IL BS7799

Relatore: Ing. Marcello Mistre, CISA
marcello.mistre@sistinf.it

ALCUNI CONCETTI FONDAMENTALI

BS 7799

ATTIVITA' DELLA SECURITY

STUDIO, SVILUPPO ED ATTUAZIONE DELLE STRATEGIE, DELLE POLITICHE E DEI PIANI OPERATIVI VOLTI A PREVENIRE, FRONTEGGIARE E SUPERARE EVENTI DI NATURA DOLOSA E/O COLPOSA CHE POSSONO DANNEGGIARE LE RISORSE MATERIALI, IMMATERIALI ED UMANE DI CUI L'AZIENDA NECESSITA PER GARANTIRSI UN'ADEGUATA CAPACITA' CONCORRENZIALE NEL BREVE, MEDIO E LUNGO PERIODO

BS 7799

BREVE STORIA

ANNI 90: IL DTI COSTITUISCE UN GRUPPO DI LAVORO PER FORNIRE ALLE AZIENDE UNA GUIDA PER IL GOVERNO DELLA SICUREZZA DEL PATRIMONIO INFORMATIVO

1993: VIENE PUBBLICATA UNA RACCOLTA DI "BEST PRACTISE" (*Code of Practice for Information Security Management*)

1995: IL BSI PUBBLICA LA PRIMA VERSIONE DEL BS7799

1998: VIENE AGGIUNTA UNA SECONDA PARTE ALLO STANDARD (*Specification for Information Security Management Systems*)

1999: REVISIONE DELLE DUE PARTI E PUBBLICAZIONE DEL BS7799-2 1999

BREVE STORIA

2000: LA PARTE 1 DELLO STANDARD DIVENTA STANDARD INTERNAZIONALE ISO (ISO/IEC 17799:200)

2002: LA PARTE 2 DELLO STANDARD VIENE AGGIORNATA PER ARMONIZZARSI CON GLI STANDARD ISO: NASCE IL BS 7799-2:2002

ESEMPIO PARTE 2

A.4 Organizational security

A.4.1 ***Information security infrastructure***
Control objective: To manage information security within the organization.
Controls

A.4.1.1 *Management information security forum*
A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place. The management forum shall promote security through appropriate commitment and adequate resourcing.

BS 7799

ESEMPIO PARTE 1

4 Organizational security

4.1 Information security infrastructure

Objective: To manage information security within the organization.

A management framework should be established to initiate and control the implementation of information security within the organization.

……...

4.1.1 Management information security forum

Information security is a business responsibility shared by all members of the management team. A management forum to ensure that there is clear direction and visible management support for security initiatives should therefore be considered. That forum should promote security within the organization through appropriate commitment and adequate resourcing. The forum may be part of an existing management body. Typically, such a forum undertakes the following:

a) reviewing and approving information security policy and overall responsibilities;

b) monitoring significant changes in the exposure of information assets to major threats;

c) reviewing and monitoring information security incidents;

d) approving major initiatives to enhance information security.

One manager should be responsible for all security related activities.

BS 7799

CARATTERISTICHE

PROPONE UN APPROCCIO PER PROCESSI

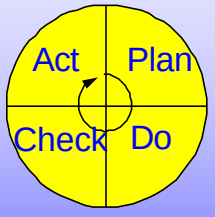
SI BASA SUL CICLO DI DEMING

RUOTA INTORNO A DUE CONCETTI:

- POLITICA DI SICUREZZA
- SISTEMA DI GOVERNO DELLA SICUREZZA

BS 7799

IL CICLO DI DEMING



Plan: stabilire gli obiettivi ed i processi necessari per fornire risultati conformi ai requisiti del cliente ed alle politiche dell'organizzazione;
Do: dare attuazione ai processi;
Check: monitorare e misurare i processi ed i prodotti a fronte delle politiche, degli obiettivi e dei requisiti relativi ai prodotti e riportarne i risultati;
Act: adottare azioni per migliorare in modo continuo le prestazioni dei processi.

BS 7799

LA POLITICA DI SICUREZZA

SPECIFICAZIONE AD ALTO LIVELLO DEGLI OBIETTIVI DI SICUREZZA (ESPRESSI, COME DI CONSUETO IN TERMINI DI VOLONTÀ DI SALVAGUARDARE LA RISERVATEZZA, L'INTEGRITÀ E LA DISPONIBILITÀ DELL'INFORMAZIONE IN PRESENZA DI MINACCE) CHE L'ORGANIZZAZIONE SI PROPONE DI CONSEGUIRE

BS 7799

I S M S

BS 7799

ISMS: Information Security Management System

È IL COMPLESSO DI PROCEDURE PER IL GOVERNO DELLA SICUREZZA ATTUATO E MANTENUTO DALL'ORGANIZZAZIONE PER GARANTIRE NEL TEMPO IL SODDISFACIMENTO DELLA POLITICA DI SICUREZZA

BS 7799

FASE DI PIANIFICAZIONE

DEFINIRE UNA POLITICA PER L'ISMS

DEFINIRE GLI OBIETTIVI

DEFINIRE PROCESSI E PROCEDURE

GESTIRE I RISCHI

MIGLIORARE LA SICUREZZA DELLE INFORMAZIONI

BS 7799

FASE DI ESECUZIONE

FORMULARE UN PIANO DI TRATTAMENTO DEI RISCHI

IMPLEMENTARE IL PIANO DI TRATTAMENTO DEI RISCHI

IMPLEMENTARE LE CONTROMISURE SELEZIONATE PER CONSEGUIRE GLI OBIETTIVI PREFISSATI

IMPLEMENTARE I PIANI DI FORMAZIONE E INFORMAZIONE

GESTIONE OPERATIVA E RISORSE

IMPLEMENTARE LE PROCEDURE DI PRIMO ALLARME E RISPOSTA

BS 7799

FASE DI CONTROLLO

ESEGUIRE LE PROCEDURE DI MONITORAGGIO

SOTTOPORRE L'EFFICACIA DELL'ISMS A REGOLARI REVISIONI

CONDURRE AUDIT INTERNI DELL'ISMS AGLI INTERVALLI PIANIFICATI

REVISIONARE I LIVELLI DI RISCHIO RESIDUO E RISCHIO ACCETTABILE

SOSTENERE LE REVISIONI DA PARTE DEL MANAGEMENT

BS 7799

FASE DI AZIONE CORRETTIVA

IMPLEMENTARE I MIGLIORAMENTI RISULTATI NECESSARI

INTRAPRENDERE LE OPPORTUNE AZIONI PREVENTIVE E CORRETTIVE BASATE SUI RISULTATI DELLA REVISIONE

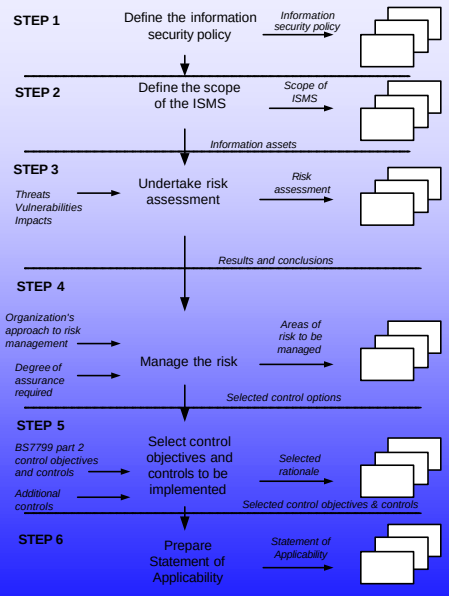
COMUNICARE I RISULTATI E LE AZIONI INTRAPRESE

GARANTIRE CHE I MIGLIORAMENTI CONSEGUANO GLI OBIETTIVI PREFISSATI

BS 7799

LE FASI DI UN ISMS

BS 7799



BS 7799

SCOPO

ANALISI DEL RISCHIO

CONTROL OBJECTIVES AND CONTROLS

POLITICHE STANDARD E PROCEDURE

DOCUMENTAZIONE E DICHIARAZIONE DI APPLICABILITA'

AUDIT E REVIEW

BS 7799

SCOPO

RAPPRESENTA L'AREA CHE DEVE ESSERE COPERTA DALL'ISMS

PUO' COPRIRE UN'INTERA ORGANIZZAZIONE O LIMITARSI A UNA SUA PARTE

È PREFERIBILE CHE SIA DEFINITO ANCOR PRIMA DELLE POLICY

DEVONO ESSERE DEFINITI TUTTI I PROCESSI CHE RIENTRANO NELLO SCOPO

BS 7799

ANALISI DEL RISCHIO

IDENTIFICAZIONE E VALUTAZIONE DEI BENI

DETERMINAZIONE DELLE MINACCE

DETERMINAZIONE DELLE VULNERABILITA'

DETERMINAZIONE DELLE PROBABILITA'

ORDINAMENTO DEI RISCHI

BS 7799

CONTROL OBJECTIVES AND CONTROLS

IDENTIFICAZIONE DEGLI OBIETTIVI DI CONTROLLO

IDENTIFICAZIONE DELLE CONTROMISURE
- SUGGERITE DA BS7799
- INDICATE DA LEGGI E REGOLAMENTI
- INDIVIDUATE DA REQUISITI DEI CLIENTI
- DEDOTTE DA REQUISITI AZIENDALI
- …QUALSIASI ALTRA CONTROMISURA ADEGUATA

BS 7799

POLITICHE, STANDARD E PROCEDURE

DEFINIRE LE POLITICHE

DEFINIRE GLI STANDARD

DESCRIVERE LE PROCEDURE

IMPLEMENTARE LE PROCEDURE

BS 7799

DOCUMENTAZIONE E DICHIARAZIONE DI APPLICABILITA’

PRODUZIONE DELLA DOCUMENTAZIONE

CONTROLLO DEI DOCUMENTI

LE REGISTRAZIONI

LO “STATEMENT OF APPLICABILITY”

BS 7799

AUDIT E REVIEW

REVISIONE CONTINUA

AUDIT INTERNI

REVISIONI DEL MANAGEMENT

BS 7799

FATTORI CRITICI DI SUCCESSO

BS 7799

L'esperienza evidenzia i seguenti fattori come critici per implementare con successo un ISMS

1. SECURITY POLICY, OBIETTIVI E ATTIVITA' CHE RIFLETTANO GLI OBIETTIVI DEL BUSINESS
2. UN APPROCCIO ALLA SICUREZZA COERENTE CON LA CULTURA AZIENDALE
3. SUPPORTO VISIBILE E CONCRETO DEL MANAGEMENT
4. BUONA COMPRENSIONE DEI REQUISITI DI SICUREZZA E DELLA METODOLOGIA ADOTTATA NELL'ANALISI DEL RISCHIO

BS 7799

5. SENSIBILIZZAZIONE ALLE PROBLEMATICHE DI SICUREZZA
6. DISTRIBUZIONE DEI DOCUMENTI DI RIFERIMENTO A IMPIEGATI, COLLABORATORI, FORNITORI
7. TRAINING E FORMAZIONE
8. SISTEMA DI MISURAZIONE

BS 7799

LA CERTIFICAZIONE

BS 7799

FASI DELLA CERTIFICAZIONE

PRE-CERTIFICAZIONE

CERTIFICAZIONE

POST-CERTIFICAZIONE

BS 7799

BENEFICI DIRETTI

Valorizzazione degli investimenti

Rafforzamento dell'immagine aziendale

Segnale forte verso un mercato sempre più sensibile alle problematiche di sicurezza

Fattore di vitalità per il sistema di gestione stesso, che ne assicura efficienza/efficacia e rispondenza ai requisiti legali e contrattuali

Strumento di supporto verso enti regolamentatori e autorizzatori

BS 7799

BENEFICI INDIRETTI

Influenza positiva sull'immagine aziendale e sui parametri di goodwill esterna, fino ad una possibile incidenza sulla valutazione patrimoniale

Valenza come strumento di gestione del risk management e delle modalità operative, anche rispetto ai parametri di legge

Riduzione dei costi di gestione della sicurezza e miglioramento nell'efficienza dei processi

Miglioramento del ROI sugli investimenti informatici dovuto a una focalizzazione mirata alla luce dell'analisi e della valutazione dei rischi