

“ 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 n. 518 del 29/12/1992** che modifica il Regio Decreto n° 633 del 1941, relativo al diritto d'autore, integrandolo con norme relative alla tutela giuridica dei programmi per elaboratore.
- **Legge n. 547 del 23/12/1993** che modifica il Codice Penale italiano introducendo il tema di criminalità informatica (cosiddetti "computer crimes").
- **Legge n. 675 del 31/12/1996** che disciplina il trattamento dei Dati Personali (Legge sulla Privacy).
- **DPR n. 513 del 10/11/1997** riguardante norme relative al documento informatico e alla firma digitale.
- **DPR n. 318 del 28/07/1999** Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei Dati Personali, a norma dell'articolo 15, comma 2, della legge n° 675 del 31/12/1996.
- **Deliberazione AIPA 42/2001, 13 dicembre 2001 e Note esplicative (G.U. n. 296 del 21-12-01)** Oggetto: Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - articolo 6, commi 1 e 2, del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28, dicembre 2000, n. 445.
- **D.Lgs. 23 gennaio 2002, n. 10 (GU n. 39 del 15-2-2002)** Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.
- **Decreto del Presidente della Repubblica 7 aprile 2003, n.137 (GU n. 138 del 17-6-2003)** Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n.10.
- **Decreto legislativo n. 196 del 30/06/2003** (Codice in materia di protezione dei dati personali).
- **Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 (GU n. 98 del 27-4-2004)** Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.
- **Decreto del Presidente della Repubblica 11 febbraio 2005, n.68 (G.U. n. 97 del 28-4-2005)** Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.

Ricordiamo inoltre la normativa CEE in materia di sicurezza

- **Direttiva 97/66/CE del 15/12/1997** sul trattamento dei Dati Personali e sulla tutela della vita privata nel settore delle Telecomunicazioni.
- **Direttiva 96/9/CE del 11/03/1996** relativa alla "Tutela giuridica delle banche di dati".
- **Direttiva 95/46/CE del 24/10/1995** relativa alla "Tutela delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali Dati".

Norme volontarie:

- **ISO 27001 (ex BS7799 - parte 2)** Information Technology Security Techniques Information Security Management Systems.
- **ISO 27002 (ex BS7799 - parte 1)** Information Technology Code of practice for Information Security Management.

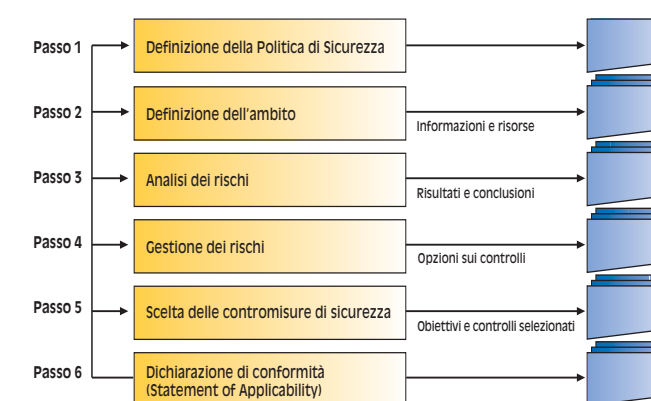
Lo schema di certificazione CSQ-DATA

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.

IMQ, LA CITTÀ DELLA QUALITÀ

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).

Alla scoperta del mondo IMQ

IMQ è la società italiana di prove e certificazioni per la sicurezza e la qualità di prodotti e aziende.

Sorti nel 1951 per volere dei principali organi scientifici e tecnici nazionali, abbiamo moltiplicato negli anni le nostre aree di competenza con l'obiettivo di affermare il nostro ruolo di punto di riferimento per la Sicurezza e la Qualità.

Consideriamo IMQ una vera e propria città della Qualità con le sue diverse aree di competenza: la certificazione di prodotto, la certificazione delle aziende, la certificazione degli impianti. Ma anche l'attività di organismo notificato per le principali direttive CE, i servizi di prova e misura, l'assistenza normativa, il supporto tecnico all'esportazione, la formazione.

Offriamo un servizio di pubblica utilità gestito da tecnici al di sopra delle parti, che usano i più perfezionati strumenti di indagine e che sono quindi in grado di esprimere giudizi tanto obiettivi quanto



scientificamente fondati.

Internazionalmente godiamo di numerosi riconoscimenti dovuti all'appartenenza agli accordi internazionali di certificazione e alla partecipazione di nostri esperti ai lavori normativi di comitati tecnici e scientifici (IEC, ISO, CENELEC,

CEN) e alle riunioni promosse dalle associazioni di costruttori, di installatori e delle commissioni operanti presso i Ministeri.

Il nostro lavoro si rivolge alle aziende e alle imprese interessate a valorizzare la qualità dei loro prodotti o del loro operato, ai consumatori e agli installatori ai quali offriamo un immediato strumento di scelta (grazie ai marchi di sicurezza e di qualità) di prodotti sicuri e di aziende qualificate.

Siamo ente di certificazione accreditato dal Sincert; laboratorio di prova accreditato dal Sinal e, relativamente alle prove di compatibilità elettromagnetica, dal Ministero delle comunicazioni; organismo notificato per le principali direttive CE. Per le verifiche su impianti elettrici e ascensori siamo organismo abilitato dal Ministero delle attività produttive.

Mod. 576/1 - 2008-07/050/Mod.

