

Indice

| | | |
|----------|---|-----------|
| 1 | Introduzione | 13 |
| 1.1 | Definizioni | 15 |
| 1.2 | Un po' di storia | 17 |
| 1.2.1 | Sicurezza degli strumenti informatici | 21 |
| 1.2.2 | Qualità del software e dei progetti di sviluppo | 22 |
| 1.3 | Schema generale | 24 |
| 2 | Minacce e vulnerabilità | 27 |
| 2.1 | Agenti | 28 |
| 2.1.1 | Agenti esterni | 28 |
| 2.1.2 | Utenti interni | 31 |
| 2.1.3 | Il fato | 32 |
| 2.2 | Le minacce | 33 |
| 2.2.1 | Minacce di carattere informatico | 33 |
| 2.2.2 | Minacce di carattere non informatico | 47 |
| 2.3 | Vulnerabilità | 51 |
| 3 | Lo scenario | 53 |
| 3.1 | Analisi dell'azienda | 53 |
| 3.2 | Vincoli | 58 |
| 3.3 | Politiche di Sicurezza | 64 |
| 3.4 | Rilevazione dell'infrastruttura del sistema informativo | 67 |
| 3.4.1 | Strumenti informatici | 68 |
| 3.4.2 | Archivi non informatici | 72 |
| 3.4.3 | Rilevazione delle informazioni | 73 |
| 3.4.4 | Posizionamento delle informazioni | 74 |

| | | |
|----------|--|-----------|
| 4 | Il rischio | 77 |
| 4.1 | Rischio operativo | 78 |
| 4.1.1 | Correlazione delle minacce ai componenti del sistema informativo | 79 |
| 4.1.2 | Valutazione delle minacce al sistema informativo | 81 |
| 4.2 | Valutare le informazioni e il sistema informativo | 87 |
| 4.2.1 | Valutazione delle informazioni | 87 |
| 4.2.2 | Valutazione dei componenti del sistema informativo | 91 |
| 4.3 | Calcolo del rischio | 94 |
| 5 | Misure di sicurezza | 99 |
| 5.1 | Misure di carattere organizzativo | 100 |
| 5.1.1 | Assegnazione delle responsabilità | 100 |
| 5.1.2 | Gestione del personale | 103 |
| 5.1.3 | Formazione e sensibilizzazione | 104 |
| 5.1.4 | Telelavoratori | 104 |
| 5.1.5 | Documentazione | 105 |
| 5.1.6 | Gestione dei fornitori | 105 |
| 5.1.7 | Business Continuity Plan | 106 |
| 5.1.8 | Gestione del flusso documentale | 106 |
| 5.1.9 | Controlli | 107 |
| 5.2 | Misure di carattere informatico | 108 |
| 5.2.1 | Identificazione e autenticazione | 108 |
| 5.2.2 | Controllo degli accessi | 116 |
| 5.2.3 | Riutilizzo degli oggetti | 125 |
| 5.2.4 | Registrazione degli eventi | 127 |
| 5.2.5 | Audit | 130 |
| 5.2.6 | Accuratezza | 133 |
| 5.2.7 | Continuità | 137 |
| 5.2.8 | Fail secure | 142 |
| 5.2.9 | Gestione | 143 |
| 5.3 | Sicurezza fisica | 146 |
| 5.3.1 | Controllo degli accessi alla sede | 146 |
| 5.3.2 | Controllo dell'accesso ai locali | 148 |
| 5.3.3 | Controllo dell'accesso agli archivi | 149 |
| 5.3.4 | Sicurezza delle informazioni su supporto fisico | 149 |

| | | |
|----------|---|------------|
| 5.3.5 | Sicurezza fisica degli impianti | 151 |
| 5.3.6 | Incendi ed allagamenti | 153 |
| 6 | Gestire il rischio | 155 |
| 6.1 | Principi fondamentali | 155 |
| 6.2 | Correlazione tra minacce e contromisure | 160 |
| 6.3 | Selezionare le contromisure | 161 |
| 6.4 | Analisi di quanto già fatto | 163 |
| 6.5 | Fare le proprie scelte | 165 |
| 7 | Implementazione delle contromisure | 169 |
| 7.1 | Misure di carattere tecnico | 170 |
| 7.2 | Misure di carattere organizzativo | 171 |
| 7.3 | Controlli periodici | 173 |
| 8 | Certificazioni | 175 |
| 8.1 | BS 7799-2:2002 | 175 |
| 8.1.1 | Pianificare | 177 |
| 8.1.2 | Fare | 179 |
| 8.1.3 | Verificare | 179 |
| 8.1.4 | Agire | 182 |
| 8.2 | Processo di certificazione | 182 |
| | Bibliografia | 185 |