

“



”



Certificazione sistemi di Gestione della Sicurezza delle Informazioni
Norma ISO 27001

“ Il CSQ, grazie alla vasta esperienza maturata nei maggiori contesti produttivi, è in grado di offrire servizi dedicati alle aziende sensibili al tema della sicurezza che vogliono confrontare le loro soluzioni con la ISO 27001 la norma di riferimento per la sicurezza delle informazioni. ”



La sicurezza dei sistemi informatici rappresenta oggi una delle priorità per molte società che operano in realtà economiche nazionali ed internazionali. Non tutte le aziende sono tuttavia a conoscenza della gamma di benefici che un sistema di sicurezza può apportare, non solo all'infrastruttura informatica aziendale, ma anche al patrimonio della proprietà intellettuale.

Una valutazione delle esigenze di sicurezza è il punto di partenza ideale per predisporre le soluzioni più adatte a soddisfare i bisogni di ogni azienda.

Se la new-economy ha portato infatti a una notevole accelerazione negli scambi attraverso i supporti elettronici (tipici sono gli esempi in settori quali il bancario, l'assicurativo e il turistico) e dunque a un'esigenza della sicurezza delle transazioni, la tutela della privacy ha comportato che anche gli archivi cartacei debbano essere soggetti ai requisiti minimi di sicurezza (come ampiamente confermato dalla Legge 675/96, dal DPR 318/99 e dal nuovo Codice in materia di protezione dei dati personali 196/03).

E' ormai noto che la sicurezza non può essere raggiunta e garantita solo attraverso mezzi tecnici (firewall, antivirus, crittografia e firma digitale); diventa dunque indispensabile rendere operativo un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) basato su un insieme di controlli, derivanti dalle politiche aziendali e da applicare a tutti i processi di business e di supporto.

Panorama normativo e legislativo per la sicurezza delle informazioni

La legislazione italiana, che disciplina il trattamento dei dati personali, l'individuazione delle misure minime di sicurezza, il diritto d'autore, la tutela giuridica dei programmi per elaboratore, la firma digitale e l'utilizzo della posta elettronica certificata, è riassunta nei seguenti principali atti.

La conformità alla direttiva

- **Decreto Legislativo 196/2003** "Codice in materia di protezione dei dati personali".
- **Decreto del Presidente della Repubblica 10 novembre 1997, n. 513** "Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59".
- **Decreto Legislativo 7 marzo 2005, n. 82** "Codice dell'amministrazione digitale", a norma dell'articolo 33 della legge 18 giugno 2009, n. 69, modificato ed integrato dal Decreto legislativo 30 dicembre 2010, n. 235.
- **Decreto Legislativo 29 dicembre 1992 n. 518** "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore".
- **Legge 23 dicembre 1993 n. 547** "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".
- **Decreto legislativo 30 maggio 2008 , n. 109** "Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE".
- **Decreto Legislativo 9 aprile 2003, n. 68** "Attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione".
- **Decreto Legislativo 16 marzo 2006, n.140** "Attuazione della direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale".
- **Decreto Legislativo 6 maggio 1999, n. 169** "Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati".



Norme volontarie:

- **ISO 27001**
Information Technology
Security Techniques
Information Security Management Systems.
- **ISO 27002**
Information Technology
Code of practice for Information Security Management.

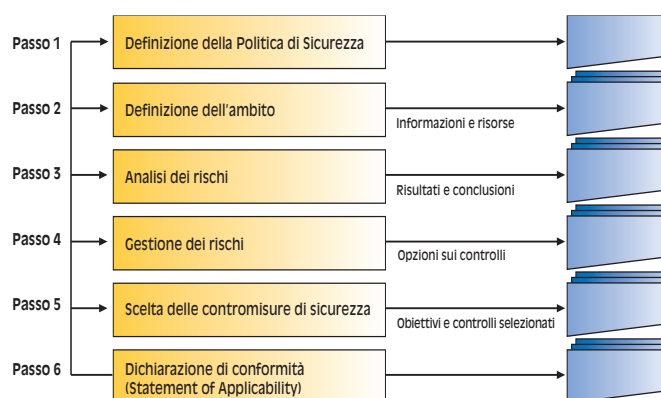
Lo schema di certificazione CSQ-DATA

Al fine del rilascio della certificazione ISO 27001 il CSQ ha sviluppato un apposito schema denominato CSQ-DATA.

CSQ-DATA è uno schema che permette alle Organizzazioni di certificare il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI), valutando in particolare i seguenti aspetti:

- Politica della Sicurezza
- Analisi delle vulnerabilità e gestione dei rischi
- Esistenza di una organizzazione dedicata alla sicurezza
- Definizione dei controlli utili a implementare la sicurezza
- Procedure per la gestione della sicurezza
- Valutazione e riesame periodico del SGSI adottato

LE TAPPE PER REALIZZARE UN SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI



Il processo di certificazione

Si svolge generalmente in almeno due fasi, entrambe per identificare la conformità alla ISO 27001.

Fase 1: Controllo documentazione

Valutazione della documentazione a supporto del SGSI, dal manuale di gestione della sicurezza al documento di analisi dei rischi. Può essere condotta nella sede dell'organizzazione ed è inerente a tutta la documentazione principale dell'Information Security Management System (ISMS).

Fase 2: Audit dell'organizzazione

Visita presso l'azienda basata su interviste, esame di documenti, confronti tra procedure formalizzate e prassi operative. Il principio è di verificare che l'organizzazione sia aderente alle proprie politiche, obiettivi, procedure e che l'ISMS sia efficace.

Gli obiettivi

Proteggere i Dati e le Informazioni da una vasta gamma di minacce (accesso non autorizzato, distruzione e furto dati, interruzione di servizio, virus informatici) al fine di assicurare la continuità dell'attività aziendale. Avere un corretto sistema di gestione della sicurezza delle informazioni significa dotarsi di tutte le misure di sicurezza, assicurando i dati in termini di riservatezza, integrità e disponibilità.

- Riservatezza: affinché tutte le informazioni siano accessibili solo alle persone autorizzate
- Integrità: per prevenire le modifiche indebite, accidentali o fraudolente alle informazioni
- Disponibilità: per assicurare che gli utenti possano accedere ai dati sulla base dei propri profili specifici di abilitazione in tempi congruenti con le proprie esigenze operative.

I vantaggi della certificazione CSQ-DATA

La certificazione del sistema di gestione della sicurezza delle informazioni permette di:

- facilitare il rispetto dei requisiti contrattuali e legislativi
- rafforzare la credibilità e la visibilità dell'azienda salvaguardandone l'immagine e il patrimonio e facilitando il reperimento delle informazioni
- gestire i costi degli incidenti della sicurezza
- finalizzare in modo efficace gli investimenti impiegati per implementare i controlli della sicurezza
- assicurare e dare evidenza agli stakeholders che si sono attuati tutti gli strumenti e le misure tecniche e organizzative necessari per garantire l'Information Security.

Gli accreditamenti IMQ

I principali traguardi raggiunti da IMQ nell'ambito degli accreditamenti della sicurezza IT sono:

1. IMQ è ente di certificazione accreditato dal SINCERT per rilasciare certificati in conformità alla norma ISO 27001 in tutti i settori corrispondenti alla classificazione internazionale EA (European Cooperation for Accreditation).
2. Il Laboratorio Prove Sicurezza (LPS) di IMQ è in grado di eseguire attività di valutazione della sicurezza informatica secondo gli standard di riferimento ITSEC e Common Criteria (ISO/IEC 15408). Esso è accreditato nello Schema Nazionale per la Valutazione e Certificazione della Sicurezza dei sistemi e prodotti ICT.

Certificazione sistemi di gestione della sicurezza delle informazioni: i settori industriali di interesse e le aree di attenzione

Una corretta gestione della sicurezza è ormai un elemento indispensabile per tutte le aziende che considerano il loro patrimonio informativo e gli Asset aziendali risorse da proteggere. Le aziende, dunque, devono identificare le specifiche criticità a seconda del settore merceologico di appartenenza.

Settore finanziario

Il mondo dei servizi finanziari comprende diversi settori, dalle banche alle società di assicurazione, tutti accomunati dalla necessità di impiegare sistemi di rete per eseguire transazioni monetarie e di dati. Elementi peculiari sono:

- Protezione delle transazioni.
- Protezione dei dati.
- Pagamenti elettronici.

Le aziende finanziarie che non sono in grado di fornire adeguati livelli di sicurezza rischiano di subire frodi di varia natura oltre ad esporre i propri clienti al pericolo di truffe informatiche.

Settore Industria

A seguito della rapida diffusione della tecnologia informatica nel settore manifatturiero, la sicurezza dei sistemi IT si sta affermando come una delle priorità tra le aziende operanti nei settori più tradizionali dell'industria. Nel mondo del manifatturiero si possono individuare le seguenti peculiarità:

- Marketplace B2B
- Accesso remoto ai lavoratori
- Vincoli legislativi in particolari settori (chimico, armamenti, agroalimentare)
- Spionaggio industriale

La protezione dei segreti industriali è quindi una delle maggiori aree di criticità dell'industria manifatturiera, da cui l'inevitabile esigenza di proteggere la proprietà intellettuale.

Settore Pubblico

Il settore pubblico raggruppa molte aree differenti, per le quali i temi della sicurezza dei sistemi IT sono di fondamentale importanza; in particolare questi riguardano la pubblica amministrazione propriamente detta (PA), la difesa e la sanità.

Per la PA le aree di interesse riguardano i progetti di e-government e le relazioni con i cittadini, con le aziende e tra dipartimenti interni. Tutte iniziative fortemente legate a Internet e con elevati rischi di interruzione del servizio. Tra le priorità in termini di sicurezza si ribadisce pertanto la gestione delle transazioni e la sicurezza dell'accesso a Internet e alle intranet pubbliche.



Per il comparto della difesa le problematiche urgenti, legate alla security, riguardano l'affidabilità dei sistemi di massima sicurezza e la protezione da attacchi, sia virtuali alle reti sia fisici alle infrastrutture.

L'integrità delle informazioni è un tema critico anche per il settore della sanità, che deve implementare sistemi efficienti di controllo degli accessi, assicurando nel contempo la disponibilità - ai professionisti del settore - di informazioni sensibili sui pazienti. Da qui la necessità di porre attenzione su soluzioni sia di tipo organizzativo che di sicurezza IT (controllo accessi, comunicazioni, difesa elettronica).

CHI È IMQ

Il Gruppo IMQ rappresenta la più importante realtà italiana nel settore della valutazione della conformità (certificazione, prove, verifiche, ispezioni). Forte della sinergia tra le società che lo compongono, dell'autorevolezza acquisita in 60 anni di esperienza, della completezza dei servizi offerti, il Gruppo IMQ si pone infatti come punto di riferimento e partner delle aziende che hanno come obiettivo la sicurezza e la qualità.

I settori di riferimento sono molteplici spaziando dall'elettrotecnica all'elettronica, dalle telecomunicazioni all'automotive, dal gas all'impiantistica, dai prodotti da costruzione all'agroalimentare e così via. Per ogni categoria merceologica, il Gruppo IMQ è in grado di offrire, a seconda dei casi, servizi di tipo orizzontale o mirato:



certificazione di prodotto, certificazione secondo le direttive CE, certificazione di sistemi di gestione aziendale, verifiche su impianti ed immobili, prove di laboratorio e per l'ottenimento di omologazioni internazionali, supporto all'esportazione, sorveglianza di produzioni all'estero, assistenza tecnico-normativa e formazione.

La completezza dei servizi erogati è assicurata grazie alla competenza maturata in molteplici aree merceologiche dalle società del Gruppo IMQ che è composto da:

IMQ S.p.A. - CSI S.p.A. - IMQ Primacontrol S.r.l. - IMQ Clima S.p.A. - ICILA S.r.l. - IMQ Iberica S.L. - IMQ Kraków R.O. (Ufficio di rappresentanza in Polonia) - IMQ Certification Shanghai Co. LTD. Il Gruppo IMQ vanta inoltre una partecipazione nell'Istituto Giordano S.p.A., in CISQCERT S.p.A. e in Icube S.A. (Argentina).

Per ulteriori informazioni

Segreteria commerciale: commerciale.csq@imq.it - tel. +39 025073222 - fax +39 0250991544

Italia - Milano - Sede principale

Via Quintiliano 43, 20138 - Milano

Tel. +39 0250731 - Fax +39 0250991500 - info@imq.it - www.imq.it

Polonia - Kraków

IMQ Krakow Rep. Office - ul. Kraszewskiego 36 - 30-110 Kraków

Spagna - Madrid

IMQ Iberica - c/Diego de León, 69 - 5a planta - 28006 Madrid

Cina - Shanghai

IMQ Certification Shanghai Co. LTD - Room 6a, Zhao Feng World Trade Building - 369, Jiangsu Road - 200050 Shanghai

Argentina - Buenos Aires

Icube - Av. Belgrano 624 (C1092AAT) - Buenos Aires

