



Introdução à Segurança da Informação Corporativa

Marcus Macedo

Secretaria de
Administração



EXPEDIENTE

Governador de Pernambuco
Paulo Henrique Saraiva Câmara

Vice-governadora de Pernambuco
Luciana Barbosa de Oliveira Santos

•

SECRETARIA DE ADMINISTRAÇÃO

Secretária
Marília Raquel Simões Lins

Secretário Executivo
Cirilo José Cabral de Holanda Cavalcante

Diretora do CEFOSPE
Analúcia Mota Vianna Cabral

Coordenação de Educação Corporativa
Priscila Viana Canto Matos

Chefe da Unidade de Coordenação Pedagógica
Marilene Cordeiro Barbosa Borges

Autor
Marcus Aurélio de Carvalho Macedo

Revisão de Língua Portuguesa
Eveline Mendes Costa Lopes

Diagramação
Sandra Cristina da Silva

•

Material produzido pelo Centro de Formação dos Servidores e Empregados Públicos do Poder Executivo Estadual – CEFOSPE

JUNHO, 2021 (1ª. ed.)

Ficha catalográfica elaborada pela BPE

M141i Macedo, Marcus
Introdução à segurança da informação corporativa / Marcus Macedo. – Recife:
Centro de Formação dos Servidores e Empregados Públicos do Poder Executivo Estadual,
2021.
.
120p. : il
Inclui referências.
Inclui curriculum do autor.
Material produzido pelo Centro de Formação dos Servidores e Empregados Públicos
do Poder Executivo Estadual – CESFOPE.

1. REDES DE COMPUTADORES – MEDIDAS DE SEGURANÇA – ESTUDO E ENSINO. 2.
EMPRESAS – REDES DE COMPUTADORES – MEDIDAS DE SEGURANÇA. 3. GOVERNANÇA
CORPORATIVA – MEDIDAS DE SEGURANÇA. 4. ADMINISTRAÇÃO DE RISCO – NORMAS.
5. PROTEÇÃO DE DADOS – POLÍTICA GOVERNAMENTAL. 6. PROTEÇÃO DE DADOS –
LEGISLAÇÃO. 7. CRIME POR COMPUTADOR. I. Título.

CDD 681.3
CDU 005.8

PeR – BPE 21-081

Sumário

Introdução	8
Capítulo 1 – Introdução aos conceitos da Segurança da Informação	9
1. 1 Considerações Iniciais	9
1. 2 Conceito de Sistemas	9
1. 1. 1. Tipos de sistema.....	10
1. 1. 2. Cibernética e Feedback.....	10
1. 1. 3. A Empresa como um Sistema	12
1. 1. 4. Dado, Informação e Conhecimento.....	12
1. 1. 5. Empresas e sistemas de informação.....	13
1. 3 Conceitos Fundamentais	14
1. 3. 1. Conceitos de Segurança.....	14
1. 3. 2. Princípios Fundamentais da Segurança da Informação	15
1. 3. 2. 1. Confidencialidade	15
1. 3. 2. 2. Integridade.....	15
1. 3. 2. 3. Disponibilidade	16
1. 3. 3. Princípios Auxiliares da Segurança da Informação	16
1. 3. 3. 1. Identificação e Autenticação.....	16
1. 3. 3. 2. Autorização e controle de acesso.....	23
1. 3. 3. 3. Auditoria	25
1. 4 Segurança nas organizações - visão de negócio	26
1. 5 Ciclo de vida da Informação.....	26
1. 6 Conceitos de Ameaças e Vulnerabilidade.....	27
1. 6. 1. Script Kiddies e Advanced Blackhats.....	28
1. 6. 2. Outras tipologias de atacantes.....	29
1. 7 Ataques e contramedidas	30
1. 8 Crimes cibernéticos	32
1. 8. 1. Backdoors	32
1. 8. 2. Ataques de negação de serviço (Denial-of-service).....	32
1. 8. 3. Eavesdropping (Espionagem).....	33
1. 8. 4. Spoofing (falsificação).....	33
1. 8. 5. Tampering (Adulteração)	33
1. 8. 6. Ataque de repúdio.....	33
1. 8. 7. Engenharia Social	33
1. 8. 8. Adware	34
1. 8. 9. Ransomware	34
1. 8. 10. Spyware	34
1. 8. 11. Scareware.....	34
1. 8. 12. Phishing.....	34
1. 8. 13. Ataques de Senha (Ataque de força bruta)	35
1. 8. 14. Footprinting	35
1. 8. 15. Malware.....	35
1. 8. 15. 1. Vírus e Worms.....	35
1. 8. 16. Bot e Botnet.....	35
1. 8. 17. Cavalos de Tróia (Trojans).....	36
1. 8. 18. Bombas Lógicas (Logic Bomb).....	36
1. 8. 19. Cryptojacking.....	36

1. 9 Tecnologias e suas vulnerabilidades	37
1. 10 Tecnologias para a segurança da informação	41
1. 10. 1. Firewall.....	41
1. 10. 2. Antivírus	41
1. 10. 3. Filtragem e cache de conteúdo da Web(URL).....	41
1. 10. 4. Filtragem de E-mail (SPAM)	41
1. 10. 5. Sistemas de detecção e prevenção de intrusão	41
1. 10. 6. Criptografia.....	42
1. 10. 6. 1. Operações de criptografia	44
1. 10. 6. 2. Algoritmos Criptográficos.....	44
1. 10. 7. Protegendo a Web	46
1. 10. 8. Certificados Digitais	47
1. 10. 9. Assinaturas Digitais	47
1. 10. 9. 1. Infraestrutura de chaves públicas do brasil (ICP-Brasil)	48
1. 11. Padrões, metodologias e práticas de segurança da informação.....	48
1. 11. 1. Modelos de gestão de segurança.....	48
1. 11. 1. 1. A família ISO 27000	48
1. 11. 1. 2. Modelos de Segurança NIST	50
Capítulo 2 – Princípios de governança de segurança da informação.....	52
2. 1. O ambiente de governança	52
2. 1. 1. Os domínios de governança.....	53
2. 1. 2. Os princípios de governança.....	53
2. 2. Conceitos de governança aplicada à segurança da informação.....	54
2. 2. 1. Princípios de gestão de segurança da informação.....	54
2. 3. Papéis e Responsabilidades.....	55
2. 3. 1. Comitê de Segurança da Informação	56
2. 3. 2. DPO (Data Protection Officer) – LGPD	57
2. 4. Estratégia de segurança da informação	57
2. 4. 1. Planos táticos	58
2. 4. 2. Planos operacionais/projetos	58
2. 5. Frameworks para governança de segurança da informação.....	58
2. 5. 1. Frameworks ITGI	59
2. 5. 2. Framework do NIST.....	60
2. 5. 3. Framework do COBIT.....	61
Capítulo 3 – Gerenciamento de Risco.....	63
3. 1. Conceitos de risco	64
3. 2. Atividades da Gestão de Risco de Segurança	66
3. 2. 1. Avaliação de risco de segurança	66
3. 2. 2. Identificação do risco	67
3. 2. 3. Análise de risco.....	68
3. 2. 4. Priorização de risco.....	68
3. 2. 5. Controle de Risco de Segurança de TI	69
3. 2. 6. Resolução do risco.....	70
3. 3. Padrões e normas	71
3. 3. 1. National Institute for Science and Technology – NIST	72
3. 3. 2. International Organization for Standardization – ISO.....	72
3. 3. 3. Federal Information Processing Standard – FIPS.....	72

3. 4. Plano de Gerenciamento de Risco.....	73
3. 5. Plano de Continuidade de negócios.....	74
3. 5. 1. Tipos de desastres – parâmetros	75
3. 5. 2. Consequências de desastres para negócios.....	75
3. 5. 3. Metodologias de recuperação	76
3. 5. 4. Modelagem de negócios.....	77
3. 5. 5. Análise de impacto no negócio – BIA	76
3. 5. 6. Análise de risco	77
3. 5. 7. Desenvolvimento de estratégia de mitigação	78
Capítulo 4 – Desenvolvimento e Implantação de Política de segurança da Informação	79
4. 1. Contexto jurídico e regulamentar	79
4. 2. Normas, procedimentos e diretrizes	81
4. 2. 1. Arquitetura de políticas de segurança	81
4.3 Metodologia de desenvolvimento e implantação	81
4. 3. 1. Desenvolvimento de política de segurança.....	81
4. 3. 2. Abordagem em fases	81
4. 3. 3. Quem contribui para o desenvolvimento da política de segurança	82
4. 3. 4. Público da política de segurança	83
4. 3. 5. Categorias de política.....	83
4. 3. 6. Formas de organização de política	84
4. 3. 7. Conscientização de segurança.....	84
4. 3. 8. Importância da conscientização sobre segurança	85
4. 3. 9. Objetivos de um programa de conscientização	85
4. 4. Políticas de Segurança existentes no Estado	86
4. 4. 1. Política Estadual de Segurança da Informação (PESI)	87
4. 4. 2. Política Estadual de Compartilhamento de Dados.....	89
4. 4. 3. Política Estadual de Transparência de Dados	89
4. 4. 4. Outras Políticas de Segurança da Informação de Órgãos	89
Capítulo 5 – Tratamento de Ameaças	90
5. 1. Conceito de Incidente.....	90
5. 2. Processo de modelagem para o tratamento de ameaças	90
5. 2. 1. Elaboração da política de resposta e tratamento de incidentes	92
5. 2. 2. Elaboração do plano de resposta e tratamento de incidentes.....	93
5. 2. 3. Elaboração dos procedimentos	94
5. 2. 4. Diretrizes para o compartilhamento de informações com terceiros	94
5. 2. 5. Estrutura da equipe de resposta a incidentes	94
5. 2. 5. 1. Modelos de equipe.....	94
5. 2. 5. 2. Modelo de composição de pessoal	95
5. 3. Tecnologias e processos de mitigação	96
5. 4. Equipe de resposta e tratamento de incidentes	97
5. 4. 1. Dependências dentro das organizações	99
5. 4. 2. Benefícios advindos da criação da equipe.....	100

Capítulo 6 – Compliance	101
6. 1. Definição de Compliance.....	101
6. 1. 1. Tipos de conformidade.....	101
6. 2. Modelo GRC	102
6. 2. 1. Padrões referenciais associadoS ao modelo GRC	104
6. 2. 2. Modelo GRC – Benefícios da integração	105
6. 2. 3. Modelo GRC – Desafios.....	105
6. 2. 4. Mecanismos de governança	107
6. 2. 4. 1. Primeira linha de defesa	106
6. 2. 4. 2. Segunda linha de defesa	107
6. 2. 4. 3. Terceira linha de defesa.....	107
6. 3. Legislações e marcos regulatórios	107
6. 3. 1. Conceito de Legislação.....	107
6. 3. 2. Conceito de Marco regulatório.....	108
6. 4. Marco Civil da Internet	109
6. 4. 1. Principais aspectos abordados pelo Marco Civil da INTERNET	111
6. 5. Lei Geral de Proteção de Dados (LGPD).....	111
6. 5. 1. O que é LGPD?	111
6. 5. 2. A quem se aplica a LGPD	113
6. 5. 1. A quem não se aplica a LGPD	113
6. 5. 4. Estrutura da LGPD.....	113
6. 5. 5. Aspectos importantes da LGPD	115
Conclusão	117
Referências	118
Sobre o autor	122

Introdução

Este curso de Introdução à Segurança da Informação Corporativa foi criado para a conscientização das questões e dúvidas acerca desta dimensão do conhecimento e sua aplicabilidade no dia a dia das organizações públicas. É um tema muito amplo, com muitos conceitos, porém necessários, tendo em vista as crescentes ameaças que impactam toda a sociedade.

O conteúdo foi idealizado para abordar os principais aspectos da segurança da informação no contexto corporativo das organizações. No início, são apresentados os conceitos básicos de segurança da informação, seus princípios e seus desafios. O segundo capítulo aborda os aspectos da governança corporativa em segurança. O terceiro capítulo apresenta a gestão de riscos de forma conceitual e com uma abordagem prática. O quarto capítulo enfoca a gestão de políticas de segurança da informação com sua contextualização para o estado. No quinto capítulo, será abordado o tratamento de ameaças, o conceito de incidente, as tecnologias e os padrões usados para a gestão de incidentes. O sexto e último capítulo enfoca a gestão de conformidade, um assunto que hoje está presente em todas as organizações, principalmente no ambiente das instituições governamentais. Assuntos atuais, tais como Marco Civil da Internet e Lei Geral de Proteção aos Dados, também são tratados.

Capítulo 1 – Introdução aos conceitos da Segurança da Informação

Este capítulo inicial aborda os conceitos básicos para a compreensão da Segurança da Informação em um contexto organizacional.

1.1 Considerações Iniciais

Para o entendimento do conteúdo desta apostila e do Curso de Introdução à Segurança da Informação Corporativa, faz-se necessária uma abordagem do contexto, ou habitat, em que os diversos problemas que envolvem a segurança da informação ocorrem.

Em geral, há uma falta de atenção para a segurança no dia a dia das pessoas. Em muitas ocasiões, desempenham suas atividades de forma automática, como se fossem robotizadas, seguindo sempre os mesmos procedimentos, sem despertar para a problemática dos riscos envolvidos.

1.2 Conceito de Sistemas

Este curso foca o contexto organizacional corporativo com suas complexidades e inicia-se com os conceitos básicos de sistemas. De acordo com Batista (2004), o conceito de sistema foi desenvolvido pelo biólogo alemão Ludwig Von Bertalanffy, em sua Teoria Geral de Sistemas, iniciada em 1924, concluída em 1937 e divulgada em 1951, com a publicação do livro General System Theory.

A Teoria Geral dos Sistemas é muito ampla e considerada interdisciplinar, uma vez que seus princípios e modelos são aplicáveis a qualquer área do conhecimento científico, demonstrando, assim, certa semelhança entre as diferentes ciências, tornando possível uma maior aproximação entre suas fronteiras.

Uma definição clássica para sistemas pode ser ***“o conjunto estruturado ou ordenado de partes ou elementos que se mantêm em interação, ou seja, em ação recíproca, na busca da consecução de um ou de vários objetivos”*** (Batista, 2004). A figura 1-1 ilustra um modelo genérico de um sistema que possui um processamento (o que ele faz), os insumos (entrada) e o resultado de seu funcionamento: o que ele produz (saída).

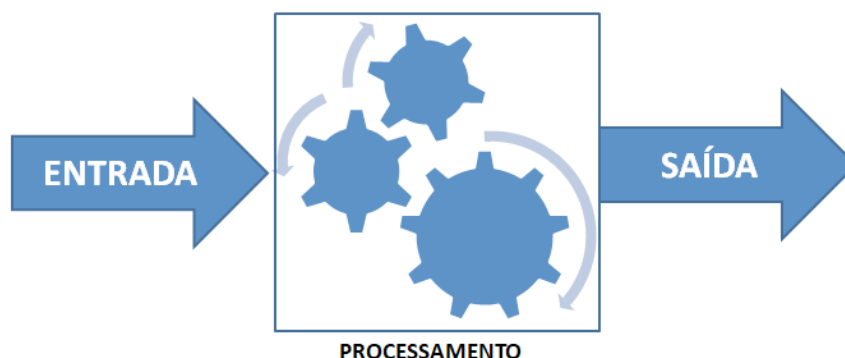


Figura 1-1. Modelo genérico de sistema

Em sua Teoria Geral de Sistema (Bertalanffy, 1968), o conceito de globalismo ou totalidade é demonstrado, e, nessa visão, um sistema é impossível de ser compreendido como um todo, mas pela análise individual de suas partes. Entendendo como funciona seus elementos, tem-se a compreensão do sistema como todo. Outro conceito fundamental é o do propósito ou objetivo, ou seja, todo sistema tem um ou mais propósitos.

Exemplos de sistema: o Corpo Humano, o Sistema Digestivo, o Sistema Solar. Sistemas criados pelo homem: sistema de transporte, sistema de água e esgoto, sistema de energia elétrica, sistema de leis etc.

1. 1. 1. Tipos de sistema

Os sistemas podem ser classificados em Abertos e Fechados. Os sistemas abertos são aqueles que sofrem ações interna e externa, ou seja, além de haver uma interação com os elementos internos, ainda ocorre uma interação com o meio exterior que, de certa forma, causa mudanças, ou interferências, em seu funcionamento. Os sistemas fechados possuem somente a interação interna dos seus elementos, não possuindo nenhuma interação com o meio exterior.

1. 1. 2. Cibernética e Feedback

A cibernética é a ciência, que estuda a comunicação e o controle dos sistemas. Segundo MIRANDA (2017), foi criada com base na Teoria Geral dos Sistemas, na década de 1940 por Norbert Wiener, abordando os mecanismos de comunicação entre os elementos de um sistema e como essa comunicação controla esses referidos elementos. Os sistemas que possuem esses mecanismos são denominados Sistemas Cibernéticos.

Exemplo: Sistema Homeostático que regula os níveis de açúcar no sangue apresentado pela figura 1-2. O corpo humano possui diversos mecanismos, que regulam o funcionamento de diferentes órgãos.

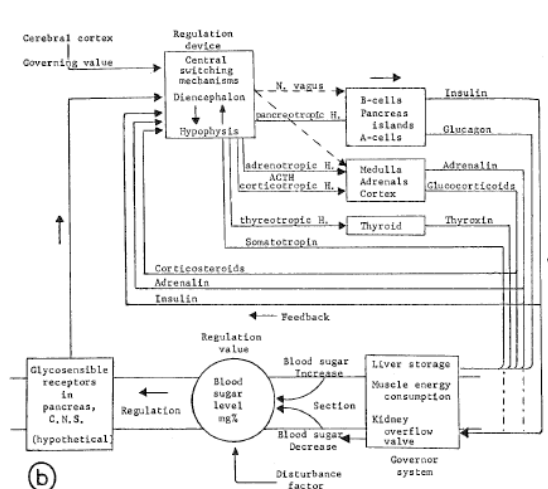


Figura 1-2. Exemplo de um sistema cibernético: Sistema Homeostático de regulação de açúcar no sangue.

Fonte: BERTALANFFY, 1968, p. 162 – figura 7.2b.

A informação que permite o controle e a regulação dos elementos de um sistema é denominada de feedback.

Os sistemas cibernéticos possuem três propriedades que os caracterizam:

- São muito complexos, necessita-se de uma abordagem com certa abstração para entendê-los;
- São probabilísticos, seu entendimento requer uma análise estatística e uma abordagem através da teoria da informação;
- São autorregulados, para entendê-los requer uma análise do feedback.

O modelo de entendimento de sistemas cibernéticos é caracterizado pela **ENTRADA** (inputs) ou **INSUMOS** necessários para o **PROCESSAMENTO**, que irá gerar a **SAÍDA** (outputs). Além disso, o modelo contempla a **RETROALIMENTAÇÃO** (feedback), conforme figura 1-3.

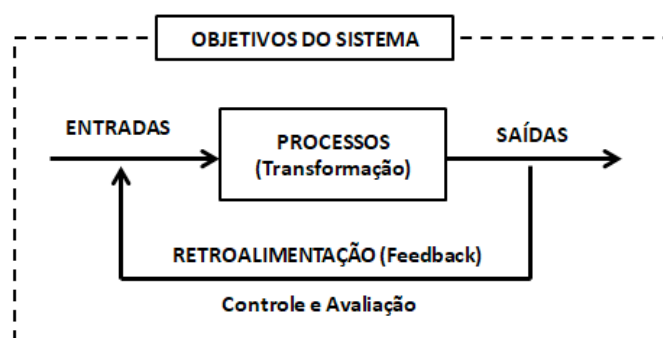


Figura 1 3. Modelo de sistema cibernético

Fonte: baseada em BATISTA, 2004.

1. 1. 3. A Empresa como um Sistema

Uma empresa ou organização pode ser compreendida, na abordagem da Teoria Geral dos Sistemas, como um Sistema Aberto. A estrutura sistêmica das organizações com seus departamentos e setores funciona, de forma integrada, para atingir propósitos ou objetivos: dar lucro e o crescer. É um sistema aberto, porque sofre interferência do meio exterior, pois ela precisa interagir com outros sistemas: sistema tributário, sistema legal etc. A figura 1-4 ilustra esse conceito.

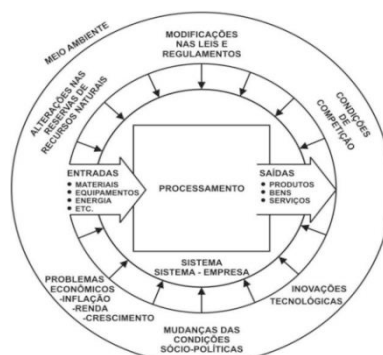


Figura 1-4. Estrutura Sistêmica das Organizações

Fonte: SILVA; SANTOS; KONRAD, 2016.

Para se gerir ou administrar uma empresa, é necessário que os elementos que a compõem estejam usando mecanismos de comunicação e controle, logo uma empresa usa sistemas cibernéticos para isso. Nesse contexto entra, então, os conceitos de informação, dado e conhecimento.

1. 1. 4. Dado, Informação e Conhecimento

Dado é o resultado de uma observação coletada do ambiente organizacional: número de peças produzidas, temperatura do forno, condições atmosféricas etc.; a informação é um dado, que contém certo significado ou valor e que causa impacto em diferentes níveis do processo organizacional, exemplo: a temperatura do forno tem que ser mantida em 1.500° C para a produção das peças, tornando-se assim um elemento-chave para a extração e criação do conhecimento. Exemplo: a temperatura de 1.500° C é uma informação, que gerou o conhecimento de como é possível produzir peças. O conhecimento é gerado pela exposição à informação. Assim, poderá haver informação sem conhecimento, mas não conhecimento sem informação.

O uso do conhecimento é fundamental e também, um fator estratégico, exemplo: a fórmula da Coca-Cola é um conhecimento, que se tornou um segredo industrial.

A informação é um elemento essencial para a geração do conhecimento, para a tomada de decisão e representa um VALOR para o negócio. Do ponto de vista financeiro, a informação no seu processamento tem um custo, que é compensado pelo retorno do investimento (ROI), logo a informação é um ATIVO valioso.

Como estabelecer o valor intrínseco da informação? Conforme BIDGOLI (2006), o valor da informação pode ser expresso com um determinado valor monetário: quanto um cliente externo ou interno estaria disposto a pagar pelo bem fornecido (informação).

Exemplo de uma fábrica com seus departamentos: Produção, Almoxarifado, Estoque, Compras, Diretoria, Contabilidade (finanças), Vendas, Recursos Humanos. Para que o Departamento de Produção funcione, é necessário que o Almoxarifado libere os insumos necessários à produção das peças e, portanto, se faltar o insumo, é necessário acionar o Departamento de Compras. Este, por sua vez, irá depender da liberação de recursos financeiros da Contabilidade. A Contabilidade para liberar o recurso tem que ser autorizada pela Diretoria, que irá verificar com o Departamento de Vendas a perspectiva de um futuro aporte de capital proveniente delas. A Diretoria precisa, então, de uma informação para a tomada de decisão: liberar ou não a compra de insumos. Várias decisões são tomadas durante o funcionamento do negócio e basta uma decisão errada para comprometer o sistema.

1. 1. 5. Empresas e sistemas de informação

De acordo com BATISTA (2004), uma determinada informação é, ao mesmo tempo, a base para a tomada de decisão e o resultado direto de suas ações. Ou seja, quando se toma uma decisão baseada numa boa informação, as ações e suas consequências serão diretamente ligadas à qualidade da informação. As informações podem ser classificadas em:

- **Operacionais** – geradas por operações nas atividades do dia a dia da empresa. Exemplo: emissão de nota fiscal, registro de ponto de um funcionário etc.
- **Gerenciais** – usadas para tomada de decisões, principalmente nas áreas táticas e estratégicas de uma empresa, variando conforme o nível gerencial. Exemplo: previsão de vendas, capacidade da produção, produtividade mensal etc.

Uma organização está fundamentada em três perspectivas: Pessoas, Processos e Tecnologias, definidas assim:

- **Pessoas** – existem na maioria das organizações e são a parte mais frágil. Uma falta de conhecimento da função na organização ou a falta de motivação poderão levar a uma queda na produtividade;
- **Processos** – são as tarefas organizadas de forma a gerar um produto, uma entrega. Quando a organização não tem processos bem definidos, ou falta de documentação de processos, ou falta de racionalização dessas atividades, a empresa pode também não funcionar adequadamente;
- **Tecnologia** – é um recurso ou ferramenta usada por pessoas para realizar os processos. Exemplo: uma caneta, um papel, computadores etc. O nível de tecnologia impacta diretamente na produtividade.

O equilíbrio ou o desequilíbrio de uma empresa podem ser avaliados em função dos problemas encontrados nessas perspectivas.

1. 3 Conceitos Fundamentais

Neste tópico, serão abordados os conceitos básicos da segurança da informação.

1. 3. 1. Conceitos de Segurança

Ao pesquisar, em um dicionário, o significado da palavra “Segurança”, obtém-se que essa palavra é um substantivo feminino, que significa, entre outras definições:

- “Situação do que está seguro; afastamento de todo perigo: viajar com segurança.”;
- “Demonstração de certeza, de convicção ou comportamento repleto de firmeza, de autoconfiança; confiança: falou com segurança.”

Portanto, pode-se entender segurança como sendo uma sensação, um sentimento. Embora, ao se perceber o comportamento humano com relação a essa sensação de segurança, geralmente umas destas atitudes ocorrem:

- Atitude de prevenção, ou estar preparado para as ações que virão;
- Atitude de negligência, ou deixar acontecer e depois resolver.

Nos dias atuais, pessoas trabalham com computadores, jogam, fazendo uso de computadores em suas casas, vão para a escola online, compram produtos de comerciantes na INTERNET, levam seus notebooks e tablets aos mais diferentes lugares para: ler e-mails, livros eletrônicos etc.; utilizam seus smartphones para verificar saldos bancários e até coletar

informações sobre os parâmetros de saúde em seus exercícios físicos, usando sensores em seus pulsos. Em outras palavras, computadores são onipresentes.

Embora a tecnologia nos permita o acesso a uma série de informações com apenas um clique do mouse ou toque na tela, ela também representa riscos de segurança. Se as informações sobre os sistemas utilizados pelas empresas ou bancos ficam expostas a um invasor, as consequências podem ser terríveis.

Nem sempre se pode prevenir de acontecimentos, pois a probabilidade de um evento acontecer é imprevisível. Porém, pode-se prevenir para os eventos fortuitos mais comuns, tomando-se medidas de segurança.

1. 3. 2. Princípios Fundamentais da Segurança da Informação

Quando se fala em Segurança da Informação, e como a informação tem um valor intrínseco e, em geral, tem um custo envolvido, pode-se dizer que consiste na proteção contra incidentes, que possam afetar os chamados princípios da segurança da informação.

1. 3. 2. 1. Confidencialidade

O princípio da Confidencialidade significa que apenas usuários autorizados podem acessar certas informações classificadas, segundo o seu uso, grau de importância e sigilo. O pilar Confidencialidade é violado, se as pessoas não autorizadas conseguirem ler ou copiar tais informações classificadas. Exemplo: as transações financeiras numa conta bancária.

1. 3. 2. 2. Integridade

O princípio da Integridade significa que as informações não são modificadas, são autênticas, completas e confiáveis. A informação perderá sua integridade, se for modificada por acidente ou por um ataque mal-intencionado.

1. 3. 2. 3. Disponibilidade

O princípio da Disponibilidade significa que os usuários autorizados ao uso de um sistema de informação são capazes de acessá-lo, introduzir, recuperar ou processar os dados necessários. A disponibilidade de informação é violada, quando os usuários autorizados não podem acessar os dados necessários para seu trabalho.

1. 3. 3. Princípios Auxiliares da Segurança da Informação

São princípios que dão suporte aos Pilares Fundamentais (CID): Confidencialidade, Integridade e Disponibilidade.

1. 3. 3. 1. Identificação e Autenticação

A Autenticação é o princípio que garante a confirmação da identidade de uma pessoa física ou jurídica. Esse princípio compreende todos os processos e mecanismos pelos quais a identidade de um usuário é confirmada, garantindo que ele é realmente quem diz ser. A autenticação é básica para garantir a confidencialidade, integridade e disponibilidade.

A privacidade e o sigilo dependem da confirmação da identificação do usuário da informação.

A Identificação é o princípio que faz uma afirmação sobre o que alguém ou algo é, e a autenticação estabelece se essa afirmação é verdadeira. Pode-se ver esse processo ocorrendo diariamente em uma ampla variedade de formas.

Um exemplo comum de identificação e autenticação é o uso de cartões de pagamento, que exige um número de identificação pessoal (PIN), chamado, por muitos, de senha do cartão. Quando o usuário passa o cartão na maquina, está afirmando que é a pessoa indicada no cartão. Nesse ponto, estabelece-se a identificação, e só. Quando é solicitada a inserção do PIN associado ao cartão, completa-se a parte de autenticação da transação, provando que a pessoa que está operando é o titular legítimo do cartão, ao menos para o sistema.

Em seguida, serão abordados os dois princípios com mais detalhes e conceitos.

IDENTIFICAÇÃO

Conforme ANDRESS (2019), o conceito de identificação, como foi visto, é simplesmente uma afirmação de quem a pessoa é. Isso pode incluir quem se afirma ser como pessoa, quem um sistema afirma ser na rede, ou quem a parte de origem de um e-mail afirma ser. Veremos alguns métodos para determinar a identidade e examinar como esses métodos são confiáveis.

Podemos nos identificar por nossos nomes completos, versões abreviadas de nossos nomes, apelidos, números de conta, nomes de usuário, cartões de identificação, impressões digitais ou amostras de DNA.

Infelizmente, com algumas exceções, tais métodos de identificação não são únicos, e até mesmo alguns dos métodos supostamente únicos de identificação, como impressões digitais que podem ser duplicadas.

VERIFICAÇÃO DE IDENTIDADE

A verificação de identidade é um passo além da identificação, mas ainda é uma etapa antes da autenticação, que será abordada na próxima seção. Quando nos é solicitado mostrar a carteira de motorista, o RG, a certidão de nascimento ou outra forma semelhante de identificação, geralmente é para verificação de identidade, não autenticação.

Os sistemas de computador também usam verificação de identidade. Quando se envia um e-mail, a identidade fornecida é considerada verdadeira; o sistema raramente executa quaisquer etapas adicionais para autenticá-lo. Essas lacunas na segurança contribuem para a enorme quantidade de tráfego de SPAM.

IDENTIFICAÇÃO FALSIFICADA

Como foram discutidos anteriormente, os métodos de identificação estão sujeitos à mudança. Como tal, também estão sujeitos à falsificação. Menores costumam usar identidades falsas para entrar em bares ou boates, enquanto criminosos e terroristas podem usá-las para uma variedade de tarefas mais nefastas.

É possível usar alguns métodos de identificação, como certidões de nascimento, para obter formas adicionais de identificação, como RG ou carteira de estudante, fortalecendo assim uma falsa identidade.

O roubo de identidade com base em informações falsificadas é uma grande preocupação hoje. Esse tipo de ataque é infelizmente comum e fácil de executar. E uma quantidade mínima de informações – geralmente um nome, endereço e rede social.

Muitas das mesmas dificuldades existem em sistemas de computador e ambientes. Por exemplo, é perfeitamente possível enviar um email de um endereço de email falsificado. Os *spammers* usam essa prática.

AUTENTICAÇÃO

Na segurança da informação, autenticação é o conjunto de métodos usados para estabelecer se uma reivindicação de identidade é verdadeira (ANDRESS, 2019). Observe que autenticação não decide o que a parte que está sendo autenticada tem permissão para fazê-la; esta é uma tarefa separada, conhecida como autorização que será apresentada em outro tópico.

Fatores de Autenticação

Existem várias abordagens para a autenticação:

- Algo que a pessoa sabe;
- Algo que a pessoa é;
- Algo que a pessoa tem;
- Algo que a pessoa faz;
- Onde a pessoa está.

Essas abordagens são conhecidas como fatores de Autenticação. Quando se está tentando autenticar uma reivindicação de identidade, pensa-se em querer usar tantos fatores quanto possível. Quanto mais fatores se usam, mais positivos serão os resultados.

Algo que a pessoa sabe – é um fator de autenticação comum, inclui senhas ou PINs (Personal Identification Number). No entanto, esse fator é um pouco fraco, porque se a informação da qual o fator depende é exposta, seu método de autenticação pode não ser mais exclusivo.

Algo que a pessoa é – é um fator baseado em algo relativamente único em termos de atributos físicos de um indivíduo, muitas vezes referidos como biometria. Embora a biometria possa incluir atributos simples, como altura, peso, cor do cabelo ou cor dos olhos, estes não são geralmente distintos o suficiente para serem identificadores muito seguros. Identificadores complexos, como impressões digitais, padrões de íris ou retina, ou características faciais, são mais comuns. Estes são fatores um pouco mais forte do que uma senha, porque forjar ou roubar uma cópia de um identificador físico é um pouco mais difícil, embora não seja impossível. Existem dúvidas se a biometria realmente conta como um fator de autenticação ou se ela apenas constitui uma verificação de identidade.

Algo que a pessoa tem – é um fator geralmente baseado em uma posse física, embora possa se estender a alguns conceitos. Exemplos comuns são cartões usados em caixas eletrônicos (ATM), *tokens* de segurança baseados em hardware, conforme mostrado na figura 1-5. Algumas instituições, a exemplo de bancos, usam o acesso a dispositivos lógicos, tais como telefones celulares ou contas de e-mail, como métodos de autenticação também.

AUTENTICAÇÃO MULTIFATOR

A autenticação multifator usa um ou mais dos fatores discutidos na seção anterior. Quando a pessoa está usando apenas dois fatores, essa prática também é, às vezes, chamada de duplo fator de autenticação (ANDRESS, 2019).

Voltemos ao exemplo do caixa eletrônico, porque ele ilustra, também, autenticação multifatorial. Nesse caso, a pessoa usa algo que ela conhece (seu PIN) e algo que ela tem (seu cartão do caixa eletrônico). O cartão ATM serve como um fator para autenticação e uma forma de identificação.

Outro exemplo de autenticação multifator está no ato de emitir um cheque. Nesse caso, a pessoa está usando algo que ela tem (os próprios cheques) e algo que ela faz (assiná-los). Aqui, os dois fatores envolvidos em escrever um cheque são bastante fracos, então a pessoa, às vezes, usa um terceiro fator – uma impressão digital – usado conjuntamente com eles.

AUTENTICAÇÃO MÚTUA

A autenticação mútua é um mecanismo de autenticação em que ambas as partes em uma transação se autenticam (ANDRESS, 2019). Essas partes são normalmente baseadas em software. Em geral, no processo padrão de autenticação unilateral, o cliente se autentica no servidor. Na autenticação mútua, não apenas o cliente autentica-se no servidor, mas o servidor autentica-se no cliente.

Nos casos em que a pessoa não executa autenticação mútua, ela se deixa vulnerável a ataques de falsificação de identidade, muitas vezes conhecido como ataques *man-in-the-middle*, em que o atacante se insere entre o cliente e o servidor. O invasor então personifica o servidor para o cliente e o cliente para o servidor, contornando o padrão normal de tráfego e, em seguida, intercepta e encaminha o tráfego que normalmente flui diretamente entre o cliente e o servidor.

MÉTODOS COMUNS DE IDENTIFICAÇÃO E AUTENTICAÇÃO

Apresentaremos três métodos comuns de identificação e autenticação em detalhes: senhas, biometria e *tokens* de hardware.

SENHAS

As senhas são familiares para a maioria dos usuários, que usam computadores regularmente. Quando combinada com um nome de usuário, uma senha irá geralmente permitir que a pessoa acesse um sistema de computador, um aplicativo, um telefone ou um dispositivo semelhante. Embora seja apenas um único fator de autenticação, as senhas podem representar um nível relativamente alto de segurança quando construídas e implementadas corretamente.

As pessoas costumam descrever certas senhas como sendo fortes, mas um termo descritivo melhor poderia ser complexidade. Ao construir uma senha que se utilizem apenas letras minúsculas, compondo oito caracteres, pode-se usar um utilitário de quebra de senha para fazê-la rapidamente. Se forem usadas uma combinação de letras maiúsculas, letras minúsculas, números e símbolos, uma senha complexa será criada, sendo mais difícil de lembrar, como: “\$sU&qw!3”, mas muito mais difícil de quebrar.

Além de construir senhas fortes, a pessoa também precisa praticar uma boa higiene de senha. Não escrever a senha em papel e colar embaixo do teclado ou do monitor; fazer isso anula completamente o propósito de se ter uma senha, em primeiro lugar.

Outro problema comum é a sincronização manual de senhas – em suma, usando a mesma senha em todos os lugares. Se a pessoa usa a mesma senha para o seu e-mail, para o seu login em trabalho e para o seu fórum de discussão on-line sobre futebol, ela coloca a segurança de todas as contas nas mãos daqueles proprietários do sistema. Se algum deles for comprometido, todas as contas se tornam vulneráveis; tudo o que um invasor precisa fazer para acessar os outros é procurar o nome da sua conta na internet para encontrar suas outras contas e fazer login, usando o padrão senha da pessoa. No momento em que o invasor entra na conta de e-mail, o jogo acabou, porque um invasor geralmente pode usá-lo para redefinir as credenciais da conta para qualquer outra conta que a pessoa tiver.

BIOMETRIA

Embora alguns identificadores biométricos possam ser mais difíceis de falsificar do que outros, isso é apenas por causa das limitações de tecnologia de hoje (ANDRESS, 2019), em algum momento no futuro, precisaremos desenvolver características biométricas mais robustas para medir ou, caso contrário, pare de usar a biometria como mecanismo de autenticação.

USANDO BIOMETRIA

Dispositivos equipados com biometria estão se tornando cada vez mais comum e barato. Pode-se encontrar uma ampla seleção por menos de R\$ 150,00. Vale a pena pesquisar esses dispositivos cuidadosamente, antes de depender deles para segurança.

Podem-se usar sistemas biométricos de duas maneiras: para verificar a declaração de identidade que alguém apresentou, como discutido anteriormente; ou para reverter o processo e usar a biometria como método de identificação. Esse processo é comumente usado por agências de aplicação da lei para identificar o proprietário de impressões digitais deixadas em vários objetos.

CARACTERÍSTICAS DOS FATORES BIOMÉTRICOS

Fatores biométricos são definidos por sete características: universalidade, singularidade, permanência, coletabilidade, desempenho, aceitabilidade e enganabilidade (ANDRESS, 2019).

- **Universalidade** significa que é possível encontrar a característica biométrica escolhida na maioria das pessoas que se espera implantar no sistema. Por exemplo, embora possa usar-se uma cicatriz como um identificador, não é possível garantir que todos terão uma cicatriz. Mesmo se for escolhida uma característica comum, como uma impressão digital, deve-se considerar o fato de que algumas pessoas podem não ter o dedo indicador na mão direita, e o sistema não esteja preparado para não ter essa informação.
- **Singularidade** é uma medida de quão única uma característica é entre os indivíduos. Por exemplo, se a pessoa escolher usar altura ou peso como um identificador biométrico, teria uma boa chance de encontrar várias pessoas em qualquer grupo que tenham a mesma altura ou peso. Deve-se tentar selecionar características com um alto grau de exclusividade, como padrões de DNA ou íris, mas mesmo estes podem ser duplicados, quer seja intencionalmente ou não. Por exemplo, gêmeos idênticos têm o mesmo DNA (não intencional), e um invasor pode replicar uma impressão digital (intencional).
- **Permanência** testa o quão bem uma característica resiste à mudança ao longo do tempo e com o avançar da idade. Se a pessoa escolher um fator que pode variar facilmente, como altura, peso ou geometria da mão, eventualmente se verá incapaz de autenticar um usuário legítimo. É melhor usar fatores como impressões digitais, que provavelmente não mudarão sem uma ação deliberada.

- **Coletabilidade** mede o quão fácil é coletar e usar uma informação biométrica. A mais comumente usada, são as impressões digitais, pois é relativamente fácil de coletar. Por outro lado, uma amostra de DNA é mais difícil de coletar, porque o usuário deveria fornecer uma amostra de material genético para se cadastrar e posteriormente se autenticar.
- **Desempenho** mede o quão bem um determinado sistema funciona com base em fatores, como velocidade, precisão e taxa de erro.
- **Aceitabilidade** é uma medida de quão aceitável a característica é para os usuários do sistema. Em geral, sistemas que são lentos ou difíceis de usar são menos prováveis de serem aceitos pelos usuários. Sistemas que exigem que os usuários tirem suas roupas, toque em dispositivos que foram repetidamente usados por outros, ou fornecer tecido ou fluidos corporais são improváveis de ter um alto grau de aceitabilidade.
- **Enganabilidade** descreve a facilidade de enganar um sistema, usando um identificador biométrico falsificado. O exemplo clássico de um ataque de enganabilidade contra a impressão digital como um método identificador biométrico é o “dedo pegajoso”. Nesse tipo de ataque, uma impressão digital é levantada de uma superfície e usada para criar um molde com o qual o atacante pode lançar uma imagem positiva da impressão digital em gelatina. Alguns sistemas biométricos têm recursos projetados especificamente para derrotar tais ataques por medição da temperatura da pele, pulso ou resposta pupilar.

TOKENS DE HARDWARE

Um token de hardware padrão (Figura 1-5) é um pequeno dispositivo, geralmente no formato de um cartão de crédito ou chaveiro. Os tokens de hardware mais simples parecem idênticos aos Pendrives e contêm um certificado ou identificador exclusivo. Eles costumam ser chamados de dongles. Tokens de hardware mais complexos incorporam display de cristal líquido (LCDs), teclados para inserir senhas, leitores biométricos, wireless e recursos adicionais para aprimorar a segurança.



Figura 1-5. Exemplos de Tokens

Fonte: <https://creditoemprestimo.com/como-pedir-o-token-do-bradesco/>

Muitos tokens de hardware contêm um relógio interno, que gera um código com base no identificador único do dispositivo, outros solicitam ao usuário a inserção do PIN ou a senha, além de outros fatores potenciais. Na maioria desses dispositivos, o código é enviado para um display no token, sendo modificado a cada 30 segundos.

O tipo mais simples de token de hardware representa apenas o fator de autenticação “*algo que a pessoa tem*” e, portanto, é suscetível a roubo e potencial uso por um criminoso experiente. Embora esses dispositivos apresentem um maior nível de segurança para contas de usuários, em geral não são úteis sem as credenciais da conta associada.

1. 3. 3. 2. Autorização e controle de acesso

Após receber a reivindicação de identidade de um usuário e estabelecido que essa reivindicação é válida, conforme discutido no tópico anterior, é preciso decidir se será permitido que esse usuário acesse os recursos. Para isso, serão considerados outros dois princípios auxiliares: Autorização e Controle de acesso.

AUTORIZAÇÃO

Autorização e Controle de Acesso são as implementações tecnológicas de separação de direitos e deveres. Quase todos os processos de negócios empregam métodos em que as pessoas em funções diferentes executam tarefas associadas a essas funções. Os dados da organização são classificados e liberados para indivíduos com base na necessidade de utilização. A autenticação é parte do meio que controla quem pode ver quais informações.

MECANISMOS DE AUTORIZAÇÃO

Controlar o acesso aos dados e funções depende muito de saber a identidade do usuário, os mecanismos de autorização são frequentemente integrados com mecanismos de autenticação. Credenciais do usuário (suas funções e o que é permitido executar) são frequentemente armazenados no mesmo banco de dados que as informações da conta do usuário (identificação do usuário e senha).

TECNOLOGIAS DE AUTORIZAÇÃO

Ao contrário da autenticação, em que um conjunto de padrões abertos está em constante evolução com grande aceitação, as tecnologias de autorização ainda são proprietárias, não compatíveis com a maioria dos aplicativos e mais difíceis de integração com empresas. Ainda assim, autorização está convergindo em torno de algumas tecnologias importantes, tais como:

- LDAP;
- Kerberos;
- Domínios do NT;
- Active Directory;
- UNIX.

Controle de acesso

O controle de acesso refere-se a uma variedade de meios técnicos para limitar o acesso às informações e infraestrutura. Esta é uma parte vital da segurança da informação, especialmente para as organizações que estão conectadas a outras organizações diretamente ou pela INTERNET.

Os controles de acesso regulam a admissão de usuários em áreas confiáveis da organização – acesso lógico aos sistemas de informação e acesso físico às instalações da organização. O controle de acesso é mantido por meio de um conjunto de políticas, processos para realizar essas políticas, e tecnologias que impõem as políticas. A aplicação de controles de acesso é realizada por quatro processos, para as áreas lógicas ou físicas:

- Obtenção da identidade do solicitante de acesso (identificação);
- Confirmação da identidade do solicitante que busca acesso (autenticação);
- Determinação em quais ações um solicitante autenticado pode atuar (autorização); e

- Documentação das atividades do solicitante autorizado nos sistemas (responsabilização).

O controle de acesso permite que as organizações restrinjam o acesso às informações, ativos de informação e outros ativos tangíveis para aqueles com uma necessidade genuína prevista. O controle de acesso é baseado em vários princípios-chave, incluindo o seguinte:

- **Menor privilégio** – esse é o princípio pelo qual os membros da organização podem acessar a quantidade mínima de informações pelo mínimo de tempo necessário para desempenhar as funções exigidas. Por exemplo, se uma tarefa requer apenas a leitura de dados, o usuário recebe acesso somente à leitura, que não lhe permitirá a criação, atualização ou exclusão de dados.
- **Precisa saber** – esse princípio limita o acesso de um usuário às informações específicas necessárias para realizar a tarefa atualmente atribuída. Por exemplo, um gerente que precisa registrar a avaliação de desempenho dos funcionários específicos de seu departamento tem acesso para ler e atualizar esses dados, mas não tem acesso aos dados das avaliações de desempenho de outros funcionários. Esse princípio é mais frequentemente associado à classificação de dados.
- **Segregação de funções** – esse princípio requer que tarefas significativas sejam divididas de tal forma que mais de um indivíduo seja responsável por sua conclusão. Por exemplo, no setor de compras, um usuário é responsável por fazer o pedido, porém outra pessoa do setor de finanças pode autorizar o pagamento e concluir o processo de compra.

1.3.3.3. Auditoria

Esse princípio complementa os demais, pois se torna necessário manter o controle das atividades que ocorrem em sua organização. Quando se permite o acesso de um usuário ou grupo de usuários aos recursos (informações), ainda é preciso se certificar de que eles se comportam de acordo com as regras estabelecidas nas políticas, particularmente aquelas relacionadas à segurança, conduta comercial e ética. Essencialmente, é preciso se certificar da responsabilização dos usuários no uso dos sistemas. A *responsabilização* significa atribuir a uma pessoa a responsabilidade por suas ações.

Isso é particularmente importante agora que a maioria das organizações abriga uma grande quantidade de informações em formato digital. E o acompanhamento de como as

peçoas acessam dados confidenciais armazenados digitalmente pode evidenciar possíveis perdas sofridas de negócios, roubo de propriedade intelectual, roubo de identidade e fraude. Além disso, uma violação de dados pode ter consequências nefastas para a organização.

Para tornar possível o processo de auditoria, muitas medidas são realizadas, visando garantir a *rastreabilidade* (produção de evidências) dos eventos ocorridos. Auditoria é o processo de revisão dos registros ou informações de uma organização. É necessário realizar auditorias para garantir que as pessoas cumpram as leis e políticas.

1. 4. Segurança nas organizações - visão de negócio

No dia 11 de setembro de 2001, o mundo inteiro ficou espantado com o acontecimento, até então inesperado: as duas torres gêmeas do World Trade Center foram atacadas e, em poucas horas, eram escombros. Além de muitas vidas serem ceifadas, muitas empresas que funcionavam naqueles prédios tiveram suas histórias interrompidas (falências, paralisação de atividades). Para os donos das empresas tal situação jamais aconteceria. Mas, aconteceu...

Como vimos, as organizações dependem de informações e, em algum nível, da infraestrutura de tecnologia da informação, que suporte essas informações. A infraestrutura é composta por computadores conectados a uma rede, acesso à internet, informações guardadas em repositórios eletrônicos etc. Para garantir a continuidade de seus negócios, as organizações precisam tomar certos cuidados para que as informações vitais aos seus negócios sejam devidamente preservadas, especialmente no caso de catástrofes.

1. 5. Ciclo de vida da Informação

O Ciclo de vida da informação é caracterizado pelos momentos decorrentes dos processos que envolvem a criação, o consumo e descarte da informação. Em algum desses momentos a informação pode ser colocada em risco.

São nessas ocasiões, do ciclo de vida da informação, que estão presentes ativos físicos, tecnológicos e humanos, que fazem uso da informação, dando sustentação aos processos que mantêm a operação da empresa.

O Ciclo de Vida da Informação compreende:

- **Manuseio** - momento em que a informação é criada e manipulada em atividades, como: digitação, cálculo, utilização de senhas para autenticação, geração de relatórios, preenchimento de um formulário;

- **Armazenamento** – momento em que a informação é guardada de forma eletrônica (digital ou não) ou analógica em uma mídia de armazenamento, que permite a recuperação em outro determinado momento;
- **Transporte** – momento em que a informação é transportada, ou encaminhada, por qualquer meio de transporte eletrônico/digital, falada ao telefone, transmitida via fax, celular, Internet etc.;
- **Eliminação** – momento em que a informação, não sendo mais necessária, por diversos fatores, é descartada, deletada, apagada, na forma de papel: fragmentada, queimada etc.

Muitas vezes, vulnerabilidades de informações são detectadas apenas quando está em um ambiente de produção online. A proteção da informação deve ser aplicada em todas as etapas de criação, consumo (quando usado por usuários) e retenção (arquivamento) para evitar problemas de privacidade.

1. 6. Conceitos de Ameaças e Vulnerabilidade

Para a segurança cibernética, o risco é o efeito integrado de vulnerabilidades, ameaças e impacto potencial de ataques cibernéticos. A vulnerabilidade é a fraqueza potencial no sistema de segurança de informação. Ameaça é uma possibilidade de ataque cibernético ao fazer uso de vulnerabilidades de um sistema (PRASAD, 2013).

Uma ameaça consiste de uma ação adversa executada por um “agente de ameaça” em um ativo. Os agentes de ameaça podem ser descritos como entidades individuais, mas, em alguns casos, são entidades, grupos de entidades etc. Exemplos de agentes de ameaça são: hackers, usuários descontentes, processos de computador e acidentes. Em geral, um agente de ameaça possui experiência, recursos, oportunidade e motivação.

Para entender o conceito de ameaça, deve-se primeiro examinar o problema, o invasor. Ao compreender quem é a ameaça e como ela opera, compreende-se melhor o valor e a função das medidas de segurança. O tipo de invasor que sempre se tenta identificar, detectar ou capturar também determinará o tipo de medida de segurança que pode ser construída e como pode ser implementada. Esse tópico ajuda a reconhecer os inimigos que se enfrenta.

1. 6. 1. Script Kiddies e Advanced Blackhats

São terminologias que descrevem categorias de atacantes. Em geral, existem dois tipos de invasores: o tipo que deseja comprometer o máximo de sistemas possível e o tipo que deseja comprometer um sistema específico ou sistemas de alto valor. Não importa se essas ameaças vêm de fora, como a INTERNET, ou de dentro, como um funcionário insatisfeito. A maioria das ameaças tende a se enquadrar em uma dessas duas categorias.

Conforme POULSEN (2020), o primeiro tipo, script kiddies, não se importa se o computador pertence a uma grande organização ou a um simples proprietário. Seu objetivo é invadir tantos sistemas quanto possível com o mínimo de esforço possível. Esses atacantes se concentram em alvos de oportunidade – morte fácil (termo usado por eles). São chamados de script kiddies, pois geralmente dependem de ataques com scripts – comandos em linguagem de computadores. Às vezes, esses invasores têm certos requisitos, como invadir sistemas com uma conexão rápida de INTERNET ou um disco rígido de grande capacidade para armazenar seus arquivos (filmes piratas, pornografia etc.). Em geral, porém, eles só se preocupam com os números (quantidade de computadores invadidos). Eles tendem a ser menos sofisticados, mas são muito mais numerosos, representando a grande maioria das sondagens (prospecção de alvos), varreduras nas redes e ataques, vistos atualmente.

O segundo tipo de invasor se concentra em alguns sistemas de alto valor. Esses indivíduos são provavelmente atacantes altamente experientes e bem-informados – chamados de advanced blackhats, ou blackhats avançados. Seus ataques geralmente têm motivação financeira ou patriótica, como o terrorismo patrocinado pelo Estado. Eles têm uma meta específica que desejam comprometer e se concentram apenas nela. Embora menos comuns e em número menor, esses atacantes são muito mais perigosos devido ao seu nível de habilidade avançado. Eles não apenas podem penetrar em sistemas altamente protegidos como também suas ações são difíceis de detectar e rastrear. Os blackhats avançados fazem pouco “alarde” ao atacar sistemas e se destacam em cobrir seus rastros.

1. 6. 2. Outras tipologias de atacantes

CRACKER

É um invasor do tipo advanced blackhat de bons conhecimentos técnicos e assim sendo, ele será capaz de apagar seus rastros de maneira mais sutil. Caracteriza-se pelo alto nível técnico, à medida que cada passo da invasão é realmente estudado e bem pensado. Esse tipo de atacante busca dados, como configurações padrões ou senhas padrões que ele possa explorar. Ele tem capacidade para desenvolver seus próprios exploits (mecanismos de exploração de vulnerabilidades). É genial e criativo para a má intenção. Realiza ataques inteligentes para comprometer a segurança da rede.

PHRACKER

São invasores, cujo alvo é o acesso não autorizado a recursos de telecomunicações.

HACKER

É um invasor do tipo script kiddies. São programadores na maioria deles inofensivos, usando o seu conhecimento para o bem. Alguns exemplos: Stallman, Linus Torvalds, Ada Lovelace, Douglas Engelbart, Dennis Ritchie, Ken Thompson, Arnaldo Melo, Marcelo Tossati, Alan Cox, entre outros.

HACKER ÉTICO

São indivíduos com formação em programação de computadores, que questionam as vulnerabilidades de segurança nas tecnologias disponíveis, provando suas teses com a execução de uma invasão “programada”, sem, entretanto, comprometer nenhum ativo de informação. Em geral, eles compartilham seu conhecimento gratuitamente, através da INTERNET.

1. 7 Ataques e contramedidas

O surgimento contínuo de novos ataques direcionados e avançados, com ameaças persistentes, exige o desenvolvimento de técnicas poderosas de segurança cibernética com novas abordagens. As pesquisas de ataque cibernético indicam que quase todos os aspectos da atividade humana estão sofrendo com esses crimes. De serviços de energia, finanças,

manufatura, serviço público, viagens, saúde, varejo, serviços profissionais etc., todos são vítimas de um ou outro crime cibernético.

O número e a gravidade dos crimes cibernéticos estão sempre aumentando com o aparecimento das novas tecnologias de computação móvel, dispositivos portáteis e a Internet das Coisas – **IoT**. Várias categorias de ciberataques incluem: malwares, ataques de rede, ataques de intrusão de rede, ataques de redes sociais, ataques de engenharia social, espionagem cibernética, ataques de acesso à rede, ciberspionagem, terrorismo digital, guerra cibernética etc., conforme mostrado na Tabela 2.1.

Tabela 2.1 Categorização de ataque cibernético

Categoria	Descrição de ataque	Subataques
Malware	Software malicioso usado para lançar ataques específicos nos sistemas dos computadores.	Adware, Spyware, Virus, Worm, Trojan, Rootkit, Backdoors, Key loggers, Rogue Security Software, Ransomware, Browser Hijacker etc.
Ataque de rede	Monitoramento ativo ou passivo de comunicações de computador e tráfego de rede.	Passivo, Ativo, Distribuído, Insider, Close-in, Phishing, Hijacking, Spoofing, Buffer overflow, Exploit, ataque de senhas (força bruta) etc.
Ataques de intrusão de rede	Qualquer atividade não autorizada em redes de computadores	Asymmetric routing, Buffer overflow, Protocol specific attacks, Traffic flooding, Trojans, Worms etc.
Engenharia Social	Usando redes sociais ou por telefone, os invasores aplicam truques de psicologia para os usuários fornecerem informações sigilosas.	Phishing, Pre-texting, Baiting, Quid Pro Quo, Tailgating etc.
Espionagem Cibernética	Espionagem de informações confidenciais de um usuário ou organização sem permissão	Espionagem industrial, Espionagem do Estado-nação, Espionagem econômica, Espionagem corporativa, Roubo de informações e sabotagem.
Reconhecimento	Ao descobrir os pontos fracos em sistemas de rede e serviços, o atacante reúne informações sensíveis sobre a rede.	Busca de informações na Internet, Varredura de ping, varredura de porta, Packet sniffers.
Ataques de Acesso à Rede	Através de pesquisas maliciosas na rede de atividades de: autenticação, FTP e web services, o intruso obtém acesso a um sistema de rede para obter informações confidenciais.	Eavesdropping, Data modification, Identity spoofing, Password-based, Denial of service, man in the middle attack, Compromised key attack, Sniffer attack, Application layer Attack, Trust exploitation etc.
Terrorismo cibernético	Uso da internet para atividades terroristas eletrônicas, como perturbação em grande escala de redes de computadores, infraestruturas críticas nacionais ou importantes operações de negócio.	Sabotagem, desfiguração de site e negação de serviço, Destruição de infraestruturas físicas críticas etc.
Guerra Cibernética	Grande perturbação em escala nacional e global, com ataques a importantes infraestruturas críticas, que afetam a vida de milhares de pessoas.	

1. 8 Crimes cibernéticos

O crime cibernético consiste essencialmente no uso de tecnologia de computador, na prática de atividade criminosa. Esse crime é materializado por meio do ataque cibernético.

O ataque cibernético é uma tentativa ilegítima de obter informações, dinheiro ou outro tipo de benefícios. Os ataques cibernéticos são classificados como ataques baseados na web e baseados em sistemas. Alguns especialistas consideram três outros tipos de ataques cibernéticos, como:

- Ataques naturais;
- Erros humanos;
- Ameaças de pessoas de dentro ou fora do país: hackers e criminosos cibernéticos.

Esse tópico cobre alguns tipos de ataques cibernéticos, como: backdoors, Ataque DoS, espionagem, falsificação, adulteração, ataque de repúdio, ataque de engenharia social, malware, adware etc.

1. 8. 1. Backdoors

É conhecido como ataque de “porta dos fundos”, pois o atacante contorna a entrada convencional de um sistema de computação e cria uma nova entrada oculta para escapar das políticas de segurança. Nesse ataque, o invasor instala software de registro de chaves ou qualquer outro software, por meio do qual obtém acesso ao sistema das vítimas. É um ataque muito sério, porque, via de regra, esse invasor modifica arquivos, informações ou instala softwares indesejados. Os ataques backdoor famosos incluem a exposição de interfaces de administração e gerenciamento, adição de recursos ou funções redundantes, criação de parâmetros ocultos, usuários redundantes, autorização para acesso de terceiros, autenticação e autorização entre os componentes de aplicativos, explora usuários antigos no sistema para permitir fraude de identidade, proteção defeituosa, exposição de dados de configuração e falha de isolamento entre diferentes ambientes.

1. 8. 2. Ataques de negação de serviço (Denial-of-service)

Os Ataques de Negação de Serviço (DoS) são usados para causar uma indisponibilidade de um recurso computacional. Nesse ataque, o atacante atinge o sistema para que o usuário real não possa acessar os dados ou recursos durante esse ataque. Isso nega ao usuário real o uso de recursos e inibe os serviços do sistema durante o ataque. Geralmente em um ataque

DoS, uma única máquina de computação ou conexão de INTERNET é usada para atacar o servidor-alvo, sobrecarregando seus recursos, como largura de banda, buffers de conexão TCP, buffer de aplicativo/serviço, ciclos de CPU etc.

Uma variante dessa modalidade são os Ataques Distribuídos de Negação de Serviço (DDoS), que usam muitos dispositivos de computação e um grande número de conexões de INTERNET para atacar um grande número de servidores, inundando seus recursos ao ponto de paralisá-los. Com o crescimento dos serviços de IoT, a ameaça de DDoS também está aumentando. O DDoS pode funcionar como uma subparte do BOTNET, comprometendo milhares de servidores em um tempo.

1. 8. 3. Eavesdropping (Espionagem)

Nesse ataque, o invasor intercepta a comunicação do sistema ou da rede sem seu conhecimento e usa essa comunicação para outro invasor ou inimigo daquela organização. É um tipo de ataque passivo, em que o bisbilhoteiro apenas observa e rouba as informações que computadores, smartphones ou outras entidades de rede estão transmitindo. Posteriormente, ajuda em ataques ativos, fornecendo todas as informações necessárias sobre a rede. Existem vários programas, como Carnivore e Narus, que fornecem informações que podem ser usadas para espionar. As redes Wi-Fi públicas são os alvos muito fáceis para ataques de espionagem, porque qualquer um pode entrar na rede e facilmente obter a senha disponível. A interceptação secreta é uma séria ameaça ao dispositivo de redes sem fio e Internet das Coisas.

1. 8. 4. Spoofing (falsificação)

Spoofing é um ataque, em que o invasor ou programa age como se fosse o verdadeiro e legítimo usuário de um sistema ou rede. Ele esconde sua originalidade e personifica o administrador do sistema ou vítima. Essas ameaças são frequentemente iniciadas por meio de e-mails, em que o endereço IP do remetente é falsificado. Roubando e usando a identidade de outra pessoa, o invasor monitora o tráfego de rede e registra informações para obter informações sobre nomes de usuários e senhas dos usuários da rede. Três tipos de ataques de spoofing são possíveis, incluindo spoofing de ARP, spoofing de IP e Falsificação de DNS. A falsificação de IP é usada em ataques DoS e em ataques *man in the middle*. O usuário nunca chega a saber sobre o ataque de spoofing, porque todos os pacotes de rede são recebidos pelo falso destinatário.

1. 8. 5. Tampering (Adulteração)

A adulteração é um ataque baseado na web, em que o invasor altera alguns parâmetros na URL do site sem o conhecimento do usuário. A URL parece legítima para o usuário. Hackers executam adulterações para obter acesso ilegal ao sistema ou algo potencialmente valioso. Com a autorização ilegal, alguns parâmetros inseridos pelo usuário em determinada página da web são capturados e alterados. Quando alguma informação está sendo trocada entre cliente e servidor, ela é manipulada pelo atacante.

1. 8. 6. Ataque de repúdio

Esse é um ataque em que um usuário nega falsamente ter realizado qualquer atividade ou se envolvido em qualquer transação eletrônica. Quando o usuário nega certas ações ou operações, então é chamado de repúdio. Esse usuário pode ser um usuário legítimo ou ator malicioso. Se o aplicativo ou sistema não tiver controles apropriados para rastrear as ações de registro do usuário, então o hacker tem a chance de controlar as informações em trânsito. É necessário um mecanismo de defesa robusto, que possa rastrear e manter o registro de todas as atividades dos usuários. O ataque de repúdio mais comum é aquele que falsifica uma mensagem de e-mail.

1. 8. 7. Engenharia Social

A engenharia social é um tipo de ataque não técnico, que se baseia no comportamento humano. Consiste em enganar o usuário e obter informações úteis dele. Usando essas informações, os invasores contornam os mecanismos de segurança empregados em rede. Ele induz o usuário a revelar suas informações secretas, quebrando assim o processo normal de segurança. Esses ataques incluem isca, phishing, spear phishing, pretextos e scareware. A arte de trapacear, utilizada por usuários malignos para satisfazer sua ganância por dinheiro ou outras coisas, nada mais é do que um ataque de engenharia social. Geralmente ocorre por meio de telefonemas ou e-mails, oferecendo cartões de crédito com inacreditáveis benefícios.

1. 8. 8. Adware

Adware é um tipo de software, que oferece suporte a anúncios incorporados em um aplicativo. Enquanto o programa está sendo executado, ele mostra um anúncio. O adware é semelhante ao malware, pois usa anúncios para infectar computadores com vírus mortais. Janelas pop-up aparecem continuamente na tela, onde o usuário está trabalhando. Geralmente, adware malicioso entra no sistema com programas e utilitários de software gratuitos baixado da Internet.

1. 8. 9. Ransomware

É um tipo de ameaça, em que os invasores restringem o acesso do usuário aos recursos do sistema e, em seguida, pedem uma quantia para remover a restrição. Esse resgate é pago online através de métodos de pagamento do tipo bitcoin, que não pode ser rastreado e, após os quais, o usuário pode acessar esse serviço. Sistemas bloqueados com ransomware simples podem ser desbloqueados com a ajuda de um especialista em segurança. Mas o ataque de ransomware avançado criptografa alguns arquivos importantes no sistema da vítima e exige algum pagamento para descriptografar e liberar os arquivos. Em 13 de maio de 2017, o ataque maciço de ransomware global “WannaCry” moveu o mundo. Atingiu centros de atendimento à saúde, indústrias e escritórios governamentais em todo o mundo, assumindo o controle de sistemas de computação afetados até que as vítimas paguem um resgate.

1. 8. 10. Spyware

Spyware é um software, que funciona como um agente secreto. O principal objetivo dos Spywares é reunir as informações com o uso da INTERNET e sem conhecimento do usuário. O spyware pode ser encontrado em um software livre, que está disponível gratuitamente na Internet para todos. Quando a vítima instala software gratuito, o spyware também é instalado no back-end por meio do qual o invasor obtém as informações do sistema da vítima.

1. 8. 11. Scareware

Scareware é um tipo de ameaça, em que mensagens sugerem o download de arquivos inúteis ou software em sistemas genuínos. O principal objetivo do Scareware é criar preocupação entre os usuários ou vítimas, provocando-os a baixar softwares irrelevantes. Uma janela de diálogo pop-up parece uma janela de diálogo do sistema, mas não é a mesma coisa.

1. 8. 12. Phishing

Phishing é uma ameaça cibernética. Seu principal objetivo é obter informações confidenciais, como nome de usuário, senha, detalhes da conta bancária etc. O invasor faz uma cópia idêntica de uma página da Web original e, em seguida, a envia para a vítima. A vítima não pode identificar as diferenças, porque a página da Web falsa e as páginas da Web originais são idênticas. A vítima fornece as informações confidenciais sobre a correspondência falsa na página da Web que, na realidade, são transferidas para o banco de dados do invasor. O atacante pode usar esses dados confidenciais para a introdução de golpes. O phishing de e-mail é famoso hoje em dia.

1. 8. 13. Ataques de Senha (Ataque de força bruta)

O ataque de senha é realizado quando um invasor quer saber a senha da vítima. Um invasor pode adivinhar a senha ou criar um programa que pode adivinhar a senha no sistema pelo método de força bruta, ou usa um banco de dados que contém um conjunto de senhas comuns e experimenta no sistema, nos campos de login de qualquer site.

1. 8. 14. Footprinting

Footprinting é um processo de fazer um mapa da rede ou sistema de uma organização. A modalidade footprinting é feita para coleta de informações. No início, um invasor deve escolher um sistema de destino, aplicativo ou localização física. Uma vez que o invasor sabe sobre um sistema de destino, pode obter informações mais específicas do destino.

1. 8. 15. Malware

É um software projetado para introduzir ações indesejadas no sistema pretendido (PRASAD; ROHOKALE, 2013), causando muitos prejuízos. Existem vários tipos de malware, tais como: vírus, worms, cavalos de Troia etc. O malware pode causar grandes danos aos discos rígidos, como também excluir alguns documentos, ou coletar alguns dados confidenciais sem qualquer permissão.

1. 8. 15. 1. Vírus e Worms

São usados para infectar ou modificar o conteúdo do sistema, a fim de facilitar que atacantes possam ter acesso aos computadores. Esses vírus e worms (vermes) agem como cavalos de Troia e backdoors. Eles são responsáveis por espalhar a infecção em grande escala, pois se replicam, daí o nome, visto que se assemelham ao comportamento de vírus e vermes da biologia. Os worms têm capacidade de autorreplicação e podem se espalhar rapidamente de sistema para sistema. Os vírus são categorizados de acordo com seu mecanismo de infecção.

1. 8. 16. Bot e Botnet

O BOT nada mais é do que um robô ou máquina com código de software autônomo embutido, que se comporta de forma inteligente. BOTs são usados por atacantes para postar mensagens de SPAM automaticamente, nas páginas da Web abertas pelos usuários.

Os ataques remotos são possíveis com a ajuda de BOTs. A BOTNET é um grupo de sistemas de máquinas robóticas infectadas, usadas principalmente para a preparação de

ataques DDoS, a produção de SPAM em grande quantidade, a criação de Golpes de marketing na Internet, roubar números de série de aplicativos, IDs de login e roubar informações confidenciais, como números de cartão de crédito etc. Com a BOTNET, dentro de uma fração de tempo, grandes redes de computadores podem ser infectadas ou paralisadas.

1. 8. 17. Cavalos de TrOia (Trojans)

São programas maliciosos, que funcionam de modo oculto para fazerem uma avaliação completa e permitirem o controle do computador ou sistema da vítima. Ao contrário do verdadeiro vírus, o cavalo de Troia não se replica, mantendo a vítima inconsciente do ataque. Os cavalos de Troia, em geral, estão escondidos dentro de algum anexo de e-mail ou de alguns programas, tais como jogos. Os ataques do cavalo de Troia são os seguintes: Backdoor ou Trojans de acesso remoto (RATs), kits de exploração, rootkits, cavalos de Troia de ransomware, Trojans de bancos, Trojan DDoS e DoS, Trojan Downloaders, Trojan Droppers, Trojans FakeAV, Trojans IM, Trojans ladrões de jogos, Trojans Sms, Trojans espões, Trojans de localização de correio etc.

1. 8. 18. Bombas Lógicas (Logic Bomb)

As bombas lógicas também são chamadas de slag code ou códigos de programação de efeito retardado. Adicionado ao software de um aplicativo ou sistema operacional, a bomba lógica permanece inativa até um evento ocorrer, acionando a ação maliciosa do código. O software malicioso pode ser acionado em resposta a um determinado evento, quando uma determinada data ou hora é alcançada. A bomba lógica espera até que o usuário faça o login no site de um banco ou site de rede social. Ela pode acionar um mecanismo denominado KEY LOGGER, que captura texto informado via teclado e envia a mensagem das credenciais da vítima para o invasor remoto.

1. 8. 19. Cryptojacking

Os cibercriminosos usam o cryptojacking para ganhar dinheiro fácil com menos esforços. Eles usam uma criptomoeda, exemplo BitCOIN, uma moeda digital. Bitcoins são criptomoedas populares usadas recentemente por sequestradores. O Cryptojacking é considerado a nova forma de Ransomware. Esses tipos de ataques são realizados principalmente em um navegador de INTERNET.

1.9 Tecnologias e suas vulnerabilidades

A criação de novas tecnologias quase sempre traz consigo um risco associado, devido às vulnerabilidades e seus efeitos adversos aos seus usuários. Quando uma vulnerabilidade é explorada, suas consequências e efeito para os negócios são sempre impactantes.

As sociedades industrializadas estão se tornando cada vez mais dependentes de computadores e, portanto, altamente vulneráveis à interrupção dos serviços baseados em computadores. A sabotagem intencional de programas vitais de computador em sistemas telefônicos, bancos ou fábricas poderia interromper grande parte do comércio.

As tecnologias quando desenvolvidas, e em função de sua complexidade, apresentam vulnerabilidades que, muitas vezes, são desconhecidas dos próprios desenvolvedores e possuem classificações, sendo uma delas denominada Zerodays (PIEKARSKI, 2018). As vulnerabilidades Zero-days são falhas novas e, tão logo que sejam detectadas, precisam ser corrigidas imediatamente.

Quanto mais complexo for o software, mais propenso a vulnerabilidades ele está (ALVES, 2017). Existem instituições que coletam vulnerabilidades de softwares descobertas por voluntários. A mais conhecida é a Common Vulnerabilities and Exposures (CVE®), que mantém um programa para identificar, definir e catalogar vulnerabilidades de segurança cibernética divulgadas publicamente (THE MITER CORPORATION, 2021). Existe um registro CVE para cada vulnerabilidade no catálogo. As vulnerabilidades são descobertas, atribuídas e publicadas por organizações de todo o mundo, que têm parceria com o Programa CVE.

Confira a lista dos 20 produtos mais vulneráveis e potencialmente perigosos e suas descrições, de acordo com o Information Technology Laboratory do NIST, na Tabela 1-1.

Tabela 11. Top 20 de produtos mais vulneráveis do ITL/NIST

Fonte: INFORMATION TECHNOLOGY LABORATORY, 2021.

CÓDIGO CVE®	DESCRIÇÃO	PUBLICAÇÃO	VERSÃO: RISCO
CVE-2021-20538	IBM Cloud Pak for Security (CP4S) 1.5.0.0 e 1.5.0.1 pode permitir que um usuário obtenha informações confidenciais ou execute ações às quais não deveria ter acesso, devido a mecanismos de autorização incorretos. IBM X-Force ID: 198919.	Publicado: 10 de maio de 2021; 1:15:07 PM -400	V3.1: 9.1 CRÍTICO V2.0: 6.4 MÉDIO
CVE-2021-20559	IBM Control Desk 7.6.1.2 e 7.6.1.3 é vulnerável a scripts entre sites. Essa vulnerabilidade permite aos usuários incorporarem código JavaScript arbitrário na IU da Web, alterando assim a funcionalidade pretendida, potencialmente levando à divulgação de credenciais.	Publicado: 10 de maio de 2021; 1:15:07 PM -400	V3.1: 5.4 MÉDIO V2.0: 3,5 BAIXO
CVE-2021-20577	IBM Cloud Pak for Security (CP4S) 1.5.0.0 e 1.5.0.1 é vulnerável a scripts entre sites. Essa vulnerabilidade permite aos usuários incorporarem código JavaScript arbitrário na IU da Web, alterando assim a funcionalidade pretendida, potencialmente levando à credencia... ler CVE-2021-20577	Publicado: 10 de maio de 2021; 1:15:07 PM -400	V3.1: 6.1 MÉDIO V2.0: 4.3 MÉDIO
CVE-2021-32399	net/bluetooth/hci_request.c no kernel Linux até 5.12.2 tem uma condição de corrida para a remoção do controlador HCI.	Publicado: 10 de maio de 2021; 18:15:06 PM -400	V3.1: 7.0 HIGH V2.0: 4.4 MÉDIO
CVE-2021-21649	Jenkins Dashboard View Plugin 2.15 e anteriores não escapam URLs referenciados em Image Dashboard Portlets, resultando em uma vulnerabilidade de cross-site scripting (XSS), que pode ser explorada por atacantes com permissão de Visualizar/Configurar.	Publicado: 11 de maio de 2021; 11h15:07 -0400	V3.1: 5.4 MÉDIO V2.0: 3,5 BAIXO
CVE-2021-21648	Jenkins Credentials Plugin 2.3.18 e anterior não escapam informações controladas pelo usuário em uma exibição que fornece, resultando em uma vulnerabilidade de cross-site scripting (XSS) refletida.	Publicado: 11 de maio de 2021; 11h15:07 -0400	V3.1: 6.1 MÉDIO V2.0: 4.3 MÉDIO
CVE-2021-32074	HashiCorp vault-action (também conhecido como Vault GitHub Action) anterior a 2.2.0 permite que invasores obtenham informações confidenciais de arquivos de log, porque um segredo de várias linhas não foi registrado corretamente com GitHub Actions para mascaramento de log.	Publicado: maio 07, 2021; 1:15:08 AM -0400	V3.1: 7.5 ALTO V2.0: 5.0 MÉDIO

CVE-2021-1520	Uma vulnerabilidade no processamento interno de mensagens de Cisco RV340, RV340W, RV345 e RV345P Dual WAN Gigabit VPN Routers pode permitir que um invasor local autenticado execute comandos arbitrários com privilégios de root no sistema operacional subjacente... ler CVE-2021-1520.	Publicado: 06 de maio de 2021; 9:15:11 AM -0400	V3.1: 6.7 MÉDIO V2.0: 7,2 ALTO
CVE-2021-1397	Uma vulnerabilidade na interface de gerenciamento baseada na web do software Cisco Integrated Management Controller (IMC) pode permitir que um invasor remoto não autenticado redirecione um usuário para uma página da web mal-intencionada. Essa vulnerabilidade se deve à entrada indevida ... leia CVE-2021-1397.	Publicado: 06 de maio de 2021; 9:15:09 AM -0400	V3.1: 6.1 MÉDIO V2.0: 5.8 MÉDIO
CVE-2021-1365	Vulnerabilidades múltiplas na interface de gerenciamento baseada na web do Cisco Unified Communications Manager IM & o serviço de presença pode permitir que um invasor remoto autenticado conduza ataques de injeção de SQL em um sistema afetado. Essas vulnerabilidades... leia CVE-2021-1365.	Publicado: 06 de maio de 2021; 9:15:09 AM -0400	V3.1: 8.1 ALTO V2.0: 5.5 MÉDIO
CVE-2021-1363	Vulnerabilidades múltiplas na interface de gerenciamento baseada na web do Cisco Unified Communications Manager IM & o serviço de presença pode permitir que um invasor remoto autenticado conduza ataques de injeção de SQL em um sistema afetado. Essas vulnerabilidades... leia CVE-2021-1363.	Publicado: 06 de maio de 2021; 9:15:09 AM -0400	V3.1: 8.1 ALTO V2.0: 5.5 MÉDIO
CVE-2021-1532	Uma vulnerabilidade na API de endpoint de vídeo (xAPI) do software Cisco TelePresence Collaboration Endpoint (CE) e do software Cisco RoomOS pode permitir que um invasor remoto autenticado leia arquivos arbitrários do sistema operacional subjacente. Este... leia CVE-2021-1532.	Publicado: 06 de maio de 2021; 9:15:11 AM -0400	V3.1: 6.5 MÉDIO V2.0: 4.0 MÉDIO
CVE-2021-1530	Uma vulnerabilidade na interface de gerenciamento baseada na web do Cisco BroadWorks Messaging Server Software pode permitir que um invasor remoto autenticado acesse informações confidenciais ou causar uma negação parcial de serviço (DoS) em um s... ler CVE-2021-1530.	Publicado: 06 de maio de 2021; 9:15:11 AM -0400	V3.1: 7.1 ALTO V2.0: 5.5 MÉDIO
CVE-2021-1478	Uma vulnerabilidade no componente Java Management Extensions (JMX) do Cisco Unified Communications Manager (Unified CM) e Cisco Unified Communications Manager Session Management Edition (Unified CM SME) pode permitir um ataque remoto autenticado... leia CVE-2021-1478.	Publicado: maio 06, 2021; 9:15:10 AM - 0400	V3.1: 6,5 MÉDIO V2.0: 6,8 MÉDIO

CVE-2017-3139	Uma falha de negação de serviço foi encontrada na forma como o BIND lidou com a validação de DNSSEC. Um invasor remoto pode usar essa falha para fazer a saída nomeada inesperadamente com uma falha de declaração por meio de uma resposta DNS especialmente criada.	Publicado: 09 de abril de 2019; 14h29h -0400	V3.1: 7.5 ALTO V2.0: 5.0 MÉDIO
CVE-2020-28198	O parâmetro 'id' do IBM Tivoli Storage Manager Versão 5 Release 2 (Interface Administrativa da Linha de Comandos, dsmdmc.exe) é vulnerável a um estouro de buffer de pilha explorável. Nota: a vulnerabilidade pode ser explorada... leia CVE-2020-28198.	Publicado: 06 de maio de 2021; 4:15:09 PM -400	V3.1: 7.0 ALTO V2.0: 4.4 MÉDIO
CVE-2021-1516	Uma vulnerabilidade na interface de gerenciamento baseada na web do Cisco AsyncOS Software para Cisco Content Security Management Appliance (SMA), Cisco Email Security Appliance (ESA) e Cisco Web Security Appliance (WSA) pode permitir uma autenticação, remot... leia CVE-2021-1516.	Publicação: 06 de maio de 2021; 9:15:10 AM -0400	V3.1: 6.5 MÉDIO V2.0: 4.0 MÉDIO
CVE-2021-1511	Múltiplas vulnerabilidades no software Cisco SD-WAN vEdge podem permitir que um invasor execute código arbitrário como usuário raiz ou causar uma condição de negação de serviço (DoS) em um dispositivo afetado. Para mais informações sobre essas vulnerabilidades, veja ... leia CVE-2021-1511.	Publicado: 06 de maio de 2021; 9:15:10 AM -0400	V3.1: 6,5 MÉDIO V2.0: 6,8 MÉDIO
CVE-2021-1510	Múltiplas vulnerabilidades no software Cisco SD-WAN vEdge podem permitir que um invasor execute código arbitrário como usuário raiz ou causar uma condição de negação de serviço (DoS) em um dispositivo afetado. Para mais informações sobre essas vulnerabilidades, veja... leia CVE-2021-1510.	Publicado: 06 de maio de 2021; 9:15:10 AM -0400	V3.1: 7.5 ALTO V2.0: 5.0 MÉDIO
CVE-2021-1509	Múltiplas vulnerabilidades no software Cisco SD-WAN vEdge podem permitir que um invasor execute código arbitrário como usuário raiz ou causar uma condição de negação de serviço (DoS) em um dispositivo afetado. Para mais informações sobre essas vulnerabilidades, veja... leia CVE-2021-1509.	Publicado: 06 de maio de 2021; 9:15:10 AM -0400	V3.1: 7,5 ALTO V2.0: 8,5 ALTO

1. 10 Tecnologias para a segurança da informação

Com a evolução das ameaças, aconteceu também uma evolução das formas de mitigação desses problemas. Essa evolução ocorreu com o desenvolvimento de tecnologias: hardwares e softwares, além de técnicas e boas práticas. Esse tópico aborda as principais tecnologias.

1. 10. 1. Firewall

Um firewall é um mecanismo para manter o controle sobre o tráfego, que entra e sai das redes. Normalmente firewalls são colocados em pontos onde ocorrem mudanças no nível de confiança, como a fronteira entre uma rede interna e a INTERNET. Também se pode instalar um firewall na rede interna para evitar que pessoas não autorizadas acessem o tráfego de rede de natureza sensível.

1. 10. 2. Antivírus

Alguns firewalls sofisticados podem detectar malwares e podem (devem) bloqueá-los na rede. Worms que tentam se propagar e se espalhar automaticamente na rede, e malware, que tenta “conexão externa”, pode ser interrompido pelo firewall, confinando seu alcance. As soluções de controle de malware devem ser colocadas em camadas, e o firewall pode formar um importante componente de um recurso de bloqueio de malware, baseado em rede para complementar softwares de antivírus de estações de trabalho (desktop) da organização.

1. 10. 3. Filtragem e cache de conteúdo da Web(URL)

Como o firewall está posicionado de forma ideal na rede, pode ser usado para filtrar o acesso a sites (entre redes internas da organização e a Internet). É possível se optar por implementar uma tecnologia em separado de Sistema ou serviço de filtragem de URL (WEB FILTER), ou implementar um firewall que tenha esse recurso integrado.

1. 10. 4. Filtragem de E-mail (SPAM)

Tal como acontece com a filtragem de conteúdo da web, os firewalls modernos podem subtrair o SPAM do seu Servidor de mensagens de e-mail antes de serem entregues. Para implementar esse serviço, necessita-se de um firewall que inclui essa capacidade.

1. 10. 5. Sistemas de detecção e prevenção de intrusão

Os sistemas de detecção e prevenção de intrusão (IDPSs) funcionam da mesma forma que um alarme contra roubo. Quando o sistema detecta uma violação – uma janela aberta ou

quebrada - ativa o alarme. Esse alarme pode ser audível e visível (ruído e luzes) ou pode ser um alarme silencioso, que envia uma mensagem para uma empresa de monitoramento. Como quase todos os IDPSs, os administradores podem escolher os níveis de configuração e alarme. Muitos IDPSs podem ser configurados para notificar os administradores através de e-mail.

Sistemas que incluem tecnologia de prevenção de intrusão tentam impedir que o ataque seja bem-sucedido por um dos seguintes meios:

- Interromper o ataque, encerrando a conexão de rede ou a sessão de usuário do invasor;
- Alterar o ambiente de segurança, reconfigurando os dispositivos de rede (firewalls, roteadores e interruptores) para bloquear o acesso ao sistema de destino;
- Alterar o conteúdo do ataque para torná-lo benigno - por exemplo, removendo um anexo de arquivo infectado de um e-mail antes que o e-mail chegue ao destinatário.

As tecnologias de prevenção de intrusão podem incluir um mecanismo que corta o circuito das comunicações - uma medida extrema que pode ser justificada, quando a organização é atingida por um grande ataque de Negação de Serviço Distribuído (DDoS) ou ataque carregado de malwares. Todos os IDPSs requerem configurações complexas para fornecer o nível apropriado de detecção e resposta. Esses sistemas são baseados em rede para proteger as informações dos ativos da rede ou são baseados em servidores para proteger o servidor ou ativos de informações de servidor. IDPSs usa um dos dois métodos básicos de detecção, baseado em assinatura ou baseado em anomalia estatística.

1. 10. 6. Criptografia

De acordo com WHITMAN; MATTORD (2014), embora não seja um aplicativo específico ou ferramenta de segurança, a criptografia representa um elemento sofisticado de controle, que geralmente é incluído em outros controles de Segurança da Informação. Na verdade, muitas ferramentas relacionadas à segurança usam tecnologias de criptografia incorporadas. O uso de ferramentas criptográficas adequadas pode garantir a confidencialidade por manter informações privadas ocultas de quem não pode vê-las. Outros métodos criptográficos podem fornecer maior integridade às informações, provendo um mecanismo para garantir que uma mensagem em trânsito não foi alterada através de um processo que cria uma espécie de verificador de integridade, ou *hash*. Em situações de e-commerce, algumas ferramentas criptográficas podem ser usadas para garantir que as partes da transação sejam autênticas e que elas não podem negar mais tarde ter participado de uma transação - um recurso frequentemente chamado de *não repúdio*.

Criptografia é o processo de conversão de uma mensagem original em um formato, que não pode ser usado por indivíduos não autorizados (POULSEN, 2020). Dessa forma, qualquer pessoa sem as ferramentas e o conhecimento para converter uma mensagem criptografada de volta ao seu formato original não será capaz de interpretá-la.

A ciência de criptografia, conhecida como criptologia, abrange duas disciplinas: criptografia e criptanálise (WHITMAN; MATTORD, 2014).

De acordo com WHITMAN; MATTORD (2014), Criptografia – das palavras gregas “kryptos”, que significa “oculto” e “Graphein”, que significa “escrever” – é o conjunto de processos envolvidos na codificação e decodificação de mensagens para impedir que outras pessoas as entendam. Criptoanálise – de “analein”, significando “Separar” – é o processo de decifrar a mensagem original (ou texto simples) de uma mensagem criptografada (ou texto cifrado), sem conhecer os algoritmos e as chaves usadas para realizar a criptografia.

Ainda de acordo com WHITMAN; MATTORD (2014), as soluções envolvendo criptografia se referem a um conjunto de termos básicos, sendo eles:

- **Algoritmo** – é um método matemático ou processo usado para converter uma mensagem não criptografada em uma mensagem criptografada;
- **Cifra** – é a transformação dos componentes individuais de uma mensagem não criptografada (caracteres, bytes ou bits) em componentes criptografados ou vice-versa (decifrar e cifrar);
- **Texto cifrado ou criptograma** – é a mensagem criptografada ou codificada ininteligível, resultante de uma criptografia;
- **Criptossistema** – é um sistema formado por conjunto de transformações necessárias para converter uma mensagem não criptografada em uma mensagem criptografada;
- **Decifrar** – é o ato de descriptografar ou converter texto cifrado em texto simples;
- **Codificar ou Cifrar** – é o ato de criptografar ou converter texto simples em texto cifrado;
- **Chave** – é uma informação usada em conjunto com o algoritmo para criar o texto cifrado a partir do texto simples; pode ser uma série de bits usados em um algoritmo matemático ou o conhecimento de como manipular o texto simples;
- **Chave Simétrica** – é uma chave usada por algoritmos de encriptação simétrica, que usam a mesma chave para executar as funções de encriptação e desencriptação.

- **Chave Assimétrica** – é usada em algoritmos de encriptação assimétrica, que usam uma chave para encriptar os dados e outra chave para descriptá-los.
- **Keyspace** – é toda a gama de valores que podem ser usados para construir uma chave individual;
- **Texto simples** – é a mensagem original não criptografada, que é criptografada e que é o resultado de descriptografia bem-sucedida;
- **Fator de trabalho** – é a quantidade de esforço (geralmente expressa em unidades de tempo) necessária para realizar a criptanálise em uma mensagem codificada, ou seja, decifrar.

1. 10. 6. 1. Operações de criptografia

A criptografia é realizada, usando algoritmos para manipular o texto simples, transformando-o num texto cifrado, usado para a transmissão de um emissor para um receptor. Algumas operações de criptografia amplamente utilizadas são explicadas a seguir.

1. 10. 6. 2. Algoritmos Criptográficos

A força, em termos de criptografia, dos algoritmos varia em função do tamanho de chave utilizada de 40 bits a 448 bits. Quanto maior o tamanho da chave, mais forte será o Algoritmo de criptografia. Para quebrar, com força bruta, uma chave de 40 bits, o fator de trabalho varia de 1,4 minutos a 0,2 segundos, dependendo da capacidade de processamento do computador. Em comparação, uma chave de 64 bits requer entre 37 dias a 50 anos para quebrar, novamente dependendo da velocidade do processador. Atualmente, qualquer chave com comprimento superior a 256 bits é considerada indecifrável.

Os algoritmos matemáticos usados para criptografia, também chamados de algoritmos criptográficos, são conhecidos por um nome e possuem objetivos específicos. Existem dois tipos de algoritmos criptográficos:

- Funções criptográficas de *hash*;
- Algoritmos de Criptografia.

As funções criptográficas de *hash* são algoritmos matemáticos unívocos, usados para mapear dados de qualquer tamanho para uma sequência de bits de tamanho fixo chamada de *HASH* (resumo). São chamadas de unívocos, porque não se consegue obter o dado original com base no resumo ou hash gerado. As funções criptográficas de hash são amplamente

utilizadas nas práticas de segurança da informação, como assinaturas digitais, códigos de autenticação de mensagens e outras formas de autenticação.

As funções de hash devem ter as seguintes propriedades (fonte: wikipedia):

- A mesma mensagem sempre resulta no mesmo valor hash, ou seja, a função é determinística;
- O valor do hash é calculado rapidamente;
- É inviável ter duas mensagens com o mesmo valor hash (conhecido como “colisão”);
- É inviável criar intencionalmente uma mensagem que produza um determinado valor de hash;
- Pequenas alterações na mensagem devem alterar o valor de hash resultante.

Os algoritmos matemáticos usados para criptografia recebem nomes e veremos os principais a seguir:

- **MD5 - Acrônimo de Message Digest 5** - é um algoritmo de hash, que usa uma entrada de comprimento aleatório para gerar um hash de 128 bits. É comum criar uma assinatura digital para acompanhar documentos e e-mails para provar a integridade da fonte;
- **SHA - Acrônimo de Secure Hash Algorithm** - também é um algoritmo de hash, que gera um resumo hash de 160 bits. O algoritmo SHA leva um pouco mais de tempo de processamento que o MD5, sendo considerado de criptografia mais forte. É o algoritmo preferido, para uso, pelas entidades de governo;
- **RC4 e RC5** - são algoritmos de cifragem de fluxo de dados em redes, que usam chave simétrica, criados em 1987 por Ronald Rivest. Esses algoritmos usam permutações matemáticas aleatórias e um tamanho de chave variável. Possuem duas funcionalidades básicas: uma para gerar uma chave que será usada para encriptar e decriptar (KSA) e outra para realizar a criptografia propriamente dita da mensagem com o uso dessa chave (PRGA);
- **Blowfish** - é um algoritmo de cifragem de bloco de 64 bits, o que significa que criptografa dados em bloco ou blocos. É mais forte que os RC4 e RC5 e tem um comprimento de chave variável entre 32 e 448 bits.

1. 10. 7. Protegendo a Web

Os Criptossistemas foram criados para ajudar a proteger a atividade na Web, especialmente as transações entre os navegadores dos clientes e os servidores da Web nos sites de comércio eletrônico. Entre os protocolos usados para essa finalidade, estão: Secure Electronic Transactions, Secure Sockets Layer, Protocolo de Transferência Segura de Hipertexto, Secure Shell e Segurança IP. Serão apresentados a seguir:

- **SECURE ELECTRONIC TRANSACTIONS (SET)** – foi desenvolvido pela MasterCard e VISA em 1997, para fornecer proteção contra fraude de pagamento eletrônico. Funciona criptografando as transferências do cartão de crédito com troca de chaves criptográficas. SET fornece a segurança para ambas as transações de cartão de crédito, baseadas na Internet e em lojas de varejo;
- **SECURE SOCKETS LAYER (SSL)** – foi desenvolvido pela Netscape em 1994, a fim de fornecer segurança para transações de comércio eletrônico online. Ele usa uma série de algoritmos, mas depende principalmente de algoritmo RSA para transferência de chave e IDEA, DES ou 3DES para transferência de dados baseada em chave simétrica criptografada;
- **PROTOCOLO DE TRANSFERÊNCIA DE HIPERTEXTO SEGURO (HTTPS)** – é uma solução criptografada para a versão não segura de HTTP. Ela provê suporte aos protocolos acima mencionados e pode fornecer transações de comércio eletrônico seguras;
- **SECURE SHELL (SSH)** – é uma extensão popular do conjunto de protocolos TCP/IP. Patrocinado pela IETF (Internet Engineering Task Force), fornece segurança para conexões de acesso remoto em redes públicas, criando uma conexão segura e persistente;
- **SEGURANÇA IP (IPSec)** – é a autenticação criptográfica primária de Protocolo de IP, desenvolvida pelo IETF (Internet Engineering Task Force). Suporta uma variedade de aplicativos, incluindo VPNs.
- **VPN** – é o acrônimo de Virtual Private Network (Rede Privada Virtual) e consiste do uso da criptografia para estabelecer uma conexão de rede, usando a INTERNET (rede pública), onde todo o tráfego de informações fica oculto, formando assim uma espécie de “Túnel”. Esse conceito de Túnel garante a privacidade entre dois pontos, pois cria uma conexão privada virtual, já que não existe uma conexão privativa real.

1. 10. 8. Certificados Digitais

Um certificado digital é exclusivo para um indivíduo, como uma carteira de motorista ou um título de eleitor, sendo composto por duas partes: uma chave pública e uma chave privada. A chave privada fica sempre com o indivíduo dono do certificado digital; a chave pública ele divulga por meio de listas de certificados digitais válidos nos sites de autoridades certificadoras.

O certificado é exclusivo para uma pessoa e, normalmente, é emitido por uma autoridade de certificação confiável, ou AC. A lista de autoridades de certificação em que a pessoa confia é distribuída automaticamente, podendo ser acessada em seu navegador. Cada computador em seu sistema operacional possui um repositório de certificados digitais, em geral atualizados quando se atualizam as versões do mesmo sistema operacional. Qualquer usuário pode ver os certificados instalados em sua máquina (seu e de outras pessoas físicas ou jurídicas) e outras autoridades de certificação em que se confia.

Todo certificado digital tem um prazo de validade. Após esse prazo, ele é considerado revogado, não sendo mais garantido pela Autoridade Certificadora que o emitiu.

1. 10. 9. Assinaturas Digitais

Uma assinatura digital é gerada por um software *assinador digital*, em que uma chave privada é usada para garantir a autenticidade de um documento: e-mail, arquivo de texto, planilhas etc. O objetivo da assinatura é duplo. O primeiro objetivo é certificar que veio de um determinado indivíduo, isso é chamado de não repúdio; o segundo objetivo é garantir que o conteúdo não tenha sido alterado, isso é chamado de integridade de dados.

A forma como um programa *assinador* faz isso é aplicando ao conteúdo da mensagem uma função hash. Isso produz um resumo criptográfico do documento, chamado de hash da mensagem. Esse é um valor único, e se o algoritmo matemático que o produz é forte, o hash da mensagem tem os seguintes atributos:

- A mensagem original não pode ser reproduzida do hash;
- Cada hash é único.

Depois que o hash é criado, ele é criptografado com a chave privada do remetente da mensagem. O hash criptografado é anexado à mensagem original junto com a chave pública do remetente. O destinatário então abre a mensagem, e o hash é descriptografado, fazendo-se uso da chave pública enviada em conjunto. O hash enviado é comparado a um hash idêntico,

gerado pelo programa assinador do destinatário. Se eles combinarem, então está tudo certo, a assinatura é válida. Caso contrário, o programa verificador de assinatura irá informar que o documento foi alterado – falha na integridade da mensagem enviada.

Para obter um certificado digital ou ID digital, é preciso entrar em contato com uma Autoridade Certificadora. Os Certificados Digitais em geral não são gratuitos, apesar de existirem certificados gratuitos.

Para fornecer o Certificado Digital, a Autoridade Certificadora irá encaminhar o solicitante a uma Autoridade Registradora, que irá realizar a prova presencial de identificação do solicitante, exigindo um documento oficial de identidade com fotografia.

1. 10. 9. 1. Infraestrutura de chaves públicas do Brasil (ICP-Brasil)

Conforme AGOSTINHO (2020), a Medida Provisória Nº 2.200/2001 criou a “AC-Raiz” – Autoridade Certificadora Central, submetida ao Comitê Gestor da ICP-Brasil, com poderes para credenciar entidades certificadoras.

As assinaturas eletrônicas produzidas sob o amparo da ICP-Brasil terão presunção de veracidade com relação aos signatários, possibilitando plena atribuição de validade jurídica a documentos eletrônicos. Essa medida, entretanto, não negou a validade de outros certificados emitidos por entidades não credenciadas, nacionais ou estrangeiras.

O Instituto Nacional de Tecnologia da Informação apresentou ao Parlamento nacional um substitutivo que seria efetivamente uma Lei para o sistema nacional de certificação digital, a Infraestrutura de chaves públicas do Brasil, a ICP-Brasil, porém esta norma ainda não foi apreciada e votada.

O Instituto Nacional de Tecnologia da Informação – ITI é o órgão nacional, que define as políticas, os processos e aprova e homologa a solução de certificação digital da ICP-Brasil.

1. 11. Padrões, metodologias e práticas de segurança da informação

Esse tópico irá abordar os principais padrões existentes no mercado, aplicáveis aos diferentes tipos de gestão de Segurança da Informação.

1. 11. 1. Modelos de gestão de segurança

As organizações podem aplicar modelos de gestão em seus processos de Segurança da Informação. Modelo de gestão, segurança e qualidade são fornecidos por organizações nacionais e internacionais de definição de padrões.

1. 11. 1. 1. A família ISO 27000

Conforme WHITMAN; MATTORD (2014), um dos modelos de gestão em Segurança da Informação mais amplamente referenciado é o Código de Práticas para Gestão de Segurança da Informação, que foi publicado originalmente como British Standard BS 7799. Em 2000, o Código de Práticas foi adotado como um código padrão internacional estruturado para Segurança da Informação pela International Organization for Standardization (ISO) e a International Electrotechnical Commission (IEC) como ISO/IEC 17799.

O documento foi revisado em 2005 (tornando-se ISO 17799: 2005) e, em 2007, foi renomeado para ISO 27002, a fim de alinhá-lo com o documento ISO 27001, conforme a Tabela 1-2. Embora os detalhes da ISO/IEC 27002 estejam disponíveis apenas para aqueles que adquirem a norma, sua estrutura e aspectos gerais de organização são bem conhecidas. A estrutura dessa norma padrão é formada pelas seguintes seções:

- Estrutura;
- Avaliação e tratamento de risco;
- Política de Segurança;
- Organização de Segurança da Informação;
- Gerenciamento de ativos;
- Segurança de Recursos Humanos;
- Segurança Física e Ambiental;
- Comunicações e operações;
- Controle de acesso;
- Aquisição, desenvolvimento e manutenção de sistemas de informação;
- Gerenciamento de Incidentes de Segurança da Informação;
- Gestão de Continuidade de Negócios;
- Conformidade.

Tabela 12. Padrões atuais e planejados da série ISO 27000

ISO 27000 Padrão da série	Ano/status	Título ou tópico	Comentário
27000	2009	Visão geral e terminologia da série	Define a terminologia e o vocabulário para a série padrão
27001	2005	Gestão de Segurança da Informação Especificação do Sistema	Extraído de BS 7799:2
27002	2007	Código de Boas Práticas para Informações Gerenciamento de segurança	Renomeado de ISO/IEC 17799, extraído de BS 7799:1
27003	2010	Segurança da Informação Sistemas de Gestão Diretrizes de Implementação	Fornece orientação para implantação de um Sistema de Gestão de Segurança da Informação (ISMS - Information Security Management System)
27004	2009	Métricas para aferição da gestão de Segurança da Informação	Projetado para ajudar a medição, relatório e melhorias para ISMS.
27005	2008/2011	ISMS Risk Management	ISO 27005: 2011 é a versão atualizada
27006	2007	Requisitos para Órgãos Fornecendo Auditoria e certificação de um ISMS	Destina-se principalmente a apoiar a aplicação de certificação de organizações no padrão ISO.
27007	Planejada	Diretrizes para auditoria de ISMS	Com foco em sistemas de gestão
27008	Planejada	Diretrizes para auditoria de ISMS	Com foco em controles de segurança
27010	2012	Gestão da Segurança da Informação para comunicação Intersetorial e interorganizacional	Concentra-se na segurança durante trocas de informações entre organizações e entidades
27011	2008	Diretrizes de Segurança da Informação para as telecomunicações e entidades setoriais.	Concentra-se na Gestão da Segurança da Informação dentro de organizações de telecomunicações e baseia-se na ISO 27002
27014	Planejada	Estrutura de Governança de Segurança da Informação	
27015	Planejada	Diretrizes de Gestão da Segurança da Informação para Setores de finanças e seguros	
27032	Planejada	Diretrizes para segurança cibernética	
27034	Planejada	Diretrizes para segurança de aplicativos	

1. 11. 1. 2. Modelos de Segurança NIST

De acordo com WHITMAN; MATTORD (2014), outras abordagens para estruturar a Gestão de Segurança da Informação são encontradas em muitos documentos de Segurança da Informação no Computer Security Resource Center do NIST (National Institute of Standards and Technology). Esses documentos são as referências adotadas pelo governo dos EUA, e as razões para não adotar os padrões ISO/IEC 17799 são:

- Eles estão disponíveis ao público gratuitamente; e

- Estão disponíveis há algum tempo e, portanto, foram amplamente revisados por profissionais do governo e da indústria.

Principais normas:

- **Publicação Especial NIST 800-12 - Computer Security Handbook** - é uma excelente referência e guia para gerenciamento de rotina de Segurança da Informação. Fornece orientação na concepção e implementação de novos sistemas de segurança.
- **Publicação Especial NIST 800-14 - Princípios geralmente aceitos e práticas para a proteção de sistemas de tecnologia da informação** - descreve as práticas recomendadas e fornece informações sobre princípios de Segurança da Informação comumente aceitos, que podem direcionar a equipe de segurança no desenvolvimento de um plano de segurança. Também descreve os princípios dos aspectos filosóficos, que a equipe de segurança deve integrar em todo o processo Segurança da Informação, ampliando nos componentes do SP 800-12.
- **Publicação Especial NIST 800-18 Rev. 1 - Guia para Desenvolvimento de planos de segurança para sistemas de informação federais** - fornece métodos detalhados para avaliar, projetar e implementar controles e planos para aplicativos de vários tamanhos.
- **Publicação Especial NIST 800-30, Rev. 1 - Guia para Gestão de Avaliações de Risco** - fornece uma base para o desenvolvimento de um programa de gestão de risco, contendo as definições e as orientações práticas necessárias para avaliar e mitigar os riscos identificados nos sistemas de TI. O objetivo final é ajudar as organizações a gerenciar melhor os riscos da missão relacionados à TI.
- **Publicações Especiais NIST 800-53 Rev. 3 e 800-53A Rev. 1 - Guia para avaliar os controles de segurança em sistemas de informação federais e Organizações: Construindo Planos de Avaliação de Segurança Eficazes** - é o sucessor funcional de “SP 800-26: Guia de autoavaliação de segurança para sistemas de tecnologia da informação”.

Capítulo 2 – Princípios de governança de segurança da informação

Conforme GUPTA; SHARMA (2009), a governança da segurança da informação é caracterizada como a quarta onda de gestão em segurança. A primeira onda foi de natureza técnica; a segunda, gerencial; a terceira, institucional e a quarta sobre governança. Todas as pessoas envolvidas com a segurança da informação, do conselho de administração aos executivos-chefes, profissionais de TI, profissionais de segurança da informação e funcionários da organização, devem preocupar-se com a sua governança.

A estrutura de governança deve ser incorporada à organização e aplicada a todas as atividades e processos, como planejamento, design, aquisição, desenvolvimento, implantação e monitoramento. A estrutura de governança abrange o ambiente de governança, domínios de governança e princípios de governança.

Este capítulo irá abordar os aspectos de governança aplicados à Segurança da Informação.

2. 1. O ambiente de governança

A governança ocorre no ambiente organizacional, que é determinado pelas condições e circunstâncias existentes que incluem:

- Leis, diretrizes e diretrizes federais e estaduais;
- Regulamentos da indústria e práticas de governança;
- Missão e estratégias da organização;
- Tolerância ao risco da organização;
- Ética, cultura e valores da organização;
- Tolerância ao risco da organização;
- Missão, visão e plano estratégico da organização;
- Localização da organização e abordagem de gestão (centralizada ou descentralizada);
- Políticas, padrões, processos e procedimentos da organização;
- Funções e responsabilidades da organização;
- Planos e relatórios da organização;
- Monitoramento da organização para conformidade.

2. 1. 1. Os domínios de governança

Os domínios da estrutura de governança são:

- **Planejamento e alinhamento estratégico** – a previsão e as capacidades necessárias para entregar valor organizacional;
- **Entrega de valor** – geração de benefícios prometidos no prazo e dentro do orçamento;
- **Gestão de risco** – um processo contínuo, que começa com a identificação do risco (ameaças e vulnerabilidades) e seu impacto sobre os ativos, mitigação do risco por contramedidas e aceitação formal do risco residual pela gestão;
- **Gerenciamento de recursos** – implantar os recursos certos (pessoas, instalações, hardware, software etc.) para satisfazer as necessidades organizacionais;
- **Medição de desempenho** – fornecer feedback de que a organização precisa, para se manter no rumo certo ou tomar medidas corretivas oportunas.

2. 1. 2. Os princípios de governança

Os princípios de governança são:

- Expectativas claras;
- Valores claros;
- Políticas e padrões explícitos;
- Comunicação forte;
- Estratégia clara;
- Manuseio responsável e claro das operações;
- Estrutura organizacional competente;
- Funções e responsabilidades claramente definidas;
- Processos e procedimentos ordenados;
- Uso eficaz da tecnologia;
- Gestão responsável de ativos;
- Gerenciamento de mudança proativo;
- Divulgações oportunas e precisas;
- Revisão independente e melhoria contínua.

2. 2. Conceitos de governança aplicada à segurança da informação

Considerando-se os conceitos de governança: ambiente, domínio e princípios, a definição para governança de segurança deverá estar totalmente alinhada, sendo seu objetivo maior de tal governança a garantia de que

- as atividades de segurança da informação estejam adequadas e sendo realizadas de forma que os riscos sejam adequadamente reduzidos;
- os investimentos em segurança da informação estejam devidamente aplicados;
- o programa de segurança tenha visibilidade para a gestão executiva; e
- a gestão esteja fazendo as perguntas apropriadas para determinar a eficácia do programa de segurança das informações.

A motivação para a governança de segurança da informação é a prevenção de fraudes financeiras por meio da manipulação dos dados eletrônicos de uma organização. As diversas tentativas de prevenção de abusos e fraudes levaram ao aumento de regulamentos, padrões e diretrizes, fazendo com que as organizações tenham mais atenção à governança, que mudou a dinâmica do gerenciamento de segurança da informação.

2. 2. 1. Princípios de gestão de segurança da informação

Diferentemente das outras equipes de gestão da organização, a equipe de gestão de Segurança da Informação opera como todas as outras gerências, pois a segurança é inerente a todos os processos organizacionais. Muitas vezes, as metas e os objetivos das demais áreas da empresa diferem das metas e dos objetivos da gestão da segurança da informação, gerando conflitos que têm de ser solucionados pela alta gestão. Os princípios de Gestão da Segurança da Informação são:

- **PLANEJAMENTO** – o planejamento na gestão Segurança da Informação é uma extensão do modelo de planejamento básico da empresa, onde são incluídas, no modelo de planejamento, as atividades necessárias da área de segurança para apoiar os projetos, a criação e implantação de estratégias de Segurança da Informação dentro do ambiente de planejamento de TI.
- **POLÍTICAS** – o conceito de política compreende o conjunto de diretrizes organizacionais, que definem determinados comportamentos dentro da empresa. Na Segurança da Informação, existem três categorias gerais de política:

- **Política de segurança da informação corporativa** – desenvolvida dentro do contexto do plano estratégico de TI, define as diretrizes para o setor de Segurança da Informação e sua atuação em toda a organização;
 - **Políticas de segurança específicas para questões** – esses são conjuntos de regras, que definem o que é comportamento aceitável dentro de uma tecnologia específica, exemplo: política de uso de senhas ou uso da INTERNET;
 - **Políticas específicas do sistema** – de natureza técnica e/ou gerencial, elas controlam a configuração e/ou utilização de um equipamento ou tecnologia.
- **PROGRAMAS** – programas são definidos como operações de Segurança da Informação gerenciadas separadamente. Um exemplo seria um programa de treinamento e conscientização de educação de segurança da informação. Outros programas que podem surgir incluem uma segurança física da organização, tais como o programa de proteção contra incêndio, acesso físico, portões, guardas e assim por diante. Os programas de segurança estão associados ao planejamento e às políticas de segurança da informação.
- **PROJETOS** – os programas de segurança são implementados através de projetos. Projeto é uma maneira de gerenciar o processo de desenvolvimento dos programas. O projeto possui um objetivo que pode ser decomposto em metas, que são desdobradas em atividades. Além disso, no projeto, são especificados os recursos humanos, materiais e financeiros para a sua realização. A gestão do projeto envolve: identificar e controlar os recursos aplicados ao projeto, bem como medir o progresso das atividades e ajustar o processo conforme o progresso é feito em direção à meta.

2. 3. Papéis e Responsabilidades

Conforme O'HANLEY; TILLER (2014), a alta administração tem a responsabilidade final pela proteção dos ativos de informação da organização. Uma das responsabilidades é o estabelecimento da função de Corporate Information Security Officer (CISO) ou Chefe de Segurança da Informação Corporativo. O CISO dirige o gerenciamento diário na organização dos ativos de informação. O administrador de segurança deve se reportar diretamente ao CIO (Chief Information Officer), que é responsável pela administração diária do programa de segurança da informação.

As funções de apoio são desempenhadas pelos prestadores de serviços e incluem operações de Sistemas, cujo pessoal projeta e opera os sistemas de computador. Eles são responsáveis por implantar a segurança técnica nos sistemas. A área de telemática é responsável por fornecer serviços de comunicação, incluindo voz, dados, vídeo e wireless.

Outros grupos de apoio incluem a equipe de Segurança Física e o grupo de Planejamento de Contingência. Esses grupos são responsáveis por estabelecer e implantar controles, podendo formar um grupo de pares para revisar e discutir os controles.

O grupo responsável pela metodologia de desenvolvimento de aplicativos auxiliará na implantação dos requisitos de segurança da informação no ciclo de vida de desenvolvimento do sistema aplicativo. A garantia de qualidade pode ajudar a assegurar que os requisitos de segurança da informação sejam incluídos em todos os projetos de desenvolvimento antes de prosseguir para a produção.

O Grupo de Aquisições pode trabalhar para obter a linguagem das políticas de segurança da informação, incluídas nos acordos de compra para pessoal contratado. Educação e Treinamento podem ajudar no desenvolvimento e condução de programas de conscientização de segurança da informação como também ajudar os supervisores de treinamento na responsabilidade de monitorar as atividades dos funcionários. Recursos Humanos será a organização responsável por tomar as medidas adequadas para quaisquer violações da política de segurança da informação da organização.

2. 3. 1. Comitê de Segurança da Informação

O comitê de segurança da informação, às vezes chamado de comitê diretor de segurança, normalmente é composto por membros do alto escalão da administração e tem uma responsabilidade direta pela segurança. Em tal comissão, consultas poderão ser solicitadas ao CISO e ao nível de gestão abaixo dele, bem como representantes de outras equipes orientadas para a segurança, como TI, compliance, auditoria, risco, assessoria jurídica, privacidade, DPO e segurança física.

O comitê de segurança da informação normalmente analisa as métricas derivadas da operação diária do programa de segurança, discute e delibera sobre orçamento de tecnologia, aprova políticas e outras orientações semelhantes da gestão de segurança da informação. Ele também pode servir como uma fonte de ajuda na resolução de problemas e tomadas de decisão que precisam ser levadas a um nível superior de gestão.

2. 3. 2. DPO (Data Protection Officer) – LGPD

O Data Protection Officer (Encarregado de Proteção de Dados) é o profissional responsável por garantir a proteção dos dados pessoais durante as etapas do ciclo de tratamento de dados pessoais (coleta, retenção, processamento, compartilhamento e eliminação), realizadas por uma empresa ou instituição. O DPO se relaciona com a autoridade supervisora, que realiza a fiscalização da LGPD (Lei Geral de Proteção de Dados), que, no Brasil, é a Autoridade Nacional de Proteção de Dados – ANPD. Essa profissão surgiu a partir da LGPD, que obriga as empresas a protegerem esses dados e a designação de um profissional especializado que atue nesse sentido.

2. 4. Estratégia de segurança da informação

Consiste na elaboração de Planos Estratégicos de Segurança da Informação. Os planos estratégicos deverão estar alinhados com os objetivos estratégicos de negócios e TI. Esses planos têm um prazo mais longo (horizonte de 3 a 5 anos ou mais) para orientar uma visão de longo prazo das atividades de segurança.

O processo de desenvolver um plano estratégico enfatiza o pensamento sobre o ambiente da empresa e os aspectos técnicos futuros desse ambiente. Metas de alto nível são estabelecidas para fornecer uma visão para projetos, facilitando o atingimento dos objetivos de negócios. Os planos estratégicos devem ser revisados pelo menos uma vez por ano, ou sempre que ocorrerem grandes mudanças no negócio, como fusão, aquisição, estabelecimento de relacionamentos de terceirização, mudanças importantes no clima de negócios, introdução de novos concorrentes e assim por diante.

As mudanças tecnológicas serão frequentes durante um período de 5 anos, então o plano deve ser ajustado regularmente. Um plano de alto nível fornece orientação organizacional para garantir que as decisões de nível inferior sejam consistentes com as intenções da gestão executiva para o futuro da empresa. Por exemplo, objetivos estratégicos podem consistir em:

Estabelecimento de políticas e procedimentos de segurança

- Implantação de servidores, estações de trabalho e dispositivos de rede com eficácia para reduzir o tempo de inatividade;
- Certificação de que todos os usuários entendam as responsabilidades de segurança e recompensem o desempenho excelente;
- Estabelecimento de uma organização de segurança para gerenciar a segurança em toda a entidade;
- Certificação de que os riscos sejam efetivamente compreendidos e controlados.

2. 4. 1. Planos táticos

Os planos táticos descrevem iniciativas amplas para apoiar e atingir as metas especificadas no plano estratégico.

2. 4. 2. Planos operacionais/projetos

Planos específicos com marcos, datas e responsabilidades fornecem a comunicação e direção para garantir que os projetos individuais estejam sendo concluídos. Por exemplo, estabelecer uma política de desenvolvimento e processo de comunicação pode envolver vários projetos com muitas tarefas:

- Realizar avaliação de risco de segurança;
- Desenvolver políticas de segurança e processos de aprovação;
- Desenvolver infraestrutura técnica para implantar políticas e controlar a conformidade;
- Treinar os usuários finais nas políticas;
- Monitorar a conformidade.

2. 5. Frameworks para governança de segurança da informação

Os frameworks são modelos usados para organizar e facilitar o processo de governança de segurança da informação. São baseados em boas práticas de gestão unidas por uma linha de racionalidade dos conceitos a serem aplicados. A figura 2-1 ilustra o modelo genérico de Estratégia de Governança de Segurança da Informação, exibindo os principais elementos que compõem a organização e os fatores que devem ser considerados para uma implantação exitosa da governança. Veremos alguns desses frameworks.

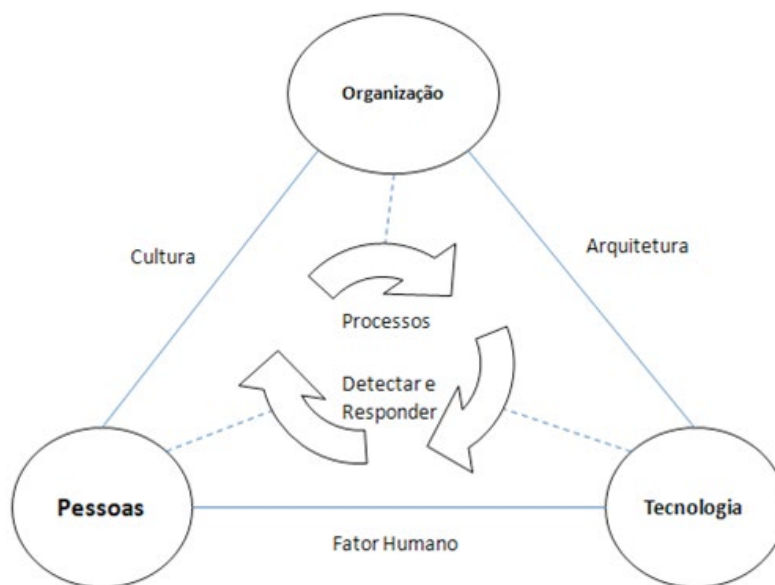


Figura 2-1. Modelo de Estratégia da Governança de Segurança da Informação

Fonte: Adaptada de O'HANLEY; TILLER, 2014.

2. 5. 1. Frameworks ITGI

É um padrão ou modelo de governança da segurança da informação desenvolvido pelo IT Governance Institute (ITGI). Conforme NETO (2011), para o ITGI, a governança da informação é parte integral da governança corporativa, e as duas deverão estar alinhadas. A governança da segurança da informação consiste em um conjunto que faz a proteção da informação, sendo composto de:

- Liderança;
- Estruturas organizacionais;
- Processos.

Nesse modelo, espera-se como resultados:

- Alinhamento estratégico da segurança da informação com o negócio da organização;
- Uma boa gestão de riscos;
- Eficiência e eficácia no uso de recursos de TI com segurança;
- Uso de métricas para a aferição do desempenho e o monitoramento, visando à garantia dos objetivos alcançados;
- Otimização dos investimentos em segurança da informação.
- Com a adoção desse modelo, esperam-se os seguintes benefícios:

- Aumento na previsibilidade proporcionada pela gestão de riscos em operações do dia a dia organizacional;
- Risco minimizado de ações judiciais decorrentes da segurança no tratamento dos dados;
- Violações de privacidade diminuídas;
- Reputação da organização preservada;
- Aumento no grau de confiança entre parceiros de negócios e clientes;
- Com resultados previsíveis e diminuição dos fatores de risco, decorrerá a redução dos custos;
- Decisões críticas mais seguras;
- Minimização de tempo e esforço em operações de incidentes de segurança;
- Integração de esforços;
- Efetividade e garantia do uso da política de segurança corporativa e seu cumprimento;
- Otimização dos recursos de segurança com o uso do framework e sua estrutura.

2. 5. 2. Framework do NIST

Esse modelo foi proposto pelo NIST, National Institute of Standards and Technology, por meio da publicação NIST 800-100, denominada Information Security Handbook: a Guide for Managers (NIST, 2006).

O conceito de governança da segurança da informação do NIST permite o alinhamento entre as estratégias de segurança da informação e os objetivos do negócio por meio de um framework, que, com suas estruturas e processos gerenciais, garante esse alinhamento.

Abaixo estão elencados os componentes da Governança da Segurança da Informação, estabelecidos pelo framework do NIST, que definem de que forma se dará o estabelecimento e a execução da governança na organização específica.

Planos Estratégicos da Organização – planos que orientam todas as ações de governança da empresa para os três componentes básicos:

- **Estrutura organizacional** – que pode ser centralizada ou descentralizada;
- **Papéis e responsabilidades** – em que são definidos os papéis e responsabilidades das principais partes interessadas; e
- **Arquitetura corporativa** – que consiste em quatro modelos: negócio, dados, aplicação e tecnologia.

No framework, encontram-se os normativos representados pelas políticas e guias, que consistem no agregado de regras e práticas, as quais orientam como a organização gerencia, protege e distribui informação. A próxima etapa é a implantação.

2. 5. 3. Framework do COBIT

COBIT significa “Objetivos de Controle de Informação e Tecnologia Relacionada”. É um conjunto de práticas fundamentais para garantir a governança de Tecnologia da Informação e, portanto, melhorar a gestão. Fornece indicações sobre a implantação de controles para Segurança da Informação. Essa metodologia pode ser usada não apenas como uma ferramenta de planejamento para Segurança da Informação, mas também como uma maneira de fornecer muito mais segurança e apoio à tomada de decisões, facilitando a comunicação e melhorando os resultados. O COBIT foi criado pela ISACA (Associação de Auditoria e Controle de Sistemas de Informação) para a Governança de TI. Esse framework foi publicado em sua primeira versão no início dos anos 1990, sendo atualizado, normalmente, a cada 3 anos. Sua versão atual é a 5, liberada em 2012.

O CobiT foi elaborado, visando aos seguintes requisitos de negócio:

- Efetividade;
- Eficiência;
- Confidencialidade;
- Integridade;
- Disponibilidade;
- Conformidade; e
- Confiabilidade.

Essa forma de visão foi criada para conduzir o alcance dos objetivos de controle da TI. O CobiT descreve as seguintes áreas de foco para a implementação da governança de TI:

- O alinhamento estratégico com foco em assegurar a estreita relação do negócio com os planos de TI;
- Que a cada ciclo de entrega seja assegurada que a TI apresente os benefícios prometidos, conforme a estratégia com otimização dos custos;
- Otimizar os investimentos e o próprio gerenciamento dos recursos críticos da TI: aplicações, informação, infraestrutura e pessoas;
- O gerenciamento de riscos com definição de responsabilidades de gerenciamento de risco na organização; e
- Monitorar e acompanhar o desempenho na implementação da estratégia, o encerramento dos projetos, a utilização dos recursos, o desempenho dos processos e a entrega de serviços.

Capítulo 3 – Gerenciamento de Risco

De acordo com BIDGOLI (2006), os riscos devem ser gerenciados, e a gestão de riscos deve fazer parte das práticas gerais de gestão de qualquer organização madura. São identificadas as seguintes atividades primárias para o gerenciamento de riscos:

- IDENTIFICAR – os riscos devem ser identificados antes de serem gerenciados;
- ANALISAR – os riscos devem ser analisados para que a administração possa tomar decisões prudentes sobre eles;
- PLANEJAR – para obter informações sobre um risco a ser transformado em ação, um plano detalhado, delineando as ações presentes e futuras, deve ser criado. Essas ações podem mitigar o risco, evitar o risco ou até mesmo aceitar o risco;
- MONITORAR – os riscos, independentemente de terem ocorrido ou não, devem ser rastreados, para que a gestão possa continuar a exercer diligência;
- CONTROLAR – mesmo que um risco tenha sido identificado e tratado, ele deve ser continuamente controlado para monitorar quaisquer desvios.

A atividade principal que une todas essas atividades é a avaliação de risco, sendo considerada central para o processo de gerenciamento de risco e subjacente a todas as outras atividades. A atividade de gerenciamento de risco tem duas subatividades principais, registradas a seguir.

- Avaliação de risco – é dividida em:
 - Identificação de risco;
 - Análise de risco; e
 - Priorização de risco.
- Controle de risco – é dividido em:
 - Identificação de risco;
 - Análise de risco; e
 - Priorização de risco.

3. 1. Conceitos de risco

Para compreender o conceito de “Risco”, serão analisadas algumas definições:

- Na ISO 31000, Risco é definido como sendo o “efeito da incerteza nos objetivos”;
- Nível de Risco é a “magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades”. Um sinônimo de consequência é impacto;
- Risco é a probabilidade de um evento acontecer, seja ele uma ameaça, quando negativo, ou oportunidade, quando positivo. É o resultado obtido pela efetividade do perigo.
- Um risco, do ponto de vista da segurança, é a probabilidade de que alguma ameaça explore, com êxito, uma vulnerabilidade em um sistema, junto com a magnitude dessa perda (impacto). Quanto maior a probabilidade de sucesso de uma ameaça, maior é a magnitude da perda potencial, e, portanto, maior o risco para a organização.
- Uma ameaça, então, é um estímulo para um risco; é qualquer perigo para o sistema, um evento indesejável. Um agente de ameaça ou fonte de ameaça é uma pessoa, que inicia ou instiga uma ameaça. Normalmente, uma ameaça tira proveito de alguma vulnerabilidade do sistema, uma condição na qual o sistema está ausente ou aplicando uma proteção ou controle de maneira inadequada. A vulnerabilidade, portanto, aumenta a probabilidade da ameaça ou seu impacto, ou possivelmente ambos. É importante observar que o sistema inclui pessoas, não apenas hardware, software e redes.
- O efeito resultante de uma vulnerabilidade, sendo explorada por um agente de ameaça, é a exposição dos ativos da organização a uma perda potencial. Essa perda pode ser na forma de destruição, divulgação de informações, corrupção das informações da organização (perda de integridade) ou negação de serviço.
- Na linguagem de risco, é necessário considerar a magnitude de todas as exposições a risco, às quais uma organização é suscetível. Isso leva à fórmula básica de risco, que tenta quantificar o risco em termos de exposição ao risco (ER):
- $ER = \text{probabilidade (perda)} * \text{magnitude (perda)}$
- Essa fórmula é frequentemente escrita como segue
- $ER = P(L) * S(L)$

- Onde:

- ER – Exposição ao risco
- P – Probabilidade
- S – Magnitude
- L – Perda

Por exemplo, se a organização calcula a probabilidade de um servidor principal ficar inativo por 2 horas como 10%, devido a ataques de negação de serviço e perda devido a esse tempo de inatividade é de R\$ 20.000,00 (magnitude), então a exposição ao risco enfrentada por devido a essa perda é R\$ 2.000,00.

Os riscos podem ser calculados e analisados de duas formas metodológicas: qualitativa e quantitativa.

A abordagem qualitativa utiliza cálculos mais simples, porém com resultados subjetivos, enquanto a abordagem quantitativa apresenta resultados em valores objetivos, como visto acima.

Existem diversos métodos para o cálculo do risco (HOFF DO AMARAL; AMARAL; NUNES, 2010), entre eles, temos:

- Método ISRAM (Information Security Risk Analysis Method) – método de análise de riscos, utilizado para avaliar risco causado por problemas de segurança da informação;
- Método AURUM (Automated Risk and Utility Management) – é uma ferramenta utilizada para automatizar a gestão de riscos e apoiar os gestores na escolha das medidas de segurança, de acordo com requisitos técnicos e econômicos;
- Método ARIMA (Austrian Risk Management Approach) – foi desenvolvido de acordo com os processos da norma ISO/IEC 27005 e com o objetivo de satisfazer os requisitos de gestão de riscos das autoridades públicas austríacas;
- Método FMEA (Failure Mode and Effect Analysis) – é uma técnica utilizada para definir, identificar e eliminar falhas conhecidas ou potenciais de sistemas, projetos, processos e/ou serviços, antes que atinjam o cliente.

3. 2. Atividades da Gestão de Risco de Segurança

Esse tópico descreve as atividades da Gestão de Risco de Segurança da Informação.

3. 2. 1. Avaliação de risco de segurança

Por definição, Segurança da Informação envolve a proteção da confidencialidade, integridade e disponibilidade de dados/informações essenciais para o sucesso de uma empresa ou organização. E naturalmente também acata proteção das pessoas envolvidas no tratamento dessas informações. A seguir, estão exemplos de consequências que podem resultar da materialização de riscos nas áreas de confidencialidade, integridade e disponibilidade:

- Perda de confidencialidade:
 - Constrangimento pessoal resultante de roubo e publicação de dados pessoais, financeiros, de saúde ou outros e possível processo e multa para indivíduos e a organização responsável por manter a confidencialidade;
 - Perda corporativa de ganhos resultante do roubo de dados técnicos antes de serem patenteados;
 - Perda de vida de um agente da Polícia Militar de São Paulo, resultante de roubo e revelação de seus dados pessoais para facções do tipo PCC.
- Perda de integridade
 - Constrangimento pessoal e possivelmente multa e prisão, resultante da inserção no banco de dados de dados financeiros falsos, implicando o sujeito em fraude ou apropriação indébita.
 - Perda da capacidade dos auditores corporativos de detectar desfalque e a consequente perda de fundos, resultante da corrupção deliberada de dados financeiros pelo desfalque.
 - Perda de vidas resultantes de alterações no banco de dados, indicando que um sujeito é um agente secreto quando ele ou ela não é.
- Perda de disponibilidade
 - Constrangimento pessoal causado pela incapacidade de cumprir compromissos, resultante da incapacidade temporária de usar a agenda eletrônica.
 - Incapacidade temporária de a empresa emitir cheques de pagamento semanais

aos funcionários, gerando insatisfação e perda de produtividade, resultante da indisponibilidade temporária de dados de horas trabalhadas.

Os termos ameaça, fonte de ameaça, vulnerabilidade, impacto e exposição ao risco são comumente usados no campo da avaliação de risco de segurança de TI.

Cenário 1 - Imagine um cenário em que um funcionário terá que ir ao trabalho em um dia de forte chuva no Recife. Ele tem a opção de usar seu carro ou utilizar um transporte público, exemplo: o metrô. Como em dia de chuva, Recife apresenta muitos alagamentos, o uso do carro parece-lhe complicado.

Em relação aos conceitos, temos os seguintes:

- A ameaça, ou fonte de ameaça, é o início de chuva, em nível suficientemente forte, durante uma parte exposta da ida ao trabalho;
- A vulnerabilidade é o fato de que a pessoa envolvida ficará encharcada, se a ameaça se materializar e a pessoa não tiver forma de abrigo (por exemplo, um guarda-chuva);
- O impacto é o dano, medido em termos de desconforto e possivelmente perda de produtividade ou mesmo de saúde, que ocorrerá, se a ameaça se materializar;
- A exposição ao risco é uma avaliação, em uma escala numérica, talvez monetária, ou em escala ordinal (por exemplo, baixa, média ou alta), da magnitude esperada da perda, dada a ameaça, a vulnerabilidade a ela e seu impacto, caso a ameaça se materialize.

3. 2. 2. Identificação do risco

A primeira etapa na avaliação de risco é a identificação de risco:

- A identificação de ameaças potenciais, vulnerabilidades a essas ameaças e impactos que resultariam, caso se materializassem;
- Todos apresentados para o cenário em discussão.

No cenário 1, existe a preocupação com fatores intangíveis, como a ameaça da chuva, a vulnerabilidade de ficar encharcado e o impacto do desconforto, bem como com itens tangíveis, como o guarda-chuva.

No campo da segurança da informação, a preocupação é com os sistemas que armazenam, processam e transmitem dados/informações. Os sistemas de informação às vezes são sediados em um único local e às vezes amplamente distribuídos; eles envolvem

hardware e software de computador, bem como outros ativos físicos e humanos. Os tangíveis incluem os vários tipos de equipamento e mídia e os locais em que eles e a equipe estão hospedados. Os intangíveis incluem noções como reputação organizacional, oportunidade ou perda desta, produtividade ou perda desta, e assim por diante.

As fontes de ameaça são de, pelo menos, três variedades: natural, humana e ambiental.

- Natural – tempestades elétricas, monções, furacões, tornados, inundações, avalanches, erupções vulcânicas, terremotos etc.;
- Humana – entrada de dados incorreta (não intencional), esquecimento de trancar a porta (não intencional), falha em destrancar a porta para permitir que o funcionário entre depois do expediente (intencional), ataque de negação de serviço (intencional), criação e propagação de vírus (intencional);
- Ambientais – falha de telhado ou parede causada pelo uso de materiais de construção ruins, infiltração de produtos químicos tóxicos através do teto, queda de energia etc.

As vulnerabilidades têm várias fontes, incluindo falhas técnicas etc. Existe uma extensa taxonomia de ameaças e vulnerabilidades publicadas por diversos pesquisadores e organizações. As ameaças (ou causas) estão sempre ligadas aos mecanismos de ataques usados. Os mecanismos de ataque estão relacionados aos mecanismos de defesa ou de mitigação, que podem ser eficazes em algumas circunstâncias.

3. 2. 3. Análise de risco

A segunda etapa na avaliação de risco é a análise de risco, em que se realiza a estimativa e o cálculo das probabilidades de risco, magnitudes, impactos e dependências.

Essa análise é fácil no caso de impactos monetários decorrentes da relação: vulnerabilidade versus ameaça. Para esses casos, a probabilidade de materialização pode ser razoavelmente calculada, mas é consideravelmente mais difícil na maioria de outros casos. Deve-se tomar cuidado especial ao atribuir probabilidades, pois a qualidade de toda a avaliação de risco depende fortemente da precisão e do realismo das probabilidades atribuídas.

3. 2. 4. Priorização de risco

É a etapa final na avaliação de risco em que é realizada a priorização de risco; isto é, priorização de todos os riscos com respeito às exposições relativas da organização a eles. Normalmente é necessário usar técnicas que possibilitem a comparação de riscos, como o cálculo da exposição ao risco em termos de perda potencial.

No cenário 1, outros riscos, além dos discutidos aqui, podem incluir aqueles associados a não afivelar o cinto de segurança durante a ida, se for usar carro próprio, o risco de um acidente durante o percurso, o risco de perder o ônibus/metrô e assim por diante.

Uma pessoa meticulosa, que sempre sai de casa mais cedo do que o necessário e que está muito consciente de tomar precauções de segurança, provavelmente classificará esses novos riscos como tendo exposições muito menores que o risco de chuva – uma pessoa menos meticulosa poderia fazer o contrário.

Em uma versão altamente simplificada de uma situação de negócios, três ameaças poderiam ser: terremoto, atraso na entrega de matérias-primas e peculato.

Uma organização localizada em Recife provavelmente atribuiria menor prioridade a terremoto que uma em Caruaru; uma organização com fornecedores que nunca se atrasaram provavelmente atribuiria uma prioridade menor à entrega atrasada que uma organização a qual usa um fornecedor pela primeira vez. Como pode haver ameaças ou vulnerabilidades que não tenham sido incluídas na análise, é conveniente aproveitar as experiências de outras pessoas para ajudar a construir uma biblioteca de ameaças e vulnerabilidades.

3. 2. 5. Controle de Risco de Segurança de TI

O objetivo da fase de controle de risco do processo de gestão de risco é a preocupação com as proteções, também conhecidas como controles de risco. As proteções ou controles de riscos se enquadram em, pelo menos, três categorias: técnicas, gerenciais e operacionais.

Exemplos de categorias de Controles de Riscos:

- Técnica – autenticação (prevenção), autorização (prevenção), controle de acesso (prevenção), detecção de intrusão (detecção), auditoria (detecção), backup automático (recuperação) etc.
- Gerencial – alocar guardas a locais críticos (prevenção), instituir procedimentos de iniciação e encerramento de conta de usuário (prevenção), política de acesso a dados necessários (prevenção), política de reavaliação de risco periódica (prevenção), treinamento de segurança em toda a organização (prevenção e detecção) etc.
- Operacional – proteger o hardware de rede contra o acesso de qualquer um, exceto administradores de rede autorizados e/ou pessoal de serviço (prevenção); rastrear pessoas de fora antes de permitir a entrada (prevenção); configurar e monitorar alarmes de movimento, sensores e circuito fechado de TV (detecção de ameaça física);

configurar e monitorar detectores de fumaça, detectores de gás, alarmes de incêndio (detecção de ameaças ambientais).

No cenário 1, a proteção que é considerada tem um componente técnico de tecnologia bastante baixa, ou seja, o guarda-chuva, e um componente operacional, isto é, carregar o guarda-chuva. Uma alternativa de proteção operacional e gerencial seria trabalhar em casa toda a manhã, se for possível, e ir ao escritório somente depois que a chuva ou a ameaça de chuva passar.

Durante a fase de controle de risco do processo de gestão de risco, as seguintes atividades são realizadas:

- Considerar proteções individuais alternativas e/ou proteções complexas que podem ser usadas para eliminar/reduzir/mitigar exposições às várias ameaças identificadas, analisadas e priorizadas (planejamento de gestão de risco);
- Realizar a análise de custo-benefício necessária para decidir quais proteções específicas empregar e instituir as mais relevantes (resolução de risco);
- Instituir um processo de monitoramento contínuo da situação de segurança de TI para detectar e resolver problemas, à medida que surgem, e decidir onde e quando é necessário atualizar ou alterar o sistema de proteções (monitoramento de risco).

3. 2. 6. Resolução do risco

Em organizações empresariais e governamentais, pode haver muitas proteções alternativas possíveis, incluindo:

- Soluções de hardware e/ou software de diferentes fornecedores para uma determinada ameaça ou grupo de ameaças;
- Gerenciamento alternativo ou proteções processuais e combinações alternativas de proteções técnicas, de gerenciamento e procedimentais.

Para complicar as coisas, existe a probabilidade de que diferentes combinações de proteções tratem de grupos de ameaças diferentes e sobrepostos.

A resolução de risco começa com a análise de custo-benefício das várias proteções e possíveis controles a serem empregados na redução, em um nível aceitável, das exposições a risco avaliadas, resultantes das várias ameaças identificadas, vulnerabilidades e impactos concomitantes.

Assim como são consideradas as ameaças, vulnerabilidades e impactos durante a avaliação de riscos, devem-se considerar as proteções, seus custos e sua eficácia durante a resolução de riscos.

No cenário 1, o custo nominal do componente técnico da proteção, guarda-chuva, é provavelmente nulo, pois a maioria das pessoas já possui ao menos um guarda-chuva; o custo operacional é o desconforto de carregar uma bolsa mais pesada. Mesmo nesse exemplo simples, a eficácia da proteção deve ser considerada. Por exemplo, se o vento for muito forte, o guarda-chuva não reduzirá a exposição de forma eficaz.

3. 3. Padrões e normas

Dada a grande variedade de modelos (frameworks) de gestão de risco disponíveis, na maioria dos casos, será aconselhável usar uma das seleções existentes. Entre os comumente usados, estão NIST, ISO e, em certos casos, o padrão federal americano de processamento de informações (FIPS). Muitas organizações acabarão usando um ou mais deles como base, quando apropriado.

3. 3. 1. National Institute for Science and Technology - NIST

A publicação especial do NIST fornece orientação para muitas áreas de computação e tecnologia, incluindo gerenciamento de risco. As duas principais publicações nesta área são: SP 800-37 - “Guia para aplicar o framework de gerenciamento de risco para sistemas de informação federais” e SP 800-53 “Controles de segurança e privacidade para sistemas de informação federais e Organizações”.

SP 800-37 - apresenta a estrutura de gerenciamento de risco, com as seis etapas que são a base para muitos programas de gestão de risco:

- **Categorizar** o sistema com base nas informações que apresentam riscos e o impacto de expor ou perder esses dados;
- **Selecionar** os controles com base na categorização e quaisquer circunstâncias atenuantes;
- **Implementar** os controles e documentar a implementação;
- **Avaliar** os controles para garantir que eles sejam implementados corretamente e com o desempenho esperado;
- **Autorizar** o uso do sistema com base no risco e nos controles implementados para mitigá-lo;

- **Monitorar** os controles para garantir que eles continuem a mitigar o risco de forma adequada.

SP 800-53 – serve para fornecer informações de controle para aqueles que estão selecionando controles, usando SP 800-37 como base.

3.3.2. International Organization for Standardization – ISO

A ISO é um órgão criado pela primeira vez em 1926 para definir padrões entre as nações. Entre os mais de 21.000 padrões criados, estão aqueles que cobrem quase todas as indústrias, de tecnologia a segurança alimentar, agricultura e saúde.

No caso da gestão de risco, a norma 31000:2009 – “Gestão de Risco – Princípios e Diretrizes” – é o padrão ISO que rege essa área.

Esse padrão fornece princípios, estrutura e um processo de gestão de risco. Embora os documentos NIST e FIPS sejam voltados principalmente para sistemas de informação federais americanos, o padrão ISO se destina ao público mais amplo possível. Além disso, o Guia ISO 73:2009 “Gestão de riscos – Vocabulário” funciona bem com a ISO 31000, fornecendo um vocabulário padronizado para tais esforços, e ISO 31010:2009 – “Gestão de risco – Técnicas de avaliação de risco” concentra os padrões de processo de avaliação de risco.

3.3.3. Federal Information Processing Standard – FIPS

Uma das diretivas do NIST, determinada pela Lei Federal de Gerenciamento de Segurança da Informação (FISMA), diz respeito ao desenvolvimento de diretrizes de implementação para sistemas de informação federais.

Nessa esfera federal de governo dos EUA, algumas das publicações do NIST têm o poder de mandatos federais. As publicações FIPS cobrem uma ampla área, mas duas em particular, FIPS 199 e FIPS 200, são os padrões obrigatórios e estão relacionados à gestão de riscos (framework).

FIPS 199 – “Padrões para categorização de segurança de informações federais e Sistemas de Informação” – define as categorias de sistemas de informação a serem usados pelo governo federal. Os requisitos de categorização sob FIPS 199 incluem a classificação de cada sistema, de acordo com a tríade – confidencialidade, integridade e disponibilidade (CID).

FIPS 200 – “Requisitos mínimos de segurança para informações federais e Sistemas de Informação” – define os padrões mínimos de segurança dos sistemas federais. Essencialmente, requer que o FIPS 199 seja usado para categorizar o sistema; em seguida, controles a serem

implementados para protegê-lo de forma adequada, usando NIST Publicação Especial 800-53 – “Controles de segurança e privacidade para informações federais Sistemas e Organizações” como base.

3. 4. Plano de Gerenciamento de Risco

Todo sistema de TI em operação apresenta algum grau de risco de segurança (BIDGOLI, 2006). Os riscos de segurança são situações ou eventos possíveis que podem causar danos a um sistema e causar algum tipo de perda. Os riscos de segurança variam em impacto de trivial a fatal e com probabilidade de certo a improvável. Daí, a necessidade da construção de Plano de Gerenciamento de Risco.

Conforme BIDGOLI (2006), para compor um Plano de Gerenciamento de Riscos, devem ser discutidos não somente aqueles riscos que são identificados como também os casos de riscos não identificados. Riscos que não são identificados ou têm impactos desconhecidos, às vezes, são rotulados vagamente como riscos devido à incerteza. No caso da segurança do sistema de TI, as considerações de risco geralmente devem se concentrar na incerteza, porque, por projeto, os riscos conhecidos e identificados são tratados ou aceitos como estando dentro de um nível “tolerável”.

O plano de gerenciamento de risco deve abordar modelos de perfil de risco, porque os riscos geralmente não são estáticos. As probabilidades e os impactos mudam com vários fatores, a exemplo: tempo, custo, estado do sistema e assim por diante. Como consequência, muitas vezes, é desejável considerar os riscos com relação a um conjunto planejado de eventos, como esforço de avaliação, tempo de operação do sistema, investimento em desenvolvimento e assim por diante. Os modelos de risco estratégico representam riscos que mudam dinamicamente em relação às atividades planejadas e podem ser usados para promover o gerenciamento de risco eficaz.

O objetivo da modelagem de risco é auxiliar na tomada de decisão de gerenciamento de risco. A gestão do risco não resulta necessariamente na remoção do risco; isso nem sempre é possível ou mesmo economicamente viável. Para qualquer risco, geralmente há apenas um grau limitado em que esse risco pode ser controlado ou mitigado (ou seja, a perda esperada reduzida).

Conforme indicado anteriormente, alguns riscos devido à incerteza não podem ser mitigados ou mesmo avaliados. A avaliação é o principal ponto de partida, pois permite obter ideias sobre os seguintes fatores:

- Quais são os riscos e onde há risco devido à incerteza;
- Diferenciação entre riscos de desenvolvimento e riscos de operação;
- Diferenciação entre riscos evitáveis e inevitáveis;
- Diferenciação entre riscos controláveis e incontroláveis;
- Custo e benefícios da mitigação, prevenção e controle de riscos.

A avaliação permitirá a escolha de uma estratégia de mitigação e controle do risco. No entanto, não é óbvio desde o início que qualquer estratégia de avaliação será eficaz, ou mesmo viável. Na verdade, uma estratégia mal escolhida pode aumentar o risco geral.

3. 5. Plano de Continuidade de negócios

No tópico anterior, foi apresentada a possibilidade de acontecimentos ou eventos que podem afetar direta ou indiretamente os negócios de uma organização. Essa possibilidade e o impacto que ela ocasiona chamou-se de risco.

Os desastres afetaram empresas de todas as formas por centenas de anos. No entanto, com o advento da comunicação de alta velocidade, dos computadores, dos dados digitalizados e da dependência cada vez maior de bancos de dados e armazenamento eletrônico de informações, as empresas têm muito mais a perder do que a infraestrutura física, em caso de desastre.

Antigamente, os planos de Continuidade de negócios e Recuperação de Desastres eram da responsabilidade dos departamentos de TI, embora alguns itens das missões críticas são certamente relacionados a TI; as funções de TI devem ser integradas ao plano geral.

De acordo com GUPTA; SHARMA (2009), deve-se aderir a uma abordagem em três etapas para preparar os planos de Continuidade de Negócios e Recuperação de Desastres. São as seguintes etapas:

- ETAPA DE RESOLUÇÃO, que envolve:
 - A avaliação dos riscos;
 - Quem deve estar envolvido;
 - Quais unidades de negócios são as mais críticas; e
 - Quais medidas podem ser tomadas para minimizar o risco.
- ETAPA DE RESPOSTA, que inclui:

- A formação da equipe de resposta a desastres;
 - Como as informações serão disseminadas aos funcionários;
 - Como os clientes e fornecedores serão notificados; e
 - Onde o pessoal irá operar e com que equipamento.
- ETAPA DE RECONSTRUÇÃO, que inclui:
 - A decisão de qual pessoal estará diretamente envolvida na avaliação de danos e reconstrução;
 - Ajustes das operações de negócios enquanto a reconstrução está em andamento; e
 - A manutenção das operações para que o negócio possa prosseguir.

3. 5. 1. Tipos de desastres – parâmetros

Existem vários parâmetros que podem ajudar a definir um desastre do ponto de vista de um impacto no negócio.

O primeiro parâmetro é a escala ou extensão geográfica. Um desastre no local é aquele que afeta apenas as operações de uma empresa em um determinado local.

O segundo parâmetro é o tipo de desastre, causado pelo homem ou natural. Exemplo: Terremotos, inundações, furacões, tornados etc.

O terceiro parâmetro é a duração do evento inicial, que constitui o desastre. Normalmente, isso é medido em minutos ou horas, mas certos incidentes, como inundações ou tempestades de neve, podem durar vários dias ou até semanas.

O parâmetro final é se ocorre algum aviso e a duração do aviso antes do desastre. A maioria dos desastres tem pouco ou nenhum aviso, embora possa haver sinais iminentes úteis, particularmente com desastres naturais, que são relacionados à probabilidade.

3. 5. 2. Consequências de desastres para negócios

Na primeira análise, os parâmetros do desastre deverão ser considerados para se definir o impacto que terá em um determinado negócio. No entanto, mais importante, é o grau em que funções críticas de uma empresa são afetadas.

O planejamento de Recuperação de Desastres também deve investigar como o desastre é gerenciado, tanto de um ponto de vista externo, como um cliente, e internamente, como é percebido pelos funcionários afetados.

Desastres mal gerenciados passam uma mensagem que pode afetar negativamente a gestão e a percepção de como os desastres são controlados.

3. 5. 3. Metodologias de recuperação

Várias metodologias são usadas em conjunto para desenvolver um plano de Continuidade de negócios e Recuperação de Desastres. Isso inclui modelagem de negócios, análise de impacto nos negócios (BIA), análise de risco e desenvolvimento de estratégia de mitigação.

3. 5. 4. Modelagem de negócios

O objetivo da modelagem de negócios é explicitar as relações entre pessoas, processos, hardware e aplicativos de software. Quanto maior e mais sofisticado o negócio, maior será a necessidade de software para orientar a equipe de planos de Continuidade de Negócios e Recuperação de Desastres.

Muitos planejadores de continuidade de negócios usam planilhas, bancos de dados e ferramentas de diagramação, para acumular, visualizar e armazenar as informações do modelo de negócios. Em qualquer caso, o uso de software pode tornar os esforços mais focados e abrangentes.

O LDPRS (Living Disaster Recovery Planning System) é um exemplo de software usado para modelar um mapa de dependência, permitindo aos usuários uma avaliação do que aconteceria com outros sistemas, se um único processo for interrompido.

Para governança, visando preencher a lacuna entre os requisitos de controle, questões técnicas e riscos de negócios, o COBIT (controlit.org) é uma possibilidade. Para planejamento de contingência de TI, ambos COSO (coso.org) e ITIL (itil-toolkit.com) contêm documentos úteis.

A saída da modelagem de negócios pode alimentar diretamente a Análise de Impacto de Negócio – BIA, uma vez que destaca como os sistemas críticos são conectados.

3. 5. 5. Análise de impacto no negócio – BIA

Decidir o que é mais crítico para uma empresa é a função da BIA (Business Impact Analysis). O processo consiste em descobrir as diferentes camadas que existem e suas inter-relações dentro e entre os diferentes sistemas que podem suportar múltiplas operações de negócios.

No mínimo, os seguintes itens devem ser avaliados, segundo GUPTA; SHARMA (2009):

- Impacto financeiro devido à ruptura de operações;
- Perda de ativos (humanos, equipamentos, infraestrutura);
- Violação de leis e regulamentos; e
- Efeito na percepção do público.

A razão pela qual a BIA é fundamental é que ela identifica os processos ou funções que são de missão crítica e que irão facilitar a elaboração do plano de recuperação de desastres (DRP).

Inicia-se a BIA, elencando-se as funções críticas prioritárias, que podem ser classificadas e suas respectivas perdas financeiras estimadas, caso as operações sejam interrompidas durante um desastre. Essencialmente, a BIA é um exercício de custo-benefício.

Depois de classificar os elementos da missão crítica, a equipe questiona:

- Que medidas podem ser instituídas para garantir que os elementos críticos sejam preservados durante um desastre?;
- Quais são os custos de cada medida?;
- Que perdas prováveis teriam, se o elemento falhasse durante um desastre?

Por exemplo, devido a um desastre, uma organização tem a indisponibilidade de um banco de dados de logística e, com isso, a paralisação do transporte de mercadorias em várias localizações geográficas e, no financeiro, as perdas são estimadas em R\$ 400.000,00 por dia. O custo para configurar um site espelho, em um local de diferente localização geográfica, seria de R\$ 500.000,00, com atualização diária, e custos anuais adicionais de R\$ 10.000,00. Então faria sentido pensar em investir em tal sistema. Para negócios de menor porte com perdas diárias estimadas em R\$ 2.000,00, neste caso, pode não ser uma solução econômica; uma resposta melhor poderia ser o uso de uma listagem em papel do estoque, atualizada todas as noites.

3. 5. 6. Análise de risco

Como visto anteriormente, o objeto de uma análise de risco é listar todas as ameaças possíveis às operações de uma empresa, quantificar, tanto quanto possível, a probabilidade de tal ameaça se materializando e avaliar o impacto da ameaça. As ameaças são agrupadas em

três categorias: natural, humana e ambiental. Para cada ameaça específica, uma estimativa de sua ocorrência (probabilidade) ao longo de um ano (geralmente até o próximo ano) é obtida, e o impacto de tal ameaça se materializando é avaliado.

3. 5. 7. Desenvolvimento de estratégia de mitigação

Quando a BIA e a análise de risco forem concluídas, o próximo passo é desenvolver estratégias ou propostas específicas para mitigar o risco de cada ameaça.

Quatro resultados são possíveis:

- Uma solução econômica foi contemplada e irá eliminar ou reduzir o risco a um nível aceitável;
- Soluções que podem reduzir o risco foram encontradas, porém o custo pode ser inaceitável;
- Aceitar o risco conforme definido (não fazer nada); e
- Os casos em que nenhuma estratégia pode ser encontrada para mitigar o risco de uma ameaça.

Estratégias podem também encontrar soluções que mitigam mais de um risco.

A definição de risco aceitável é um julgamento que deverá ser feito pela alta administração, mas a decisão pode ser auxiliada pelo desenvolvimento de uma matriz probabilidade/impacto. Esse é um método de classificação de probabilidades de eventos em alta, média e baixa, e a atribuição de critérios para o impacto em alto, médio ou baixo para cada evento.

Por exemplo, se a probabilidade de perda de energia elétrica da concessionária por 1 dia, ocorrendo nas dependências de uma empresa, é baixa, da ordem de $< 0,01$ por cento, e o impacto é baixo, já que o datacenter possui gerador, então isso é um risco aceitável.

Por outro lado, um evento que tem um impacto médio, mas que tem uma probabilidade média – por exemplo, um grande incêndio no local – é um evento que precisa de desenvolvimento de uma estratégia de mitigação.

Uma vez que as estratégias de mitigação sejam desenvolvidas para as ameaças, é aconselhável realizar novamente a BIA e a análise de risco com a solução proposta no local, visando garantir sua eficácia. Além disso, uma análise de custo-efetividade deve ser realizada para cada estratégia, a fim de determinar o ROI – Retorno do Investimento.

Capítulo 4 – Desenvolvimento e Implantação de Política de segurança da Informação

A quantidade e a gravidade dos ataques a computadores e sistemas de informação nas últimas duas décadas têm aumentado constantemente, e, com isso, o uso de políticas de segurança pelas organizações tem sido uma saída para a proteção de ativos digitais e físicos. Isso porque o elemento humano é considerado o elo mais fraco em segurança da informação.

Conforme GREGORY (2003), as políticas de segurança definem os limites de comportamento aceitável por parte das pessoas e as características operacionais por parte da tecnologia da informação e comunicação. No entanto, cada organização, com sua missão e formas exclusivas de fazer negócios, terá práticas e necessidades exclusivas que exigem políticas e requisitos específicos.

Uma política de segurança é a base essencial para uma implantação de programa de segurança eficaz e abrangente. Ela define um conjunto específico de intenções e condições que ajudarão a proteger os ativos de uma organização e sua capacidade de conduzir negócios.

Uma boa política de segurança deve ser uma declaração formal, resumida e de alto nível das práticas de segurança, que a gerência espera que os funcionários e outras partes interessadas sigam. Por isso, ela deve ser concisa e fácil de entender para que todos possam seguir as orientações nela estabelecidas.

Em sua forma básica, uma política de segurança é um documento que descreve os requisitos de segurança de uma organização e especifica o que deve ser feito, não como; também não especifica tecnologias ou soluções específicas.

4. 1. Contexto jurídico e regulamentar

Uma política de segurança da informação não poderá existir isolada. Existem outras normas superiores que limitam seu escopo de atuação. Exemplo: a Constituição do Brasil é o arcabouço jurídico de maior relevância. Nenhuma norma legal pode mudar os princípios, diretrizes e conceitos dela. Muito menos normas, cujo âmbito de atuação é a organização.

Ao se elaborar a política de segurança da informação de uma organização, é necessário verificar sua aplicabilidade ou possíveis conflitos com quaisquer estatutos ou regras legais ou regulamentares, sejam na esfera municipal, estadual ou federal.

O exemplo mais recente está sendo a LGPD - Lei Geral de Proteção de Dados - cujo normativo está interferindo em todas as políticas de segurança até então implantadas,

no que diz respeito à privacidade. Essa situação ilustra o quão dinâmico é o contexto dos marcos regulatórios. Basta uma mudança em um dispositivo legal para afetar as políticas organizacionais.

Além disso, a Política de Segurança deverá sempre estar alinhada com as políticas da organização.

4. 2. Normas, procedimentos e diretrizes

Para o entendimento desse tópico, torna-se necessária a abordagem de arquitetura de políticas.

4. 2. 1. Arquitetura de políticas de segurança

Uma arquitetura de política de segurança é um conjunto de documentos criados e projetados para demonstrar o curso de ação da empresa para protegê-la como também os seus ativos.

É um conjunto integrado de documentos, que fornece orientação para os requisitos de negócios. Uma arquitetura de política de segurança da informação é a base dos blocos de construção do programa de segurança da informação.

Para fins de desenvolvimento do conceito de uma arquitetura de política de segurança da informação, tem-se a seguinte estrutura hierárquica de grau de importância da maior para a menor:

- **POLÍTICA** – é o nível mais alto na hierarquia, ela estabelece os objetivos, comportamentos e consequências. Uma política de segurança é a principal maneira pela qual as expectativas da administração quanto à segurança são fornecidas aos desenvolvedores, instaladores, mantenedores e usuários dos sistemas de informação de uma organização;
- **DIRETRIZES** – são elaboradas para integrar uma política. São conselhos sobre como atingir os objetivos da política de segurança, mas são sugestões, não regras;
- **PADRÕES** – são as regras e procedimentos requeridos para cumprir as diretrizes de uma determinada política. Os padrões especificam como configurar dispositivos, instalar e configurar software e usar sistemas de computador e outros ativos organizacionais para estar em conformidade com as intenções da política.
- **PROCEDIMENTOS** – os procedimentos, processos e instruções de trabalho são normas construídas para implementar as diretrizes de uma política. Eles especificam

as instruções passo a passo, para realizar várias tarefas de acordo com as políticas e padrões.

Dessa maneira, define-se primeiramente a política; depois suas diretrizes e os padrões adotados, e, posteriormente, são definidas as normas procedimentais.

4.3 Metodologia de desenvolvimento e implantação

É importante planejar uma abordagem para o desenvolvimento de políticas que seja consistente, exequível e direta. Uma abordagem de cima para baixo (Top-Down) para o desenvolvimento de políticas de segurança fornece ao profissional de segurança um roteiro para uma produção consistente e bem-sucedida de políticas.

O desenvolvedor da política deve ter tempo para entender o cenário regulatório da organização, objetivos de negócios e preocupações de gerenciamento de risco, incluindo as declarações de política geral da empresa, missão, objetivos estratégicos etc. Assim, um mapeamento prévio de requisitos deve incorporar as regulamentações específicas, às quais a organização está subordinada.

4.3.1. Desenvolvimento de política de segurança

Ao desenvolver uma política de segurança pela primeira vez, uma abordagem útil durante todo o processo é enfocar: o porquê, quem, onde e o quê.

- Por que a política deve abordar essas questões específicas? (Objetivo)
- A quem a política deve se dirigir? (Responsabilidades)
- Onde a política deve ser aplicada? (Escopo)
- O que a política deve conter? (Conteúdo)

Para cada um desses componentes de desenvolvimento de política de segurança, uma abordagem em fases é usada, conforme discutido a seguir.

4.3.2. Abordagem em fases

O desenvolvimento da política de segurança deverá possuir as seguintes fases:

- Levantamento de requisitos:
 - Requisitos regulamentares (específicos da tecnologia);
 - Requisitos de consultoria (melhores práticas);

- Requisitos informativos (específicos da organização);
- Definição e proposta do projeto com base nos requisitos;
- Desenvolvimento de políticas;
- Revisão e aprovação;
- Publicação e distribuição;
- Manutenção contínua (e revisão).

Após a política de segurança ser aprovada, padrões e procedimentos devem ser desenvolvidos para garantir uma implantação tranquila. Isso exigirá que o desenvolvedor da política trabalhe em conjunto com a equipe técnica para desenvolver padrões e procedimentos relacionados a computadores, aplicativos e redes.

4. 3. 3. Quem contribui para o desenvolvimento da política de segurança

Diferentes grupos e indivíduos devem participar e serem representados a fim de garantir que todos estejam integrados no esforço, que todos estejam dispostos a cumprir e que os melhores interesses de toda a organização sejam representados.

Ao criar uma política de segurança, os seguintes grupos podem ser representados:

- **Recursos Humanos** – a aplicação da política de segurança, quando envolve recompensas e punições de funcionários, é geralmente de responsabilidade do departamento de RH;
- **Jurídico** – muitas vezes, uma organização que tem um departamento jurídico interno ou representação legal externa deseja que esses advogados analisem e esclareçam os pontos legais no documento e aconselhem sobre pontos específicos de adequação e aplicabilidade;
- **Técnicos de Tecnologia da Informação e Comunicação** – a política de segurança da informação tende a se concentrar nos sistemas de computador e, especificamente, nos controles de segurança integrados à infraestrutura de computação e telemática. Então os funcionários de TI são geralmente os maiores consumidores das informações da política;

- **Segurança Física** – os departamentos de Segurança Física (ou Instalações) geralmente implementam os controles de segurança física especificados na política de segurança. Em alguns casos, o departamento de TI pode gerenciar os componentes dos sistemas de informação de segurança física.

4. 3. 4. Público da política de segurança

O público-alvo das políticas de segurança são todos os indivíduos que lidam com as informações da organização, tais como:

- Funcionários;
- Empresas terceirizadas e trabalhadores temporários;
- Consultores, integradores de sistema e prestadores de serviços;
- Parceiros de negócios e fornecedores terceirizados;
- Funcionários de subsidiárias e afiliadas;
- Clientes que usam os recursos de informação da organização.

4. 3. 5. Categorias de política

As políticas de segurança podem ser subdivididas em três categorias principais:

- **REGULATÓRIA** – para fins de auditoria e conformidade (compliance), é útil incluir essa categoria específica. A política geralmente é preenchida com uma série de declarações legais, detalhando o que é necessário e por que é necessário. Os resultados de uma avaliação de requisitos regulatórios podem ser incorporados a esse tipo de política.
- **CONSULTIVA** – esse tipo de política informa todas as partes afetadas sobre políticas específicas de negócios e pode incluir políticas relacionadas a sistemas e redes de computadores, pessoal e segurança física. Esse tipo de política geralmente se baseia nas melhores práticas de segurança.
- **INFORMATIVA** – esse tipo de política existe para garantir que as políticas não cobertas por Regulamentação e Consultoria sejam contabilizadas. Essas políticas podem se aplicar a unidades de negócios específicas, parceiros de negócios, fornecedores e clientes que usam os sistemas de informação da organização.

4. 3. 6. Formas de organização de política

A política de segurança deve ser concisa e fácil de ler para ser eficaz. Uma política incompreensível ou excessivamente complexa corre o risco de ser ignorada por seu público e deixada acumulando poeira em uma prateleira, a famosa lei-morta, deixando de influenciar os esforços operacionais atuais.

Deve ser uma série de declarações simples e diretas das intenções da alta administração.

A forma e a organização das políticas de segurança podem ser refletidas em um formato de esboço com os seguintes componentes:

- **AUTOR** – é o redator da política;
- **PATROCINADOR** – é o gestor executivo;
- **AUTORIZADOR** – é o signatário executivo com autoridade final;
- **DATA DE VIGÊNCIA** – quando a política entra em vigor; geralmente quando autorizada;
- **DATA DE REVISÃO** – sujeito a acordo por todas as partes; em geral, anualmente, pelo menos;
- **OBJETIVO** – por que a política existe; regulatória, consultiva ou informativa;
- **ESCOPO** – quem a política afeta e onde a política é aplicada;
- **DEFINIÇÃO** – do que se trata a política;
- **EXCEÇÕES** – quem ou o que não é coberto pela política.
- **EXECUÇÃO** – como a política será aplicada e as consequências por não a seguir (penalidades);
- **CONCEITOS E DEFINIÇÕES** – termos que o leitor pode precisar saber;
- **REFERÊNCIAS** – links para outras políticas relacionadas e documentos corporativos.

4. 3. 7. Conscientização de segurança

Como a maioria das coisas, o elemento humano é o menos previsível e mais fácil de explorar.

Funcionários confiáveis são corrompidos ou induzidos a fornecer, sem querer, informações valiosas que ajudam os invasores. Devido ao alto nível de confiança depositado nos funcionários, eles são o elo mais fraco em qualquer cadeia de segurança.

Os invasores geralmente “minam” informações dos funcionários por telefone, computador ou pessoalmente, obtendo informações que parecem inócuas por si mesmas, mas fornecem uma imagem mais completa quando reunidas com outros fragmentos de informações.

As organizações que possuem uma infraestrutura de segurança de rede forte podem ter sua segurança enfraquecida, se os funcionários forem convencidos a reduzir os níveis de segurança ou revelar informações confidenciais.

4. 3. 8. Importância da conscientização sobre segurança

Um programa contínuo de conscientização sobre segurança deve ser implantado para todos os funcionários. Os programas de conscientização de segurança variam em escopo e conteúdo.

Práticas que colocam o programa de segurança da informação em riscos acontecem todos os dias nas empresas, por meio de funcionários que fornecem suas informações de conta e senha, jogam fora documentos sigilosos.

4. 3. 9. Objetivos de um programa de conscientização

Os programas de conscientização sobre segurança têm como objetivo mudar comportamentos, hábitos e atitudes. Para ter sucesso nisso, um programa de conscientização deve apelar para preferências positivas.

Por exemplo, uma pessoa que acredita que é aceitável compartilhar informações confidenciais com um colega ou dar sua senha a um novo funcionário deve ver que as pessoas são respeitadas e reconhecidas na organização por proteger dados confidenciais e não, por compartilhá-los.

A prática de conscientizar cada indivíduo na organização é semelhante à propaganda comercial de produtos. A mensagem deve ser entendida e aceita por cada pessoa, pois cada funcionário é fundamental para o sucesso do programa de segurança. Um elo fraco pode derrubar todo o sistema.

Comunicar a mensagem é o objetivo principal, e as informações absorvidas pelos funcionários são o catalisador para a mudança de comportamento.

4. 4. Políticas de Segurança existentes no Estado

A Agência Estadual de Tecnologia da Informação de Pernambuco (ATI), por meio da Unidade de Segurança da Informação (USI), desenvolveu um projeto de criação de um arcabouço de políticas de segurança a serem aplicadas no âmbito da própria organização.

Iniciou com um programa de conscientização sobre o tema Segurança da Informação, por meio de cartilhas educativas etc., visando à criação da cultura de segurança na instituição. Houve a criação de uma página destinada a esse programa, contendo:

- Guia de Instalação e Uso de Criptografia Pessoal;
- Cartilha sobre Aplicações Seguras;
- Cartilha de Boas Práticas em Segurança da Informação;
- Cartilhas sobre uso de Internet, Senhas e Redes Sociais;
- Conteúdo web sobre os principais conceitos em Segurança da Informação;
- Recomendações;
- Termos e Definições, além de links para conteúdos sobre o tema.

Em maio de 2013, foi criado o Comitê Gestor de Segurança da Informação (CGSI), ligado diretamente à Presidência ATI e composto pelos gestores dos principais setores. Nessa mesma ocasião, foi criado o regimento interno do CGSI.

O arcabouço de Políticas de Segurança foi criado com a Política de Segurança da Informação da ATI (PSI) e hoje conta com as seguintes normas técnicas:

- ATI-SGR-PR/001.1:09 – Norma para Desenvolvimento Seguro de Aplicações Web;
- ATI-SGR-PR/001.2:09 – Norma de Segurança para Uso de Rede Sem Fio;
- Normas Gerais de Utilização da Rede, Uso de E-mail Corporativo e Acesso Internet;
- ATI-SGR-PR/001.1:13 – PSI – Termos e Definições Gerais.

Em um contexto mais amplo, algumas Políticas foram criadas, destacando-se:

4. 4. 1. Política Estadual de Segurança da Informação (PESI)

Criada através do Decreto Estadual nº 49.914, de 10 de dezembro de 2020 (PERNAMBUCO, 2020), tem como conteúdo:

- Abrangência: órgãos e entidades da administração pública estadual;
- Princípios fundamentais: confidencialidade, integridade, disponibilidade e autenticidade das informações;
- Contempla os conceitos de segurança da informação;
- Objetivos da PESI:
 - Posicionar a segurança da informação como um dos elementos fundamentais nas ações públicas e no planejamento estratégico da administração pública estadual;
 - Dotar os órgãos e as entidades da administração pública estadual de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;
 - Garantir a conformidade, a padronização e a normatização das atividades de gestão de segurança da informação no âmbito da administração pública estadual;
 - Promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da administração pública estadual e as instituições públicas e privadas sobre as atividades de segurança da informação;
 - Estabelecer um referencial de segurança de informação a fim de nortear as aquisições e a contratação de serviços de Tecnologia da Informação (TI), no âmbito da administração pública estadual, bem como o desenvolvimento e respectivas evoluções dos sistemas de informação;
 - Assegurar a interoperabilidade entre os sistemas de segurança da informação;
 - Criar, manter e aperfeiçoar conhecimentos de segurança da informação no corpo técnico funcional dos órgãos e das entidades públicas da administração pública estadual;
 - Disseminar a cultura de segurança da informação e suas normas no âmbito da administração pública estadual; e

- Garantir a continuidade das atividades do governo que dependem de informação e sistemas de informação.
- Contempla as seguintes diretrizes:
 - Estabelecer a proporcionalidade das medidas acerca da elaboração de normas e procedimentos de segurança da informação, baseadas em classificação prévia;
 - Controlar o acesso aos sistemas, aos dispositivos, às mídias e a quaisquer outros meios de armazenamento, organização, exibição e transporte de informação, observados os privilégios mínimos necessários, a efetiva gestão de identidades e as restrições oriundas das classificações de criticidade e privacidade das informações;
 - Realizar o registro de acessos e alterações de dados em sistemas de informação que possibilite auditorias e investigações;
 - Estabelecer o acompanhamento permanente do cumprimento da PESI por meio de instrumentos necessários, como o monitoramento do tráfego e o armazenamento de informação;
 - Implantar o processo de gestão de riscos de Tecnologia da Informação e Comunicação (TIC) para análise periódica e sistemática do impacto na área de negócio;
 - Implantar o processo de gestão da qualidade da segurança da informação;
 - Implantar o processo de gestão de continuidade de serviços da TIC.
- Define as competências do Comitê Técnico de Governança Digital (CTGD), criado pela Lei Estadual nº 16.379, de 6 de junho de 2018:
 - Deliberar o plano quadrienal estratégico para a área de segurança da informação com acompanhamento anual de indicadores de desempenho;
 - Aprovar os complementos e evoluções da PESI; e
 - Monitorar o efetivo cumprimento da PESI.
- O papel da Agência Estadual de Tecnologia da Informação (ATI) – atuará como órgão consultor de segurança da informação junto com os demais órgãos e entidades da administração pública estadual.

4. 4. 2. Política Estadual de Compartilhamento de Dados

Criada pelo Decreto Estadual nº 50.474, de 29 de março de 2021, gera a Plataforma de Compartilhamento e Análise de Dados dos órgãos e entidades da administração direta e indireta do Poder Executivo Estadual (PERNAMBUCO, 2020).

Política Estadual de Proteção de Dados Pessoais

Criada pelo Decreto Estadual nº 49.265, de 6 de agosto de 2020, institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual em consonância com a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) (PERNAMBUCO, 2020).

4. 4. 3. Política Estadual de Transparência de Dados

Criada pelo Decreto Estadual nº 30.236, de 02 de março de 2007, dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública estadual por meio da Rede Mundial de Computadores – Internet (PERNAMBUCO, 2020).

4. 4. 4. Outras Políticas de Segurança da Informação de Órgãos

Política de Segurança da Informação (PSI) da Secretaria da Educação do Estado de Pernambuco – criada em 2017, atualmente está na versão 2.0 de 31/07/2018.

Política de Segurança da Informação de SUAPE – criada em 2020.

Capítulo 5 – Tratamento de Ameaças

Os ataques relacionados à segurança cibernética tornaram-se, infelizmente, notícia frequente. Os atacantes exploram as fragilidades dos sistemas, percebidas pelo crescente número de vulnerabilidades encontradas, quando essas não são corrigidas por empresas ou organizações, segundo dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR).

5. 1. Conceito de Incidente

É qualquer evento, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, levando à perda de um ou mais propriedades básicas de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

As organizações devem reduzir a frequência de incidentes, garantindo efetivamente redes, sistemas e aplicações. A prevenção de problemas é, muitas vezes, menos onerosa e mais eficaz do que a reação a eles depois de ocorrerem. Assim, a prevenção de incidentes é um complemento fundamental para potencializar a capacidade de resposta a estes.

Uma organização que não implementa controles ou quando estes são insuficientes, a consequência é o aumento no volume de incidentes. Isso sobrecarrega os recursos de resposta aos incidentes, o que pode resultar numa recuperação tardia ou incompleta e possivelmente em danos maiores aos serviços, além da indisponibilidade de informações.

5. 2. Processo de modelagem para o tratamento de ameaças

Uma equipe de tratamento e resposta de Incidente de Segurança tornou-se um componente importante da Tecnologia da Informação (TI). Possuir uma capacidade de resposta a incidentes é, portanto, necessária para detectá-los rapidamente, minimizando a perda e destruição, atenuando os pontos fracos que foram explorados e restaurando os serviços de TI.

Executar a resposta a incidentes de forma eficaz é uma tarefa complexa e, para estabelecer uma capacidade de resposta, será necessário um planejamento e uso de recursos substanciais. Além disso, o monitoramento contínuo de ataques é essencial.

Um fator crítico de sucesso é o estabelecimento de procedimentos claros de priorização de tratamento de incidentes, implementação de métodos eficazes de coleta e análise de dados, além da notificação de incidente.

A compreensão das ameaças e a identificação de formas de ataques em seus estágios iniciais são fundamentais para evitá-las, além do compartilhamento proativo de informações entre os órgãos da administração pública estadual na pesquisa e monitoramento dos sinais desses ataques como forma de identificá-los de maneira mais eficaz.

O processo de tratamento de ameaças consiste basicamente na criação e estruturação de uma Equipe de Resposta e Tratamento de Incidentes para fornecer e operar uma capacidade formal de resposta a incidentes.

O estabelecimento de uma capacidade de resposta a incidentes deve incluir as seguintes ações:

- Criação de uma política e plano de resposta a incidentes como parte da Política de Segurança da Informação da organização;
- Desenvolvimento de procedimentos para a execução de tratamento de incidentes e emissão de relatórios e notificações;
- Definição de diretrizes para a comunicação com terceiros sobre incidentes;
- Seleção de uma estrutura de equipe e modelo de pessoal;
- Estabelecimento de relações e linhas de comunicação entre a equipe de resposta a incidentes e outros setores;
- Determinação de quais serviços a equipe de resposta a incidentes deverá prover;
- Formação e treinamento da equipe de resposta a incidentes.

A atividade de tratamento de incidentes deve ter sempre recursos adequados para sua capacidade de resposta e, assim, manter ativamente a segurança de redes, sistemas e aplicações. Isso inclui o treinamento da equipe de TI no cumprimento das normas de segurança da organização e a sensibilização dos usuários para a utilização das políticas e procedimentos adequados de redes, sistemas e aplicações.

A metodologia para criação de uma Equipe de Resposta e Tratamento de Incidentes – CSIRT (Computer Security and Incident Response Team) é composta das seguintes etapas:

5. 2. 1. Elaboração da política de resposta e tratamento de incidentes

A política de resposta a incidentes deverá ser criada, incluindo os seguintes elementos-chave:

- Declaração de compromisso da administração;
- Finalidade e objetivos da política;
- Âmbito da política (a quem e o que se aplica e em que circunstâncias);
- Definição de incidentes de segurança informática e termos relacionados;
- Estrutura organizacional e definição de funções, responsabilidades e níveis de autoridade;
- Classificação de prioridade ou gravidade de incidentes;
- As métricas de desempenho;
- Formulários, relatórios e contatos.

Deve-se incluir a autoridade da equipe de resposta a incidentes em alguns casos: confiscar ou desconectar equipamentos e monitorar atividades suspeitas; os requisitos para relatar certos tipos de incidentes; os requisitos para comunicações externas e compartilhamento de informações, por exemplo, o que pode ser compartilhado com quem, quando e em que canais, e os pontos de transferência e escalonamento no processo de gestão do incidente.

5. 2. 2. Elaboração do plano de resposta e tratamento de incidentes

Para a implantação de um tratamento de incidentes, é necessário elaborar o Plano de Respostas que atenda aos seus requisitos exclusivos, missão, abrangência, estrutura e funções da organização. Esse plano deverá estabelecer os recursos necessários e suporte de gestão.

O plano de resposta a incidentes deve incluir os seguintes elementos:

- Missão;
- Estratégias e metas;
- Aprovação da alta direção;
- Abordagem organizacional da resposta a incidentes;
- Como a equipe de resposta a incidentes se comunicará com o resto da organização e com outras instituições;

- Métricas para medir a capacidade de resposta a incidentes e sua eficácia;
- Roteiro para a maturação da capacidade de resposta a incidentes;
- Alinhamento com a Política de Segurança da Informação existente.

A missão, as estratégias e os objetivos da organização para a resposta a incidentes devem ajudar a estruturação de sua capacidade de resposta a estes. A estrutura do programa de resposta a incidentes deverá também ser discutida no plano.

Uma vez que seja desenvolvido o Plano de Resposta e obtida a aprovação pela gerência, o passo seguinte é a sua implementação e, pelo menos anualmente, realizar uma revisão nele, a fim de garantir que a organização esteja seguindo o roteiro para amadurecimento da capacidade e cumprimento de suas metas de resposta a incidentes.

5. 2. 3. Elaboração dos procedimentos

Os procedimentos devem ser baseados na política e no plano de resposta a incidentes.

Os Procedimentos Operacionais Padronizados (POPs) definem os processos técnicos específicos, as técnicas utilizadas, as listas de verificação e os formulários usados no tratamento e na resposta aos incidentes.

Os POPs devem ser abrangentes e detalhados para garantir que as prioridades da organização sejam refletidas nas operações de resposta. Além disso, a sequência de respostas deve minimizar os erros, particularmente aqueles que podem ser causados por manipulação de incidentes em situações estressantes. Os POPs devem ser testados para validar sua exatidão e utilidade.

Os usuários devem ser capacitados para a utilização dos POPs; os documentos do POP podem ser usados por meio de ferramentas.

5. 2. 4. Diretrizes para o compartilhamento de informações com terceiros

A CSIRT precisará, muitas vezes, se comunicar com entidades externas sobre um incidente e deve realizar, sempre que necessário, os seguintes procedimentos: contatar órgãos de polícia para aplicação da lei, contatar os meios de comunicação e o intercâmbio para experiências externas.

Outro exemplo é discutir incidentes com outras partes envolvidas, como Provedores de serviços de Internet (PSIs), fornecedores de softwares vulneráveis, ou outras equipes de resposta a incidentes.

A CSIRT também pode compartilhar proativamente informações relevantes de indicadores de incidentes com detecção e análises.

A equipe de resposta a incidentes deve discutir o compartilhamento de informações com o setor de comunicação da organização, com o setor jurídico e administrativo, antes que ocorra um incidente. Caso contrário, informações sensíveis de incidentes podem ser fornecidas a entidades não autorizadas, o que pode conduzir a perturbações adicionais e até mesmo perdas financeiras.

A equipe deverá documentar todos os contatos e comunicações realizados, indicando os respectivos responsáveis e as evidências coletadas.

5. 2. 5. Estrutura da equipe de resposta a incidentes

Uma equipe de resposta a incidentes deve estar disponível para qualquer pessoa que descubra ou suspeite de um incidente envolvendo a organização. O incidente deverá ser tratado por um ou mais membros da equipe, dependendo da sua magnitude e disponibilidade de pessoal.

Os técnicos da equipe de tratamento de incidentes deverão determinar o impacto do incidente e agir adequadamente para limitar os danos e fazer voltar os serviços a sua normalidade. O sucesso da equipe de resposta a incidentes depende da participação e cooperação dos indivíduos de toda a organização.

5. 2. 5. 1. Modelos de equipe

As estruturas possíveis para uma equipe de resposta a incidentes incluem o seguinte:

- **Equipe Central de Resposta a Incidentes** – uma equipe de resposta a incidentes única que atua no tratamento de incidentes da organização. Esse modelo é eficaz para pequenas organizações e para aquelas com diversidade geográfica, em termos de recursos de computação.
- **Equipes de Resposta a Incidentes Distribuída** – a organização tem várias equipes de resposta a incidentes, responsável por um determinado segmento lógico ou físico da organização. Esse modelo é eficaz para grandes organizações e para organizações com grandes recursos em locais distantes. No entanto, as equipes devem fazer parte de uma única entidade coordenada para que o processo de resposta a incidentes seja consistente em toda a organização, e as informações sejam compartilhadas entre as equipes.

- **Equipe Coordenadora** – uma equipe de resposta a incidentes fornece consultoria para outras equipes sem autoridade sobre estas.

5. 2. 5. 2. Modelo de composição de pessoal

As equipes de resposta a incidentes também podem usar qualquer um dos três modelos de pessoal:

- **Empregados** – a organização executa todo o trabalho de resposta a incidentes, com apoio administrativo limitado dos contratantes;
- **Parcialmente terceirizado** – a organização terceiriza partes de seu trabalho de resposta a incidentes. Apesar de as responsabilidades de resposta a incidentes poderem ser divididas entre a organização e um ou mais terceirizados, um arranjo tornou-se muito comum: a terceirização do monitoramento 24/7 de sensores de detecção de intrusão, firewalls e outros dispositivos de segurança. Essa empresa terceirizada identificará e analisará as atividades e relatará cada incidente detectado para a equipe de resposta a incidentes da organização.
- **Totalmente terceirizado** – a organização terceiriza completamente o trabalho de resposta a incidentes através da contratação de uma empresa. Esse modelo é mais adequado a ser usado quando a organização precisa, em tempo integral, de uma equipe de resposta a incidentes no local, mas não tem recursos suficientes disponíveis nem funcionários qualificados. Nesse caso, assume-se que a organização terá funcionários supervisionando o trabalho do subcontratado.

Ao selecionar modelos de estrutura e de pessoal adequados para uma equipe de resposta a incidentes, as organizações devem considerar os seguintes fatores:

- Necessidade de disponibilidade 24/7;
- Disponibilidade de membros da Equipe: Dedicção Integral versus Parcial;
- Disposição de Empregados – estressamento;
- Custo;
- Experiência do pessoal;
- Qualidade de trabalho atual e futuro.

Ao considerar a terceirização, as organizações devem manter as seguintes questões em mente:

- Qualidade de trabalho atual e futuro;
- Divisão de Responsabilidades;
- Informação Sensível revelada ao Terceirizado;
- Falta de Conhecimento Específico da Organização;
- Falta de correlação;
- Manipulação de incidentes em vários locais;
- Mantendo as habilidades de resposta a incidentes na casa.

5. 3. Tecnologias e processos de mitigação

O processo de Resposta e Tratamento de Incidentes tem uma característica de serviço de emergência e, para isso, deve possuir ferramentas adequadas e planos organizados para uma resposta eficaz.

Um plano de resposta deverá determinar que tipo de serviço pode ser disponibilizado para o enfrentamento do incidente. Os principais tipos de serviço são:

a) Serviços Reativos:

- Tratamento de incidentes;
- Detecção e rastreamento de invasões;
- Análise de artefatos: malwares;
- Perícia Forense Computacional.

b) Serviços Proativos:

- Análise de Vulnerabilidades;
- Monitoramento de atividades suspeitas;
- Configuração e manutenção dos sistemas;
- Desenvolvimento de ferramentas;
- Divulgação de alertas e orientações.

c) Serviços de Gestão da Qualidade de Segurança:

- Auditoria;
- Análise de Riscos;
- Avaliação de Produtos;
- Análise de Indicadores de desempenho;
- Treinamentos e Conscientização.

Existe um conjunto de ferramentas tecnológicas que poderão ser utilizadas nas atividades dos serviços de uma Equipe de Resposta e Tratamento de Incidentes, entre elas:

- Sistema de Gestão de Incidentes;
- Sistema de Gestão de Vulnerabilidades;
- Ferramentas de Auditoria;
- Ferramentas de Pentests;
- Ferramentas para varreduras de vulnerabilidades em software e infraestrutura de TIC;
- Ferramentas de Perícia Forense Computacional;
- Ferramentas para correlação de logs;
- Sistemas de Monitoramento de Ativos;
- Sistemas de Sensores com alertas.

5. 4. Equipe de resposta e tratamento de incidentes

Em uma Equipe de Resposta e Tratamento de Incidentes, um único funcionário, com um ou mais suplentes designados, deverá ser responsável pela resposta do incidente. Em um modelo totalmente terceirizado, essa pessoa da organização terá por função a supervisão e avaliação do trabalho dos subcontratados. Todos os outros modelos de Equipe geralmente têm um gerente de equipe e um ou mais colaboradores que assumem autoridade na ausência do líder de equipe.

Os gerentes normalmente executam uma variedade de tarefas, incluindo atuar na gestão de outras equipes da instituição, operando em situações de crise e garantindo que a equipe tenha o pessoal necessário, recursos e habilidades advindas da capacitação.

Eles também devem ser tecnicamente peritos e ter excelentes habilidades de comunicação, particularmente a habilidade para se comunicar com vários tipos de públicos:

funcionários, imprensa, polícia, etc. Os gerentes são responsáveis por garantir que as atividades de resposta a incidentes sejam executadas adequadamente.

Além do gerente de equipe e vice, algumas equipes também têm uma liderança técnica - uma pessoa com grande competência técnica e experiência em resposta a incidentes, que assume a supervisão e responsabilidade final na qualidade do trabalho técnico da equipe. A posição de liderança técnica não deve ser confundida com a posição de firmeza perante o incidente.

Dependendo do tamanho da equipe de resposta a incidentes e da magnitude do incidente, o gestor da equipe poderá não executar tratamentos de incidentes, mas sim, coordenar as atividades dos colaboradores, fornecer atualizações de incidentes para outros grupos e garantir que as necessidades da equipe sejam atendidas.

Os membros da equipe de resposta a incidentes devem ter excelentes habilidades técnicas, administração, administração de rede, programação, suporte técnico ou detecção de intrusão. Cada membro da equipe deve ter boas habilidades de resolução de problemas e habilidades de pensamento crítico.

Não é necessário que cada membro da equipe seja especialista técnico, mas é necessário ter, pelo menos, uma pessoa altamente proficiente em cada área de tecnologia. Também pode ser útil ter alguns membros da equipe se especializando em áreas técnicas específicas, como detecção de intrusão de rede, análise de malware ou perícia forense. Também é útil fazer uso temporário de especialistas técnicos para compor a equipe.

É importante a motivação do pessoal, proporcionando oportunidades de aprendizado e crescimento.

Para a construção e manutenção de competências da equipe, algumas providências podem ser tomadas, a exemplo:

- Manter um orçamento suficiente para suprir, aprimorar e expandir a proficiência em áreas técnicas e de segurança, bem como temas menos técnicos, como os aspectos jurídicos da resposta a incidentes; envio de técnicos para conferências;
- Garantir aos membros da equipe oportunidades de realizar outras tarefas, como criar materiais educacionais, realização de oficinas de conscientização de segurança e realização de pesquisas;
- Manter pessoal suficiente para que os membros da equipe possam ter tempo de trabalho ininterrupto (por exemplo, férias);

- Criar um programa de tutoria para permitir que a equipe técnica superior ajude o pessoal menos experiente a aprender, tratar e se precaver de incidentes.

5. 4. 1. Dependências dentro das organizações

É importante identificar outros grupos dentro da organização que precisam participar do tratamento de incidentes para que sua cooperação possa ser solicitada antes de ser necessária. Cada equipe de resposta a incidentes deverá agregar pessoas que tenham experiência, competências e habilidades necessárias, incluindo:

- **Gestão** – é a gerência, que estabelece a política de resposta a incidentes, o orçamento e o pessoal necessário. Em última instância, a gestão é a responsável por coordenar a resposta a incidentes entre as várias partes interessadas, minimizando danos e reportando ao Comitê de Informática;
- **Garantia da informação** – alguns funcionários responsáveis pela segurança da informação podem ser necessários durante o tratamento de incidentes (por exemplo, prevenção, contenção, erradicação e recuperação) para alterar Controles de segurança (por exemplo, conjuntos de regras de firewall);
- **Suporte de TI** – especialistas em TI (por exemplo, administradores de sistemas e de rede) possuem não só habilidades para ajudar mas também têm uma melhor compreensão da tecnologia que eles gerenciam no dia a dia. Esse entendimento pode garantir que as ações apropriadas sejam tomadas para o sistema afetado;
- **Assessoria Jurídica** – os especialistas em legislação devem analisar os planos, políticas e procedimentos de resposta para garantir a sua conformidade com a lei, incluindo o direito à privacidade;
- **Assessoria de Comunicação** – dependendo da natureza e do impacto de um incidente, pode ser necessário dispor de especialista para informar os meios de comunicação e, por extensão, o público;
- **Recursos humanos** – se um empregado for suspeito de causar um incidente, o setor de recursos humanos deve ser envolvido – por exemplo, na aplicação de processo disciplinar;
- **Segurança Física e Gestão de Instalações** – alguns incidentes podem ocorrer com violações de segurança física ou que envolvam ataques físicos e lógicos coordenados. A equipe de resposta a incidentes poderá precisar de acesso às instalações durante

o tratamento de incidentes – por exemplo, acesso a uma estação de trabalho comprometida a partir de uma sala fechada.

5. 4. 2. Benefícios advindos da criação da equipe

Os benefícios possíveis são os seguintes:

- Dispor de uma equipe de segurança da informação dedicada à ajuda aos setores da organização para atenuarem e prevenirem os incidentes graves, bem como a proteção de seus valiosos recursos;
- Ter uma coordenação centralizada para as questões de segurança da informação no âmbito geral (Ponto de Contato, PoC);
- Gestão e resposta centralizadas e especializadas em matéria de incidentes de segurança;
- Contar com peritos disponíveis para apoiarem e ajudarem os usuários na recuperação dos ativos, quando da ocorrência dos incidentes de segurança;
- Tratar das questões jurídicas e preservar as provas em caso de ação judicial;
- Acompanhar a evolução no domínio da segurança da informação;
- Estimular a cooperação em matéria de segurança da informação no âmbito da comunidade de usuários (sensibilização).

Capítulo 6 – Compliance

Os profissionais de segurança da informação se deparam com tecnologias em constante evolução, criminosos cibernéticos sofisticados e determinados, um cenário de várias ameaças combinadas. Até mesmo os profissionais de segurança que trabalham em ambientes não regulamentados devem seguir um conjunto comum de práticas, critérios e padrões. Sendo assim, é essencial a compreensão das leis, regulamentos e padrões, que se aplicam no campo da segurança da informação.

6. 1. Definição de Compliance

Compliance significa Conformidade. Estar em conformidade, então, pode ser entendido como praticar ou realizar os processos organizacionais dentro das leis, regulamentos, normas e padrões. Simplificando, conformidade é a adesão às regras e regulamentos, que regem as informações com que a pessoa lida no setor onde trabalha.

Há alguns anos, a maioria dos esforços de segurança da informação seguia apenas algumas políticas e uma ordem geral para manter os invasores afastados. As regulamentações destinadas a proteger os dados e seus usuários tinham definições vagas, e as normas governamentais eram aplicadas sem muito rigor. Hoje, as leis e regulamentações são mais rígidas, em parte porque grandes violações colocam as questões de conformidade sob uma vigilância crescente.

As regulamentações modernas são atualizadas e evoluem constantemente, criando um alvo móvel para as empresas que precisam cumprir as regras. Em geral, mede-se a conformidade em relação ao padrão ao qual se está aderindo. Em vários setores, pode-se até ter que cumprir mais de um conjunto de regras.

6. 1. 1. Tipos de conformidade

Existem dois tipos principais de conformidade: regulatória e do setor.

CONFORMIDADE REGULATÓRIA - é a adesão às leis específicas do setor onde a organização está operando.

Em quase todos os casos, a conformidade regulamentar envolve auditorias e avaliações cíclicas para garantir que a pessoa está realizando tudo de acordo com as especificações.

A preparação para essas auditorias pode ser uma parte valiosa de um programa de conformidade, pois podem educar os participantes e fornecer oportunidades para localizar e corrigir problemas.

CONFORMIDADE SETORIAL – é a adesão aos regulamentos que não são exigidos por lei, mas que podem, no entanto, ter graves impactos sobre sua capacidade de conduzir negócios.

Por exemplo, as organizações que aceitam cartões de crédito geralmente devem cumprir o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS), um conjunto de regras criado por um grupo de emissores de cartão de crédito (incluindo Visa, American Express e Mastercard) para processamento de cartão de crédito transações.

O padrão define requisitos para um programa de segurança, critérios específicos para proteção de dados e controles de segurança necessários. As empresas emissoras de cartão de crédito atualizam seus padrões com um intervalo curto de meses para acompanhar as condições e ameaças atuais. Embora essas emissoras de cartão de crédito não possam impor legalmente a conformidade com seus padrões, se uma empresa ou pessoa física quiser trabalhar com cartões de pagamento terá que se submeter a esses requisitos.

Os comerciantes que processam transações de cartão de crédito com base em cartões de membros do PCI devem se submeter a avaliações anuais de suas práticas de segurança. Organizações com baixo número de transações podem simplesmente preencher uma autoavaliação, que consiste em um pequeno questionário.

Conforme o número de transações cresce, os requisitos se tornam progressivamente mais rigorosos, culminando em visitas de avaliadores externos, especialmente certificados, testes de penetração obrigatórios, requisitos para varredura de vulnerabilidades interna e externa e muitas outras medidas.

6. 2. Modelo GRC

A sigla GRC é um acrônimo para Governança, Riscos e Compliance. Como sugere a sigla, o modelo GRC visa à integração da Governança de Segurança da Informação, Gestão de Riscos e Compliance.

Devido aos cenários mundial e brasileiro, nas duas últimas décadas, têm surgido casos que levam as entidades governamentais a estabelecerem leis ou regulamentos para coibir certas práticas de desvio de conduta por organizações. Em 2002, nos Estados Unidos da América, a Lei Sarbanes-Oxley (conhecida como SOX), aprovada pelo Congresso americano, devido ao escândalo das fraudes Enron, definiu padrões mais rigorosos de GRC para as organizações com ações negociadas em bolsas de valores.

No Brasil, devido aos casos de corrupção investigados pela Operação Lava-Jato, a Lei nº 12.846/13, conhecida como Lei Anticorrupção, definiu os acordos de leniência, cuja publicidade afetou a GRC das empresas envolvidas.

O modelo GRC tem esta integração entre a Governança Corporativa, a Gestão de Riscos e a Conformidade.

G de GOVERNANÇA CORPORATIVA

Na década de 1990, começaram as discussões que definiram os conceitos de Governança e, em 1992, na Inglaterra, a publicação do Relatório Cadbury. No Brasil, em 1999, ocorreu a publicação de um código de melhores práticas pelo Instituto Brasileiro de Governança Corporativa (IBGC).

O conceito de Governança Corporativa corresponde a um conjunto de exercícios de práticas, que definem a maneira pela qual uma organização é dirigida, alinhando as expectativas de acionistas, administradores, pessoal, consumidores, fornecedores, credores, governo e a sociedade em geral.

As bases da Governança Corporativa: transparência, equidade, prestação de contas e responsabilidade corporativa.

R de GESTÃO DE RISCOS

O conceito de risco já foi definido anteriormente no capítulo 2.

C de GESTÃO DE CONFORMIDADE (COMPLIANCE)

O conceito de Compliance ou em Gestão de Conformidade é a maneira de garantir que os negócios e as atividades de uma organização sejam geridos com:

- Padrões da legislação e dos regulamentos oficiais vigentes;
- Políticas empresariais e normas internas de procedimentos; e
- Sem que haja conflitos ou colisões entre esse regulamento.

O principal objetivo do Compliance é o zelo pela Integridade da organização representado pelo comportamento adotado por seus administradores, colaboradores e representantes.

6. 2. 1. Padrões referenciais associados ao modelo GRC

Entre as referências teóricas de GRC, têm-se:

- International Organization for Standardization (ISSO) – com as normas:
 - ISO 31.000 – que trata da Gestão de Riscos; e
 - ISO 37.001 – que trata de sistemas de prevenção à corrupção, como documentos ligados à GRC.
- COSO® (Committee of Sponsoring Organizations of the Treadway Commission) – é uma organização privada, criada nos EUA, em 1985, para prevenir e evitar fraudes nos procedimentos e processos internos de empresas. Foi fundado por entidades ligadas a contabilistas, auditores internos e executivos de finanças. Entre seus objetivos, destacam-se a produção e a divulgação de documentos que ajudam os mercados.

Documentos publicados:

- Sobre Controles Internos, a partir de 1992 – até hoje;
- Prevenção à Fraude em 1999;
- Gestão de Riscos Corporativos em 2004;
- Gestão de Riscos Corporativos revisada, com a inclusão da perspectiva de integração com as estratégias e desempenho das empresas, 2017.
- Instituto Brasileiro de Governança Corporativa (IBGC) – é uma organização sem fins lucrativos, referência nacional e internacional em governança corporativa.

Documentos publicados:

- Código das melhores práticas, em 1999, hoje já está na 5ª edição.;
- Código Brasileiro de Governança Corporativa – Companhias Abertas, de 2016;
- Agenda Positiva de Governança: Medidas para uma governança que inspira, inclui e transforma em 2020.
- Compliance à Luz da Governança Corporativa em 2017;
- Caderno 19 – Gerenciamento de riscos corporativos: evolução em governança e estratégia em 2017.

6. 2. 2. Modelo GRC – Benefícios da integração

Tendo em vista uma melhor e mais eficiente alocação de tempo e recursos, a integração proposta pelo Modelo GRC em uma única estrutura visa:

- Eliminar redundâncias nos trabalhos realizados;
- Reduzir a demanda sobre as áreas de primeira linha de defesa;
- Amplificar a eficiência da segunda linha de defesa; e
- Facilitar a atuação da terceira linha de defesa, representada pela Auditoria Interna.

Outros benefícios advindos da integração:

- Interação entre áreas e a melhoria da performance e dos resultados;
- Diminuição de custos, decorrente da eficiência dos projetos, dos processos e dos controles existentes;
- Maior segurança e confiabilidade nas informações obtidas, o que pode ser traduzido na geração de valor perceptível pelos acionistas e investidores; e
- Diminuição de fraudes e maior controle dos processos.
 - Objetivos estratégicos
 - Aquelas inerentes a riscos, Procedimentos, práticas de Compliance, controles internos e gestão de processos, aspectos atuariais e Compliance.
 - Monitoramento periódico e sistemático da qualidade e do desempenho das atividades de primeira e de segunda linhas de defesa.

6. 2. 3. Modelo GRC – Desafios

O grande desafio da integração de Governança Corporativa, Gestão de Riscos e Gestão de Conformidade é a mudança cultural da organização. A cultura da empresa, em muitos casos, é responsável pelo sucesso ou fracasso da implantação de um modelo integrado de GRC.

Torna-se fundamental a elaboração de um programa de GRC, que irá mostrar sua essencialidade, por meio da busca constante de uma maior eficiência das práticas de governança corporativa, gestão de riscos e Compliance. A conscientização das pessoas em prol dessa abordagem irá, sem dúvida, levar a organização a um desempenho superior com maior transparência.

6. 2. 4. Mecanismos de governança

Assemelham-se aos mecanismos de governança corporativa, compostos por um conjunto de dispositivos que visa à criação de valor da organização.

O Institute of Internal Auditors (IIA) elaborou uma abordagem estratégica por meio do Modelo de Três Linhas de Defesa.

Nesse modelo, representado por três planos de atuação, que visam ao gerenciamento de riscos, evita-se o comprometimento dos objetivos estratégicos e as atividades de controle, cuja missão é mitigação com a distribuição de papéis e responsabilidades nos diferentes níveis da empresa.

A figura 6-1 ilustra essa abordagem.



Figura 6-1. Abordagem do Modelo de três linhas de defesa

Fonte: CNSeg, 2018.

6. 2. 4. 1. Primeira linha de defesa

A primeira linha de Defesa tem por responsabilidade gerenciar os procedimentos e controles de riscos, além de manter a eficácia dos controles internos. Seus objetivos são:

- Identificação, avaliação, controle e mitigação de riscos;
- Orientação no desenvolvimento e na implantação de políticas e procedimentos internos;
- A garantia da conformidade entre as atividades, metas e objetivos associados;
- Desenvolvimento e implantação de procedimentos detalhados de controles;
- Determinar a conformidade e reportar, segundo o caso, as falhas de controle, processos inadequados e eventos inesperados.

6. 2. 4. 2. Segunda linha de defesa

A segunda linha de defesa tem por responsabilidade facilitar e monitorar a eficácia e a implantação de políticas de gerenciamento para a gerência operacional.

Objetivos:

- Auxílio aos responsáveis pela gestão dos riscos para a definição da meta de exposição ao risco, além de reportar informações relacionadas aos riscos em toda a organização;
- Monitoramento de riscos específicos do tipo: a não conformidade com leis e regulamentos aplicáveis e com políticas e normas internas;
- Comunicação direta à alta administração e a setores de negócio e órgão de governança;
- Monitoramento de conformidades específicas;

6. 2. 4. 3. Terceira linha de defesa

A terceira linha de defesa tem por responsabilidade avaliar a eficiência e eficácia das operações.

Objetivos:

- Comunicação da análise dos casos de não conformidade ao Conselho de Administração ou à alta administração;
- Aferição da confiabilidade e integridade dos processos de comunicação de casos;
- Declaração de conformidade de procedimentos internos com a legislação aplicável;
- Verificação do alinhamento dos procedimentos internos com os regulamentos e normas.

6. 3. Legislações e marcos regulatórios

6. 3. 1. Conceito de Legislação

Conforme CÂMARA DOS DEPUTADOS (2021), “a legislação de um estado democrático de direito é originária de processo legislativo, que constrói, a partir de uma sucessão de atos, fatos e decisões políticas, econômicas e sociais, um conjunto de leis com valor jurídico, nos planos nacional e internacional, para assegurar estabilidade governamental e segurança jurídica às relações sociais entre cidadãos, instituições e empresas”.

“Quanto ao Poder Legislativo, a ele compete produzir e manter o sistema normativo, ou seja, o conjunto de leis que asseguram a soberania da justiça para todos – cidadãos, instituições públicas e empresas privadas”.

De acordo com PORTAL EDUCAÇÃO (2021), Normas são o conjunto de regras colocadas de forma simples ou pode ser um documento, que contém especificações técnicas ou outros critérios a serem seguidos ou respeitados.

Não existe uma quantidade exata de normas, elas podem ser elaboradas de acordo com as necessidades das instituições, órgãos públicos de um país, empresas ou grupos políticos.

Tipos de normas existentes

- Normas Técnicas;
- Normas da ABNT;
- Normas Jurídicas;
- Normas Morais;
- Norma Regional;
- Norma Estadual;
- Norma Internacional;
- Normas Administrativas;
- Normas Constitucionais.

6. 3. 2. Conceito de Marco regulatório

Segundo WOLFFENBÜTTEL (2006), para que um agente privado preste serviços denominados de utilidade pública, é necessária a criação de um conjunto de normas, leis e diretrizes para regular o funcionamento desses setores.

O marco regulatório é o termo usado para definir a criação de um ambiente, cujos interesses das empresas do ponto de vista econômico-financeiro sejam conciliados com as exigências e as expectativas do mercado consumidor. Ele deverá ser concebido de forma clara e precisa, visando estimular a confiança de investidores e consumidores e para uma boa estrutura e funcionamento do setor.

Ele estabelece as regras de funcionamento do setor e os mecanismos de fiscalização do cumprimento destas por meio de indicadores de qualidade e auditorias técnicas. Para garantir essas atividades, o marco regulatório define uma entidade que irá regular o setor.

São as agências reguladoras, que são independentes e possuem as condições necessárias para a defesa dos interesses dos cidadãos, do governo e das empresas que irão explorar o setor.

Exemplo: no caso específico da telefonia, esse Órgão é a Agência Nacional de Telecomunicações (Anatel). Existem muitas outras agências reguladoras, como a Agência Nacional de Energia Elétrica (Aneel) e a Agência Nacional de Petróleo (ANP).

6. 4. Marco Civil da Internet

O Marco Civil da Internet garante a privacidade e proteção de dados pessoais, mas garante a disponibilização de dados mediante Ordem Judicial. A Lei 12.965, de 23/04/2014, conhecida como “Marco Civil da Internet”, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

O Marco Civil da Internet abrange (BRASIL, 2014):

- CAPÍTULO I DISPOSIÇÕES PRELIMINARES – apresenta as diretrizes e conceitos da lei;
- CAPÍTULO II DOS DIREITOS E GARANTIAS DOS USUÁRIOS – define os direitos e garantias dos usuários da Internet;
- CAPÍTULO III DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET – define os temas relativos à provisão de conexão e de aplicações de Internet:
 - Seção I – Neutralidade de Rede;
 - Seção II – Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas:
 - Subseção I – Guarda de Registros de Conexão;
 - Subseção II – Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão;
 - Subseção III – Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações;
 - Seção III – Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros;
 - Seção IV – Requisição Judicial de Registros.
- CAPÍTULO IV DA ATUAÇÃO DO PODER PÚBLICO – define os temas relativos à atuação do Poder Público na governança e promoção da internet;
- CAPÍTULO V DISPOSIÇÕES FINAIS – apresenta os dispositivos normativos finais.

6. 4. 1. Principais aspectos abordados pelo Marco Civil da INTERNET

Alguns são considerados uma evolução importante para os usuários da Internet, como veremos a seguir (BRASIL, 2014):

- Artigo 7º - Privacidade dos usuários - os dados pertencem aos seus titulares, não de terceiros - proibido repassar suas informações sem o seu consentimento expresso e livre. A proteção aos dados dos internautas é garantida e só pode ser quebrada mediante ordem judicial.
- Artigo 9º - Neutralidade da rede - Tratamento isonômico entre quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
- Artigo 18º Responsabilidade civil dos provedores de Internet.
- O Capítulo II define os Direitos e Garantias dos Usuários da Internet
 - Proteção à privacidade e aos dados pessoais;
 - Garantia ao usuário de inviolabilidade da intimidade e da vida privada;
 - Inviolabilidade e sigilo às comunicações na internet e àquelas armazenadas privativamente, salvo por ordem judicial;
 - Obrigação de sigilo na guarda de registros de acesso (de conexão e aplicações); e
 - Não fornecimento a terceiros de dados pessoais, inclusive registros de conexão e de acesso à aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
 - Proteção a dados pessoais e privacidade;
 - Direito a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais.
 - Tais dados somente poderão ser utilizados para finalidades que:
 - justifiquem sua coleta;
 - não sejam vedadas pela legislação; e
 - estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet.

- Sanções ou Penalidades
 - Imposição de sanções para os provedores que não respeitarem os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros:
 - Advertência;
 - Multa de 10% do faturamento líquido do grupo econômico no Brasil;
 - Suspensão temporária das atividades; e
 - Proibição do exercício das atividades.
 - Tratando-se de empresa estrangeira, responde solidariamente sua filial, sucursal, escritório ou estabelecimento situado no País pelo pagamento das multas.

6. 5. Lei Geral de Proteção de Dados (LGPD)

Em 14 de agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados (LGPD), que regulamenta a privacidade e a proteção de dados pessoais, garantidas pelo Marco Civil da Internet, e define o poder das entidades regulamentadoras para realizar a fiscalização das organizações.

Todas as empresas deverão adequar os mecanismos, previstos na lei, de interação com o titular dos dados e garantir a segurança de tais informações de forma transparente, sob pena de, não cumprido o prazo de adequação, pagamento de multas que variam de 2% do faturamento bruto até R\$ 50.000.000,00 (cinquenta milhões de reais).

6. 5. 1. O que é LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709, de 14 de agosto de 2018) foi promulgada, visando à proteção dos direitos fundamentais de privacidade e liberdade e à livre formação da personalidade de cada indivíduo. Em seu Artigo 2º, são definidos os fundamentos norteadores (BRASIL, 2018):

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;

- VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Essa lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, realizado por pessoa física ou jurídica de direito público ou privado, e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

6. 5. 2. A quem se aplica a LGPD

No Artigo 3º, está definida a aplicabilidade da lei (BRASIL, 2018):

Essa lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- I – a operação de tratamento seja realizada no território nacional;
- II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
- III – os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

Consideram-se coletados no território nacional os dados pessoais, cujo titular nele se encontre no momento da coleta. Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º dessa lei.

6. 5. 1. A quem não se aplica a LGPD

No Artigo 4º, está definida a não aplicabilidade da lei (BRASIL, 2018):

Essa lei não se aplica ao tratamento de dados pessoais:

- I – realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
- II – realizado para fins exclusivamente:
 - Jornalísticos e artísticos; ou
 - Acadêmicos, aplicando-se a essa hipótese os arts. 7º e 11 dessa lei.
- III – realizado para fins exclusivos de:

- Segurança pública;
 - Defesa nacional;
 - Segurança do Estado; ou
 - Atividades de investigação e repressão de infrações penais; ou
- IV – provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nessa lei.
 - § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nessa lei.
 - § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º desse artigo.
 - § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput desse artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º desse artigo.
 - § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput desse artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
 - § 4º Em nenhum caso, a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput desse artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

6. 5. 4. Estrutura da LGPD

A Lei Geral de Proteção aos Dados (LGPD) está assim estruturada (BRASIL, 2018):

- CAPÍTULO I – DISPOSIÇÕES PRELIMINARES

- CAPÍTULO II – DO TRATAMENTO DE DADOS PESSOAIS
 - Seção I – Dos Requisitos para o Tratamento de Dados Pessoais
 - Seção II – Do Tratamento de Dados Pessoais Sensíveis
 - Seção III – Do Tratamento de Dados Pessoais de Crianças e de Adolescentes
 - Seção IV – Do Término do Tratamento de Dados
- CAPÍTULO III – DOS DIREITOS DO TITULAR
- CAPÍTULO IV – DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO
 - Seção I – Das Regras
 - Seção II – Da Responsabilidade
- CAPÍTULO V – DA TRANSFERÊNCIA INTERNACIONAL DE DADOS
- CAPÍTULO VI – DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS
 - Seção I – Do Controlador e do Operador
 - Seção II – Do Encarregado pelo Tratamento de Dados Pessoais
 - Seção III – Da Responsabilidade e do Ressarcimento de Danos
- CAPÍTULO VII – DA SEGURANÇA E DAS BOAS PRÁTICAS
 - Seção I – Da Segurança e do Sigilo de Dados
 - Seção II – Das Boas Práticas e da Governança
- CAPÍTULO VIII – DA FISCALIZAÇÃO
 - Seção I – Das Sanções Administrativas
- CAPÍTULO IX – DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE
 - Seção I – Da Autoridade Nacional de Proteção de Dados (ANPD)
 - Seção II – Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade
- CAPÍTULO X – DISPOSIÇÕES FINAIS E TRANSITÓRIAS

6. 5. 5. Aspectos importantes da LGPD

Direitos do Titular

Os direitos do titular de dados pessoais estão garantidos durante a existência do tratamento dos dados pessoais realizado pelo órgão ou empresa. Esses direitos estão estabelecidos no Artigo 6º da LGPD e são decorrentes dos princípios definidos (BRASIL, 2018).

- Inciso I – Princípio da finalidade – Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
- Inciso II – Princípio da adequação – Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
- Inciso III – Princípio da necessidade – Direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.
- Inciso IV – Princípio do livre acesso – Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
- Inciso V – Princípio da qualidade dos dados – Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento.
- Inciso VI – Princípio da transparência – Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
- Inciso VII – Princípio da segurança – Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
- Inciso VIII – Princípio da prevenção – Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

- Inciso IX - Princípio da não discriminação - Direito de não ser discriminado de forma ilícita ou abusiva.
- Inciso X - Princípio da responsabilização e prestação de contas - Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Além dos direitos dos titulares de dados que são decorrentes do art. 6º da LGPD, a lei apresenta direitos específicos dos titulares de dados.

Conclusão

O campo de estudo da Segurança da Informação é muito amplo. Ele acompanha todos os aspectos, desde os processos humanos de gestão e operação de organizações a todas as tecnologias e seu uso no dia a dia. Como se não bastasse a complexidade desse enfoque, ainda se têm as questões das atividades criminosas, as ameaças ao funcionamento das instituições.

Este curso tem um propósito de introduzir o público-alvo, servidores públicos, nos principais conceitos desse universo da Segurança da Informação. Cada capítulo se fosse abordado com mais profundidade seriam cursos completos com uma carga horária maior.

Assim, esperamos que tenha cumprido os seus objetivos: expandir os conhecimentos sobre segurança da informação, conhecer as modalidades de planejamento, compreender os conceitos e as abordagens de governança de segurança, gestão de riscos, gestão de políticas.

Referências

- AGOSTINHO, Denilson A. Leis de segurança da informação, Universidade Federal de Santa Catarina, Artigo disponível no site: <<http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/Trabalhos%202004-2/artigo-LeisDeSeguranca.pdf>>. Acesso em: 12 mai. 2021.
- ALEXANDER, Philip. Information security. A manager's guide to thwarting data thieves and hackers., Praeger Security International, 2008, ISBN-13: 978-0-313-34558-6.
- ALVES, Henrique Ferrera. Um estudo da relação entre complexidade estrutural e vulnerabilidades de software, Dissertação (Mestrado em Informática) - UFAL - Instituto de Computação, 2017, p. 19.
- ANDRESS, Jason; LEARY, Mark. Building a Practical Information Security Program., Syngress Media, Inc., 2017, ISBN: 978-0-12-802042-5.
- ANDRESS, Jason. Foundations of information security, A Straightforward Introduction., No Starch Press, San Francisco, 2019, ISBN-13: 978-1-7185-0004-4.
- BACIK, Sandy. Building an Effective Information Security Policy Architecture., CRC Press, 2008, ISBN 978-1-4200-5905-2.
- BATISTA, Emerson O. Sistemas de Informação, o uso consciente da tecnologia para o gerenciamento, Editora Saraiva, 2004, ISBN 85-02-04249-1, p. 13.
- BEAVER, Kevin; DAVIS, Peter T., Hacking Wireless Networks For Dummies., Wiley Publishing, Inc, 2005, ISBN-13: 978-0-7645-9730-5.
- BENIAS, Nikolaos; LEVENTOPOULOS, Sozon A., Cyber warfare: a beyond the basics approach., Nova Science Publishers, Inc., Capítulo 4, 2019, ISBN: 978-1-53614-385-0.
- BERTALANFFY, Ludwig Von, General System Theory: a new approach to unit of science, human biology., Library of Congress Catalog, 1968, Card Number 68-25176.
- BIDGOLI, Hossein. Handbook of information security Volume 1, Key Concepts, Infrastructure, Standards, and Protocols, John Wiley & Sons, Inc., 2006, ISBN-13: 978-0-471-64830-7.
- BIDGOLI, Hossein. Handbook of information security Volume 2, Information Warfare; Social, Legal, and International Issues; and Security Foundations, John Wiley & Sons, Inc., 2006, ISBN-13: 978-0-471-64831-4.
- BIDGOLI, Hossein. Handbook of information security Volume 3, Threats, Vulnerabilities, Prevention, Detection, and Management, John Wiley & Sons, Inc., 2006, ISBN-13: 978-0-471-64832-1.
- BIDWELL, Teri. Hack proofing your identity in the information age, Protect Your Family on the Internet!, Syngress Publishing, Inc., 2002, ISBN: 1-931836-51-5.
- BLOCH, Matthieu; BARROS, João. Physical-Layer Security From Information Theory to Security Engineering., Cambridge University Press, 2011, ISBN 978-0-521-51650-1.
- BURGESS, Christopher; POWER, Richard., Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21st Century, Syngress Publishing, Inc., 2008, ISBN-13: 978-1-59749-255-3.
- CALASHAIN, Tara., Google Hacks, 100 Industrial-Strength Tips & Tools., O'REILLY, 2002.
- CÂMARA DOS DEPUTADOS, Portal da Câmara dos Deputados, O que é Legislação Institucional. Dis-

ponível em: <<https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-mistas/cpcms/normativas/oqueelegislacao.html>> Acesso em: 10 mai. 2021.

CNSeg, Governança, Risco e Compliance no Setor de Seguros, Cnseg - Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização. Programa Educação em Seguros. Livreto Educação em Seguros, 2018.

COLE, Dr. Eric; RING, Sandra., Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft., Springer Nature, Switzerland, 2016, ISBN: 1-59749-048-2.

DYNAMICS, SPL., SQL Injection Are Your Web Applications Vulnerable? Artigo da SPI Dynamics, Inc, 2002.

FINK, Steven., Sticky fingers: managing the global risk of economic espionage., Dearborn Trade, a Kaplan Professional Company, 2002, ISBN 0-7931-4827-8.

FORESTI, Sara; LOPEZ, Javier., Information Security Theory and Practice., Springer Nature, Switzerland, 2016, ISBN 978-3-319-45931-8.

GRAVES, Kimberly., CEH Official Certified Ethical Hacker, Review Guide., Wiley Publishing, Inc., Indianápolis, Indiana, 2007, ISBN-13: 978-0-7821-4437-6.

GREENBERG, Michael R., Explaining risk analysis: Protecting health and the environment., 1. ed. Routledge, 2017, ISBN: 978-1-315-64757-9.

GREENBERG, Michael R., Explaining Risk Analysis - Protecting health and the environment., Routledge, 2017, ISBN: 978-1-315-64757-9.

GREGORY, Peter H., Enterprise Information Security, Information security for non-technical decision makers., Pearson Education Limited, 2003, ISBN 0-273-66157-4.

GUPTA, Jatinder N.D.; SHARMA, Sushil K., Handbook of Research on Information Security and Assurance, IGI Global, 2009, ISBN 978-1-59904-856-7.

GUPTA, Manish; SHARMAN, Raj., Social and Human Elements of Information Security: Emerging Trends and Countermeasures, IGI Global, 2009, ISBN 978-1-60566-037-0.

HENDERSON, Lance., TOR and the Dark Art of Anonymity, How to Be Invisible From NSA Spying., Lance Henderson, 2015.

HERZOG, Pete; TRUETT, Check; BARCELÓ, Marta; TRUETT, Kim, Hacker Highschool, Security Awareness fir Teens., www.isecom.org, 2000-2004.

HOFF DO AMARAL, Érico; AMARAL, Marisa M.; NUNES, Raul C., Metodologia para Cálculo do Risco por Composição de Métodos, X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2010, UFPR - Departamento de Informática.

HORTON, Mike; MUGGE, Clinton., Hacknotes - Network Security Portable Reference, McGraw-Hill/Osborne, 2003, ISBN 0-07-222783-4.

INFORMATION TECHNOLOGY LABORATORY, National Vulnerability Database., NIST - National Institute of Standards and Technology. U.S. Department of Commerce, 2021. Disponível em: <<https://nvd.nist.gov/>>. Acesso em: 15 mai. 2021.

LONG, Johnny; PINZON, Scott; WILES, Jack., No Tech Hacking: A guide to social engineering, dumpster diving, and shoulder surfing., Syngress Publishing, Inc., 2008, ISBN-13: 978-1-59749-215-7.

LUDWIG, Mark., The Little Black Book of Computer Viruses., Eletronic Edition, American Eagle Publications, Inc., 1996, ISBN 0-929408-02-0.

McCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George., Hacking exposed: network security, secrets and solutions, third edition, Osborne/McGraw-Hill, 2001, ISBN 0-07-219381-6.

MIRANDA, Rhoxanna Christianth Farago., Análise da sistemática de homologação e certificação de produtos cibernéticos: estudo de caso comparativo entre empresas e órgãos reguladores, 2017. 155 f. Dissertação (Mestrado) – Curso de Engenharia Mecatrônica, Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2017.

MITNICK, Kevin d.; SIMON, William L., The art of deception, Controlling the Human Element of Security., Ed. Banned, 2001, ISBN-13 978-0764542800.

MITNICK, Kevin D.; SIMON, William L., The art of intrusion, The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers, Wiley Publishing, Inc., Indianapolis, Indiana. 2005, ISBN 0-7645-6959-7.

NASHERI, Hedieh., Economic Espionage and Industrial Spying., Cambridge University Press, 2005, ISBN-13 978-0-511-08074-6.

NETO, João Souza., Política e Cultura de Segurança, Gestão da Segurança da Informação e Comunicações, 2011, UNIVERSIDADE DE BRASÍLIA, Programa de Formação de Especialistas para a Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações – CEGSIC 2009-2011.

NIST, Information Security Handbook: a Guide for Managers, NIST 800-100, 2006. Disponível em: <<http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>>. Acesso em: 10 jan. 2019.

O'DEA, Michael., HackNotes: Windows Security Portable Reference, McGraw-Hill/Osborne, 2003, ISBN 0-07-222785-0.

O'HANLEY, Richard; TILLER, James S., Information Security Management Handbook; Sixth Edition; Volume 7., CRC PRESS - Auerbach Publication Taylor & Francis Group, 2014, ISBN-13: 978-1-4665-6752-8.

OGAWA, Kazuto; YOSHIOKA, Katsunari, Advances in Information and Computer Security, 11th International Workshop on Security, IWSEC 2016., Springer Nature, Switzerland, 2016, ISBN 978-3-319-44524-3.

PELTIER, Thomas R., Information Security Policies and Procedures, A Pratitioner's Reference, Second Edition, CRC PRESS - Auerbach Publication Taylor & Francis Group, 2004, ISBN-13: ISBN 0-203-48873-3.

PELTIER, Thomas R., Information Security Risk Analysis, Third Edition, CRC PRESS - Auerbach Publication Taylor & Francis Group, 2010, ISBN-13: ISBN 978-1-4398-3956-0.

PELTIER, Thomas R., Information Security Fundamentals. Second Edition., CRC Press, 2014.

PERNAMBUCO, Decreto nº 40.654, de 29 de abril de 2014 - Dispõe sobre o monitoramento e o controle dos serviços de acesso à Internet corporativa pelos órgãos e entidades da Administração Direta e Indireta do Poder Executivo Estadual, dependentes do Tesouro Estadual, Institucional. Disponível em: <<http://legis.alepe.pe.gov.br/texto.aspx?id=11818>> Acesso em: 21 abr. 2021.

PERNAMBUCO, Decreto nº 49.265, de 6 de agosto de 2020, Política Estadual de Proteção de Dados Pessoais, Institucional. Disponível em: <<https://legis.alepe.pe.gov.br/texto.aspx?id=51399&tipo=>>> Acesso em: 17 mar. 2021.

PERNAMBUCO, Decreto nº 49.914, de 10 de dezembro de 2020, Política Estadual de Segurança da Informação – PESI, Institucional. Disponível em: <<https://legis.alepe.pe.gov.br/texto.aspx?id=53674&tipo=>>> Acesso em: 08 abr. 2021.

PERNAMBUCO, Decreto nº 50.474, de 29 de março de 2021, Política Estadual de Compartilhamento de Dados, Institucional. Disponível em: <<https://legis.alepe.pe.gov.br/texto.aspx?id=54743&tipo=>> Acesso em: 27 abr. 2021.

PIEKARSKI, Joseli I., Vulnerabilidade digital de novas tecnologias: técnicas utilizadas através do meio digital que podem ser aplicadas em processo de espionagem e no cybercrime, TCC do curso Gestão de Segurança da Informação, da UNISUL, Curitiba, 2018.

PIOTROWSKI, Michal., Dangerous Google – Searching for Secrets., Artigo publicado na Haking magazine, edição 4/2005.

PORTAL EDUCAÇÃO, O que são normas? Disponível em: <<https://www.portaleducacao.com.br/conteudo/artigos/administracao/o-que-sao-normas/50930>> Acesso em: 10 mai. 2021.

POULSEN, Kevin L., Hack Proofing Your Network: Internet Tradecraft., Syngress Media, Inc., 2000, ISBN: 1-928994-15-6.

PRASAD, Ramjee; ROHOKALE, Vandana., Cyber Security: The Lifeline of Information and Communication Technology., Springer Nature, Switzerland, 2020, ISBN 978-3-030-31703-4.

RHODES-OUSLEY, Mark., Information Security, The Complete Reference., McGraw-Hill Companies. 2013, 2. ed., ISBN: 978-0-07-178436-8.

ROGERS, Russ., Hacking a Terror Network – The silent threat of covert channels, Syngress Publishing, Inc., 2005, ISBN: 1-928994-98-9.

SCAMBRAY, Joel; SHEMA, Mike., Hacking exposed web applications., McGraw-Hill, 2002, ISBN 0-07-222438-X.

SCOTTO, Procolo., Darknet Master, TOR and Deep Web Secrets., e-book, 2020.

SILVA, Alcineide P.; SANTOS, Júlio C.; KONRAD, Márcia R., Teoria geral dos sistemas: diferencial organizacional que viabiliza o pleno entendimento da empresa, FACEQ. Educação, Gestão e Sociedade: revista da Faculdade Eça de Queirós, ISSN 2179-9636, Ano 6, número 22, junho de 2016.

SYNGRESS, Hack Proofing Your Network: Internet Tradecraft., Syngress Media, Inc., 2000, ISBN: 1-928994-15-6.

SYSTEMS, Internet Security, Ethical Hacking, Student Guide., Internet Security Systems, Inc., 2000.

THE MITER CORPORATION, Lista CVE, The MITRE Corporation, 1999–2021. Disponível em: <<https://cve.mitre.org/index.html>>. Acesso em: 15 mai. 2021.

TIPTON, Harold F.; KRAUSE, Micki., Information Security Management Handbook. Sixth Edition., CRC PRESS – Auerbach Publication Taylor & Francis Group, 2007, ISBN-13: 978-0-8493-7495-1.

WHITMAN, Michael E.; MATTORD, Herbert J., Management of Information Security, Fourth Edition, Cengage Learning, 2014, ISBN-13: 978-1-285-06229-7.

WOLFFENBÜTTEL, Andréa, O que é? – Marco regulatório, Revista Desafios do Desenvolvimento, Brasília-DF, 2006. Ano 3. Ed. 19 – 7/2/2006 – site: <http://desafios.ipea.gov.br/index.php?option=com_content&view=article&id=2093;catid=28&Itemid=23#:~:text=Al%C3%A9m%20de%20estabelecer%20as%20regras,estabelecimento%20de%20indicadores%20de%20qualidade.> Acesso em: 08 mar. 2021.

Sobre o autor

Graduado em Ciência da Computação pelo Departamento de Informática da Universidade Federal de Pernambuco (UFPE, 1983) e pós-graduado em Mestrado em Ciência da Computação pelo Departamento de Informática (UFPE, 1991).

Analista de Gestão em Tecnologia da Informação do quadro da Agência Estadual de Tecnologia da Informação (ATI), com 37 anos de trabalho, lotado atualmente na Gerência de Projetos e Gestão de Segurança da Informação (GSI), nas áreas de gestão de incidentes e análise de vulnerabilidades.

Professor Universitário (2002 – 2010) nos cursos de Sistemas de Informação, Administração e Petróleo e Gás, pela Faculdade Integrada do Recife (FIR).

Ministrou diversos cursos presenciais, como Excel Básico, Excel Intermediário e Excel Avançado para CEFOSPE, ATI, Secretaria Geral de Controladoria do Estado, Secretaria de Saúde, entre outros. Também ministrou os cursos presenciais de UBUNTU Básico, UBUNTU Avançado, BR OFFICE Básico, BR OFFICE Avançado e Informática Básica.

Participou de curso de Instrutoria pelo IRH; curso de tutor do CEFOSPE, na Plataforma Online Microsoft Teams; e curso OFFICIAL (ISC) CISSP CBK – Certified Information System Security Professional.

