dimostrare che l'azienda è in grado di garantire che le informazioni gestite (incluse quelle relative ai clienti e segreti industriali), siano riservate, ottenute da fonti integre e prontamente disponibili.

La ISO 27001 è facilmente integrabile con altri sistemi di gestione, quali ISO 9001 (sistema di gestione della qualità), ISO 45001 (sistemi per la salute e sicurezza sul lavoro), ISO 14001 (sistemi di gestione ambientale) e ISO 50001 (sistemi di gestione dell'energia), ed i suoi obiettivi possono essere inclusi nel piano di miglioramento continuo.

## DESTINATARI

La Norma ISO 27001 si rivolge a qualsiasi tipologia di organizzazione pubblica o privata, di ogni settore e dimensione, manifatturiera o di servizi.

## VANTAGGI

- Miglioramento dell'immagine e della reputazione sul mercato
- Capacità di soddisfare le esigenze e le aspettative dei clienti
- Gestione in modo tracciato dei flussi delle informazioni
- Analisi preventiva e predittiva delle minacce e delle vulnerabilità
- Attuazione di piani di business continuity nella gestione delle informazioni

## ITER DI CERTIFICAZIONE

- Riesame del Contratto e invio dell'offerta
- Ricezione dell'offerta e pianificazione dell'audit
- Esecuzione dell'audit di Certificazione (Stage1 e Stage2)
- Decisione per il rilascio della Certificazione
- Rilascio del certificato
- Sorveglianze periodiche per la conferma della Certificazione

### BRESCIA

Le Tre Torri - Via Flero, 46  
25125 Brescia (BS)

### MILANO

Via Vittor Pisani, 8  
20124 Milano (MI)

### TORINO

Corso Vinzaglio, 12  
10121 Torino (TO)

### CAMPIONE D'ITALIA

Via Belvedere, 14  
22060 Campione d'Italia (CO)

### SOFIA

Ul. Georgi Benkovski, 14  
1000 Sofia Center

Tel. +39 030 447 51  
info@q-aid.it  
www.q-aid.it

## RIFERIMENTI NORMATIVI

- ISO/IEC 27001, Sistemi di gestione per la sicurezza delle informazioni - Requisiti
- ISO/IEC 27002, Codice di condotta per i controlli di sicurezza delle informazioni
- ISO/IEC 27003, Guida all'implementazione dei SGSI
- ISO/IEC 27004, Gestione della sicurezza delle informazioni - Misurazione
- ISO/IEC 27005, Gestione dei rischi per la sicurezza delle informazioni
- ISO/IEC 27006, Requisiti per gli organismi che forniscono audit e certificazione dei SGSI
- ISO/IEC 27007, Linee guida per la verifica dei SGSI
- ISO/IEC TR 27008, Linee guida per i revisori dei controlli di sicurezza delle informazioni
- ISO/IEC 27009, Applicazione specifica per settore di ISO / IEC 27001 - Requisiti
- ISO/IEC 27013, Guida per l'implementazione integrata di ISO/IEC 27001 e ISO/IEC 20000-1
- ISO/IEC 27014, Governance della sicurezza delle informazioni
- UNI CEI EN ISO/IEC 17021-1:2015 - Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione

### BRESCIA

Le Tre Torri - Via Flero, 46  
25125 Brescia (BS)

### MILANO

Via Vittor Pisani, 8  
20124 Milano (MI)

### TORINO

Corso Vinzaglio, 12  
10121 Torino (TO)

### CAMPIONE D'ITALIA

Via Belvedere, 14  
22060 Campione d'Italia (CO)

### SOFIA

Ul. Georgi Benkovski, 14  
1000 Sofia Center

Tel. +39 030 447 51  
info@q-aid.it  
www.q-aid.it