

ÍNDICE

1 - PORQUÊ SEGURANÇA? 1

| | |
|---|----|
| 1.1 Introdução | 1 |
| 1.2 Princípios de Segurança | 4 |
| 1.3 Dificuldades na Segurança Informática..... | 10 |
| 1.4 Pré-Condições para a Segurança..... | 13 |
| 1.5 Conceção do Sistema – Conceção do Processo de Negócio | 16 |
| 1.5.1 Integridade Organizacional..... | 18 |
| 1.5.2 Contratos de Externalização de Serviços..... | 19 |
| 1.5.3 Análise de Risco | 20 |
| 1.5.4 <i>Standards</i> de Certificação..... | 28 |
| 1.5.5 Critérios de Classificação de Segurança..... | 31 |

2 - MODELOS E POLÍTICAS DE SEGURANÇA 37

| | |
|--|----|
| 2.1 Introdução | 37 |
| 2.2 Modelos..... | 38 |
| 2.2.1 Bell-LaPadula..... | 39 |
| 2.2.2 Harrison-Ruzzo-Ullman | 40 |
| 2.2.3 Chinese-Wall..... | 41 |
| 2.2.4 Biba | 41 |
| 2.2.5 Goguen-Meseguer | 42 |
| 2.2.6 Sutherland..... | 42 |
| 2.2.7 Clark-Wilson | 43 |
| 2.2.8 Outros Modelos | 44 |
| 2.3 Políticas e Procedimentos | 45 |
| 2.3.1 Autenticação e Controlo de Acesso..... | 48 |
| 2.3.2 Criação e Gestão de Palavras-Passe | 49 |
| 2.3.3 Níveis de Serviço..... | 49 |
| 2.3.4 Cópias de Segurança e Recuperação de Desastre..... | 49 |
| 2.3.5 Gestão do Perímetro de segurança..... | 51 |
| 2.3.6 Formação e Treino em Segurança Informática..... | 52 |
| 2.3.7 Aquisição de Produtos e Sistemas Informáticos..... | 52 |
| 2.3.8 Segurança na Transmissão de Dados..... | 53 |
| 2.3.9 Informação aos Novos Utilizadores..... | 53 |
| 2.3.10 Segurança na Externalização de Serviços..... | 53 |
| 2.3.11 Contratação e Saída de Recursos Humanos..... | 53 |

| | |
|---|----|
| 2.3.12 Acesso Físico às Instalações..... | 54 |
| 2.3.13 Acesso Físico à Infra-Estrutura e Sistemas Computacionais..... | 56 |
| 2.3.14 Configuração e Gestão de Equipamentos Clientes | 58 |
| 2.3.15 Uso Aceitável | 59 |
| 2.3.16 Protecção contra Vírus..... | 61 |
| 2.3.17 Utilização da Internet..... | 62 |
| 2.3.18 Correio Electrónico | 63 |
| 2.3.19 Ligações e Acessos Remotos..... | 66 |

3 - IDENTIFICAÇÃO, AUTENTICAÇÃO E CONTROLO DE ACESSO 69

| | |
|---|-----|
| 3.1 Introdução | 69 |
| 3.2 Noções Básicas de Criptografia | 80 |
| 3.2.1 Criptografia Convencional | 83 |
| 3.2.2 Criptografia Baseada em Chave | 84 |
| 3.2.2.1 Criptografia Simétrica..... | 84 |
| 3.2.2.2 Criptografia Assimétrica | 87 |
| 3.2.3 Algoritmos de <i>Message Digest</i> | 91 |
| 3.2.4 Comparação entre Operações Criptográficas | 92 |
| 3.3 Infra-Estrutura de Chave Pública..... | 94 |
| 3.4 Sistemas Híbridos | 97 |
| 3.5 Identificação e Autenticação | 97 |
| 3.5.1 Autenticação Baseada em Palavra-Passe..... | 99 |
| 3.5.2 Autenticação Baseada em Certificados Digitais | 102 |
| 3.5.3 Autenticação Baseada em Tokens | 105 |
| 3.5.4 Autenticação Kerberos | 108 |
| 3.6 Assinatura Digital | 113 |
| 3.7 Engenharia Social | 116 |
| 3.7.1 Engenharia Social por Aproximação Directa | 118 |
| 3.7.2 Engenharia Social por Personificação | 118 |
| 3.7.3 Engenharia Social Reversa | 119 |
| 3.8 Exemplos de Aplicação | 119 |
| 3.8.1 Esteganografia com JPHS | 119 |
| 3.8.2 <i>Message Digest</i> | 125 |

4 – SEGURANÇA E SOFTWARE 129

| | |
|---|-----|
| 4.1 Introdução | 129 |
| 4.2 Software Malicioso e Vírus Digitais | 132 |
| 4.2.1 Tipificação..... | 136 |
| 4.2.2 Protecção e Detecção..... | 142 |
| 4.2.2.1 Métodos para a Detecção de <i>Malware</i> | 146 |
| 4.2.3 Sistemas Antivírus..... | 153 |
| 4.3 Segurança no Modelo Java..... | 156 |

| | |
|--|------------|
| 4.3.1 Segurança na Máquina Virtual Java | 159 |
| 4.3.2 Contenção de Código: Características da Linguagem | 164 |
| 4.3.3 Gestão da Segurança..... | 165 |
| 4.3.4 Criptografia e Certificados | 167 |
| 4.3.5 Segurança na Comunicação..... | 175 |
| 4.3.6 Controlador de Acessos e Permissões | 179 |
| 4.3.7 Segurança a Nível da API..... | 186 |
| 4.3.8 Autenticação e Autorização de Utilizadores..... | 188 |
| 4.4 Segurança no Modelo Microsoft .Net..... | 206 |
| 4.4.1 Segurança Baseada em Funções (<i>role-based security</i>)..... | 208 |
| 4.4.1.1 Autenticação | 209 |
| 4.4.1.2 Autorização..... | 210 |
| 4.4.1.3 <i>Principal e Identity</i> | 210 |
| 4.4.2 Segurança de Aplicações Web | 211 |
| 4.4.3 Segurança Baseada em Evidência | 211 |
| 4.4.4 Segurança no Acesso ao Código..... | 214 |
| 4.4.5 Comunicação Segura | 221 |
| 4.4.6 Criptografia | 226 |
| 4.4.7 Código Não Gerido..... | 230 |
| 4.4.8 Domínios de Aplicação | 230 |
| 4.4.9 Autenticação e Autorização do Utilizador..... | 233 |
| 4.4.9.1 <i>Identities</i> | 234 |
| 4.4.9.2 <i>Web Mechanisms</i> | 235 |
| 4.5 Metodologia para Desenvolvimento de Código | 242 |
| 4.5.1 O <i>Framework</i> Genérico | 244 |
| 4.5.2 <i>Framework</i> de Certificação | 246 |
| 4.5.3 Conjunto de Conhecimento | 249 |
| 4.5.4 Ferramentas | 250 |
| 4.5.5 Metodologia de Ataque | 251 |
| 4.6 Conclusão..... | 254 |
| 5 - SEGURANÇA DA REDE E SISTEMAS 259 | |
| 5.1 A Segurança Física..... | 259 |
| 5.1.1 Riscos e Ameaças | 262 |
| 5.1.2 Controlos de Segurança..... | 267 |
| 5.2 Firewalls..... | 268 |
| 5.2.1 Tipologia | 272 |
| 5.2.1.1 Filtro de Pacotes..... | 272 |
| 5.2.1.2 Filtro de Circuito..... | 277 |
| 5.2.1.3 Ponte Aplicacional..... | 279 |
| 5.2.2 A Implementação do Sistema | 282 |
| 5.2.2.1 Conceito de Bastião de Segurança..... | 282 |
| 5.2.2.2 Arquitecturas de Implementação..... | 283 |
| 5.2.2.3 <i>Screened-Host Firewall Systems</i> | 285 |
| 5.2.2.4 <i>Screened Subnet Firewall System</i> | 286 |
| 5.2.3 A Selecção de um Sistema de <i>Firewall</i> | 287 |

| | | |
|--|---|------------|
| 5.2.4 | Questões Genéricas a Analisar | 292 |
| 5.2.5 | A Gestão e Administração de um <i>Firewall</i> | 293 |
| 5.2.5.1 | A Administração do Sistema..... | 293 |
| 5.2.6 | Criação da Política de <i>Firewall</i> | 296 |
| 5.2.6.1 | Construção de Políticas de <i>Firewall</i> | 297 |
| 5.3 | Sistemas de Detecção de Intrusões..... | 306 |
| 5.4 | Iscos e Chamarizes..... | 316 |
| 5.5 | VPNS..... | 321 |
| 5.5.1 | Dispositivos de VPN | 322 |
| 5.5.2 | Túneis e Protocolos VPN | 323 |
| 5.5.3 | Protocolo IPSec | 325 |
| 5.5.4 | Estabelecimento de uma VPN | 334 |
| 5.5.4.1 | Controlo da SA | 336 |
| 5.5.4.2 | A Gestão de Chaves..... | 337 |
| 5.5.5 | Estabelecimento de Confiança entre Sistemas..... | 339 |
| 5.6 | Redes Sem Fios..... | 342 |
| 5.6.1 | Ameaças e Riscos | 345 |
| 5.6.2 | Medidas de Protecção..... | 349 |
| 5.6.3 | Ferramentas de Segurança | 354 |
| 5.7 | Protocolo SSL..... | 355 |
| 5.7.1 | Fragilidades do Protocolo..... | 358 |
| 5.8 | O Serviço de <i>Network Address Translation</i>..... | 359 |
| 5.9 | Elementos para a Disponibilidade dos Sistemas..... | 362 |
| 5.9.1 | RAID | 362 |
| 5.9.2 | Redundância de Servidores | 371 |
| 5.9.3 | Cópias de Segurança..... | 373 |
| 5.9.3.1 | <i>Hardware</i> de Cópias de Segurança..... | 374 |
| 5.9.4 | Sistemas de Alimentação Ininterrupta | 375 |
| 6 - IMPLEMENTAÇÃO E GESTÃO DA SEGURANÇA | | 377 |
| 6.1 | A Segurança na Organização..... | 377 |
| 6.2 | Implementação da Segurança..... | 389 |
| 6.2.1 | Políticas e Procedimentos..... | 394 |
| 6.2.1.1 | Treino e Sensibilização | 395 |
| 6.2.1.2 | Protecção contra Código Malicioso | 395 |
| 6.2.1.3 | Protecção de Sistemas e Aplicações | 396 |
| 6.2.1.4 | Protecção Antivírus..... | 396 |
| 6.2.1.5 | Protecção do Computador Pessoal..... | 396 |
| 6.2.1.6 | Protecção de Servidores | 397 |
| 6.2.1.7 | Protecção do Perímetro | 397 |
| 6.2.1.8 | Protecção da Infra-Estrutura de <i>Routing</i> | 397 |
| 6.2.1.9 | Pesquisa de Vulnerabilidades..... | 398 |
| 6.2.1.10 | Sistemas de Computação Móvel..... | 398 |

| | |
|--|------------|
| 6.2.1.11 <i>Firewalls</i> Pessoais..... | 398 |
| 6.2.1.12 Pesquisa e Actualização..... | 399 |
| 6.2.2 Controlos de Segurança..... | 399 |
| 6.2.3 A Rede e os Serviços..... | 400 |
| 6.2.3.1 Fronteiras de Sub-redes..... | 400 |
| 6.2.3.2 Identificação e Autenticação..... | 401 |
| 6.2.3.3 Infra-estrutura Física de Rede e Topologia..... | 401 |
| 6.2.3.4 Serviços de Rede..... | 404 |
| 6.2.3.5 Correio-Electrónico..... | 405 |
| 6.2.3.6 Dispositivos Móveis..... | 412 |
| 6.3 Auditoria de Segurança..... | 416 |
| 6.3.1 Auditoria à Segurança na Perspectiva do Negócio..... | 418 |
| 6.3.1.1 Requisitos Organizacionais..... | 418 |
| 6.3.1.2 Segurança Física..... | 418 |
| 6.3.1.3 Identificação e Autenticação..... | 421 |
| 6.3.1.4 Controlo de Risco..... | 422 |
| 6.3.2 Auditoria à Segurança na Perspectiva Técnica..... | 422 |
| 6.3.2.1 Aplicações e Servidores Web..... | 422 |
| 6.3.2.2 Perímetro..... | 424 |
| 6.3.2.3 Computadores Pessoais..... | 426 |
| 6.3.2.4 Configuração de Servidores..... | 427 |
| 6.3.2.5 Desenvolvimento de <i>Software</i> | 428 |
| 6.3.2.6 Aplicações..... | 428 |
| 6.3.2.7 <i>Software</i> Antivírus..... | 429 |
| 6.3.3 Auditoria à Administração de Sistemas..... | 429 |
| 6.3.4 Ferramentas de Auditoria e Defesa da Rede..... | 430 |
| 6.3.4.1 Monitores de Rede e de Pacotes..... | 431 |
| 6.3.4.2 <i>Scanners</i> e <i>Port Scanners</i> | 437 |
| 6.3.4.3 Descoberta de Palavra-passes..... | 439 |
| 6.3.4.4 Ferramentas de <i>Hacking</i> na Web..... | 439 |
| 6.3.4.5 <i>Backdoors</i> e Ferramentas de Acesso Remoto..... | 440 |
| 6.4 A Resposta a Incidentes..... | 441 |

GLOSSÁRIO 447**REFERÊNCIAS BIBLIOGRÁFICAS 471****ÍNDICE REMISSIVO 485**