



## Gli standard per un "Sistema di Gestione della SICUREZZA delle INFORMAZIONI"

Il British Standards Institution ha redatto le regole di base per la sicurezza dei sistemi IT in UK mediante due documenti: **BS7799-1**, noto come Standard Code of Practice, che fornisce una guida su come rendere sicuro un Sistema Informativo, e **BS7799-2**, noto come Standard Specification, che descrive, in termini di requirement, gli obiettivi di controllo. Nel corso del 2000, il British Standard 7799-1 è diventato standard **ISO 17799** con il titolo di **Code of Practice for Information Security Management**. Obiettivo di tali standard è fornire raccomandazioni per la gestione della sicurezza delle informazioni.

## OBIETTIVI DEL SEMINARIO

Il Seminario ha l'obiettivo di illustrare i nuovi Standard BS/ISO per la gestione della sicurezza dei Sistemi Informativi. Si tratta di una preziosa opportunità per valutare *se e in che misura* l'adozione di questi standard fornisce reali **garanzie di affidabilità** per l'azienda. Particolare enfasi verrà posta alla *valutazione dei costi, dei tempi e delle risorse* necessarie per ottenere la certificazione. Inoltre, poichè ogni azienda ha caratteristiche ed esigenze diverse, il Seminario si soffermerà ad analizzare *se - e a chi* conviene ottenere la certificazione oggi, e fino a che punto questa può costituire un reale strumento di competitività.

# Conoscere i nuovi Standard per la CERTIFICAZIONE BS7799

## Sistema di Gestione della Sicurezza delle Informazioni

Valutare quando e quanto conviene certificarsi

Milano, 10 Ottobre 2002

9.00 *Registrazione dei partecipanti*

9.30 *Apertura dei lavori*

### Introduzione al seminario

- Organizzazione e processi per la sicurezza
- Comportamenti e tecnologia per la sicurezza delle informazioni
- Definizione del Sistema di Gestione

### IN CHE COSA CONSISTE IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

#### Code of Practice (BS7799 part. 1)

- I *control* (elementi di gestione)
- **Norma per l'assessment e la certificazione (BS7799 part. 2)**
- L'infrastruttura del sistema di gestione
- Quali sono le Politiche di Sicurezza
- Come viene effettuata una precisa Analisi di Rischio
- Come viene concretamente gestito il Rischio
- Come avviene la selezione dei *control*
- La dichiarazione di applicabilità

#### Il recepimento in ISO/IEC della BS7799 part 1 (ISO/IEC 17799)

- Modifiche e considerazioni
- Destinazione della norma

### IN CHE MISURA L'OTTENIMENTO DELLA NUOVA CERTIFICAZIONE FORNISCE GARANZIE PER L'AFFIDABILITÀ DEI SISTEMI

#### Valutare quando e quanto conviene adottare gli standard o conseguire la certificazione

- Per quali aziende la certificazione costituisce un fattore di competitività

- Cosa comporta la certificazione a livello organizzativo
- Quanto tempo richiede l'ottenimento delle certificazioni
- I costi da sostenere in funzione delle caratteristiche dell'azienda

### Strumenti operativi pubblici per la creazione di un Sistema di gestione della sicurezza conforme a BS 7799 part 2

- La serie GMITS (ISO/IEC TR 13335)
- La definizione delle Politiche di Sicurezza
- Metodologie pubbliche di *Risk Assessment*
- La selezione delle contromisure

### Cenni ai criteri per la valutazione della sicurezza dei sistemi informatici e loro utilizzo nel sistema di gestione della sicurezza

- Funzionalità e *Assurance* (Garanzia)
- Criteri ITSEC
- Common Criteria (ISO/IEC 15408)
- Protection Profiles e Security Target
- L'utilizzo dei *Security Target* di prodotti certificati

17.30 *Chiusura dei lavori*

### Relatori:

Vittorio Asnaghi  
*Direttore Sviluppo Servizi Informatica*  
Antonella Barberis Rondone  
*Valutatore senior Sicurezza Informatica*  
Mauro Parmagnani  
*Valutatore senior Sicurezza Informatica*  
IMQ

*Durante il seminario sono previsti due Coffee Break e una colazione di lavoro alle 13.00 incluse nel prezzo*

## A CHI SI RIVOLGE IL SEMINARIO

Fin dalla loro nascita questi standard hanno attirato sempre più l'interesse delle aziende tecnologicamente avanzate, nelle quali le informazioni hanno una valenza strategica. In particolare questo seminario si rivolge a:

- Banche e Assicurazioni
- Società di Outsourcing di Sistemi Informatici
- Service Provider
- Operatori di Commercio Elettronico
- Autorità di Certificazioni
- ....e a tutte le aziende che esigono un'alta affidabilità dei propri sistemi informativi

A breve e medio termine si prevede un crescente numero di certificazioni soprattutto da parte dei Vendor ICT, per i quali la certificazione può costituire un importante criterio di selezione da parte dei propri clienti.

**La scorsa edizione di questo seminario (maggio 2002), ha riscontrato un notevole successo: l'indice di soddisfazione è stato infatti del 100%. Lo riproponiamo a grande richiesta!**