

3

Princípios da Segurança da Informação

Para começar

Como já aprendemos os conceitos gerais sobre a segurança da informação, neste capítulo vamos explorar e conhecer mais detalhadamente os princípios básicos da garantia desta segurança e quando ocorrem as violações destes princípios. Vamos estudar também as vulnerabilidades que podem e devem ser combatidas para a manutenção dos princípios, e o que são e como atuam as políticas de segurança da informação na garantia também destes princípios.

São três os princípios que orientam e sustentam a segurança da informação, quais sejam:

- 1) Integridade;
- 2) Confidencialidade;
- 3) Disponibilidade.

3.1 Princípio da integridade de informação

O primeiro dos três princípios da segurança da informação que estudaremos é a integridade.

É ela que garantirá que a informação não será alterada de forma não autorizada. Portanto, é íntegra, mas com um detalhe a ser considerado: íntegra não significa exata. Ou seja, com uma informação podemos ter integridade, mas não exatidão. Por outro lado, não podemos ter exatidão sem integridade.



Figura 3.1 – Integridade 1.

O controle da integridade deve proteger a informação de ameaças involuntárias ou intencionais, controlando os direitos de acesso, bloqueando os acessos indevidos de pessoas não autorizadas.

Para considerarmos uma informação íntegra, ela não pode ter sido alterada de forma indevida ou não autorizada. Por exemplo, o valor de seu salário bruto no sistema de folha de pagamento com valor diferente e menor do que o do mês passado. Neste caso, ele pode ter sido alterado por erro de operação (manutenção indevida de dados) ou por um funcionário mal-intencionado que modificou os valores nos bancos de dados da empresa.

A integridade da informação é fundamental para os negócios da empresa e para a comunicação interna ou com outras empresas.

Quem recebe uma informação necessita ter a segurança de que a informação recebida, lida ou ouvida é exatamente a mesma que foi colocada à sua disposição por quem a emitiu para esta finalidade.

Ser íntegra significa estar em seu estado original, sem ter sofrido qualquer alteração por alguém não autorizado. Se uma informação sofre alterações em sua versão original, ela perde sua integridade, levando a erros e fraudes, prejudicando a comunicação e os processos de decisão de uma empresa como um todo. Isto não significa que uma informação original não possa ser alterada, mas que qualquer alteração só pode ser feita por pessoa autorizada, ou seja, com direito de acesso e alteração de uma informação.

A perda de integridade ocorre quando uma informação é corrompida, falsificada, indevidamente alterada, ou excluída. Por exemplo, você acessa seu banco pela internet e seu saldo aparece zerado, sem que tenha ocorrido nenhuma movimentação da conta, ou simplesmente sua conta desapareceu e você recebe uma mensagem de que a conta não existe ou é inválida. Isso seria um caso de perda de integridade.

Uma informação poderá ser alterada de várias formas, tanto em seu conteúdo quanto no ambiente que lhe oferece suporte, isto é, o ambiente onde se encontra armazenada. Desta forma, a perda de integridade de uma informação poderá ocorrer sob duas formas:

- » Alterações do conteúdo dos dados;
- » Quando forem realizadas inclusões, alterações ou exclusões de parte de seu conteúdo;
- » Alterações no ambiente que oferece suporte ou armazena a informação.

Isto acontece quando são realizadas alterações na estrutura física e/ou lógica onde a informação está armazenada, seja nos sistemas e programas que apresentam a informação, seja nas estruturas de bancos de dados que armazenam estes dados.

Para garantirmos a integridade das informações temos de assegurar que apenas as pessoas ou sistemas autorizados possam fazer alterações na forma e no conteúdo de uma informação ou que alterações causadas por acidentes ou defeitos de tecnologia não aconteçam também no ambiente de hardware (computadores, servidores, meios magnéticos de armazenagem) e comunicações (redes) no qual ela é armazenada e pela qual transita.

Em síntese, integridade significa que nos dados originais nada foi acrescentado, retirado ou modificado.

A integridade de informações também diz respeito ao nível de confiança das informações do banco de dados, ou seja, a credibilidade e a lógica das informações.

Regras de restrição de integridade configuram um banco de dados a ser alimentado por informações com características lógicas específicas, validadas antes do seu armazenamento, diminuindo a probabilidade de falta de integridade no banco de dados. Estes aspectos são tratados no projeto e modelagem de dados em um processo de desenvolvimento de sistema de informações.

Para revermos o que é a quebra de integridade, citamos:

- » Um funcionário que modifica o valor do seu salário sem autorização no sistema de RH;
- » Um vírus modifica arquivos em um computador;
- » Hackers modificam um site.

Estes são alguns exemplos simples de quebra de integridade de informação.

Mais adiante você conhecerá mecanismos de controle para a garantia da integridade das informações.

Temos de considerar que hardware, software e os mecanismos de comunicação devem trabalhar de forma conjunta para manter e processar dados corretamente, assim como mover os dados para os destinos previstos, sem nenhuma alteração não prevista.

Como princípio, os sistemas operacionais de computadores e as redes devem ser protegidos contra interferências e contaminações do ambiente exterior.

Para assegurar que atacantes externos ou erros cometidos por usuários não comprometam a integridade dos sistemas ou dados, todos os ambientes computacionais devem fornecer mecanismos de controle de segurança.

Os usuários geralmente afetam um sistema ou a integridade de seus dados por engano e não intencionalmente, embora usuários internos de uma empresa também possam realizar atos mal-intencionados.



Gst/Shutterstock.com

Figura 3.2 – Acesso aberto à informação.

Programas de sistemas devem fornecer mecanismos que verifiquem os valores de entrada, se os mesmos são válidos e razoáveis. Isto é parte das obrigações dos programadores e analista de sistemas em relação à integridade da informação.

Os bancos de dados devem deixar apenas que indivíduos autorizados possam modificar dados, e os dados em trânsito devem ser protegidos por criptografia ou outros mecanismos que garantam o não acesso, ou modificação, deles sem autorização.

Fique de olho!

Mais à frente, falaremos mais sobre criptografia.

Quando um ataque externo inserir um vírus, uma bomba lógica, ou um programa backdoor (estudaremos adiante em detalhes) em um sistema, a integridade dos dados e informações de um sistema é comprometida.

Inserção e alteração de dados com erros por parte de um usuário também comprometem uma informação em sua integridade, lembrando que as informações se propagam rapidamente em um ambiente computacional, assim como os erros, tornando-se alto o custo para corrigi-los.

3.2 Princípio da confidencialidade de informação

Nem todas as informações são sigilosas, ainda que sejam informações importantes, consideradas críticas.

Algumas informações ou dados necessitam de confidencialidade ou sigilo, entre elas:

- 1) dados pessoais (por exemplo, número de telefone, endereço, CPF e RG, senha de acesso a bancos ou outros sites comerciais);
- 2) dados de cartões de crédito (por exemplo, número do cartão, código de segurança, senha);
- 3) dados de fornecedores ou de clientes de uma empresa;
- 4) dados de políticas financeiras de uma organização, ou de uma pessoa, como seu saldo bancário; e
- 5) dados de marketing, ou política de preços de uma empresa, ou seus dados de rendimentos pessoais mensais, anuais etc.

A perda desta confidencialidade provoca custos e prejuízos a empresas e pessoas, como perdas de clientes e fornecedores, perda de vendas e faturamento, perdas na imagem pública de uma empresa ou pessoa.

O princípio de manutenção da confidencialidade deve ser dirigido para o direito das pessoas e empresas e na classificação dos dados e informações.



Ducur59us/Shutterstock.com

Figura 3.3 – Confidencialidade e privacidade.

O princípio da confidencialidade da informação tem como objetivo garantir que apenas a pessoa certa tenha acesso à informação devida para ela, ou seja, informação correta para a pessoa correta.

Ampliando nossos conceitos podemos afirmar que as informações trocadas entre pessoas e empresas normalmente não deverão ser do conhecimento de todos que fazem parte de uma empresa.

Muitas das informações geradas por algumas pessoas se destinam a um grupo específico de pessoas em uma empresa ou de sua rede de amigos e, muitas vezes, a uma única pessoa. Isso significa que esses dados deverão ser acessados e conhecidos apenas por um grupo limitado de pessoas, que deve ser definido pela pessoa ou, no caso de uma empresa, por um responsável pelas informações.

As informações devem possuir um grau de confidencialidade para cada uma, que deverá ser mantido para impedir que as pessoas não autorizadas tenham acesso a ela.

3.2.1 Engenharia social

Você conhecerá agora um pouco sobre engenharia social.

A engenharia social é enganar outra pessoa para obter o compartilhamento de informações confidenciais, colocando-se como uma pessoa autorizada a acessar essas informações.

Alguns usuários podem intencionalmente ou acidentalmente revelar informações sigilosas por não criptografá-las antes de enviá-las a outras pessoas. Eles podem, ainda, ser vítimas de um ataque de engenharia social, que se caracteriza pelo compartilhamento de segredos comerciais de uma empresa, pela falta dos cuidados necessários na proteção de informações confidenciais quando estas são processadas por sistemas, ou pelo envio de mensagens de sistemas via e-mails automáticos.

A confidencialidade pode ser fornecida por meio da criptografia de dados, uma vez armazenados e transmitidos durante o tráfego em rede, de um rigoroso controle de acesso aos dados, de uma rigorosa classificação de dados sigilosos ou não e principalmente de treinamento de pessoal nas empresa, sobre quais são os procedimentos adequados com a informação.

Quando falamos em tráfego de rede, queremos dizer que ter confidencialidade na comunicação é ter a segurança de que o que foi enviado a alguém ou escrito em algum lugar (um e-mail, por exemplo) só será acessado ou lido por quem tiver autorização para tal.

Fique de olho!

Pensemos no caso de um cartão de crédito. O número do cartão só deverá ser conhecido por seu proprietário e pela loja onde é usado no momento da compra. Se esse número for descoberto por alguém mal-intencionado, como nos casos noticiados sobre crimes da internet, o prejuízo causado pela perda desta confidencialidade poderá ser muito alto. Esse número poderá ser usado por alguém para fazer compras na internet ou em qualquer estabelecimento que receba pagamentos com cartão de crédito, trazendo prejuízos financeiros e uma grande dor de cabeça para o proprietário do cartão, além de afetar a imagem da empresa que recebeu pagamento com estes cartões.



Exemplo

Jantávamos eu e um colega, mestre e escritor, ainda no tempo em que se passava o cartão de crédito em uma maquininha com carbono, como ocorria antigamente. Já naquela época, o atendente do restaurante fez duas cópias dos dados do cartão, fazendo com que no extrato de meu colega constasse duas vezes cobrança no mesmo estabelecimento com valores inclusive diferentes.

Hoje em dia isso é mais fácil ainda de ocorrer, se você falar ou mostrar algum papel com a senha de seu cartão de crédito, ou os sistemas do estabelecimento que guardam e transmitem os dados do cartão para a operadora forem atacados e estes dados confidenciais, copiados.

Isto é perda de confidencialidade e uma grave falha em segurança da informação.

Manter a confidencialidade é um dos fatos mais determinantes para a segurança e uma das tarefas mais difíceis de implementar, pois envolverá todos os elementos que compõem a comunicação de informações, desde quem a emite, passando pelo caminho percorrido, até quem a recebe.

Além disso, as informações têm diferentes graus de confidencialidade, normalmente associados a seus valores sociais ou empresariais.

Quanto maior for o grau de confidencialidade de uma informação, maior será o nível de segurança necessário na estrutura tecnológica e humana que participar destes processos: utilização, acesso, trânsito e armazenamento das informações.

3.2.2 Grau de confidencialidade

As informações geradas pelas pessoas tanto no ambiente pessoal quanto em uma empresa têm uma finalidade específica e destinam-se a um indivíduo ou grupo de indivíduos dentro da empresa.

Portanto, é necessário a existência de uma classificação com relação à sua confidencialidade.

É o que chamamos de grau de sigilo, isto é, a graduação atribuída a cada tipo de informação com base no grupo de usuários que possuem as permissões de acesso a esta mesma informação.

O grau de confidencialidade é um dos componentes mais importantes no processo de classificação da informação.

Normalmente as informações possuem os seguintes tipos de classificação quanto à confidencialidade:

- » Confidencial.
- » Restrito.
- » Sigiloso.
- » Público.

Dizem que o único computador totalmente seguro é aquele desligado da tomada. A arte da engenharia social concentra-se no elo mais fraco da corrente da segurança de computadores: os seres

humanos. Logo o aspecto acesso à informação, mesmo aquelas com nível de classificação de confidencialidade mais alto, pode ser obtido por meio de pessoas ou ingênuas ou mal-intencionadas.

Como um ataque da chamada “engenharia social” pode revelar muitas informações, como tornar um sistema de computadores mais seguro?

A resposta é educação e difusão da classificação da informação, explicando aos empregados e pessoas ligadas direta ou indiretamente a um determinado sistema a importância de uma política de segurança e confidencialidade. Assim evitar-se-á o ataque de pessoas que poderão tentar manipulá-los para ganhar acesso a informações privadas.

Podemos dizer e afirmar que este é um excelente começo para tornar segura sua rede ou sistema de informações.

O controle de acessos será alvo de nossos estudos nos próximos capítulos deste livro, quando veremos características de uma política de segurança.

Analisaremos políticas de controle de acessos a arquivos de senhas, programas fonte de sistemas, arquivos de dados, arquivos de log (registro de transações em bancos de dados), programas utilitários e sistema operacional de computadores e redes.

Amplie seus conhecimentos

Existem casos de pessoas que ligam para o provedor de acesso à internet e perguntam: “Por favor, perdi minha senha de internet. Poderia olhá-la para mim?” Alguns provedores pedem documentação para comprovar que é o dono da conta, outros (funcionários insatisfeitos em sua maioria) não ligam e passam até o número do cartão de crédito de algum usuário se lhe pedirem. Esse método é utilizado também para conseguir informações sobre uma pessoa em especial.

Vá a uma companhia telefônica e peça a segunda via de uma conta de telefone qualquer. Na maioria das vezes não lhe pedem documento e você consegue o endereço residencial de qualquer pessoa. Alguns filmes como *Hackers* e *Caçada Virtual* mostram bastante essa técnica.

3.3 Princípio da disponibilidade de informação

Toda e qualquer informação deve estar disponível sempre que for necessário. Deriva deste princípio a ideia de que devemos ter “a informação certa, na hora certa para a pessoa certa”, o que une os três princípios da segurança da informação.

Os recursos tecnológicos da informação devem ser mantidos sempre em bom funcionamento e devem ser capazes de ser recuperados de forma rápida e completa, em casos de desastres naturais ou acidentais.

O caso citado neste livro sobre ataque DDoS ao site da Origin®, que o tornou indisponível, caracteriza perfeitamente bem uma quebra da disponibilidade da informação.

A disponibilidade da informação se refere a toda estrutura física e tecnológica necessária para permitir o acesso, o tráfego e o armazenamento das informações e dados.

Por exemplo, se durante uma reunião de diretoria de uma empresa os serviços de banco de dados falham, e com isso impede que seja tomada uma determinada decisão em pauta, estaremos com uma quebra de disponibilidade também.

Se você acessa seu banco pela internet para saber seu saldo antes de emitir um cheque, por exemplo, e o site de seu banco está fora do ar, ou sobrecarregado e não responde, isto também caracteriza uma indisponibilidade de informação. Ou seja, a quebra do princípio que estamos discutindo.

Para proteger a disponibilidade da informação, é necessário saber quem são seus usuários e organizar e definir, para cada caso, as formas de disponibilização da informação. Em outras palavras, quem tem acesso e uso para quando for necessário.

A disponibilidade da informação é sempre considerada com base no valor que esta informação tem e no impacto da indisponibilidade dela. Sites de internet, em particular, têm a necessidade de garantir de maneira ininterrupta o acesso e a disponibilidade de informações e recursos.

Podemos considerar então a existência da preocupação com a proteção da informação na internet, pois o avanço tecnológico traz consigo o surgimento de novos métodos de ataques de hackers atrelado a uma maior vulnerabilidade de sistemas que não se atualizam no mesmo ritmo.

Logo, manter disponibilidade é um princípio, porém é mais um ponto da segurança que deve ser sempre considerado.

É necessário que haja sempre controle sobre pontos específicos de falhas que devem estar em vigor, caso as medidas necessárias de backup tenham de ser tomadas. Outrossim, mecanismos de redundância de dados (bancos de dados espelhados) devem estar no local quando necessário. Desta forma, os efeitos negativos de componentes ambientais que geram indisponibilidade de informação poderão ser evitados. Por exemplo, um servidor de banco de dados parar por falha de hardware, como queima do equipamento por sobrecarga elétrica, deixaria indisponíveis todas as suas informações.

Uma medida de segurança seria o backup frequente dos bancos de dados para recuperação em outro equipamento, ou então a existência de um equipamento sobressalente, em que estariam duplicadas todas as informações. Este equipamento redundante substituiria automaticamente o equipamento queimado ou interrompido.

A disponibilidade de informações pode ser afetada por falha de hardware ou por falha de software, por isso a importância de backups para permitir a recuperação e a continuidade da disponibilização das informações.

Observe que as questões ambientais como calor, frio, umidade, eletricidade estática, bem como a contaminação por vírus ou ataques, também podem afetar a disponibilidade de um sistema de informações.

Então o princípio da disponibilidade deve impedir a interrupção dos serviços e produtividade com sistemas de informação.

3.3.1 Vulnerabilidades

As vulnerabilidades são os pontos que, ao serem explorados por pessoas mal-intencionadas, afetam a confidencialidade, a disponibilidade e a integridade das informações de um indivíduo ou empresa.

Um dos primeiros passos para a implementação da segurança é rastrear e eliminar os pontos vulneráveis de um ambiente de tecnologia da informação.

Muitas vezes as palavras ameaça, vulnerabilidade, exposição e risco são usadas para representar a mesma coisa, apesar de terem diferentes significados e relações entre si.

É importante compreender a definição de cada uma delas, mas o mais importante é que você compreenda a associação de uma às outras.

Vulnerabilidade pode ser um software, hardware ou falha de um processo que pode fornecer a um atacante uma porta aberta que ele está à procura, para entrar em um computador ou rede e ter acesso não autorizado aos recursos dentro deste ambiente.

Uma ameaça é qualquer perigo potencial para a manutenção dos princípios da segurança da informação.

Um agente de ameaça pode ser um intruso que venha a acessar uma rede por meio de uma porta no firewall (mais adiante, veremos em detalhes o que é um firewall), um determinado processo de sistemas acessando de forma que viole as políticas de segurança, um furacão (tempestade) destruindo uma instalação de um centro de processamento de dados, ou um empregado que venha a cometer um erro não intencional que poderia expor informações confidenciais ou então destruir a integridade dos dados de um arquivo.

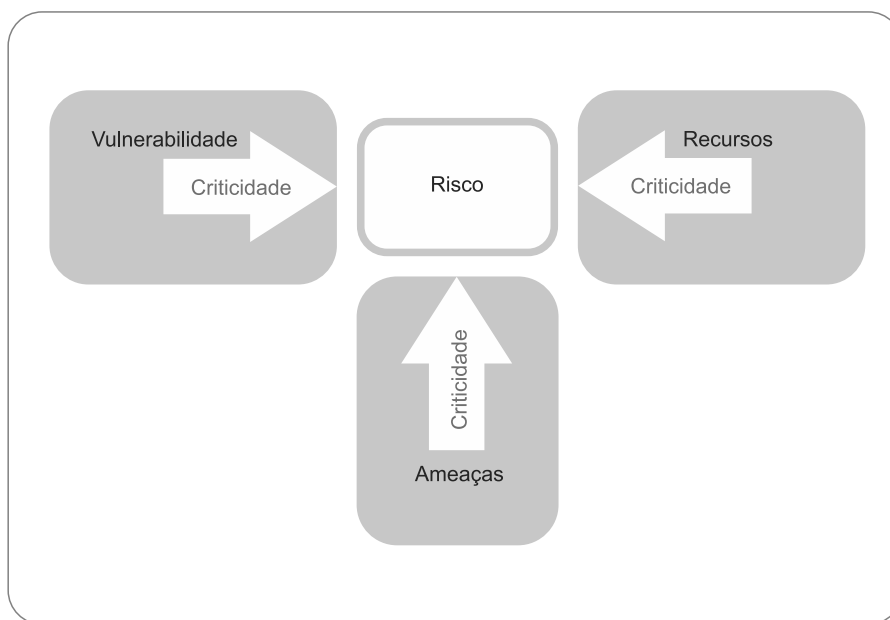


Figura 3.4 – Ameaças e Riscos.

A exposição é o fato de as informações e sistemas de tecnologia da informação serem expostos a perdas a partir de um agente de ameaça interna ou externa.

Uma vulnerabilidade pode causar danos e perdas a uma organização, se exposta a possíveis danos por esta exposição.

Por exemplo, se o gerenciamento de senhas é frouxo e as regras de senha não são aplicadas ou não existem, a empresa pode ter suas senhas de usuários expostas, capturadas e utilizadas de forma distinta de seu titular, com finalidades destrutivas ou de violação de confidencialidade.

É muito normal em empresas existirem regras para as senhas de acesso a rede e banco de dados com no mínimo oito caracteres, sendo obrigatório que um deles seja numérico. Além disso, elas não podem conter nome, sobrenome ou data de nascimento, e o usuário é obrigado a trocá-las com uma frequência determinada.

Hoje, até mesmo alguns bancos solicitam que seus clientes troquem de senha com frequência. Do contrário, informam, por exemplo, que a senha não é trocada há mais de seis meses.

Na prática, alguém do RH utiliza uma senha simples para usuário. Outra pessoa mal-intencionada pode copiá-la a fim de ter acesso aos salários de outros funcionários, mesmo que seja somente para consulta.

Contramedida, ou salvaguarda, é o que atenua um risco potencial.

Uma medida preventiva é uma configuração de software, hardware ou um procedimento que elimina uma vulnerabilidade dos sistemas ou reduz o risco de um agente de ameaça de ser capaz de explorar uma vulnerabilidade.

Contramedida pode ser um forte gerenciamento de senhas, uma espécie de guarda de segurança, de acesso, assim como mecanismos de controle dentro de um sistema operacional, a implementação de um sistema básico entrada/saída (BIOS), senhas e treinamento de conscientização de segurança.

No próximo capítulo estudaremos as ameaças.

3.4 Políticas de segurança

O que é uma política de segurança?

Em síntese, é um programa de segurança que busca garantir os três princípios que aprendemos neste capítulo:

- 1) Integridade;
- 2) Confidencialidade;
- 3) Disponibilidade.

Na política de segurança de uma empresa, a gestão estabelece como um programa de segurança será criado e as metas deste programa, atribui as responsabilidades, mostra o valor estratégico e tático da segurança e descreve como a aplicação desta política deve ser realizada.

Políticas devem abordar questões específicas de segurança que a administração vier a determinar que precisam de explicação mais detalhada e mais atenção, para termos certeza de que é uma estrutura de procedimentos bem abrangentemente e construída para que todos os funcionários da empresa entendam que devem respeitá-las.

As empresas podem optar por uma política de segurança de e-mail. Nela descreverão o que a administração pode ou não fazer com mensagens de e-mail dos funcionários, como os funcionários podem ou não usar as funcionalidades de e-mail de forma diferente, assim como as questões de privacidade específicas dos endereços.

Uma política específica de sistemas deve apresentar as decisões da administração que estão mais próximas dos computadores atuais, redes, aplicativos e dados.

Este tipo de política deve fornecer uma lista de softwares aprovados que podem ser instalados em estações de trabalho individuais. Deve, ainda, descrever como as bases de dados serão protegidas (regras de autorizações de acesso aos dados), como os computadores podem ser bloqueados e como ferramentas tipo firewall, sistemas de detecção de intrusão e scanners devem ser utilizados na empresa (aprenderemos sobre estas tecnologias em mais detalhes nos próximos capítulos).

As políticas são escritas como uma visão geral e com objetivo de dar conta de muitos assuntos.

Muito mais detalhamento é necessário para desenvolver as formas e métodos que precisam acontecer para realmente apoiar e efetivar esta política.

A política de segurança prevê as bases da garantia de segurança de informação.

Os procedimentos e seus componentes, assim como as implementações e mecanismos tecnológicos, são usados para preencher um quadro de especificações desta política, criar um programa de segurança total e garantir uma infraestrutura segura.

Uma política compõe-se de quatro grandes conjuntos de elementos, quais sejam:

- » Normas.
- » Linhas básicas (baselines).
- » Diretrizes.
- » Procedimentos.

3.4.1 Normas

As normas especificam como produtos de hardware e software devem ser utilizados.

Estas normas podem ser, por exemplo, um padrão da empresa que exige que todos os funcionários tenham e usem seus crachás de identificação na empresa, com os dados sobre a sua pessoa, em todos os momentos. Ou então que indivíduos desconhecidos fora dos quadros funcionais da empresa devem ser questionados sempre sobre a sua identidade e seu propósito (por que estão ali) ou, ainda, que todas as informações confidenciais devam ser criptografadas.

3.4.2 Linhas recomendadas (baselines)

As linhas recomendadas têm como objetivo prover o nível mínimo de segurança necessário para toda a empresa.

Na maioria das vezes, as linhas de base são implementações de segurança de uma única plataforma necessárias para fornecer o nível desejado de proteção e segurança da informação.

Por exemplo, uma empresa pode exigir que todas as suas estações de trabalho tenham ao menos um nível de segurança, chamado C2.

O nível de segurança da linha de base seria C2, e a linha de base, o apoio aos procedimentos que forneçam instruções passo a passo sobre como o sistema operacional e os componentes dessa estação de trabalho têm de ser instalados para atingir esse nível de segurança específico.

Isto é o conceito de linha de base, ou baseline.

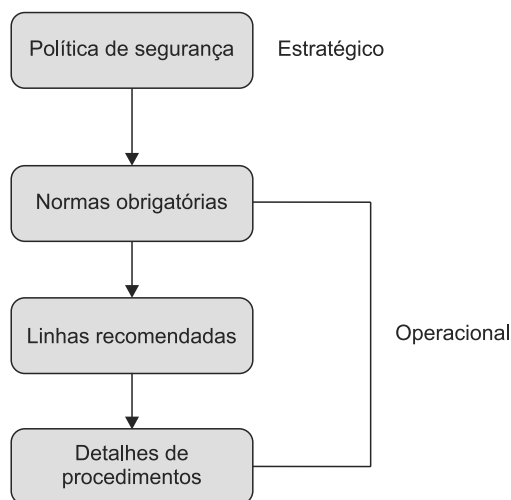


Figura 3.5 – Uma política é estabelecida nos planos estratégicos da empresa, e os elementos mais baixos, como normas, fornecem o apoio tático, ou melhor, operacional para sua aplicação.

3.4.3 Diretrizes

Diretrizes são ações de recomendação e guias operacionais para os usuários, a equipe de TI da empresa, a equipe de operações e outros usuários, quando uma norma específica não se aplica, ou não existe uma norma específica a uma determinada situação de utilização dos recursos de TI da empresa.

Elas lidam com as metodologias de segurança de computadores e de seus softwares.

Sempre existem áreas não muito claras para um usuário, onde acontecem situações que nunca haviam sido definidas, ou ações não previstas. Portanto, algumas orientações podem ser utilizadas como referência nestes momentos.

Considerando que as normas são atividades obrigatórias específicas, as diretrizes são orientações gerais que fornecem a flexibilidade necessária para as circunstâncias imprevistas.

Uma política pode determinar que o acesso a dados confidenciais deve sempre ser auditado, ou seja, deve existir registro completo deste acesso.

Uma diretriz de apoio poderia explicar melhor o que estas auditorias devem conter de informações, para serem capazes de permitir a conciliação com outros detalhes deste mesmo conjunto de diretrizes.

3.4.4 Procedimentos

Procedimentos são as ações detalhadas, passo a passo, para a realização de uma determinada tarefa.

Estes passos podem ser aplicados por usuários, pela equipe de TI, pelo pessoal operacional, pelos membros da equipe de segurança e por quem mais precise instalar ou configurar um componente de um computador.

Muitas empresas escrevem e têm procedimentos sobre a forma como os sistemas operacionais devem ser instalados, como mecanismos de segurança devem ser configurados, como configurar uma lista de controle de acessos, como criar novas contas de usuário, como atribuir privilégios, como registrar e fazer auditoria, procedimentos para destruição de materiais, relatórios de incidentes etc.

Procedimentos são o nível mais baixo da cadeia de uma política de segurança, porque eles estão mais próximos dos computadores e fornecem instruções detalhadas para problemas de configuração e instalação de software e hardware.

Normas, diretrizes e linhas básicas (baselines) não devem estar em um documento grande.

Cada uma tem uma finalidade específica e um público diferente.

Um documento que descreve como estar em conformidade com uma regulamentação específica pode ir para a equipe de gestão. Enquanto isso, um procedimento detalhado sobre como proteger adequadamente um sistema operacional específico é dirigido a um membro de TI.

Cada um dos elementos ser independente e realizado de natureza modular ajuda na sua distribuição, compreensão e atualização adequada, quando se fizer necessário.

Os documentos devem expor a forma como as políticas, normas e diretrizes serão realmente implementadas em um ambiente operacional.

A implementação de políticas de segurança e os itens que a apoiam deve receber o devido cuidado da empresa e de sua equipe de gestão.

Deve ser informado, de maneira clara, aos funcionários da empresa o que se espera deles e as consequências do não cumprimento dos elementos das políticas de segurança, destacando a responsabilidade de cada um.

Se uma empresa despede um empregado porque ele estava baixando material pornográfico no computador de trabalho, o empregado pode levar a empresa à justiça e ganhar, caso consiga provar que ele não foi devidamente informado sobre o que era considerado de uso aceitável e inaceitável de propriedade da empresa e quais seriam as consequências. Por incrível que pareça, os elementos da política de segurança estudados, explicitando nas normas e linhas de base as restrições, devem ser obrigatoriamente divulgados para assegurar que funcionários respeitarão a política de segurança da informação da empresa.

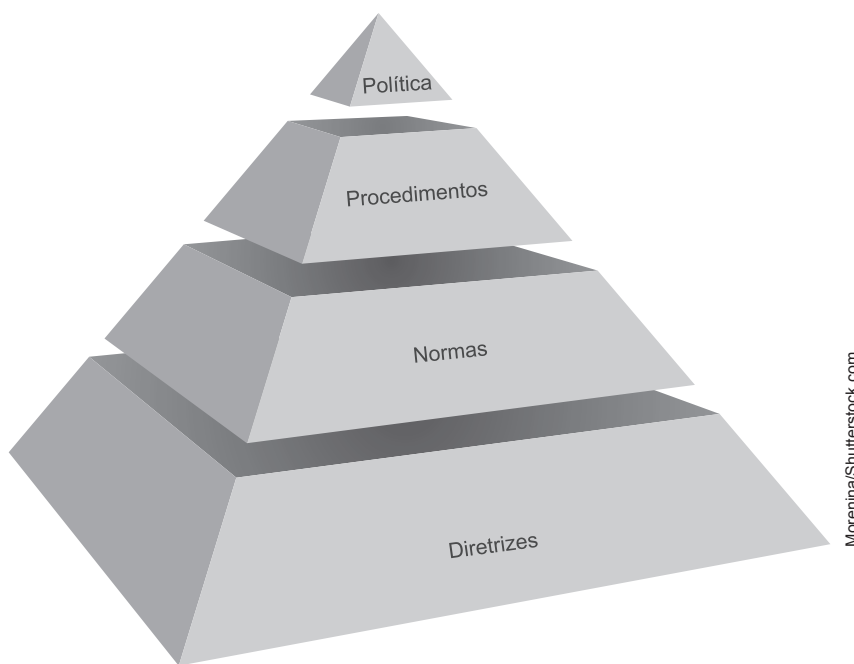


Figura 3.6 – Políticas de segurança, procedimentos, padrões e diretrizes trabalham juntos.

Vamos recapitular?

Neste capítulo estudamos mais detalhadamente os três princípios da segurança da informação. Aprendemos, também, quando estamos violando estes princípios, o que são vulnerabilidades e para que serve e o que uma política de segurança busca criar e manter os ambientes de redes seguras.



Agora é com você!

- 1) Qual é o princípio que trata de garantir que a informação não foi modificada e é confiável?
- 2) Explique qual é a relação existente entre vulnerabilidade e disponibilidade:
- 3) Normas, diretrizes e linhas básicas fazem parte de que princípio?
- 4) Veja na sua escola ou em alguma empresa como as informações são protegidas de exposição externa, e descreva como esta proteção é feita, se existir.