# SEGURANÇA DE DADOS E REDES

Thálisson de Oliveira Lopes

INFORMAÇÃO E COMUNICAÇÃO

NT EDITORA

# SEGURANÇA DE DADOS E REDES

Thálisson de Oliveira Lopes

INFORMAÇÃO E COMUNICAÇÃO

NT EDITORA

**Autor**

Thálisson de Oliveira Lopes

Graduação em Tecnologia em Processamento de Dados (2007), Especialista em Gestão de Tecnologia da Informação (2008 e 2010) e Mestre em Gestão do Conhecimento e Tecnologia da Informação (2013). Experiência na área de educação a distância, produção de softwares desktop e web, atuando principalmente nos seguintes temas: Gestão de Tecnologia da Informação, Gerenciamento de Projetos, Engenharia de Software, Desenvolvimento de Sistemas, PHP, RIA, ActionScript, Adobe Flash e Adobe Flex.

**Design Instrucional**
NT Editora

**Projeto Gráfico**
NT Editora

**Revisão**
NT Editora

**Capa**
NT Editora

**Editoração Eletrônica**
NT Editora

**Ilustração**
NT Editora

**NT Editora, uma empresa do Grupo NT**
SCS Quadra 2 – Bl. C – 4° andar – Ed. Cedro II
CEP 70.302-914 – Brasília – DF
Fone: (61) 3421-9200
sac@grupont.com.br
www.nteditora.com.br e www.grupont.com.br

Lopes, Thálisson de Oliveira.
Segurança de dados e redes / Thálisson de Oliveira Lopes – 1. ed. – Brasília: NT Editora, 2014.
86 p. il. ; 21,0 X 29,7 cm.

ISBN 978-85-8416-149-2

1. Rede. 2. Dados. 3. Criptografia.
I. Título

Copyright © 2014 por NT Editora.
Nenhuma parte desta publicação poderá ser reproduzida por qualquer modo ou meio, seja eletrônico, fotográfico, mecânico ou outros, sem autorização prévia e escrita da NT Editora.

## ÍCONES

Prezado(a) aluno(a),
Ao longo dos seus estudos, você encontrará alguns ícones na coluna lateral do material didático. A presença desses ícones o(a) ajudará a compreender melhor o conteúdo abordado e a fazer os exercícios propostos. Conheça os ícones logo abaixo:

**Saiba mais**
Esse ícone apontará para informações complementares sobre o assunto que você está estudando. Serão curiosidades, temas afins ou exemplos do cotidiano que o ajudarão a fixar o conteúdo estudado.

**Importante**
O conteúdo indicado com esse ícone tem bastante importância para seus estudos. Leia com atenção e, tendo dúvida, pergunte ao seu tutor.

**Dicas**
Esse ícone apresenta dicas de estudo.

**Exercícios**
Toda vez que você vir o ícone de exercícios, responda às questões propostas.

**Exercícios**
Ao final das lições, você deverá responder aos exercícios no seu livro.

**Bons estudos!**

## Sumário

# APRESENTAÇÃO

A segurança da informação é um elemento de vital importância para o acompanhamento do crescimento de transações *online* – intranet, internet ou extranet –, e do uso de redes de computadores, pois hoje, é quase impossível para as corporações manterem uma comunicação eficiente entre filiais, clientes (interno ou externo) e prestadores de serviços, sem o auxílio destas tecnologias.

A internet, da mesma forma que torna possível toda esta comunicação, seja pela disponibilização da informação em sites e/ou portais, ou pela utilização do seu meio físico de comunicação para a implantação de redes privadas utilizando, por exemplo, a tecnologia VPN, também abre portas para a entrada de possíveis invasores com o objetivo de destruir, roubar ou simplesmente invadir a privacidade dos usuários de determinada rede.

Quando organizações privadas ou governamentais têm suas redes invadidas, gera-se uma insegurança entre seus clientes e usuários, afetando diretamente a reputação e os resultados comerciais destas organizações. Sendo assim, o principal ponto de ação da segurança da informação deve ser: proteger os servidores e os dados neles armazenados; proteger a informação que trafega entre servidores e usuários; proteger as informações existentes nos computadores dos usuários, sejam elas de propriedade da organização ou do usuário.

O principal objetivo deste livro é capacitá-lo a identificar os pontos de risco existentes na rede de uma organização, bem como a elaborar e a implantar uma política de segurança adequada para a organização.

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

# 1 INTRODUÇÃO

## 1.1 Histórico

O grande "estouro" da informática iniciou-se na década de 80 com o advento do computador pessoal. Da mesma forma que invadiu as residências, o computador proliferou nas empresas, multiplicando as UCPs e criando o processamento distribuído.

O processamento distribuído, contudo, só permitia a comunicação entre a UCP central, operando como host, e uma UCP remota, mas não entre as UCPs remotas. Notou-se logo a necessidade desta comunicação entre unidades de processamento, que permitiria uma maior eficiência e rapidez no trânsito da informação.

A solução desse problema nasceu com as redes de computadores. Um conceito que traduz bem o significado da expressão: rede de computadores é o seguinte:

> "Rede de computadores é um conjunto de computadores autônomos, interconectados através de um determinado meio podendo ou não ter um servidor central, capaz de trocar informações e compartilhar recursos".

Como esperado, as redes de computadores proporcionaram um ganho de desempenho nas empresas que as adotaram. E a área de redes, assim como os demais setores da informática, evoluiu substancialmente nos últimos anos.

As redes são hoje uma realidade e já constituem uma necessidade básica. É quase impossível pensar em uma empresa cujos computadores não estejam interconectados. Entre os benefícios proporcionados pela implantação de uma rede, podem ser citados:

- Compartilhamento de recursos, tais como, impressoras, bancos de dados, etc.;
- Transferência de informações;
- Meio de comunicação alternativo com a utilização de mensagens eletrônicas;
- Redução dos custos relativos a investimentos e *upgrades*.

Contudo, a popularização das redes de computadores trouxe consigo grandes preocupações em termos de segurança, como a perda de informação decorrente de falhas na comunicação interna à rede e o acesso de usuários não autorizados ao sistema.

**Computador Pessoal**: Derivado do inglês *Personal Computer* – PC.

**UCP**: Sigla do inglês CPU – *Central Processing Unit*, com sua tradução para língua portuguesa, Unidade Central de Processamento.

**Host**: Em informática um host é qualquer máquina cuja comunicação é obtida por meio de uma conexão direta em rede, como computadores pessoais, impressoras, roteadores, etc.

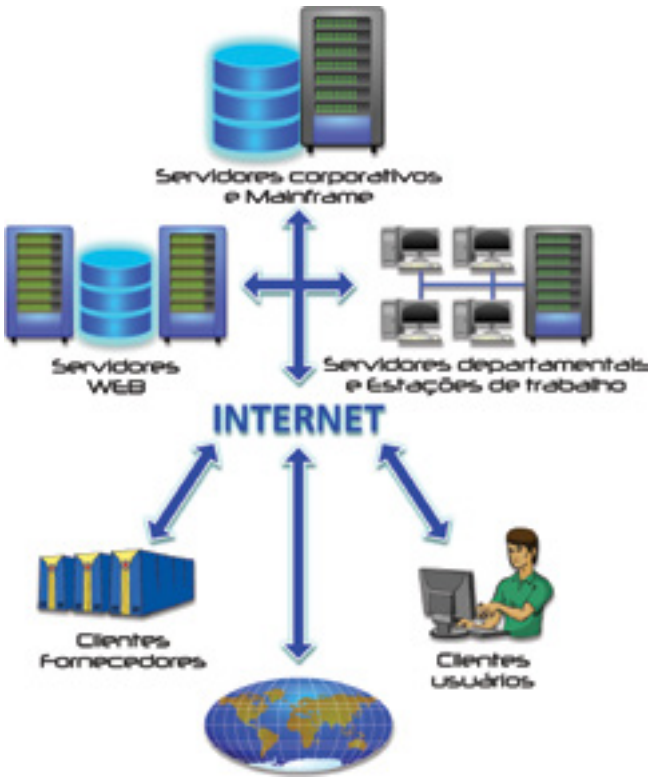
Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

## 1.2 Redes de computadores – um panorama global

Servidores corporativos e *mainframes* são mais comuns em grandes redes locais e em redes de grande área de abrangência, devido ao seu elevado custo e capacidade.

Servidores departamentais são computadores de média capacidade que, entre outras atividades, podem gerenciar intranets, pequenas redes locais, prover serviços de rede, etc.

Servidores web estão ligados à grande rede mundial, oferecendo serviços e disponibilizando arquivos e páginas.




Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

Do outro lado da internet, empresas e usuários domésticos acessam a rede e, por meio dela, chegam à ambientes de outras redes de computadores.

E é neste ponto que nasce um grande problema: o trânsito e o armazenamento de informações em computadores ligados a redes deixam essas mesmas informações vulneráveis, tanto a erros acidentais de usuários descuidados, quanto a ataques diretos de pessoas movidas por má-fé, ou simplesmente interessadas em invadir sistemas alheios e bisbilhotar arquivos com conteúdos privados.

## 1.3 Informação e segurança

A segurança da informação torna-se um elemento de vital importância no contexto atual, consistindo na proteção às informações arquivadas em computadores contra ações não autorizadas relativas à sua divulgação, transferência, modificação ou destruição intencional ou acidental.

Informação, de acordo com o *Dicionário Aurélio da Língua Portuguesa* é um conjunto de conhecimentos sobre alguém ou alguma coisa. Conforme o *Dicionário Houaiss da Língua Portuguesa* é o conhecimento obtido por meio de investigação ou instrução. Mensagem suscetível de ser tratada pelos meios informáticos; conteúdo dessa mensagem. Já para a NBR ISO/IEC 17799 a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida. Ela pode existir em muitas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, mostrada em filmes ou falada em conversas.

**NBR ISO/IEC 17799**: Norma ISO para segurança da informação.

**Ativo**: Tudo aquilo que manipula a informação, inclusive ela própria: infraestrutura, tecnologia, aplicações, informações e pessoas.

Segurança, para o Dicionário Aurélio da Língua Portuguesa é o estado, qualidade ou condição de seguro. Condição daquele ou daquilo em que se pode confiar. Certeza, firmeza, convicção. Segundo a NBR ISO/IEC 17799, significa proteger a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio. Seja qual for a forma apresentada ou o meio pelo qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

## 1.4 Conceito básico de segurança da informação

Para a NBR ISO/IEC 17799, segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação, esses formam os três princípios básicos, podendo acrescentar também princípios adicionais, autenticidade, irretratabilidade (nãorepúdio), privacidade, consistência, isolamento, auditoria e legalidade. A seguir, serão abordados alguns destes conceitos:

- **Confidencialidade** é a garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;
- **Integridade** é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- **Disponibilidade** é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Autenticidade** é a garantia da origem da informação;
- **Irretratabilidade** é a garantia da impossibilidade de negação da origem da informação;
- **Legalidade** é a conformidade com a legislação vigente.

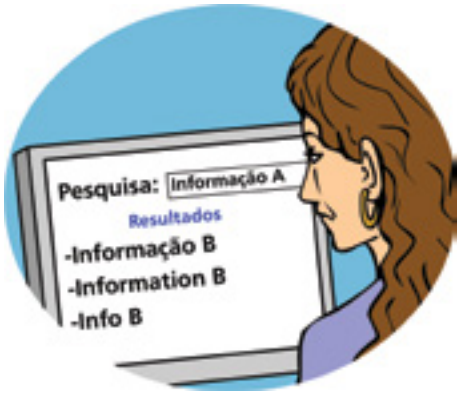
Você deve começar a se habituar a todos estes termos, pois eles representam algumas das preocupações necessárias para se garantir a segurança da informação em redes de computadores, e serão revistas ao longo deste livro.

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

Uma informação para ser considerada segura precisa manter seus aspectos de confidencialidade, integridade e disponibilidade. A ausência de qualquer destes aspectos pode causar prejuízos, com consequências diversas para cada caso.

**Exemplo**


Suponha que exista uma informação "A" em um sistema.




Em um dado momento, um usuário acessa o sistema em busca da informação "A" mas recebe a informação "B".

Isso significa que a segurança da informação foi quebrada em termos de integridade. Assim, o usuário pode acabar transmitindo uma informação errada adiante, baseado no dado que recebeu, levando a uma decisão errada e posterior perda de credibilidade do sistema.

Digamos que o problema de integridade tenha sido resolvido. O mesmo usuário retorna ao sistema em busca da informação "A" mas, ao procurar o arquivo correspondente, não consegue mais acessá-lo.

Neste caso, a segurança foi quebrada por uma questão de disponibilidade. Este usuário, na melhor das hipóteses, perderá produtividade aguardando suporte técnico para resolver seu problema.

Imagine que o departamento técnico foi acionado e a informação está finalmente disponibilizada. Outro usuário vagando pela rede esbarra na informação "A", este não é um usuário autorizado, mas o arquivo é aberto sem problema.

A segurança foi, então, quebrada quanto ao aspecto da confidencialidade. Uma pessoa agindo com interesses escusos poderia fazer mau uso da informação assim conseguida. Neste caso, houve uma falha na segurança do sistema, você deverá tomar medidas necessárias para proteger as informações.

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

## 1.5 Ciclo de segurança

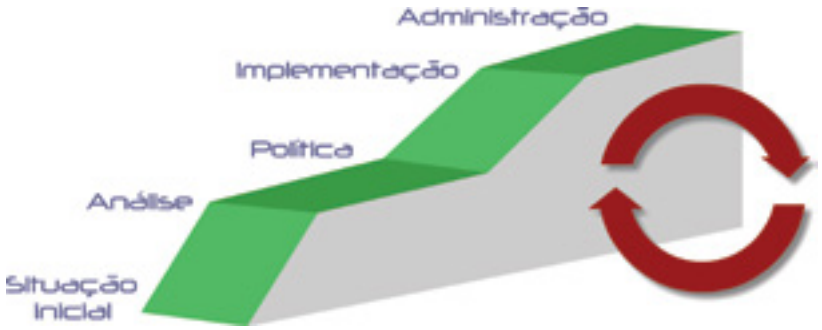
No exemplo apresentado, devem ser tomadas medidas de segurança necessárias para proteger os ativos. Estes apresentam vulnerabilidades que permitem ameaças, que causam a perda de integridade, confidencialidade e disponibilidade, gerando impactos no negócio, que, por sua vez, são a razão de se tomar novas medidas de segurança, completando o ciclo.


Cada etapa deste ciclo expõe a informação ao risco de possíveis danos, até que ele seja reduzido pelas medidas de segurança.

## 1.6 Riscos, ataques e ameaças

A primeira medida de segurança é a análise de riscos, que visa identificar vulnerabilidades e ameaças, associando-as aos bens de informação, identificando o impacto, em caso de sua ocorrência, e sugerindo contramedidas. A partir desta análise, é traçada uma política de segurança com a definição das medidas a serem tomadas, e em seguida, aplicam-se estas medidas.

Durante a administração ou manutenção das medidas de segurança, surgirão novos riscos, fazendo com que se retorne à situação inicial.




**Vulnerabilidades**: Fraqueza ou inexistência de controles visando à redução de riscos.

**Ameaças**: Evento indesejável que pode ocorrer devido à existência de vulnerabilidades.

**Risco**: probabilidade de um fato. No caso de segurança, probabilidade de concretização de ameaça.

**Dano**: impacto no negócio quando se concretiza uma ameaça.

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

## 1.7 Tipos de segurança na prática

Segurança de computadores é a proteção da informação armazenada nos sistemas de computação, podendo incluir desde processos administrativos e uso de senhas até recursos de sistemas operacionais e proteção da informação.

Segurança das comunicações é a proteção da informação enquanto a mesma está sendo transmitida por meio de enlace telefônico, micro-onda, satélite ou outros meios, visando proteger o acesso pela da rede ou os dados durante a transmissão.

Segurança física é a proteção dos equipamentos de computação contra danos causados por desastres naturais e intrusos físicos, garantindo a integridade dos ativos da empresa que se encontram sob controle dos sistemas computadorizados. Para garantir a segurança física, você deve atender a alguns itens básicos:

- Evitar prédios próximos a depósitos inflamáveis ou sujeitos a inundação;
- Manter atenta vigilância contra incêndios, instalando equipamentos como extintores e sensores de gás e fogo;
- Evitar que cabos de eletricidade e de lógica compartilhem o mesmo duto;
- Garantir energia para os computadores no caso de blackouts por meio de no-breaks e geradores.

Estas são recomendações bastante genéricas. Para se ter um plano de proteção, consequentemente, uma segurança eficaz, é preciso ter em mente as diversas maneiras pelas quais você pode ser atacado e sofrer algum tipo de dano.

## 1.8 Tipos de ataque

**Interrupção**: Consiste na interrupção da prestação de serviços impedindo que a informação continue chegando ao receptor, o que afeta a disponibilidade.


**Modificação**: Consiste no desvio da informação e o seu posterior reenvio, ficando disponível para um usuário não autorizado, que poderá até mesmo substituí-la por outra, o que afeta a confidencialidade e a integridade.


Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

**Fabricação**: Consiste na criação e envio de dados falsos ou incorretos, o que afeta a integridade da informação.


**Negação**: Consiste na obstrução da prestação dos serviços antes mesmo de estabelecida a conexão, impedindo que a informação deixe o emissor, o que afeta a disponibilidade.


**Interceptação**: Consiste na captura de uma cópia da informação, possibilitando a disponibilização para usuários não autorizados, o que afeta a confidencialidade.


## 1.9 Avaliação de riscos

Para se ter uma ideia do que estes ataques podem representar, basta ter em mente o que a ausência da segurança de redes põe em risco.

Ameaça é qualquer fato capaz de impedir o pleno funcionamento de um negócio. Expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo da informação.

Vulnerabilidade é a possibilidade de sofrer uma ameaça. Fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque.

Risco é a probabilidade de concretização de uma ameaça. Combinação da probabilidade de um evento e sua consequência.

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

**São exemplos de ameaças a uma rede de computadores:**

- Sniffers;
- Spoofing de endereços;
- Vírus;
- Código Java e ActiveX maliciosos;
- E-Mail falso;
- SYN Flood;
- Ping alterado;
- Alteração de DNS;
- Alteração de roteamento;
- ICMP alterado;
- Ataque a aplicações;
- FTP alterado;
- UDP bomb.

**São vulnerabilidades de uma rede de computadores:**

- Falhas intrínsecas da arquitetura de sistemas operacionais e aplicações;
- Falhas e *bugs* de sistemas operacionais;
- Deficiências na infraestrutura de comunicação;
- Falta de proteção de conteúdo;
- Falhas na definição da política de segurança;
- Falhas na implementação da política de segurança;
- Falhas e deficiências nos serviços de rede: FTP, HTTP, ICQ, POP3, SMTP, etc.

**São tipos de riscos de uma rede de computadores:**

- Roubo de informações;
- Alteração de informações;
- Perda de dados;
- Pichamento de sites;
- Uso interno indevido;
- Perda de produtividade;
- Sabotagem;
- Fraude financeira;
- Violação de correio eletrônico;
- Interrupção de funcionamento (denial-of-service).

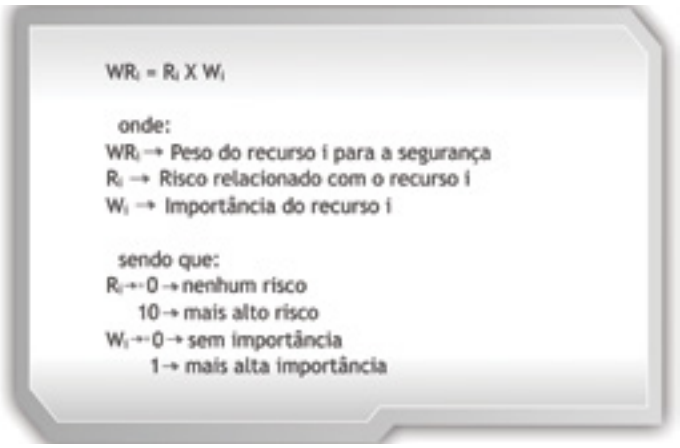
Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

É preciso sempre ter em mente que cada caso expõe o ativo a diferentes riscos e, portanto, requer diferentes medidas. Esta é a base da avaliação de riscos que deve começar com uma série de perguntas básicas, cujas respostas comporão o cerne do projeto de segurança. As principais perguntas são:

- Quais são os riscos potenciais?
- Quais seriam os custos de prevenção desses riscos?
- Quais seriam os custos de recuperação, caso os ataques se concretizassem?
- O que é necessário proteger? De quem? Como?

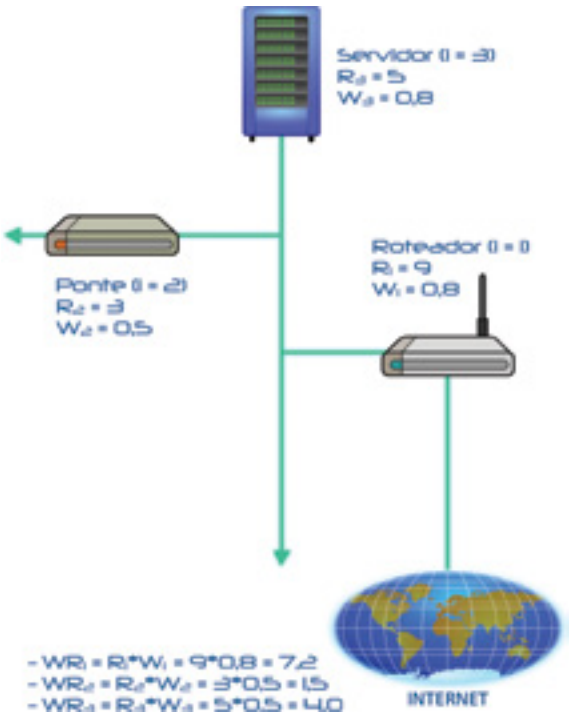

Depois do levantamento inicial, passa-se à ordenação das prioridades que, em termos de segurança, está baseada em duas variáveis principais: o risco em si e o impacto deste no negócio.

Você pode calcular a importância individual de um determinado recurso para a segurança pela análise de risco. Basta aplicar a fórmula:




No caso da rede apresentada na figura a seguir, o roteador é o recurso mais crítico para a segurança. Com base na fórmula anterior, observe, na parte inferior da figura, o resultado da avaliação de riscos de cada ponto ( i ).

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.




## 1.10 Projeto de segurança

Depois de toda esta teoria, você está apto a iniciar o planejamento de um projeto de segurança. Basicamente, ele deve definir mecanismos e sistemas com capacidade para bloquear tudo o que não é explicitamente permitido e, ainda, controlar, examinar e auditar tudo aquilo que for permitido. Ao desenvolver um projeto de segurança, você precisa ter em mente uma solução corporativa e as ferramentas de proteção a serem utilizadas.

Uma solução corporativa de segurança consiste em um conjunto de medidas tomadas por uma entidade para garantir a segurança da informação. Entre as medidas, destacam-se:

- Controle centralizado e auditabilidade;
- Ambiente padronizado;
- Política de segurança;
- Conhecimento de ameaças e vulnerabilidades;
- Pessoal técnico capacitado;
- Velocidade na implementação de soluções; e
- Integração com o negócio.

Há dois principais métodos de se alcançar uma solução corporativa:

**Top-down** (de cima para baixo): O primeiro passo é a análise da situação corporativa; a seguir, procede-se uma identificação das prioridades e, finalmente, é traçado um plano de ação;

**Bottom-up** (de baixo para cima): Começa-se com a seleção de aplicações estratégicas; depois, adota-se uma metodologia e, por fim, implementa-se a solução completa.

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

Uma das medidas mais importantes de uma solução corporativa é a política de segurança da informação e para que ela seja realmente efetiva, os seguintes elementos são fundamentais:

- *Firewall*;
- Controle de acesso;
- Segurança do *host*;
- Criptografia.

Além da política de segurança, algumas ações complementares relativamente simples podem contribuir para a solução corporativa de segurança:

- Padrões de configuração;
- Política de *backup*;
- Política de contas;
- Política de senhas; e
- Monitoração.

Os diversos tipos de riscos exigem diferentes ferramentas para combatê-los. Além de saber da existência das várias ferramentas, é preciso escolher as mais adequadas ao seu projeto de segurança.

Selecionar os recursos mais eficientes para cada caso torna-se mais simples se os seguintes aspectos forem considerados:

- Avaliar a real necessidade;
- Avaliar a capacidade da rede;
- Integração com sistemas herdados;
- Definir metas e objetivos;
- Mapear a experiência da equipe;
- Identificar as limitações existentes;
- Elaborar uma política de segurança.

Um projeto de segurança fornece proteção principalmente por meio de três aspectos: controle de acesso ao sistema; controle de acesso aos dados; administração da segurança e do sistema.

**Criptografia**: Do grego "kriptós" que significa escondido, oculto, mais "gráfho", que significa grafia, escrita, é a arte ou ciência de escrever em códigos, de forma que apenas o destinatário decifre e compreenda a mensagem.

## Controle de acesso ao sistema

- Garantir que pessoas não autorizadas não tenham acesso ao sistema;
- Conscientizar os usuários autorizados (modificação periódica de senhas, etc.);
- Proteger arquivos de dados de senhas;
- Registrar quem está fazendo o que no sistema (quem se conecta ao sistema, quem abre arquivos, quem utiliza privilégios especiais, etc.).

## Controle de acesso aos dados

- Monitorando quem acessa que tipo de dado e com que propósito;
- Determinando, quando necessário, quais usuários podem ler ou modificar seus dados;

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

- Determinando regras de acesso baseadas no nível de segurança dos usuários;
- Detalhando a política de segurança.

### *Administração da segurança e do sistema*

- Definindo as responsabilidades do administrador do sistema;
- Treinando os usuários corretamente;
- Monitorando os usuários de forma a garantir que as regras definidas na política de segurança estejam sendo seguidas;
- Identificando as falhas de segurança do sistema e especificando mecanismos para corrigi-las.

## Exercitando o conhecimento

Analise as frases a seguir, que transmitem ideias importantes sobre a segurança de um modo geral e em redes de computador.

( ) "Soluções isoladas não protegem o negócio. Por exemplo, de nada adianta ter um *firewall* se ele não estiver inserido em um projeto mais amplo".

( ) "O poder de proteção do projeto de segurança está associado ao seu elo mais fraco, não importando quão protegidos estejam os demais".

( ) "Segurança não é somente um problema de tecnologia, é a gestão inteligente da informação em todos os ambientes".

( ) "O objetivo não é ter um *patchwork* (uma colcha de retalhos) de segurança, mas sim um *framework* (estrutura fundamental) de segurança".

( ) "Não basta apenas implantar a segurança: é preciso também operá-la, mantê-la e auditá-la".

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

## Exercícios

**Questão 1** – Os princípios básicos da segurança da informação são:

a) consistência, integridade e isolamento;

b) privacidade, irretratabilidade e integridade;

c) disponibilidade, integridade e confidencialidade;

d) integridade, isolamento e disponibilidade.

**Questão 2** – A propriedade que permite identificar usuários em sistemas é a:

a) integridade;

b) irretratabilidade;

c) autenticidade;

d) privacidade.

**Questão 3** – Para o comércio eletrônico, a garantia de que o comprador não irá negar a autoria da transação efetuada é de vital importância. A propriedade que evita a negação de autoria de uma transação digital é denominada:

a) integridade;

b) consistência;

c) isolamento;

d) irretratabilidade.

**Questão 4** – _____ são tipos de ataques que afetam a disponibilidade.

a) Negação e interrupção.

b) Fabricação e modificação.

c) Modificação e negação.

d) Interrupção e interceptação.

**Questão 5** – Se um vírus altera uma parte de um arquivo de seu computador pessoal, este é um problema de:

a) consistência;

b) privacidade;

c) disponibilidade;

d) integridade.

Parabéns, você finalizou esta lição!

Agora responda às questões ao lado.

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.

**Questão 6** – _____ são tipos de ataques que afetam a confidencialidade.

a) Fabricação e modificação.

b) Interceptação e modificação.

c) Modificação e negação.

d) Negação e interrupção.

**Questão 7** – A probabilidade de concretização de uma ameaça é chamada de:

a) vulnerabilidade;

b) risco;

c) ameaça;

d) erro ou falha.

**Questão 8** – São ações complementares que podem contribuir para a solução corporativa de segurança:

a) política de senhas e monitoração;

b) segurança do *host* e pessoal técnico capacitado;

c) alteração de informações e política de contas;

d) integração com o negócio e *firewall*.

**Questão 9** – _____ não é um tipo de risco de uma rede de computadores.

a) A alteração de informações;

b) A deficiência na infraestrutura de comunicação;

c) O uso interno indevido;

d) A fraude financeira.

**Questão 10** – Um *bug* num sistema operacional de rede é um caso típico de:

a) ataque;

b) erro ou falha;

c) vulnerabilidade;

d) ameaça.

Reprodução proibida. Copyright © NT Editora. Todos os direitos reservados.