SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI UNI CEI ISO/IEC 27001:2006

OBIETTIVI PRIMARI

- **Tutelare il proprio capitale intellettuale**
- **Dotarsi di un sistema di gestione delle informazioni sicuro**
- **Assicurare la continuità aziendale tramite la salvaguardia delle informazioni**
- **Minimizzare i possibili danni legati ad una errata gestione delle informazioni o il loro furto**
- **Garantire l'affidabilità del dato raccolto, ossia essere protetto e garantito nella sua veridicità**
- **Garantire la riservatezza del dato raccolto, ossia essere protetto da utenti non autorizzati al suo trattamento e quindi, garantito nella sua segretezza**
- **Garantirne la reperibilità del dato raccolto, ossia essere sempre disponibile e consultabile dagli operatori autorizzati**
- **La tutela del proprio investimento commerciale, inteso come patrimonio di informazioni sulle indagini di mercato, sull'attività di ricerca scientifica svolta, sulla progettazione e sviluppo dei propri prodotti o servizi e altro**
- **Dotarsi di uno strumento che faciliti il rispetto delle leggi in vigore in termini di tutela dei dati personali, in particolare se sensibili**
- **Integrare la gestione delle informazioni con gli aspetti legati alla qualità, all'ambiente e alla sicurezza sul lavoro (ISO 9001, ISO 14001, OHSAS 18001)**
- **Crescere di competitività e credibilità/visibilità sul mercato di riferimento**
- **Vantare una certificazione di validità mondiale su un tema all'avanguardia**

DISCIPLINA GENERALE

La BS 7799:2 - *Information Security Management System (ISMS)* - è stata la principale norma di riferimento per l'applicazione di un Sistema di gestione per la sicurezza delle informazioni, oggi evoluta nella UNI CEI ISO/IEC 27001:2006 (*ISMS: Information technology -- Security techniques -- Information security management systems -- Requirements*). Tale norma introduce il concetto di "*Sistema di Gestione*", uno strumento che permette di tenere sotto controllo in modo sistematico e continuativo tutti i processi legati alla sicurezza delle informazioni tramite la definizione di ruoli, responsabilità e procedure formali sia per l'operatività aziendale, che per la gestione delle emergenze. Si parla quindi di Sistema di Gestione per la Sicurezza delle Informazioni (SGSI). In origine la BS 7799 era divisa in 2 parti: la parte 1 era la Linea Guida e la parte 2 era lo standard vero e proprio. L'ISO ha adottato con una dichiarazione formale la parte 1 (Linea Guida) del documento BSI (British Standard Institute), che è pertanto diventata ISO 17799:1 (Information technology -- Security techniques -- Code of practice for information security management); e nell'ottobre 2005 ha recepito la seconda parte della BS 7799, che è così diventata la ISO 27001:2005. Se la ISO 17799:1 fornisce delle indicazioni non prescrittive per proteggere il patrimonio informativo di un'azienda, il documento normativo al quale un'organizzazione che intenda certificarsi deve far riferimento è la ISO 27001:2005. Con la serie 27000 (altre norme seguiranno alla 27001) si intende, nei prossimi anni, normare tutto il settore della sicurezza delle informazioni, della gestione dei rischi, delle problematiche di metrica e misurazione, soprattutto dell'efficacia dei sistemi di sicurezza implementati, delle metodologie di attuazione. La serie ISO 27000 è così prevista (ed in parte ancora in fase di realizzazione e pubblicazione):

- ISO/IEC 27000: *Principles and vocabulary*
- ISO/IEC 27001: *Information security management system – Requirements*
- ISO/IEC 27002: *Information technology - Security techniques - Code of practice for information security management*
- ISO/IEC 27003: *ISMS Implementation guidance*
- ISO/IEC 27004: *Information security management metrics and measurement*
- ISO/IEC 27005: *ISMS Risk management*

In un contesto dove le violazioni dei sistemi di sicurezza (**crimini ed attacchi informatici**) sono in continuo aumento, è diventato necessario dotarsi di un **sistema che garantisca una gestione "*sicura*" delle informazioni (rischi informatici).**

Le informazioni custodite con mezzi informatici rappresentano ormai oltre il 60% del "*capitale intellettuale*" aziendale. Sono pertanto un "*patrimonio aziendale*" la cui gestione diventa strategica per la tutela e lo sviluppo aziendale.

Si tratta di garantire:

- Riservatezza
- Disponibilità
- Integrità

CAMPO DI APPLICAZIONE

Rientrano nell'ambito di applicazione della norma **tutte le imprese ed organizzazioni di tutti i settori e dimensioni**.

COME ADEGUARSI?

Secondo la norma ISO/IEC 27001 **la sicurezza viene vista come un processo indipendente dalla tecnologia**. Deve coprire tutti i processi che impattano sulle caratteristiche di *security* del prodotto o servizio immesso sul mercato. Per cui insiste molto sugli aspetti organizzativi e poco su quelli tecnologici. L'impostazione dello standard ISO/IEC 27001, così come della ISO/IEC 17799:2005 (destinata a diventare ISO/IEC 27002), è coerente con quella del Sistema di Gestione per la Qualità ISO 9001:2000 e il *risk management*: l'approccio per processi, la politica della sicurezza, l'identificazione ed analisi dei rischi, la valutazione e trattamento dei rischi, il modello PDCA (*Plan, Do, Check, Act*), utilizzo di procedure e di strumenti come audit interni, esterni di stage 1 e stage 2, non conformità, azioni correttive e preventive, sorveglianza, miglioramento continuo.

A CHI RIVOLGERSI?

Adottare per la propria organizzazione le misure necessarie per adottare un sistema di gestione per la sicurezza delle informazioni certificato secondo la UNI CEI ISO/IEC 27001:2006 **non è particolarmente difficoltoso** se ci si affida ad un buon servizio di consulenza: ELIOS ingegneria è uno studio associato che offre i propri servizi mediante le competenze di ingegneri di diversa formazione, in modo da svolgere un'attività con **standard qualitativi elevati** e con **costi commisurati al servizio** grazie ad una efficiente organizzazione aziendale. Ricordiamo comunque che il servizio risulta essere estremamente impegnativo sul piano tecnico, pertanto vi sono comunque delle difficoltà legate alla complessità delle tematiche trattate.

I SERVIZI DI ELIOS ingegneria

ELIOS ingegneria offre un **Check up iniziale gratuito**: esso consiste in una visita presso la Vostra sede, durante la quale i nostri professionisti definiscono il quadro generale della Vostra situazione, individuando gli adeguamenti obbligatori per la norma. Sulla base del sopralluogo vengono offerti, con la **consulenza alla progettazione del SGSI**, i seguenti servizi:

- **Documenti**
  - Redazione del Manuale della Sicurezza delle Informazioni
  - Redazione delle procedure previste dalla UNI CEI ISO/IEC 27001:2006
  - Redazione delle istruzioni operative necessarie e della modulistica per le registrazioni richieste
- **Formazione e addestramento**
  - Corsi formazione e addestramento al personale per l'applicazione del Sistema di Gestione per la Sicurezza delle Informazioni
- **Assistenza**
  - Consulenza continuativa per la corretta applicazione dei dettami previsti dalle norme e dal Sistema di Gestione per la Sicurezza delle Informazioni adottato
  - Ruolo di Responsabile del Servizio Gestione Sicurezza delle Informazioni esterno
  - Visite ispettive interne
  - Assistenza in occasione della visita ispettiva da parte dell'Ente di certificazione

CONTATTACI

ELIOS ingegneria Studio associato

Via del Redolone 49, Loc. Ponte Stella - 51030 Serravalle Pistoiese (PT)

Tel. 0573 527074 Fax. 0573 520970

www.eliosingegneria.it

info@eliosingegneria.it