



LIVRO

Gestão da Segurança da Informação: uma visão executiva

Marcos Semola
www.semola.com.br

Editor Campus Elsevier
ISBN: 9788535211917
Autor: Marcos Sêmola
Lançamento: 11/12/2002
+ VENDIDO
Indicado ao Prêmio JABUTI 2003
Páginas: 184

PREFÁCIO - XIII

CAPÍTULO 1: SOCIEDADE DO CONHECIMENTO - 1

- 1.1 Informação: ativo cada vez mais valorizado - 1
- 1.2 Crescimento da Dependência - 2
- 1.3 Visão holística do Risco - 5
- 1.4 Receita explosiva - 7
- 1.5 Ciclo de Vida da Informação - 9
 - Manuseio - 10
 - Armazenamento - 10
 - Transporte - 10
 - Descarte - 10

CAPÍTULO 2: DESAFIOS - 13

- 2.1 Anatomia do Problema - 13
- 2.2 Visão Corporativa - 16
 - Vulnerabilidades × Ameaças - 18
- 2.3 Pecados praticados - 20
- 2.4 Conscientização do Corpo Executivo - 20
- 2.5 Retorno sobre o Investimento - 23
- 2.6 Posicionamento Hierárquico - 27
- 2.7 Gerência de Mudanças - 28
- 2.8 Modelo de Gestão Corporativa de Segurança - 31
 - Comitê Corporativo de Segurança da Informação - 33
 - Mapeamento de Segurança - 33
 - Estratégia de Segurança - 33
 - Planejamento de Segurança - 34
 - Implementação de Segurança - 34
 - Administração de Segurança - 35
 - Segurança na Cadeia Produtiva - 35
- 2.9 Agregando Valor ao Negócio - 36

CAPÍTULO 3: KNOWLEDGE CHECKPOINT 1 - 39

- Informação: ativo cada vez mais valorizado - 39
- Crescimento da Dependência - 39
- Visão holística do Risco - 39
- Receita explosiva - 39
- Ciclo de Vida da Informação - 40
- Desafios - 40
- Anatomia do Problema - 40
- Visão Corporativa - 40
- Pecados praticados - 40
- Conscientização do Corpo Executivo - 40
- Retorno sobre o Investimento - 40

Posicionamento Hierárquico - 40
Gerência de Mudanças - 41
Modelo de Gestão Corporativa de Segurança - 41
Agregando Valor ao Negócio - 41

CAPÍTULO 4: SEGURANÇA DA INFORMAÇÃO - 43

- 4.1 Conceitos de Segurança - 43
 - Segurança da Informação - 43
 - Conceitos básicos da Segurança da Informação - 45
 - Informação - 45
 - Ativo - 45
 - Aspectos da Segurança da Informação - 46
 - Aspectos associados - 46
 - Ameaças - 47
 - Vulnerabilidades - 48
 - Medidas de Segurança - 49
 - Riscos - 50
 - Impacto - 50
 - Incidente - 50
- 4.2 Teoria do Perímetro - 50
- 4.3 Barreiras da Segurança - 52
 - Barreira 1: Desencorajar - 53
 - Barreira 2: Dificultar - 53
 - Barreira 3: Discriminar - 53
 - Barreira 5: Deter - 54
 - Barreira 6: Diagnosticar - 54
- 4.4 Equação do Risco - 55
 - Interpretação da equação - 55
 - Risco tendendo a zero - 56
- 4.5 Comitê Corporativo de Segurança da Informação - 56
 - Objetivos - 57
 - Coordenador do Comitê Corporativo de Segurança da Informação - 58
 - Estrutura Básica do Comitê - 58
 - Estrutura, Funções e Responsabilidades - 60
 - Perfil dos Executores - 61
- 4.6 Papel do Security Officer - 63
 - Fatores importantes para o adequado exercício da atividade de Security Officer - 63
 - Macrodesafios do Security Officer - 64
- 4.7 Como conduzir internamente a negociação - 64
- 4.8 Sabendo identificar o parceiro externo - 67
 - Características desejadas na Consultoria externa - 68
- 4.9 Conformidade com Norma específica - 69
 - Tendência - 72
- 4.10 Norma versus Metodologia - 72
 - Exemplos de ferramentas metodológicas - 73

CAPÍTULO 5: KNOWLEDGE CHECKPOINT 2 - 75

- Conceitos de Segurança - 75
- Teoria do Perímetro - 75
- Barreiras da Segurança - 75
- Equação do Risco - 76
- Comitê Corporativo de Segurança da Informação - 76
- Papel do Security Officer - 76
- Como conduzir internamente a negociação - 76
- Sabendo identificar o parceiro externo - 76
- Conformidade com Norma específica - 76
- Norma x Metodologia - 77

CAPÍTULO 6: ORIENTAÇÃO AO SECURITY OFFICER - 79

- 6.1 Solução Corporativa de Segurança da Informação - 79
 - Objetivo - 82
 - Fases - 83

- 6.2 Plano Diretor de Segurança - 86
 - Metodologia - 87
 - 1. Identificação dos Processos de Negócio - 88
 - 2. Mapeamento da Relevância - 89
 - Critérios - 90
 - 3. Estudo de Impactos CIDAL - 91
 - 4. Estudo de Prioridades GUT - 92
 - Dimensão: Gravidade - 92
 - Dimensão: Urgência - 93
 - Dimensão: Tendência - 93
 - Critérios - 93
 - 5. Estudo de Perímetros - 94
 - 6. Estudo de Atividades - 96
 - Organização do Comitê Corporativo de Segurança - 97
 - Organização do Security Office - 97
 - Organização de Comitês Interdepartamentais de Segurança - 98
- 6.3 Plano de Continuidade de Negócios - 98
 - Análise de Impactos no Negócio - 100
 - Estratégias de Contingência - 101
 - Hot-site - 101
 - Warm-site - 101
 - Realocação de Operação - 102
 - Bureau de Serviços - 102
 - Acordo de Reciprocidade - 102
 - Cold-site - 103
 - Auto-suficiência - 103
 - Planos de Contingência - 103
 - Plano de Administração de Crise - 104
 - Plano de Continuidade Operacional - 104
 - Plano de Recuperação de Desastres - 104
- 6.4 Política de Segurança da Informação - 105
- 6.5 Análise de Riscos e Vulnerabilidades - 108
- 6.6 Teste de Invasão - 114
- 6.7 Implementação de Controles de Segurança - 116
 - Autenticação e autorização - 118
 - O que você sabe - 118
 - O que você tem - 119
 - O que você é - 119
 - Combate a ataques e invasões - 120
 - Firewall - 120
 - Detector de Intrusos - 121
 - Privacidade das comunicações - 122
 - Simétrica ou de chave privada - 122
 - Assimétrica ou de chave pública - 123
 - Virtual Private Network - 124
 - Public Key Infrastructure - 125
 - Esteganografia - 129
- 6.8 Treinamento e Sensibilização em Segurança - 129
 - Seminários - 130
 - Campanha de Divulgação - 130
 - Carta do Presidente - 131
 - Termo de Responsabilidade e Confidencialidade - 131
 - Cursos de Capacitação e Certificação - 131
- 6.9 Equipe para Resposta a Incidentes - 132
- 6.10 Administração e Monitoração de Segurança - 133

CAPÍTULO 7: KNOWLEDGE CHECKPOINT 3 - 135

- Orientação ao Security Officer - 135
- Solução Corporativa de Segurança da Informação - 135
- Plano Diretor de Segurança - 135
- Plano de Continuidade de Negócios - 135
- Política de Segurança da Informação - 136

Análise de Riscos e Vulnerabilidades - 136
Teste de Invasão - 136
Implementação de Controles de Segurança - 136
Treinamento e Sensibilização em Segurança - 136
Equipe para Resposta a Incidentes - 137
Administração e Monitoração de Segurança - 137

CAPÍTULO 8: CONFORMIDADE COM A NORMA ISO17799 - 139

8.1 Framework e os controles de segurança - 141
8.2 Teste de conformidade - 143
 Objetivo do Teste - 143
 Instruções - 143
 Política de segurança - 143
 Segurança organizacional - 144
 Classificação e controle dos ativos de informação - 145
 Segurança em pessoas - 145
 Segurança física e de ambiente - 146
 Gerenciamento das operações e comunicações - 146
 Controle de acesso - 148
 Desenvolvimento e manutenção de sistemas - 149
 Gestão da continuidade do negócio - 149 Conformidade - 150
 Tabela de pontuação - 150
 Índices de Conformidade com a norma ISO 17799 - 150
 Resultado entre 80-54 - 151
 Resultado entre 53-27 - 151 Resultado entre 26-0 - 151

CONCLUSÕES FINAIS - 153

BIBLIOGRAFIA RECOMENDADA - 155

O Autor - 159