



Interativa

Segurança Física e Lógica

Autor: Prof. Ricardo Sewaybriker

Colaboradoras: Profa. Elisângela Mônaco de Moraes
Profa. Iza Melão

Professor conteudista: Ricardo Sewaybriker

Pós-graduado em Gestão da Segurança da Informação pelo Instituto de Pesquisas Energéticas e Nucleares (Ipen-USP) (2005). Formado em Administração de Empresas pelas Faculdades Integradas Campos Salles (Fics) (2002). Professor da Universidade Paulista (UNIP) desde 2007. Profissional de segurança da informação, atua em instituição financeira há 27 anos.

Dados Internacionais de Catalogação na Publicação (CIP)

S514s Sewaybriker, Ricardo.

Segurança Física e Lógica / Ricardo Sewaybriker. – São Paulo: Editora Sol, 2018.

164 p., il.

Nota: este volume está publicado nos Cadernos de Estudos e Pesquisas da UNIP, Série Didática, ano XXIV, n. 2-119/18, ISSN 1517-9230.

1. Segurança em redes. 2. Sistemas de autenticação. 3. Segurança da informação. I. Título

CDU 681.3.004.4

Prof. Dr. João Carlos Di Genio
Reitor

Prof. Fábio Romeu de Carvalho
Vice-Reitor de Planejamento, Administração e Finanças

Profa. Melânia Dalla Torre
Vice-Reitora de Unidades Universitárias

Prof. Dr. Yugo Okida
Vice-Reitor de Pós-Graduação e Pesquisa

Profa. Dra. Marília Ancona-Lopez
Vice-Reitora de Graduação

Unip Interativa – EaD

Profa. Elisabete Brihy
Prof. Marcelo Souza
Prof. Dr. Luiz Felipe Scabar
Prof. Ivan Daliberto Frugoli

Material Didático – EaD

Comissão editorial:

Dra. Angélica L. Carlini (UNIP)
Dra. Divane Alves da Silva (UNIP)
Dr. Ivan Dias da Motta (CESUMAR)
Dra. Kátia Mosorov Alonso (UFMT)
Dra. Valéria de Carvalho (UNIP)

Apoio:

Profa. Cláudia Regina Baptista – EaD
Profa. Betisa Malaman – Comissão de Qualificação e Avaliação de Cursos

Projeto gráfico:

Prof. Alexandre Ponzetto

Revisão:

Ricardo Duarte
Fabrícia Carpinelli

Sumário

Segurança Física e Lógica

APRESENTAÇÃO	7
INTRODUÇÃO	7

Unidade I

1 FUNDAMENTOS DE SEGURANÇA EM REDES	9
1.1 Conceito de segurança da informação	9
1.2 Pilares da segurança em redes de dados e comunicação	11
1.3 Ciclo de vida da informação	15
1.4 Classificação da informação	16
1.5 Análise e gerenciamento de riscos	21
1.5.1 Análise de riscos	21
1.5.2 Gerenciamento de riscos	22

Unidade II

2 SISTEMAS DE AUTENTICAÇÃO	29
2.1 Autenticação	29
2.2 Autorização	34
2.2.1 Autorização por serviços de diretório	34
2.2.2 Autorização por SSO (single sign-on)	35
2.2.3 Autorização por AMS (account management system)	35
2.3 Auditoria	36
2.4 Exemplos de solução AAA	38

Unidade III

3 MECANISMOS E ESTRATÉGIAS DE SEGURANÇA EM REDES	42
3.1 Segurança física	42
3.2 Estratégias de segurança	50
3.3 Criptografia e infraestrutura de chaves	53
3.3.1 Segurança e ataques criptográficos	57
3.4 Certificados digitais	57

Unidade IV

4 AMEAÇAS E MECANISMOS DE ATAQUE A REDES	60
4.1 Formas de ataque	61
4.2 Hackers e crackers	63

4.3 Ferramentas de ataque	64
4.3.1 Bombas de correio eletrônico e listas de mala direta.....	65
4.3.2 Negação de ferramentas de serviço.....	67
4.3.3 Softwares maliciosos.....	67
4.4 Detecção e proteção	74

Unidade V

5 DISPOSITIVOS DE SEGURANÇA PARA REDES	84
5.1 Roteador de borda e NAT	84
5.2 Firewall e proxy	86
5.3 Bastion host.....	95
5.4 Perímetro de segurança.....	95
5.5 Sistemas de detecção, prevenção e reação	98

Unidade VI

6 VPN, VLANS, WLANS E IPSEC	105
6.1 VPN.....	105
6.2 VLANS	112
6.3 WLANS.....	114
6.4 IPSec	120

Unidade VII

7 TESTE DE INVASÃO E SEGURANÇA EM TECNOLOGIAS EMERGENTES	123
7.1 Teste de invasão.....	123
7.2 Etapas de um teste de invasão	124
7.2.1 Coleta de informações.....	126
7.2.2 Descoberta de vulnerabilidades.....	126
7.2.3 Captura de tráfego.....	127
7.2.4 Ataque a senhas.....	128
7.2.5 Exploração de falhas do lado da organização.....	130
7.3 Segurança em tecnologias emergentes.....	131
7.3.1 Computação em nuvem.....	131
7.3.2 Criptomoeda e blockchain	134
7.3.3 Internet das coisas	138

Unidade VIII

8 PROCESSOS DE SEGURANÇA DA INFORMAÇÃO	140
8.1 Política, normas e procedimentos de segurança da informação.....	140
8.1.1 Padrões de segurança da informação	144
8.2 Legislação e direito digital.....	146
8.3 Time de resposta a incidentes computacionais.....	149
8.4 Plano de continuidade de negócios	155

APRESENTAÇÃO

Caros alunos,

Esta disciplina tem por objetivo discutir os principais aspectos da proteção dos ativos que circulam interna e externamente nas redes corporativas e públicas.

A importância de desenvolver projetos de rede com segurança não diz respeito apenas às grandes redes corporativas, mas a qualquer tipo e tamanho de rede, incluindo as domésticas. Todos estamos expostos à ação de crackers, o que se relaciona às vulnerabilidades contidas nas redes.

A preocupação com segurança nem sempre foi significativa. Em meados da década de 1960, quando as primeiras redes iniciaram o processo irreversível de transporte de dados, não se imaginava que as redes ligariam o mundo e que a informação seguiria de um ponto a outro do planeta em frações de segundo.

As primeiras redes desenvolvidas, com tecnologia arcaica e abrangência limitada, sofriam poucas ações de invasão. Quando estas ocorriam, não visavam obter lucro financeiro, mas testar a habilidade dos invasores em quebrar os mecanismos de segurança das redes. Os invasores usavam tais práticas para expor seus talentos e vangloriar-se entre os amigos.

Ao longo das últimas décadas, as redes evoluíram e tornaram-se parte do universo corporativo, governamental e pessoal. Inúmeras informações trafegam através delas. Com o advento da internet e sua evolução constante, nós nos tornamos cada vez mais dependentes do seu funcionamento, e, portanto, dos mecanismos de segurança usados para proteger os ativos de informação que nela trafegam.


Da segurança das redes depende o processo progressivo de massificação do uso da informação, principalmente nas redes corporativas, que movimentam muita informação e, consequentemente, muitos valores financeiros, alvo dos criminosos do presente e, por que não dizer, dos criminosos do futuro, os crackers.

Ataques às redes corporativas são cada vez mais frequentes, e agora em escala global, afetando empresas em diversos países simultaneamente. Com o surgimento da computação em nuvem e da internet das coisas, a segurança em redes tornou-se ainda mais fundamental, sendo relevante para o futuro de todas as esferas do cotidiano.

INTRODUÇÃO

O conteúdo apresentado visa despertar a curiosidade do aluno pelo assunto, uma vez que as redes de dados e comunicação são o principal alvo de um ataque, ou estão diretamente ligadas à possível concretização dele.

A princípio, veremos os fundamentos de segurança em redes: conceito de segurança da informação, pilares da segurança da informação, classificação da informação, análise e gestão de riscos, sistemas de autenticação em redes, vulnerabilidades, ameaças e impactos.



Em seguida, trataremos dos mecanismos e das estratégias de segurança em redes, com destaque para segurança física, criptografia, infraestrutura de chaves e certificados digitais. Estudaremos as formas e as ferramentas de ataque à rede, as vulnerabilidades e as ameaças, e a diferença entre hacker e cracker.

Depois, discutiremos os dispositivos de segurança em redes, como roteador de borda, firewall, proxy e bastion host.

Por fim, abordaremos testes de invasão, tecnologias emergentes e processos de segurança da informação.

Bons estudos!

Unidade I

1 FUNDAMENTOS DE SEGURANÇA EM REDES

As informações que trafegam nas redes são compostas de dados agrupados de forma lógica, os quais de alguma maneira são significativos para pessoas, processos ou organizações.

As redes são fundamentais no processo de transporte e troca de informações e, de forma direta ou indireta, adicionam mais valor a essas informações. Quando nos referimos à segurança da informação, a transição das informações de um ponto a outro representa o maior risco.

Os desafios dos profissionais que trabalham na administração das redes são inúmeros. Entre eles, está a necessidade de proteger as informações que trafegam na rede sob sua gestão, a fim de evitar vazamentos, furtos e falhas. É por isso que os profissionais de rede devem estar atentos aos fatores humanos e ao estabelecimento de processos estruturados.

São três os elementos de segurança da informação que, agregados, formam os ativos da segurança.

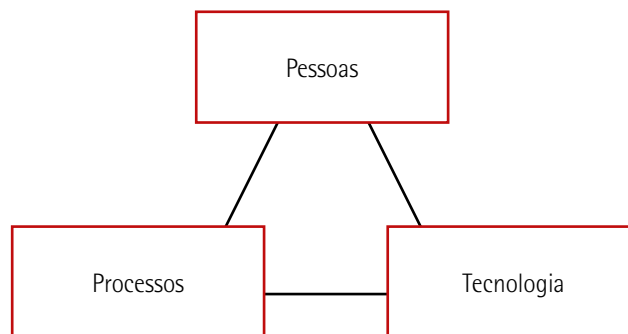


Figura 1 – Elementos de segurança da informação

Todas as ameaças que rondam a segurança da informação visam explorar as vulnerabilidades desses elementos. À primeira vista, é possível imaginar que os profissionais de redes devem preocupar-se apenas com as ameaças que exploram os elementos tecnológicos. No entanto, deixar de avaliar um dos elementos do conjunto talvez dê uma visão incorreta e uma falsa sensação de segurança, o que pode levar a incidentes de segurança da informação.

1.1 Conceito de segurança da informação

Segundo Moraes (2010, p. 19), "a segurança da informação pode ser definida como um processo de proteger a informação do mau uso tanto accidental como intencional, por pessoas internas ou externas à informação, incluindo empregados, consultores e hackers".

Para compreender os processos de proteção da informação, é preciso entender o que influencia todas as decisões na segurança das informações.

O **valor da informação** é seu grau de importância para a organização. Isso parece lógico e simples, mas não é. O valor da informação deve ser determinado por um conjunto de fatores, entre eles o valor financeiro, o valor de imagem, a importância estratégica e o atendimento às leis locais e internacionais. Essa determinação levará à classificação das informações, à análise de riscos e, posteriormente, à priorização de investimentos em mecanismos de proteção.

As **proteções** são definidas a partir do valor e da importância que o ativo de informação tem para a organização, e podem ser desenvolvidas para processos (p. ex., políticas e normas), pessoas (p. ex., portas, alarmes e treinamentos) e tecnologias (p. ex., permissões de acesso e firewalls).

Os tipos e as medidas de proteção são apresentados no quadro a seguir.

Quadro 1 – Tipos e medidas de proteção

Tipo de proteção	Medida de proteção	Elemento influenciado
Lógica	Permissão em sistemas de arquivo Firewalls Perfis de usuário em aplicações	Tecnologia
Física	Porta Fechadura Vigilantes	Pessoas
Administrativa	Política Normas Procedimentos	Processos

Vale ressaltar que mecanismos de proteção implantados de forma isolada são pouco eficazes.

As **ameaças** são ocasiões ou eventos com potencial para causar prejuízo aos ativos de informação. Elas podem explorar vulnerabilidades a fim de se concretizar, e têm origem natural, acidental ou intencional.

Quadro 2 – Tipos de ameaça

Tipo de ameaça	Exemplo	Agente
Natural	Fenômenos da natureza (enchentes, furacões etc.)	Natureza
Acidental	Erros de usuários Falhas sistêmicas Falta de energia	Falta de conhecimento
Intencional	Invasões, terrorismo Chantagem, extorsão Espionagem	Crackers Funcionários insatisfeitos

Os profissionais de rede devem estar alertas aos agentes de ameaças que exploram as vulnerabilidades, como crackers, que atacam a organização de fora para dentro, e funcionários

insatisfeitos, que atacam de dentro da própria organização. A experiência mostra que esse segundo agente é difícil de prever e conter.

As **vulnerabilidades** são brechas que permitem a concretização de um incidente ou ataque à segurança da informação, o que pode causar impacto no negócio da organização.

O **risco** é matemático, ou seja, é a probabilidade de alguma ameaça explorar uma vulnerabilidade e afetar a segurança da informação. Ele pode ser positivo ou negativo, porém, quando o assunto é segurança da informação, lidamos com o risco negativo.

O **impacto** geralmente é definido como o dano causado pela concretização do risco. Quando representado por prejuízos financeiros, é fácil mensurá-lo. No entanto, quando falamos de danos causados à imagem ou aos controles regulatórios, determinar o impacto não é uma tarefa simples, pois ele pode afetar o negócio, os acionistas, os fornecedores e terceiros.

1.2 Pilares da segurança em redes de dados e comunicação

A fim de obter maior proteção, devemos desenvolver um modelo que sirva de parâmetro para orientar as decisões de segurança da informação.

Moraes (2010) menciona o modelo constituído em referência a equipamentos de rede, sistemas de autenticação, sistemas de auditoria e informações extremamente importantes que trafegam nas redes.

Quando falamos de equipamentos de rede, incluímos aí elementos como roteadores, servidores de comunicação, switches de rede local e gateways.

Entre os sistemas de autenticação, podemos mencionar biometria, assinatura digital, certificados digitais, gestão de acessos, tokens etc.

Os sistemas de auditoria relacionam-se ao fato de que as organizações devem, periodicamente, medir os seus controles a fim de testar a real eficácia deles e sua conformidade com o que foi previamente definido.

Quanto às informações extremamente importantes que trafegam nas redes, é fundamental aos profissionais de redes identificá-las para desenvolver mecanismos que as protejam.

Os serviços de segurança em redes devem estar atentos aos pilares implementados e sustentados pelo sistema, que contribuem para a integridade, a confidencialidade, o controle de acesso, a disponibilidade, o não repúdio e a auditoria.

Integridade

Refere-se a garantir que a informação trafegue de um ponto a outro da rede sem sofrer alterações, ou seja, que a informação chegue íntegra a seu destino, sem modificações no caminho.

A integridade de dados tem por objetivo prevenir erros de processamento e fraudes (ameaças acidentais e intencionais). Para alguns sistemas, como o tráfego aéreo e o comércio eletrônico, a integridade é fundamental.

As principais ameaças à integridade das informações estão associadas à ação de crackers, usuários não autorizados, programas maliciosos ou incidentes que alteram o estado original da informação.

Os principais controles de segurança para garantir a integridade estão descritos no quadro a seguir.

Quadro 3 – Controles de segurança para garantir a integridade da informação

Controle	Descrição
Rotation of duties (troca de equipe)	Consiste em trocar constantemente funcionários que ocupam cargos e funções essenciais, a fim de evitar fraudes em sistemas e processos
Need to know (o que os usuários precisam saber)	Originado no meio militar, consiste em permitir acesso apenas àquilo de que os usuários necessitam para executar seu trabalho, bloqueando todo o resto
Separation of duties (divisão de responsabilidades)	Consiste em dividir o processo de execução: quem autoriza não faz, e quem faz não autoriza

Adaptado de: Moraes (2010, p. 26).

Para assegurar a integridade na transmissão de dados em redes e também no armazenamento, uma excelente opção é empregar as funções de hashing, isto é, atribuir ao processo de transporte e armazenamento de informações o resultado de uma função matemática. Quando ocorre a transmissão, a mensagem é processada na origem e calcula-se o hash com o dado a ser transmitido. Em seguida, eles são enviados juntos. Ao chegar ao destino, o dado é separado do hash e o cálculo é refeito, devendo ser idêntico ao criado na origem. Caso haja alteração no valor, o dado foi alterado e sua integridade foi comprometida. Para os casos de armazenamento de informação, o hash é calculado e deixado com a informação armazenada. No momento de usá-la, calcula-se o hash novamente para verificar se continua o mesmo criado na época do armazenamento.

As características de hashing são:

- O valor de entrada da função pode ter qualquer tamanho para o cálculo.
- O hash, que é o digest, tem sempre tamanho fixo.
- O hash é sempre unidirecional, impossível de inverter.
- O hash é livre de colisão, ou seja, dois textos não podem ter o mesmo hash.

Os principais algoritmos de hashing são SHA (secure hash algorithms), MDS (model-driven security) e HMAC (hash-based message authentication code).



Observação

Message digests são funções hash que geram um código de tamanho fixo, em uma única direção, a partir de dados de tamanho arbitrário. Códigos hash são úteis para a segurança de senhas.

Confidencialidade

O princípio de confidencialidade visa proteger a informação em sistemas, recursos e processos, de modo que ela não possa ser acessada por pessoas sem autorização (MORAES, 2010).

Dessa forma, é correto afirmar que preservar a confidencialidade passa por não disponibilizar a informação a quem não esteja autorizado a acessá-la, sendo mais um elemento entre os mecanismos que protegem a privacidade de dados.

As principais ameaças à confidencialidade residem na ação de crackers e de usuários mal-intencionados ou descuidados.

Quadro 4 – Ameaças à confidencialidade

Ameaça	Ação
Atividade não autorizada	Usuários não autorizados têm acesso aos sistemas e comprometem os arquivos
Download não autorizado	Informações são movimentadas de ambientes seguros para ambientes inseguros
Rede	Dados confidenciais que trafegam na rede precisam ser criptografados para assegurar seu sigilo
Vírus e trojan	Códigos maliciosos instalados nos sistemas atacam, buscando informações confidenciais
Engenharia social	Ataques que não fazem uso da tecnologia, mas dos fatores humanos

Adaptado de: Moraes (2010, p. 28).

Nos dados armazenados ou que vão ser transmitidos, a confidencialidade pode ser obtida por meio de criptografia, restrição de acesso, classificação de dados e desenvolvimento de normas e procedimentos de segurança da informação.

Controle de acesso

Quando nos referimos a controle de acesso lógico a redes, falamos em métodos de identificação, autenticação e autorização.

- **Identificação:** o usuário (ou programa, ou processo) deve apresentar ao sistema sua identidade, sua credencial.

- **Autenticação:** depois de identificar-se para o sistema, o usuário deve empregar algum mecanismo que valide seu acesso. Esse mecanismo pode ser, por exemplo, uma senha ou um dispositivo de acesso (como um token). Em geral, o uso de mais de um mecanismo de autenticação é necessário para acessos que requerem maior segurança na confidencialidade e na integridade. A isso chamamos de duplo fator de autenticação, isto é, dois mecanismos distintos de autenticação simultânea.
- **Autorização:** mesmo identificado e autenticado, o usuário precisa estar autorizado a acessar a rede, os sistemas, os aplicativos, os arquivos etc. Assim, o sistema deve verificar os privilégios de acesso previamente definidos. Vale ressaltar que, para garantir a segurança, o ideal é que os usuários tenham privilégios mínimos, reduzidos ao necessário para a execução de suas atividades cotidianas.

Os mecanismos de proteção relacionam-se a:

- **O que o usuário conhece:** normalmente uma senha ou uma frase secreta.
- **O que o usuário tem:** um cartão, um token, uma chave criptografada ou um certificado.
- **O que o usuário é:** características biométricas únicas, como digital, íris e geometria da palma da mão.

Disponibilidade

É o sistema estar sempre acessível quando o usuário precisa. Esse ponto é fundamental para os profissionais de redes, que devem mantê-las sempre operantes.

As ameaças à disponibilidade estão associadas aos ataques que visam interromper o serviço. Os mais conhecidos são os de DDoS (distributed denial of service), de negação de serviço. Desastres naturais – enchentes, terremotos etc. – e atos humanos também podem ser mencionados como ameaças.

Os ataques de negação de serviço foram desenvolvidos para derrubar os servidores de acesso (principalmente web) e, dessa forma, tornar o acesso indisponível. O método mais empregado é o acesso massivo a determinado serviço/servidor, sobrecarregando os recursos de rede além de sua capacidade e derrubando os links de comunicação.

Os ataques de negação de serviço são causados por máquinas invadidas por crackers, os quais utilizam esses equipamentos como soldados sob seu comando, os chamados **zumbis**, que em certo momento acessam simultaneamente o alvo e derrubam os serviços (MORAES, 2010).

Os profissionais devem projetar sistemas com capacidade de prover níveis compatíveis de performance. Uma saída para aumentar a disponibilidade é usar sistemas redundantes, que sustentem o serviço em caso de sobrecarga de acesso.

Não repúdio

Consiste em desenvolver técnicas e métodos para que o remetente de uma informação não possa negar tê-la enviado, algo muito comum em e-commerce e internet banking.

Auditoria

É um procedimento muito importante para os serviços de rede. Através dela, é possível manter registros de tudo o que acontece no ambiente da rede, os chamados **logs**, que são armazenados e podem ser consultados sempre que houver necessidade de averiguar irregularidades.

Basicamente, a auditoria verifica as atividades dos sistemas e seus controles de acesso. Determina o que foi feito, por quem, quando e como. O processo de auditoria abarca todos os usuários, autorizados e não autorizados.

Em aplicações críticas, faz-se necessário aumentar o nível de detalhamento nos registros da auditoria, inclusive para realizar o retorno ao estado inicial de uma informação.

Um problema é que os logs demandam espaço de armazenamento. Por isso, é preciso desenvolver uma política de retenção e de exclusão deles.

1.3 Ciclo de vida da informação

Toda informação é perecível, tem um prazo de validade determinado, o chamado **ciclo de vida da informação**. Os diversos estágios do ciclo de vida de uma informação devem ter formas diferenciadas para o seu tratamento e manutenção e para a implantação de mecanismos de proteção. Por esse motivo, é fundamental entender o que cada etapa do ciclo de vida da informação necessita.

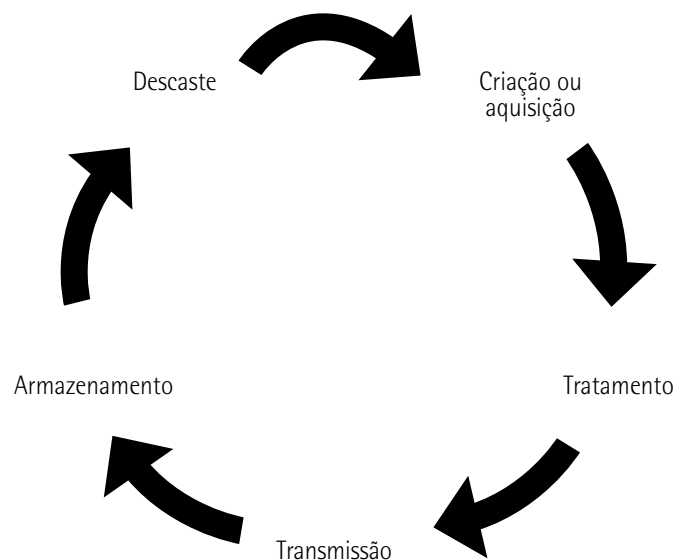


Figura 2 – Ciclo de vida da informação

Depois de ser criada ou adquirida, a informação passa por uma fase de tratamento, em que é estruturada, organizada, modificada, agrupada ou condensada, a fim de se transformar num autêntico ativo de informação.

A etapa seguinte é a transmissão, em que por algum motivo a informação é passada de um ponto a outro através de um canal de comunicação – canais estruturados, como e-mail, internet e link dedicado, e canais não estruturados, como a voz.

Na fase de armazenamento, os ativos de informação que já foram tratados ou transmitidos são guardados de forma organizada para possíveis consultas futuras. Os locais mais comuns de armazenamento são os arquivos físicos e os bancos de dados.

Na etapa de descarte, a informação, por não ser mais necessária, é excluída do rol de informações da organização. No entanto, embora ela não tenha mais importância, o descarte inadequado pode causar prejuízos à segurança da informação.

Salientamos que é na fase de transmissão que a informação corre mais risco em seu ciclo de vida. Ao ser transmitida, ela não está na posse de nenhum dos lados (emissor ou receptor), o que favorece a interceptação, a adulteração ou o furto dela pelos crackers. Por esse motivo, a primeira área corporativa a se preocupar com a segurança da informação foi a área de redes.

1.4 Classificação da informação

Classificar a informação refere-se a conhecer todos os ativos de informação e definir os que requerem maior cuidado. Quem deve fixar o valor da informação é sempre o proprietário dela.

O processo de classificação da informação consiste em organizá-la por seu grau de importância e, a partir disso, determinar quais níveis de proteção cada ativo de informação demanda. Desse modo, evitam-se a implantação desnecessária de proteção para ativos de pouca importância e a aplicação de mecanismos inferiores para ativos sensíveis ou extremamente importantes, o que os deixaria vulneráveis.

Podemos dizer que os objetivos básicos da classificação da informação são:

- **Proteção:** as organizações manipulam diversos ativos de informação, e estes podem estar em qualquer fase do ciclo de vida. Por essa razão, é necessário avaliar cada um para saber em que fase ele está e qual nível de proteção será aplicado, a fim de atingir o máximo de eficácia no uso do mecanismo de proteção.
- **Economia:** quanto maior a necessidade de proteção para o ativo, maior o investimento financeiro em mecanismos de proteção. Na prática, isso quer dizer que, se a classificação das informações estiver correta, ela proporcionará economia para a organização, uma vez que esta investirá seu dinheiro em mecanismos que protegem seus ativos mais importantes.

O processo de classificar as informações traz diversos benefícios para uma organização. Entre os benefícios tangíveis, podemos mencionar a conscientização, a responsabilidade, os níveis de proteção, a tomada de decisões e o melhor uso dos recursos.

A classificação da informação não é imutável. Como a informação tem um ciclo de vida, a classificação da informação muda conforme o estado e a importância dela. O balanço patrimonial de uma empresa, por exemplo, inicia seu ciclo de vida no nível mais alto de classificação e termina esse ciclo no menor nível de classificação possível, publicado nas mídias.

Não existe um modelo padrão para classificar a informação. Recomenda-se que sejam definidos ao menos três níveis de classificação, mas não muitos mais, para não dificultar a organização. Definir níveis auxilia na identificação e na implantação de critérios e mecanismos de proteção.

A classificação da informação pode ter diversas formas, dependendo de qual princípio ela pretende atender, e a rotulação deve seguir um ponto de vista determinado e suas exigências.

Pelo princípio de confidencialidade, o sigilo deve ser preservado, sempre de acordo com a importância das informações, a fim de que apenas as pessoas autorizadas tenham acesso a elas. Em alguns casos, manter a confidencialidade é uma exigência legal.

Algumas questões devem ser respondidas por aqueles que estabelecem a classificação da informação sob o aspecto da confidencialidade. Por exemplo: "O que aconteceria se alguém que não pudesse ter acesso à informação de repente obtivesse tal acesso?"

No que se refere à confidencialidade, as organizações podem adotar diversos esquemas de classificação das informações. Muitas recorrem a estas três categorias para facilitar a análise e a implantação de mecanismos de proteção: confidenciais, restritas e públicas.

Pelo princípio de disponibilidade, a preocupação é como recuperar as informações e como mantê-las sempre disponíveis para o acesso de usuários autorizados.

Diante desse princípio, a classificação é determinada pelo tempo que a informação pode ficar inacessível aos usuários autorizados. Assim, quanto menor o tempo que ela puder ficar inacessível, maior será a sua categoria de classificação.

O princípio de integridade tem por objetivo classificar os ativos de informação para que sob hipótese alguma sejam modificados ou adulterados.

Por último, o princípio de autenticidade, derivado do princípio de integridade, visa garantir "que a informação é legítima, criada por alguém com autoridade para fazê-lo e oriunda da fonte à qual é atribuída" (BEAL, 2005, p. 69). As informações destinadas ao público externo, por exemplo, requerem verificação da autenticidade.

A classificação de ativos físicos, softwares e serviços não é uma tarefa fácil. Geralmente, é feita com a criação de grupos de ativos, levando-se em conta limites preestabelecidos por características comuns, como tipo de usuário. A segmentação dos ativos permite criar estratégias diferenciadas de proteção.

É impossível estabelecer um modelo único de segmentação de ativos físicos, de software e de serviços capaz de atender às necessidades de todos os tipos de organização. Os esforços gastos no desenvolvimento de uma forma de classificação e segmentação desses ativos, adaptada às características e necessidades próprias do negócio, são recompensados pelo entendimento claro dos diferentes requisitos associados aos diferentes objetivos de segurança (BEAL, 2005, p. 70).

Classificar as informações leva a investir financeiramente na proteção delas e sujeitá-las a certos mecanismos de proteção. Algumas organizações criam um nível básico de proteção para todas as informações classificadas e nenhum nível de proteção para as não classificadas.

Como as informações têm vida, às vezes, é necessário reclassificá-las. Assim, é importante que as organizações disponham de processos formalizados e padronizados de reclassificação.

A desclassificação das informações acontece na etapa final de sua vida, o descarte, em que a informação é devidamente apagada por não mais ser útil à organização.

Os processos de classificação, reclassificação, desclassificação e de introdução e manutenção dos mecanismos de proteção para os ativos de informação devem ser elaborados e mantidos exclusivamente pelo proprietário da informação. Em geral, essa atribuição recai sobre os gerentes de área.

Logo abaixo do proprietário da informação vem o chamado **custodiante da informação**, aquele que de alguma forma zela pelo armazenamento e pela preservação de informações que não lhe pertencem, mas que delas faz uso em suas atividades cotidianas. Existem dois tipos de custodiante: um deles é o profissional de perfil técnico responsável pela administração e pelo funcionamento de algum sistema; o outro é o proprietário de processo, pessoa encarregada de um processo de negócio que usa informações que não lhe pertencem, mas que fazem parte do processo sob sua responsabilidade.

A equipe de segurança deve ser o ponto de apoio das áreas de negócio; deve desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos de proteção dos ativos de informação.

Os gerentes de usuários têm a responsabilidade de responder pela ação dos membros de sua equipe, e também a função de multiplicar o conceito de classificação determinado pela organização.

Por sua vez, os usuários finais dos ativos de informação são os principais responsáveis pela execução das recomendações de classificação da informação, uma vez que estão diretamente ligados ao operacional.

A implantação de mecanismos de controle após o processo de classificação visa assegurar a proteção dos ativos de informação. Os mecanismos mais comuns são os que buscam proteger a confidencialidade

das informações da organização, bem como sua integridade e sua disponibilidade. Podemos dividir esses mecanismos sob a esfera da proteção de dados, da proteção física e dos controles administrativos.

No âmbito da proteção de dados, destaca-se o uso da criptografia. Por meio desse mecanismo, é possível oferecer, de forma segura e eficaz, uma série de serviços, mantendo a confidencialidade, a disponibilidade e a integridade das informações.

O uso de cópias de segurança, também conhecidas como backups, tem a finalidade de permitir que as informações de um sistema sejam armazenadas num arquivo, com um mecanismo de recuperação em caso de falha na informação original.

Os sistemas redundantes, apesar de semelhantes aos backups, são utilizados em situações nas quais a informação processada é ainda mais crítica, não podendo a organização dispor dela mesmo que por um curto período de tempo. Equivalem a deixar um sistema secundário e semelhante à espera de que o sistema principal, por algum motivo, venha a parar de funcionar, a fim de assumir o lugar dele sem interrupções.

A implantação de controles de acesso busca proteger os dados contra problemas de segurança relacionados, principalmente, à quebra de confidencialidade e de integridade. Sua função é garantir que apenas usuários e processos autorizados tenham acesso a determinadas informações, e que estes executem somente ações previamente definidas.

Na esfera física, podemos citar estes mecanismos:

- **Catracas e portas de acesso inteligentes:** impedem a entrada em ambientes nos quais o acesso é restrito a pessoas autorizadas.
- **Cofres:** protegem os ativos de informação físicos (contratos e fitas de backup, por exemplo) contra furtos e roubos, bem como, no caso de alguns modelos especiais, contra incêndios.
- **Circuitos fechados de TV:** permitem resolver incidentes (furtos de informação, por exemplo), além de ter um caráter desencorajador.

Quando a informação é transportada fisicamente, ela corre uma série de ameaças. Por isso, o transporte seguro visa reduzir as vulnerabilidades. As proteções empregadas vão desde envelopes com lacre inviolável até carros-fortes.

Os controles administrativos, por outro lado, são as medidas associadas à forma como os procedimentos devem ser executados e à necessidade de interação entre as pessoas. As políticas são o principal controle administrativo no que se refere à segurança da informação e, através da política de classificação da informação, definem padrões de conduta, que são os passos necessários para a execução segura dos procedimentos. As políticas também alinham os mecanismos de proteção e a legislação e estabelecem uma relação jurídica para punir legalmente ações não autorizadas.

O processo de revisão e aprovação estabelece que qualquer ação individual de maior importância, do ponto de vista da segurança, deva ser realizada em mais de uma etapa, ressaltando a necessidade de que a execução e a aprovação sejam feitas por pessoas distintas, o que coíbe a tentativa de fraude.

O monitoramento das atividades é outro mecanismo de proteção relevante para descobrir falhas de segurança, e também tem um papel desencorajador.

Nas atividades cotidianas envolvidas na classificação da informação, podemos recorrer à rotulação (documentos impressos e eletrônicos) e ao controle de acesso (físico e lógico).

Quando o assunto é rotulação de documentos com vistas à classificação da informação, a primeira coisa que vem à mente são os documentos impressos, mais fáceis de rotular. A rotulação, além de inibir a ação de fraudadores, visa salvaguardar a organização em caso de violação da segurança da informação em algum nível de classificação.

Para rotular papéis, é recomendado o uso de etiquetas, carimbos, marcas visuais no rodapé de documentos ou até mesmo marca-d'água.

A rotulação de documento eletrônico requer maior atenção, e a marca da classificação deve ser mostrada no conteúdo dele. Por exemplo: e-mails precisam conter informações de classificação no corpo da mensagem ou no campo de assunto.

Sistemas e aplicativos devem mostrar visualmente o nível da classificação de um registro quando este é acessado. As mídias podem ser rotuladas com etiquetas, assim como os documentos impressos.

A segunda forma de criar mecanismos cotidianos é o controle de acesso, que pode ser feito por meio dos níveis de classificação. Essa forma de controle é o principal benefício buscado pela classificação da informação.

O controle de acesso lógico nos remete ao controle de acesso a redes e dados. Um bom exemplo é o logon: é necessário ter um nome de usuário válido e uma senha pessoal e intransferível para acessar determinado segmento de rede.

O controle de acesso físico está ligado ao uso de ferramentas criptográficas, como os certificados digitais. A biometria é outro recurso útil.



Lembrete

A classificação por si própria não consegue proteger as informações. Essa tarefa cabe aos mecanismos de proteção.

1.5 Análise e gerenciamento de riscos

Para decidir qual é o mecanismo mais eficiente na proteção dos ativos de informação, dois processos são necessários: a já vista classificação da informação, que define o que realmente é importante proteger, e a análise e o gerenciamento de riscos, que verificam perdas e impactos causados.

1.5.1 Análise de riscos

A análise de riscos parte do pressuposto de que não temos como proteger o que não conhecemos. Assim, por meio da identificação e do mapeamento dos ativos de informação, podemos escolher o mecanismo de proteção mais adequado.

Para redes corporativas, é importante avaliar os riscos de forma bem específica.

Quadro 5 – Análise de riscos para redes corporativas

Elementos envolvidos
Controle dos usuários e nível de autenticação
Sistemas e serviços criptográficos
Segurança física na empresa e no data center
Identificação dos sistemas de missão crítica
Cumprimento de normas de segurança da informação, como ISO/IEC 27001
Importância e nível de sensibilidade das informações
Riscos relativos a sistemas de comunicação
Aspectos de contingência

Adaptado de: Moraes (2010, p. 32).

A análise de riscos também tem um caráter de gestão. O custo da implantação de mecanismos de proteção é alto, e a análise de riscos consegue dimensioná-la de maneira mais eficaz.

É tarefa da análise de riscos fazer o inventário de todos os bens da empresa que precisam ser protegidos, o que engloba tanto os bens tangíveis, como ativos de informação, computadores, equipamentos de rede, impressoras e discos, quanto os bens intangíveis, como imagem da organização, gestão do conhecimento, pessoas e reputação.

Existem basicamente duas formas de análise de riscos: a quantitativa e a qualitativa.

Análise quantitativa

"Está relacionada com o lado financeiro e a estimativa de custos e valores ligados a ameaças e à proteção" (MORAES, 2010, p. 33). A grande dificuldade aqui consiste em calcular a probabilidade de que eventos ou ameaças ocorram, principalmente porque, em boa parte dos casos, os percentuais são inferiores a 1%.

A seguir, as etapas detalhadas desse processo:

- Descubra as ameaças (criminosos, terroristas, hacking, fenômenos naturais etc.) que podem afetar as operações críticas e os ativos.
- Estime a probabilidade de um evento ocorrer com base no histórico das informações e em julgamentos individuais.
- Identifique e classifique o valor, o nível de sensibilidade e a criticidade das operações. Determine as perdas ou os danos que podem acontecer se a ameaça se realizar, bem como os custos de recuperação.
- Pondere as ações por meio da análise de custo-benefício na condução da redução do risco. Elas podem incluir a implementação de novas políticas organizacionais, novos procedimentos e controles técnicos e físicos mais amplos.
- Documente os resultados e, posteriormente, crie um plano de ação.

Análise qualitativa

"É a técnica mais usada na análise de riscos, em que dados probabilísticos não são analisados, apenas uma estimativa da perda é utilizada" (MORAES, 2010, p. 34). Esse tipo de abordagem trabalha com ameaças, vulnerabilidades e mecanismos de controle.

O método qualitativo estima o risco como alto, médio ou baixo. Porque não se mensuram valores numéricos para os componentes de risco, o processo é mais rápido. Em contrapartida, é necessário que os responsáveis pela análise tenham conhecimento mais avançado sobre os componentes de risco e sobre a organização.

Se comparamos as duas metodologias, vemos que ambas têm vantagens e desvantagens. No entanto, o método qualitativo é o mais utilizado devido a sua agilidade e à facilidade de entendê-lo e implantá-lo.

1.5.2 Gerenciamento de riscos

Para lidar com os riscos, é necessário selecionar e implementar mecanismos que os reduzam. Tais medidas visam mantê-los em níveis aceitos pela organização, definidos pelos critérios de risco.

Medidas preventivas são controles que reduzem a probabilidade de uma ameaça se concretizar ou diminuem o grau de vulnerabilidade do ambiente/ativo/sistema, reduzindo assim a probabilidade de um ataque (BEAL, 2005, p. 27).

Medidas corretivas ou reativas reduzem o impacto de um ataque/incidente. São aquelas tomadas após a ocorrência de um evento.

Métodos detectivos expõem ataques/incidentes e disparam medidas reativas para evitar o dano, reduzi-lo ou impedir que ele volte a acontecer.

Diante de um risco, é possível adotar medidas para combatê-lo ou limitar suas consequências:

- **Evitar:** não expor o ativo a situações de risco.
- **Transferir:** fazer um seguro que cubra os prejuízos causados por algum impacto.
- **Reter:** fazer um autosseguro.
- **Reduzir:** implementar uma proteção que diminua o risco.
- **Mitigar:** tomar providências que diminuam apenas o impacto.



Um exemplo de medida de proteção que reduz a probabilidade de uma ameaça ocorrer é a mudança física de um data center (alvo) por causa de enchentes constantes na região.

Dependendo do caso, pode-se também **aceitar o risco**. Isso acontece quando o custo para proteger um ativo em relação a determinado risco simplesmente não vale o benefício, quando os mecanismos de proteção excedem o valor do próprio ativo de informação ou quando os riscos que o ativo está correndo ficam dentro dos critérios de aceitação definidos pela organização. Aceitar um risco não quer dizer que sua presença seja ignorada; pelo contrário, ela é reconhecida, e a decisão de aceitá-lo é considerada uma forma de tratamento do risco.

Comunicar o risco nada mais é do que divulgar as informações sobre os riscos identificados, tratados ou não, para todas as partes envolvidas.

A comunicação dos riscos é um modo de tornar responsáveis todos os que têm efetivamente que cuidar dos ativos de informação. A melhor maneira de fazer isso é de forma genérica, para evitar exposição e para fornecer a todos informações sobre os riscos organizacionais.

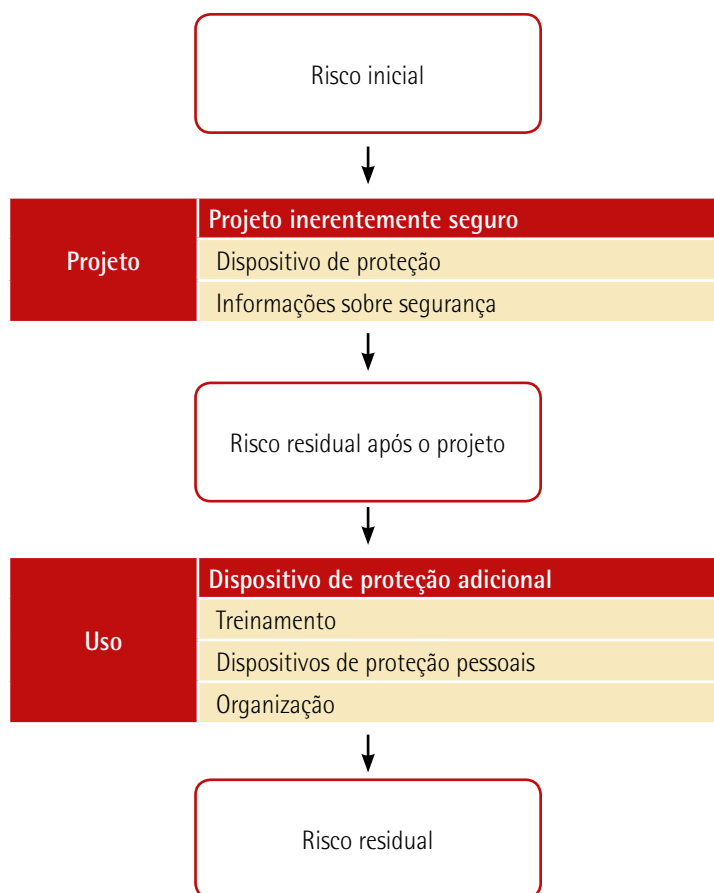


Figura 3 – Tratamento do risco

O sistema de gestão de riscos remete aos conceitos de administração, estratégia e processo decisório. A palavra **sistema**, por sua vez, remete a um conjunto organizado que trabalha em prol de um resultado comum. O sistema de gestão de riscos nada mais é do que administrar o risco criando mecanismos para identificá-lo, analisá-lo, tratá-lo e comunicar as decisões sobre as formas de geri-lo mais alinhadas com a estratégia da organização.

O conceito de gestão pressupõe a existência de um planejamento de como o risco deve ser trabalhado. Esse planejamento cria um modelo corporativo de gestão de riscos. O sistema de gestão de riscos precisa estar alinhado com os aspectos jurídicos e culturais, as práticas de mercado e as normas.

Os benefícios do uso sistemático de um programa de gestão de riscos são evidentes. Quando implantado e seguido de maneira eficiente, as organizações conseguem conhecer melhor os riscos, saber quais mecanismos têm consenso administrativo, obter maior embasamento para adotar proteções e ter uma métrica com indicadores de resultado realmente eficazes.

A introdução de um sistema de gestão de riscos nas organizações é um processo trabalhoso, que depende da cooperação de todos e da anuência da executiva da organização.

Um dos maiores desafios é conseguir aperfeiçoar o tempo dos processos sem deixar passar informações importantes e, simultaneamente, maximizar os resultados.

Muitos ativos de informação são extremamente dinâmicos, sobretudo os tecnológicos, o que dificulta a análise e pode torná-la imprecisa.

Também é necessário transpor desafios estruturais. Um exemplo é a escassez de informações. Há uma grande dificuldade em obter dados estatísticos e qualitativos sobre os ativos de informação. Essa dificuldade afeta as estimativas de probabilidade e de impacto na análise de um evento.

Outro desafio estrutural é estabelecer uma estimativa de custos. Em geral, custos diretos, decorrentes de algum problema, são relativamente fáceis de calcular. No entanto, custos indiretos, como produtividade, imagem e mercado, são bastante complexos, e, às vezes, totalmente imprecisos.

Apesar das dificuldades, a grande maioria dos especialistas em segurança da informação concorda que a implantação de um sistema de gestão de riscos é fundamental para as organizações.

A implantação de um sistema de gestão de riscos deve ser tratada como um projeto de grande porte da organização, o que vai requerer disciplina, planejamento, recursos e boa dose de jogo de cintura para lidar com os problemas que aparecerão ao longo do processo. Recomenda-se que uma metodologia de gerenciamento de projetos seja seguida.

É aconselhável que cada organização respeite suas características, como cultura e disponibilidade de recursos. Para implantar um sistema de gestão de riscos, é preciso seguir sete fases ou etapas.

A primeira consiste em **definir o escopo do projeto**, que é basicamente apresentar a justificativa dele, seus limites e o que será entregue ao final. A definição do escopo costuma ser o fator mais importante para o sucesso de um projeto.

No que tange à segurança da informação, o levantamento do escopo pode ser realizado por meio de entrevistas com os gestores de processos. Toda organização tem seus processos, uns mais críticos que outros, e cabe aos gestores de processos definir a importância deles.

A definição do escopo também inclui o plano de trabalho a ser seguido, com cronogramas, alocação de recursos e orçamentos.

Uma vez definido o escopo, é necessário **identificar as possíveis ameaças** às quais cada ativo está sujeito. Essa fase é crítica. Grande parte dos profissionais procura trabalhar com uma lista completa e, para isso, empreende uma busca interminável na internet. Vale, portanto, tomar alguns cuidados:

- **Trabalhe com ameaças genéricas:** em vez de relacionar uma infinidade de ameaças, trabalhe com a indisponibilidade de sistema (erro de usuário, falha de sistema, contaminação por vírus etc.). O motivo para adotar essa estratégia reside no fato de que assim os problemas de indisponibilidade serão tratados de forma semelhante.

- **Mantenha o foco nas ameaças mais comuns:** o número de ameaças que podem assolar um ativo é infinito. Por isso, concentre-se nas ameaças mais comuns, que representam cerca de 80% dos casos de incidentes de segurança.
- **Utilize listas prontas de possíveis ameaças:** criar uma lista própria demanda tempo e pessoal habilitado. É bem mais simples e barato utilizar listas elaboradas e mantidas por grupos de pesquisa, institutos e comunidades, ou inseridas em softwares de gestão de riscos.

O próximo passo é **estimar a probabilidade de ocorrência das ameaças**. Isso pode ser feito por meio de dois fatores: frequência e vulnerabilidade.

A frequência representa o número de vezes que se espera que uma ameaça tentará causar dano a um ativo. Independentemente desse número, ela só terá êxito se conseguir explorar alguma vulnerabilidade.

A vulnerabilidade, como já visto, é a ausência de mecanismos de proteção ou a falha num mecanismo de proteção existente. Para analisar as vulnerabilidades, é preciso identificar as falhas ou ausências de proteção para determinado ativo. Essa tarefa, porém, não é fácil, principalmente em relação aos componentes de TI (tecnologia da informação). Para estes, é recomendado o uso de ferramentas que capturam as vulnerabilidades de maneira automatizada. Algumas dessas ferramentas têm listas com pontos de verificação para os ativos.

Seguindo no processo de implantação da gestão de riscos, encontramos a etapa de **estimar o impacto das ameaças**, que se refere a avaliar o impacto que a concretização de uma ameaça pode causar em determinado ativo. Diferentes ameaças causam diferentes impactos, e quanto maior o número de ameaças, maior o risco. O valor do ativo de informação para a organização também deve ser levado em conta. Esse valor é demonstrado por seu valor absoluto (o preço para adquirir outro igual) ou relativo (o benefício que ele traz).

Estimado o impacto das ameaças, é necessário **identificar os ativos de maior risco**. Nesse momento, já estão devidamente documentados os processos do negócio, as ameaças às quais os ativos estão sujeitos e a probabilidade de as ameaças se concretizarem. Estão preparados, assim, os componentes para o cálculo do risco. Os ativos que correm mais risco devem ser priorizados na implantação dos mecanismos de proteção. Isso, no entanto, não é uma regra, uma vez que as organizações podem optar por mecanismos secundários para ativos de maior importância, isto é, por mecanismos que sanem a vulnerabilidade em mecanismos já instalados, os quais recebem, portanto, apenas um complemento.

Depois de identificar os ativos de maior risco, entramos na fase de **avaliar as melhores proteções**. Qualquer profissional de segurança da informação sabe que todos os ativos de informação estão sujeitos a algum tipo de risco; sabe, ao mesmo tempo, que os recursos destinados à proteção deles são limitados e, às vezes, mal permitem alcançar patamares aceitáveis em relação ao que estabelecem os critérios de risco.

A escassez de recursos obriga os profissionais a priorizar os riscos maiores. A quantidade de ativos que poderá ser priorizada vai depender de dois fatores: a disponibilidade de recursos e a eficácia no uso dos recursos disponíveis. A eficácia está relacionada à capacidade dos profissionais de segurança de escolher as proteções que tenham melhor custo-benefício.

Existem diversas formas de avaliar o custo-benefício das proteções que serão implantadas. Vejamos um exemplo:

- Primeiro, estime o que a organização perderá em um ano, levando em conta o impacto e a probabilidade de as ameaças se concretizarem.
- A seguir, avalie as soluções disponíveis para resolver ou amenizar o problema. Essa fase divide-se em três momentos:
 - Estime as perdas a que a organização estará sujeita após a implementação da proteção. Dessa forma, conhecerá exatamente o percentual do montante original que a proteção ajudará a reduzir.
 - Com o percentual bruto gerado, calcule o percentual líquido para determinado período, considerando os custos ligados à implementação da ferramenta.
 - Com o percentual líquido, identifique quanto será o aporte financeiro inicial para a implementação da proteção. Caso o montante seja maior do que o que espera economizar, o investimento no mecanismo de proteção ficará inviável.
- Depois de checar a "sanidade" do investimento, implemente as proteções escolhidas.
- Por último, defina e monitore as métricas, a fim de averiguar se os mecanismos escolhidos e implementados estão realmente atingindo os índices de eficiência estipulados. Uma estimativa mal elaborada pode ter o resultado inverso: em vez de proteger o ativo de informação, deixá-lo ainda mais vulnerável.

A última etapa do processo da implantação da gestão de riscos é **implementar as proteções**, o que pode durar vários meses e demandar atividades que afetarão o cotidiano da empresa.



Observação

A implantação dos mecanismos de proteção interfere no cotidiano da rede. Por essa razão, recomenda-se a utilização de planos de teste, homologação e gerenciamento de mudanças para a conclusão do processo.



Resumo

Nesta unidade, vimos os principais fundamentos da segurança da informação. Abordamos as ideias de integridade, confidencialidade, controle de acesso, disponibilidade, não repúdio e auditoria. Consideramos o ciclo de vida da informação, enfatizando que o ponto crítico desse ciclo é a transmissão.

Discutimos também a classificação da informação, cujos benefícios incluem a conscientização, a responsabilidade, os níveis de proteção, a tomada de decisões e o melhor uso dos recursos. Assinalamos que a classificação precisa estar atenta ao ciclo de vida da informação, adaptando-se constantemente a ele. Classificar é o primeiro passo para identificar vulnerabilidades, ameaças, agentes e riscos no cenário da rede analisada.

O auge da segurança é o gerenciamento de riscos, isto é, a seleção e a implementação de mecanismos que os reduzam. Esses mecanismos têm por objetivo mantê-los em níveis aceitos pela organização, definidos pelos critérios de risco. Apresentamos, por fim, os passos necessários para estabelecer um sistema de gestão de riscos.

[illegible]