Unidade III

3 MECANISMOS E ESTRATÉGIAS DE SEGURANÇA EM REDES

Ramos (2008) afirma que a proteção de redes e de dispositivos de telecomunicações é uma das áreas mais importantes da segurança da informação. Por conta dos altos níveis de automatização existentes hoje na maioria das organizações e do papel que a internet assumiu como principal meio de comunicação empresarial, desbancando em poucos anos até as redes de telefonia convencional, grande parte das informações que precisamos proteger encontra-se armazenada em computadores ou trafegando por diversos tipos de tecnologia de rede e comunicação remota.

Proteger as informações requer conhecimento específico e abordagens estruturadas de avaliação das reais condições de segurança. Os profissionais que se especializam em segurança em redes costumam adquirir um amplo conhecimento sobre o funcionamento desse processo e sobre as tecnologias que o suportam. A maioria dos gestores, porém, não precisa se aprofundar demasiadamente nos detalhes técnicos. Contudo, entender a finalidade das diversas tecnologias, os problemas de segurança e as soluções disponíveis para resolvê-los é uma necessidade fundamental, que demanda preparo e capacitação.

3.1 Segurança física

A segurança física cuida da proteção dos ativos valiosos da organização. Sua abrangência é extensa e inclui todas as instalações físicas (internas e externas) da organização. A segurança física também cuida da proteção dos ativos – por exemplo, valores ou fitas de backup – quando estão em transporte.

Quando nos referimos à segurança física, a palavra **prevenção** vem em primeiro lugar. Medidas preventivas são chamadas de **barreiras de segurança**. Beal (2005) as caracteriza como obstáculos que se colocam para prevenir um ataque. Cercas elétricas e paredes são exemplos de segurança física. Um processo de logon para acessar determinada rede é um exemplo de segurança lógica. Quando ambos os tipos de segurança são combinados, compõe-se o **perímetro de segurança.**

A ISO/IEC 27001 (ABNT, 2006) define perímetro de segurança como quaisquer elementos que estabeleçam uma barreira ao acesso indevido.

O perímetro de segurança funciona como uma linha delimitadora, que indica uma área separada, protegida por um conjunto de barreiras físicas e lógicas.

Algumas barreiras que podem formar um perímetro de segurança são: salas-cofre, roletas de controle de acesso físico, tokens, dispositivos biométricos, circuitos fechados de TV, detectores de fumaça, sirenes e alarmes de incêndio, acionadores de água para combate a incêndio.

O quadro a seguir apresenta algumas recomendações da ISO/IEC 27001 em relação à segurança física.

Quadro 10 – Itens de segurança física definidos pela ISO/IEC 27001

Determinar claramente o perímetro de segurança
Assegurar-se de que o perímetro de prédios ou locais que contenham recursos de processamento de dados seja fisicamente consistente (sem brechas que facilitem a invasão)
Implantar uma área de recepção ou outro meio de acesso físico ao local e restringir o acesso apenas a pessoas autorizadas
Quando necessário, adotar barreiras físicas estendidas do piso até a laje, para prevenir acessos não autorizados ou contaminação ambiental causada por fogo, inundação, fumaça etc.
Instalar portas de incêndio no perímetro de segurança com sensores de alarme e mola para fechamento automático

Diante do escopo abrangente da segurança física, é preciso adotar práticas de gestão idênticas às adotadas na gestão da segurança da informação: análise e avaliação de risco e elaboração de normas. Tais práticas são necessárias para a introdução correta e eficaz de um processo de gestão da segurança física.

Compreender o ambiente físico da organização é o primeiro passo para identificar vulnerabilidades que podem estar abrindo brechas para ameaças ao ambiente físico da organização.

As ameaças e as vulnerabilidades mais comuns estão exemplificadas a seguir.

Quadro 11 – Ameaças e vulnerabilidades à segurança física

Ameaça	Vulnerabilidade
Roubo e furto	Ausência de (ou falha no) controle de acesso físico aos edifícios da organização
Sabotagem e vandalismo	Exposição desnecessária dos ativos físicos
Sequestro e chantagem	Ausência de (ou falha na) proteção física dos ativos de informação ou dos colaboradores da organização
Terrorismo ideológico ou criminoso	Falha em evitar que a organização entre em temas polêmicos ou ideológicos
Interrupção em serviços básicos, como água, energia e gás	Ausência de (ou falha em) planos de contingência
Problema em sistemas de suporte, como ar condicionado e ventilação	Ausência de (ou falha em) planos de contingência
Fogo e fumaça	Ausência de (ou falha em) mecanismos de detecção de incêndio
Enchente e vazamento de água	Ausência de (ou falha em) mecanismos de prevenção

A análise de riscos auxilia na identificação das instalações físicas e dos ativos de negócio associados à proteção física e, com isso, na adoção de mecanismos que contrabalancem investimento e benefício, uma vez que controles físicos requerem investimentos razoavelmente altos.

A segurança da informação deve interferir o mínimo possível na rotina de uma organização. No entanto, quando se trata de segurança física, essa intervenção é inevitável e necessária para tornar o

ambiente seguro. Devem ser adotados padrões para a proteção física da organização, de seus ativos de informação e de seus colaboradores.

Quanto maior a necessidade de proteção, maior a intervenção da segurança da informação na rotina da organização, e consequentemente maior o desconforto causado aos colaboradores. Especificamente em relação à segurança física, o grande desafio da segurança da informação é adotar mecanismos de proteção sem cair num excesso de procedimentos de controle.

O uso de planos de conscientização ajuda a dividir a responsabilidade e a reduzir a sensação de desconforto decorrente da implantação de mecanismos de proteção física no ambiente da empresa.

A padronização dos mecanismos nas áreas comuns da organização é uma preocupação que transcende a segurança da informação e envolve a própria estrutura da organização.

O conceito de **prevenção criminal através do desenho ambiental** vem sendo desenvolvido ao longo das últimas décadas. Elaborado inicialmente nos anos 1960, foi em 1972 que Oscar Newman estabeleceu as bases desse conceito no livro *Defensible Space*.

Essa teoria refere-se à possibilidade de reduzir o crime e o medo por meio de certas medidas de planejamento de áreas. Para isso, utilizam-se duas abordagens básicas.

A primeira diz ser possível desenhar ambientes que reduzem as oportunidades de um crime acontecer.

A segunda volta-se para a redução do medo do crime e o aumento da sensação de segurança pessoal, melhorando assim a qualidade de vida das pessoas e seu relacionamento com as medidas necessárias de segurança.

Alguns princípios fundamentais são dispostos por essa teoria e devem ser seguidos pelos responsáveis por projetar construções e espaços urbanos:

- Deve-se adotar uma iluminação adequada tanto para o dia quanto para a noite. Isso aumenta a sensação de segurança e desencoraja a prática do crime, porque inibe a ação do criminoso e expande a capacidade de vigilância.

- Devem-se projetar as áreas de modo que os usuários tenham um campo de visão amplo, o que lhes permite antecipar os arredores de onde estão, dando-lhes a sensação de segurança. Um bom campo de visão aumenta naturalmente a quantidade de pessoas vigiando um ambiente.

- Para não facilitar a ação de criminosos, devem-se evitar pontos de esconderijo, como vielas e reentrâncias, e construções que preveem o movimento das pessoas, como passarelas e túneis para pedestres.

- Deve-se optar pela mistura de áreas residenciais e comerciais, o que assegura uma boa distribuição de pessoas em diversos horários e vigilância a qualquer hora do dia.

- Devem-se priorizar espaços geradores de atividades, que tragam pessoas para ocupá-los, como parques e praças de alimentação em ambientes abertos.

- Para criar um senso de propriedade nos que utilizam as áreas, devem-se programar manutenções constantes. Essa prática, além de manter a limpeza, desencoraja a ação de vândalos.

- Devem-se sinalizar claramente as localidades e os caminhos possíveis. Isso transmite uma sensação de segurança aos usuários, os quais podem identificar facilmente pontos de apoio ou rotas de fuga.

Outro aspecto importante para a segurança física diz respeito à localização geográfica das instalações. Ela interfere diretamente na segurança da informação e é crucial na hora de identificar ameaças, vulnerabilidades e riscos ao ambiente. Por meio da localização geográfica, é possível analisar a probabilidade de problemas naturais ou climáticos.

Perguntas que devem ser respondidas na análise da localização geográfica:

- O local pode ser alvo de ataques terroristas?

- Manifestações públicas são constantes ou esperadas?

- Existe histórico de problemas recorrentes com o fornecimento de serviços básicos?

- A área traz riscos inerentes, como proximidade com aeroportos, bases militares ou zonas de alta incidência de crimes?

Para garantir que a operação da organização não seja interrompida, os projetos de construção devem considerar os aspectos de segurança relacionados à entrada de veículos, colaboradores, visitantes, prestadores de serviços e entregadores; à logística; ao fornecimento de serviços básicos; e ao sistema de ar condicionado e ventilação. Deve-se pensar na implantação de mecanismos de proteção na própria concepção do projeto. A primeira forma de proteção é a chamada **proteção perimetral** ou **periférica**.

Quadro 12 – Barreiras perimetrais ou periféricas

Barreira	Característica
Cerca	Pode ser construída com aço galvanizado ou ferro e ser eletrificada. Serve para demarcar a fronteira externa de uma construção. Seu maior benefício é manter o nível de visão, e sua desvantagem é ser facilmente transposta.
Paisagismo	Tem como principal objetivo criar barreiras naturais de proteção. Arbustos e paredes feitas de árvores são alguns exemplos.
Portão	Mecanismo de controle de acesso físico que se aplica a pessoas e, com maior frequência, a veículos.
Barreira veicular	Formada por colunas de concreto ou metal e colocada nas calçadas, busca impedir a aproximação ou o estacionamento de veículos, sem atrapalhar o tráfego de pedestres.

As barreiras de proteção podem ter efeitos preventivos e detectivos. São exemplos desses mecanismos:

- **Iluminação**: não apenas deixa o ambiente mais claro, mas aumenta o campo de visão no período noturno, inibindo a ação de intrusos e prevenindo a ocorrência de crimes.

- **Alarmes**: em geral, são usados como barreiras externas e têm a finalidade de alertar sobre a existência de um possível intruso no perímetro de proteção. Pequenos fios são colocados na extensão total dos muros; quando rompidos, disparam um alarme sonoro ou visual, chamando a atenção dos seguranças.

- **Sensores de presença**: utilizam diversos tipos de tecnologia na tentativa de detectar a presença de pessoas não autorizadas em ambientes controlados. As tecnologias mais comuns são:

  – **Quebra de circuito elétrico**: um circuito elétrico funciona quando a transmissão da corrente é interrompida, acusando assim a violação.

  – **Interrupção do feixe de luz**: dispositivos fotoelétricos produzem um feixe de luz; caso este seja interrompido, dispara-se um alarme para acusar a intrusão. O feixe pode ser visível ou invisível e também pode ser utilizado como detector de incêndio.

  – **Infravermelho passivo**: funciona como o feixe de luz, mas a energia infravermelha é emanada no ambiente por um único sensor, capaz de detectar variações na reflexão causadas pelo movimento.

  – **Detectores ultrassônicos**: produzem no ambiente padrões de energia acústica, que se alteram caso uma pessoa entre no ambiente. A vantagem desse sistema é ser imperceptível ao ser humano. A desvantagem é que barulhos externos podem gerar um alarme falso.

  – **Dispositivos de micro-ondas**: assemelham-se aos dispositivos ultrassônicos, com a vantagem de não sofrer interferência externa. Utilizam antenas que permitem monitorar uma área ampla. A dificuldade reside em conseguir confinar o sinal a um ambiente.

- **Circuitos fechados de TV**: é um sistema de monitoramento que capta imagens por meio de câmeras. As imagens geradas podem servir de prova num processo de investigação. De acordo com a qualidade das imagens e a frequência com que são capturadas, os circuitos fechados de TV são classificados em alguns níveis básicos:

  – **Nível detectivo**: indicam a presença de um corpo estranho, sem que se possa identificá-lo.

  – **Nível de reconhecimento**: permitem diferenciar um homem de um animal, por exemplo.

  – **Nível de identificação**: identificam um corpo em detalhes; verificam inclusive os traços faciais.

Os componentes básicos também refletem a qualidade dos circuitos fechados de TV.

Quadro 13 – Componentes básicos de circuitos fechados de TV

Componente	Descrição
Câmeras e lentes	As imagens são captadas por lentes intercambiáveis, isto é, que podem ser substituídas de acordo com necessidade.
Iluminação	A luz é um fator primordial para a captação de imagens. Em última instância, é exatamente aquilo que a câmera capta.
Mídia de transmissão	A transmissão pode ocorrer com ou sem fio. Existe a possibilidade de usar cabos coaxiais, linhas telefônicas, redes elétricas, redes de dados, redes Wi-Fi e outras.
Monitores	Os monitores são utilizados na visualização de imagens. A tecnologia deles interfere na qualidade das imagens que apresentam.
Dispositivos de armazenamento	O armazenamento é opcional e pode ser realizado em sistemas digitais ou analógicos.

Tratamos, na sequência, de outras recomendações da norma ISO/IEC 27001 (ABNT, 2006):

- Escritórios, salas e instalações de processamento devem ser devidamente fechados, e equipamentos devem efetuar o bloqueio de acesso por inatividade, evitando assim o acesso indevido.

- Áreas de expedição e descarga devem ter acesso restrito e supervisão constante, a fim de prevenir atividades não autorizadas. Os mecanismos de proteção indicados para essas áreas são os equipamentos de gravação. Recomenda-se que as áreas de expedição e descarga fiquem distantes e isoladas das áreas de processamento. O isolamento evita que pessoas ou empresas acessem locais que guardam informações confidenciais.

- Documentos em papel devem ser protegidos durante todo o seu ciclo de vida. Para isso:

  – Use rótulos na identificação de documentos que requerem tratamento confidencial.

  – Estabeleça uma política para o armazenamento de papéis que garanta a guarda de informações confidenciais ou críticas ao negócio em lugares seguros, como cofres ou arquivos resistentes ao fogo.

  – Adote procedimentos especiais para a impressão e a transmissão via fax de documentos confidenciais, bem como para o envio desses documentos via correio ou entregador.

- Mídias de computador (CDs, DVDs, disquetes, fitas magnéticas, discos removíveis etc.) também precisam ser controladas e protegidas, especialmente as fitas de backup. As principais medidas de proteção para mídias digitais estão descritas no quadro a seguir.

Quadro 14 – Medidas de proteção para mídias digitais

Armazenamento em ambiente protegido contra furto e compatível com as especificações do fabricante
Preservação, por meio de procedimentos e normas, de mídias que serão levadas para fora das instalações
Uso de rótulos para identificar mídias com conteúdo confidencial
Remoção do conteúdo de qualquer meio magnético reutilizável
Descarte seguro (por exemplo, trituração ou incineração)

Documentos eletrônicos, "cada vez mais presentes nas organizações, alteram o foco da gestão para questões como a exigência de mediação e a exigência de mecanismos de segurança" (BEAL, 2005, p. 84).

Pela exigência de mediação, para serem compreensíveis aos seres humanos, os documentos eletrônicos devem utilizar aparatos técnicos e informáticos, ou seja, softwares que exerçam uma função mediadora no acesso a eles.

Pela exigência de mecanismos de segurança, por serem mais suscetíveis a adulterações do que os documentos em papel, os documentos eletrônicos devem receber maior atenção. É preciso haver mecanismos que protejam a confidencialidade, a integridade e a disponibilidade das informações.

Com relação à guarda permanente de documentos eletrônicos, ela deve ser feita de uma forma que facilite consultas futuras.

Também é necessário preservar os dispositivos de hardware. A proteção física de computadores enfrenta as mesmas dificuldades que a proteção de outros ativos físicos. Por um lado, eles podem ser facilmente furtados. Por outro, estão expostos a ameaças como descargas elétricas causadas por raios, excesso de umidade no ambiente e derramamento de líquido no teclado. Deve-se zelar pela integridade física do hardware, a fim de que ele opere de maneira adequada. "A proteção de problemas ambientais e acidentais depende de um planejamento cuidadoso de medidas de proteção, a começar pelo levantamento dos ativos físicos existentes e de sua localização e importância para a organização"" (BEAL, 2005, p. 86).

A segurança da informação deve ainda prever falhas no hardware, como defeitos de fabricação ou mau funcionamento, que podem ocasionar danos irreversíveis nos ativos de informação de uma organização. A manutenção correta dos equipamentos pode minimizar a ocorrência de falhas no hardware.

A instalação de qualquer tipo de equipamento relacionado à TI só deve ser feita após uma avaliação do ambiente. É preciso reduzir o nível de exposição a sabotagem, espionagem etc.

Para a correta proteção dos ativos físicos, devem-se criar regras inibidoras de ações que coloquem os equipamentos em risco, "políticas específicas para a restrição de alimentos, bebidas e fumo próximo às instalações de processamento de informações e para a monitoração de aspectos ambientais que possam afetar as instalações" (BEAL, 2005, p. 88).

A remoção, o descarte e o transporte de equipamentos devem receber atenção especial. É necessário implementar controles específicos para evitar o vazamento de informações. O furto de componentes (discos rígidos ou peças de computador) pode ser combatido com a adoção de lacres ou cadeados nos equipamentos.

Quando não se adotam procedimentos que protejam as informações armazenadas num equipamento, o envio dele para a manutenção representa mais um risco. Contratos de confidencialidade podem ser firmados para salvaguardar as informações. Outra opção é retirar o disco rígido antes do envio. Toda e qualquer intervenção técnica num equipamento precisa ser acompanhada por uma pessoa responsável.

Em caso de descarte definitivo, recomenda-se a correta eliminação de todos os softwares e dados contidos nos equipamentos. Quando há informações sensíveis, confidenciais ou importantes num equipamento, a destruição definitiva do disco rígido é uma alternativa mais segura.

Equipamentos portáteis levados por colaboradores em viagens devem ser transportados como bagagem de mão e acondicionados em recipientes que não revelem tratar-se de um equipamento. O uso de senhas de acesso e de mecanismos criptográficos é uma ação de proteção recomendável.

A segurança física do cabeamento elétrico e de telecomunicação também é contemplada pela ISO/IEC 27001 (ABNT, 2006).

Quadro 15 – Recomendações da ISO/IEC 27001 para o cabeamento

Sempre que possível, utilize linhas elétricas e linhas subterrâneas, ou pelo menos sujeitas a uma proteção alternativa adequada
Adote um cabeamento de rede protegido contra interceptações não autorizadas ou danos – por exemplo, usando conduítes ou evitando a instalação em áreas públicas
Opte por cabos elétricos separados dos cabos de comunicação para prevenir interferências
Implante controles adicionais para sistemas críticos, como conduítes blindados, salas ou gabinetes trancados nos terminais e pontos de inspeção, cabeamento de fibra ótica e varredura para identificar dispositivos não autorizados conectados aos cabos

Observação

A segurança física é muito eficaz para a proteção de estruturas de rede cabeada, mas pode ser ineficiente em estruturas de rede sem fio.

A organização deve considerar a adoção de uma política de mesa limpa, para papéis e mídias removíveis, e uma política de tela limpa, para recursos de processamento da informação, de forma que se reduzam os riscos de acesso não autorizado, perda e dano à informação durante e fora do horário normal de trabalho. Essas políticas devem levar em conta as classificações da segurança da informação, os riscos correspondentes e os aspectos culturais da organização. Informações deixadas na mesa de trabalho também são alvo de dano ou destruição em caso de incêndio, inundação ou explosão. Recomenda-se que os seguintes controles sejam considerados:

- Papéis e mídias de computador devem ser guardados, quando não em uso, em gavetas adequadas, com fechadura, ou em outras formas seguras de mobiliário, especialmente fora do horário normal de trabalho.

- Informações sensíveis ou críticas ao negócio, quando não requisitadas, devem ser guardadas num local distante (de preferência num cofre ou num arquivo resistente a fogo), especialmente quando o escritório estiver vazio.

- Computadores e impressoras não devem ser deixados ligados quando não assistidos, e devem ser protegidos por senhas, chaves ou outros controles quando não em uso.

- Pontos de recepção e envio de correspondência e máquinas de fax e telex não assistidas devem ser protegidos.

- Copiadoras devem ser travadas (ou protegidas de alguma forma contra o uso não autorizado) fora do horário normal de trabalho.

- Informações sensíveis e classificadas, quando impressas, devem ser imediatamente retiradas da impressora.

Algumas áreas requerem mais segurança porque tratam de assuntos confidenciais ou têm ativos físicos de maior valor ou importância para a organização. São chamadas de áreas de segurança.

Controles adicionais podem ser necessários a fim de melhorar as condições de uma área de segurança. Isso inclui controles para o pessoal da organização, para os prestadores de serviços que trabalham em área de segurança e para as atividades terceirizadas que ocorrem nessa área. A seguir, algumas recomendações a esse respeito:

- Colaboradores só devem ter conhecimento da existência da área de segurança ou de atividades dentro dela quando necessário.

- Trabalho sem supervisão em áreas de segurança deve ser evitado, tanto para contribuir com a segurança como para prevenir atividades maliciosas.

- Áreas de segurança desocupadas devem ser mantidas fisicamente fechadas e ser verificadas periodicamente.

- Pessoal de serviço de suporte terceirizado deve ter acesso restrito às áreas de segurança ou às instalações de processamento de informações.

- Barreiras adicionais para controlar o acesso físico podem ser necessárias em áreas com diferentes requisitos de segurança dentro de um mesmo perímetro de segurança.

- Equipamentos de foto, áudio e vídeo não devem ser permitidos.

3.2 Estratégias de segurança

Durante muito tempo, a segurança em redes foi considerada uma alternativa à segurança em estações. O principal argumento era a facilidade e a praticidade, já que diversas máquinas podiam ser protegidas desde que a rede à qual essas máquinas estivessem conectadas fosse segura. Com o passar do tempo, a adoção de criptografia nos protocolos de rede fez essa abordagem perder espaço. Uma vez que os pacotes estavam codificados para o destino final, equipamentos que tentassem analisá-los no meio do caminho não poderiam ler seus dados. Desde então, a discussão sobre a complementação

dessa abordagem com medidas de segurança em hosts vem se aprofundando. Aproveitando esse nicho de mercado, diversas empresas têm elaborado soluções comerciais que permitem gerenciar de maneira centralizada mecanismos de proteção semelhantes aos de rede, porém executados de maneira distribuída, em diversas máquinas.

A **segurança via obscuridade**, de acordo com Ramos (2008), parte do princípio de que um ativo de informação só poderia ser atacado se alguém soubesse de sua existência. Portanto, uma empresa que tivesse um servidor desconhecido pelo mundo externo estaria segura. Esse conceito pode ser expandido para qualquer situação em que a segurança dependa total ou parcialmente do conhecimento de como funcionam os controles ou os ativos a proteger. Por razões óbvias, essa abordagem nunca se mostrou eficaz de maneira isolada. No entanto, ocultar informações que poderiam ser usadas por um atacante é uma excelente prática, que melhora a segurança como um todo.

A **segurança na comunicação** é fundamental, pois, além de trafegar em redes e estações de trabalho, as informações trafegam também por componentes bastante específicos das redes: os links de comunicação. As tecnologias podem ser dos mais diversos tipos: internet, linhas privadas, links de rádio, frame relay etc. Cada uma delas traz preocupações particulares para a segurança; o objetivo desta, porém, deve ser sempre o mesmo: garantir a confidencialidade, a integridade e a autenticidade da comunicação.

Essa abordagem é bastante útil quando há um grande controle no acesso aos dispositivos de determinado ambiente, mas o mesmo controle não é possível nos links, ou porque são fornecidos por terceiros, ou porque utilizam tecnologias passíveis de interceptação, como comunicação via rádio.

As **estratégias de proteção** são muito importantes, mas devem se adequar às situações definidas. Podem estar presentes no ambiente como um todo, sobrepondo-se e complementando-se.

A estratégia de **confiança** é uma das mais utilizadas, embora isso nem sempre seja evidente. Quando uma pessoa passa um cartão de crédito num restaurante, de certa forma ela confia os dados do cartão ao estabelecimento. O leitor pode ter sido adulterado para coletar dados sem que o cliente perceba, o que permite clonar o cartão. Normalmente, os leitores têm lacres, os quais, quando violados, podem indicar modificações não autorizadas, mas esse procedimento nem sempre é seguido e ensinado aos clientes. Pode-se dizer que o que a maioria das pessoas faz, mesmo que inconscientemente, é apenas confiar.

Quando se olha para o ambiente da maioria das empresas, vê-se uma situação bastante similar: muitas vezes, não existem controles de segurança porque a estratégia utilizada é confiar nas pessoas. Não se deve, porém, utilizar a confiança de maneira irresponsável. Como toda medida de segurança, ela deve ser fruto de uma relação de custo-benefício, com riscos calculados e conhecidos.

No momento em que um funcionário é contratado, o RH tem a obrigação de fazer todos os testes possíveis para avaliar a idoneidade dele. Ao começar a trabalhar, ele assina uma série de termos que permitirão à empresa processá-lo caso cometa algum tipo de violação, como vazar informações. Esse procedimento funciona como um desencorajador.

Busca-se abarcar outras situações por meio de ferramentas como câmeras em áreas críticas e monitoramento do uso da internet. No entanto, o que existe no final é, ainda, um número imenso de situações para as quais não há controle, e por isso decidimos simplesmente confiar, seja porque o custo de proteção não compense o benefício obtido, seja porque o volume de perdas estimado não justifique as medidas.

O mais importante, contudo, é não confiar de forma não calculada; é ter uma visão clara de até onde chega a confiança nas pessoas, até onde existem controles disponíveis e quais os riscos envolvidos.

A estratégia de **privilégio mínimo** baseia-se na restrição das permissões de acesso atribuídas aos componentes de um sistema, normalmente usuários. A ideia é que esses componentes, sempre que possível, tenham somente os privilégios necessários para desempenhar suas tarefas, nunca privilégios adicionais, que aumentam os riscos sem nenhum benefício em troca.

Quando entramos num prédio, normalmente passamos por vários tipos de controle, como portão externo com guarita, recepção interna com câmeras e catracas nos andares. A estratégia por trás dessa estrutura é chamada de **defesa em profundidade**, a qual prega que, do ponto de vista da segurança, é muito mais eficaz investir os recursos em diversos controles, que se complementem e sirvam de redundância entre si, do que num único controle.

A ideia básica é que não existem controles infalíveis. Sempre há espaço para brechas na segurança, mesmo que mínimas, e os controles devem se complementar para reduzir as vulnerabilidades. A defesa em profundidade aumenta o número de proteções que um atacante necessita burlar, dificultando seu trabalho.

A estratégia do **ponto de estrangulamento**, por sua vez, afirma que,

> [...] quanto menos entradas um prédio tem, mais fácil e mais barato fica protegê-las e vigiá-las. Esse mesmo conceito se aplica de forma perfeita para a segurança em redes: quanto menos entradas determinada rede possui, mais fácil é o processo de monitorá-las e torná-las seguras (RAMOS, 2008, p. 122).

A estratégia do **elo fraco** diz que a segurança de um sistema é igual à segurança de seu dispositivo mais frágil. Proteger um ambiente é uma tarefa assimétrica: quem protege deve estar atento a todos os pontos; quem ataca precisa achar apenas um ponto falho para ter sucesso. Por isso, com frequência, compara-se essa situação a uma corrente: qualquer estratégia séria de proteção deve considerar os elos fracos, que todo ambiente tem, e tratá-los de forma especial. Em muitos casos, os usuários são vistos como o elo mais fraco da estrutura, por serem mais suscetíveis à manipulação e mais difíceis de controlar.

Pela estratégia de **fail-safe**, em caso de falha nos controles de segurança, é preferível que eles bloqueiem todos os acessos em vez do contrário. Imagine a catraca de um prédio: numa situação de falta de energia, é melhor ela não deixar ninguém entrar do que permitir o acesso a qualquer pessoa; obviamente, ela deve ter um mecanismo manual de abertura e de liberação da entrada e da saída.

Muitos dos controles de segurança existentes num ambiente são implementados por meio de procedimentos. Uma rede pode ter, por exemplo, diversas máquinas Unix conectadas. Para que o ambiente tenha um bom nível de segurança, costumam-se padronizar as configurações de algumas máquinas. Tal medida será mais efetiva, porém, se todas as máquinas estiverem de acordo com o procedimento. O mesmo vale para os procedimentos seguidos pelos usuários. Buscar a uniformidade na aplicação das medidas de segurança é uma estratégia que denominamos **participação universal**, a qual, na maioria das vezes, vai além dos aspectos técnicos, envolvendo procedimentos de treinamento e conscientização dos usuários.

A estratégia de defesa em profundidade vista há pouco só é eficaz se os muitos controles utilizados forem diferentes. De nada adianta colocar dez portas iguais entre uma rua e um data center. Se o atacante for capaz de abrir uma, ele será capaz de abrir todas. Por isso, deve-se trabalhar a ideia de profundidade com diversidade, variando-se os tipos de controle utilizados.

A **simplicidade** talvez seja a mais importante estratégia de segurança. Se ela não for considerada no momento de projetar os controles, os ambientes poderão tornar-se desnecessariamente complexos, fazendo a simples avaliação de brechas, por exemplo, ser uma tarefa mais difícil do que deveria.

Lembrete

A adoção de uma única estratégia de proteção não impede a invasão. Os profissionais de redes devem sempre pensar em mais de uma estratégia, a fim de evitar uma falsa sensação de segurança.

3.3 Criptografia e infraestrutura de chaves

A criptografia é uma ciência fundamental para a segurança e serve de base para diversas tecnologias e protocolos. Suas propriedades de confidencialidade, autenticidade, integridade, autenticação e não repúdio garantem o armazenamento, a comunicação e as transmissões de forma segura.

Para entender como chegamos aos conceitos aplicados atualmente, vamos voltar ao passado e observar de que maneira tudo começou. Por volta de 1900 a.C., escribas hebreus utilizaram um sistema de substituição do alfabeto. Esse método, que ficou conhecido como **atbash**, permitia cifrar mensagens.

Tempos depois, entre 100 e 44 a.C., Júlio César, militar e político romano, utilizou um sistema chamado de **cifra de César**, que consistia em deslocar as letras do alfabeto em algumas posições. Por exemplo, utilizando a chave 3, o alfabeto cifrado seria:

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Por meio dessa técnica, a frase "Bom dia" ficaria "Erp gla".

Até os dias de hoje muita coisa aconteceu, e os métodos de criptografia evoluíram bastante. Surgiram, por exemplo, novos algoritmos, como DES (data encryption standard), 3DES (triple DES), twofish e blowfish.

Os serviços de segurança que a criptografia oferece resumem-se em:

- **Confidencialidade**: protege as informações contra acesso de terceiros não autorizados.
- **Autenticação**: verifica a identidade de um indivíduo ou de um sistema.
- **Autenticidade**: assegura a autoria de uma mensagem.
- **Integridade**: garante que as informações não foram alteradas desde a sua criação.
- **Não repúdio**: impede que uma pessoa ou um sistema negue a responsabilidade por seus atos.

Para utilizar cada um desses serviços, recorre-se a diversas técnicas, as quais serão detalhadas na sequência.

Pode-se definir a **criptografia simétrica** por meio de dois elementos fundamentais: um algoritmo e uma chave. Esta deve ser compartilhada entre os participantes da comunicação. A mesma chave é usada tanto para codificar como para decodificar as mensagens.

Considerando que toda a segurança do sistema depende do sigilo da chave, o canal de transmissão das informações (da chave e da mensagem) não pode ser o mesmo. Por isso, utilizam-se canais seguros para transmitir a chave, devido ao alto custo, e canais não tão seguros para transmitir as mensagens.

A figura a seguir demonstra como funciona a criptografia simétrica.

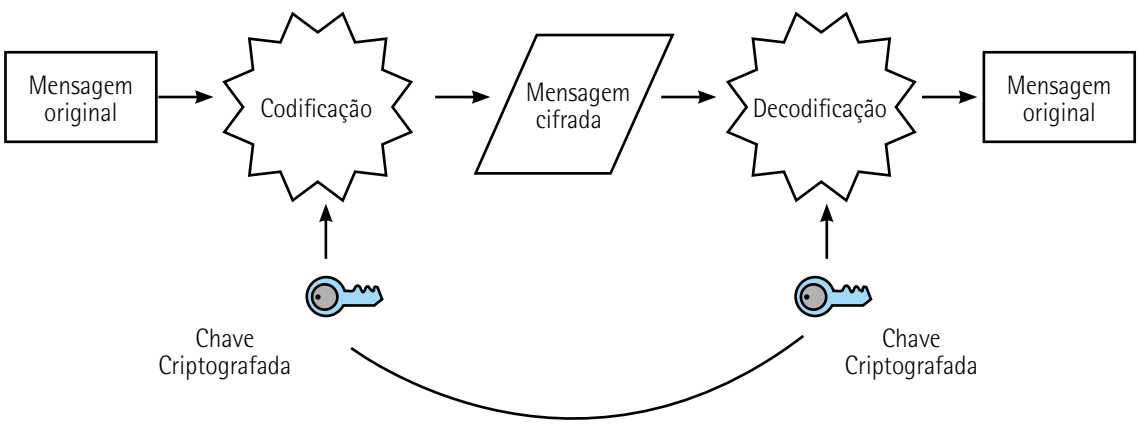

Figura 8 – Criptografia simétrica

Esse mecanismo tem algumas desvantagens, como não garantia de não repúdio e falta de mecanismos seguros de autenticação. Como vantagem, é possível citar a baixa demanda de processamento e memória. O quadro a seguir traz alguns exemplos de algoritmo simétrico e suas particularidades.

Quadro 16 – Exemplos de algoritmo simétrico

Algoritmo	Comprimento da chave	Descrição
DES	56 bits	Primeiro padrão mundial
3DES	168 bits (efetivo de 112)	Nova versão do DES
Blowfish	Variável até 448 bits	Alternativa ao DES
RC4 (Rivest cipher 4)	Variável de 40 a 256 bits	Utilizado nos protocolos SSL, WEP e WPA

As **funções de hashing** visam assegurar que uma mensagem não seja alterada no caminho. Para isso, a mensagem a ser criptografada recebe uma chave simétrica, que é utilizada para gerar o MAC (message authentication code). Nesse processo, são usadas funções cujo cálculo é fácil numa direção e bastante difícil na direção contrária.

A chave para gerar o MAC não pode ser a mesma para criptografar a mensagem, ou seja, deve haver um canal seguro para a troca das chaves. Com isso, quanto mais usuários se servem desse mecanismo, mais chaves são necessárias, o que torna o processo de gestão extremamente complicado. A fim de resolver esse problema, surgiu o conceito de **chaves assimétricas**.

Esse conceito prescreve o uso de duas chaves matematicamente relacionadas, uma pública e outra privada; quando uma mensagem é codificada com a chave pública, ela só pode ser interpretada por meio da chave privada, e vice-versa.

Tecnicamente, esse mecanismo parte do princípio de que a multiplicação de dois números primos é algo fácil de fazer, mas sua fatoração (o processo inverso), a fim de descobrir os números iniciais, é um problema bastante difícil. Um exemplo de aplicação dessa metodologia é o algoritmo RSA, proposto por Rivest, Shamir e Adleman em 1977.

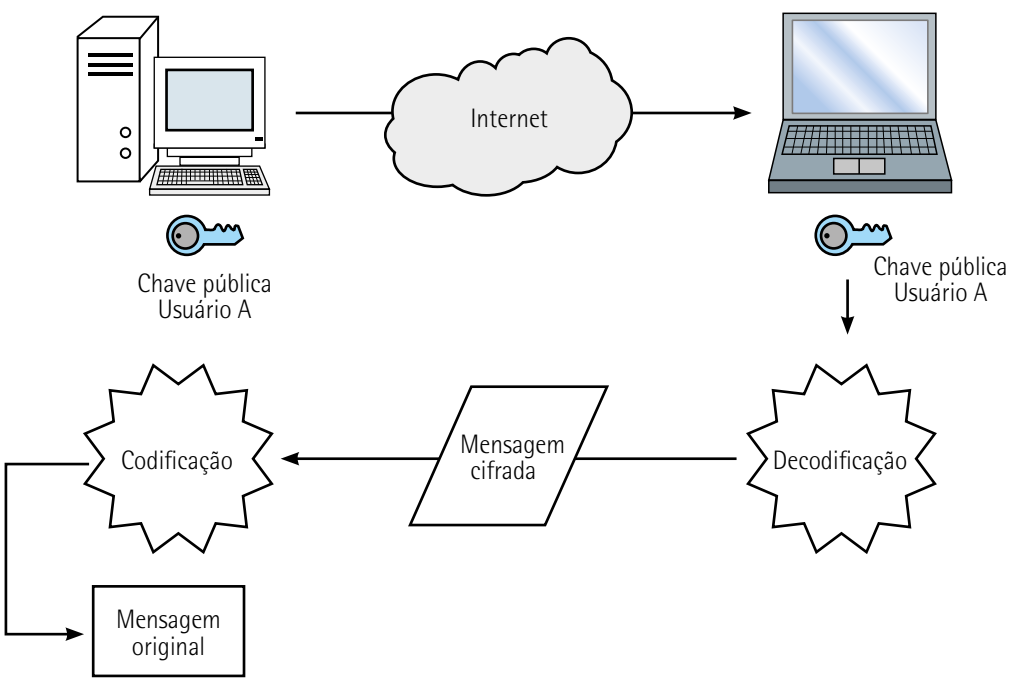

Figura 9 – Criptografia assimétrica

Até hoje, a complexidade dos problemas, assim como o tamanho das chaves utilizadas, garante o sucesso desse algoritmo. Contudo, devido à quantidade de cálculos, o modelo exige uma grande capacidade de processamento.

Para resolver questões ligadas à verificação da autenticidade de uma mensagem, os sistemas de chave pública utilizam as chamadas **assinaturas digitais**. Nesse procedimento, o remetente gera um hash da mensagem a ser enviada, o qual codifica com sua chave privada, gerando uma assinatura digital, e adiciona a mensagem, que é cifrada com a chave pública do destinatário. Se o hash da assinatura for igual ao gerado a partir da mensagem recebida, a assinatura será confirmada e a mensagem considerada autêntica e íntegra.

Percebe-se, pelo descrito, que tanto os algoritmos simétricos quanto os assimétricos têm vantagens e desvantagens. O quadro a seguir apresenta uma comparação entre os dois modelos.

Quadro 17 – Comparativo entre criptografia simétrica e assimétrica

Simétrica	Assimétrica
É mais rápida	É mais lenta
Oferece elevado nível de segurança	Necessita de uma chave maior para obter segurança
Tem baixa escalabilidade	Tem maior escalabilidade
Não proporciona outros serviços	É utilizada em outros serviços, como assinatura digital
As chaves devem ser trocadas num canal seguro	As chaves podem ser negociadas num canal inseguro

Para aproveitar melhor essas tecnologias, alguns produtos utilizam uma abordagem mista conhecida como **criptografia híbrida**, que se beneficia das vantagens de cada sistema.

Nesse modelo, a mensagem é codificada por criptografia simétrica, com uma chave gerada de forma pseudorrandômica, e sua transmissão ocorre através de algoritmos assimétricos. Um exemplo é o protocolo SSL, em que uma das partes (cliente) gera uma chave simétrica e a codifica com uma chave pública do servidor; quando a chave é recebida, o servidor a abre utilizando um algoritmo simétrico, para decodificar a mensagem. Nesse exemplo, utilizam-se o desempenho da criptografia simétrica e a segurança na troca das chaves da criptografia assimétrica.

Saiba mais

Para conhecer mais sobre a aplicação prática da criptografia como fator de segurança e vantagem estratégica, veja o filme:

O JOGO da imitação. Dir. Morten Tyldum. Reino Unido: Black Bear Pictures; Bristol Automotive, 2014. 114 minutos.

3.3.1 Segurança e ataques criptográficos

A avaliação da segurança de algoritmos está na facilidade/dificuldade de decifrar as mensagens. Além dos ataques de força bruta, a forma mais simples e também a menos eficiente de atacar algoritmos (e às vezes impossível de ser implementada devido ao tamanho das chaves), existem outras técnicas:

- **ACPA (adaptive chosen-plaintext attack)**: o criptoanalista envia diversos pequenos blocos de dados, adaptados conforme ele vai coletando informações.
- **COA (ciphertext-only attack)**: o criptoanalista tem acesso a uma ou mais mensagens codificadas.
- **CPA (chosen-plaintext attack)**: o criptoanalista é capaz de escolher o texto plano que será cifrado.
- **KPA (known-plaintext attack)**: o criptoanalista tem acesso ao texto cifrado e ao texto plano que o originou.

Todos os sistemas criptográficos têm níveis diferentes de segurança, dependendo da facilidade/dificuldade de quebrá-los.

A segurança de um criptossistema não deve basear-se nos algoritmos que cifram as mensagens, mas no tamanho das chaves usadas. Um algoritmo é considerado forte quando é praticamente impossível quebrá-lo no intervalo de tempo em que as informações são relevantes e podem ser usadas por pessoas não autorizadas.

Geralmente, a maneira mais fácil de determinar a força de um algoritmo é publicar sua descrição, permitindo que várias pessoas testem e avaliem sua eficiência. Programas que usam algoritmos proprietários não divulgam a especificação deles. Isso costuma acontecer porque a simples divulgação do método revelaria também seus pontos fracos.

3.4 Certificados digitais

Os sistemas de chaves públicas e os sistemas híbridos resolveram uma série de problemas. Entretanto, uma pergunta permaneceu: como garantir a propriedade de uma chave pública em todos esses processos? Para que isso aconteça, é necessário haver uma entidade terceira, responsável por verificar a identidade do proprietário de uma chave pública, assinando digitalmente sua comprovação. As ACs (autoridades certificadoras) foram criadas com o objetivo de atestar a propriedade de uma chave pública. Na troca de informações, cada uma das partes solicita à outra seus respectivos certificados digitais.

Esse modelo, porém, não seria viável devido às diferenças de localização e à quantidade de solicitações para uma única AC. Tal impasse foi resolvido com o relacionamento entre as ACs, que pode ser classificado em três tipos básicos:

- **Hierárquico**: uma AC raiz tem a função de assinar o certificado de outras ACs, as quais podem ter outras ACs subordinadas, e assim por diante.

- **De certificação cruzada**: a AC raiz de uma cadeia assina o certificado da AC raiz de uma nova cadeia.

- **Híbrido**: os dois conceitos anteriores são usados; por exemplo, se a AC raiz X assina o certificado da AC raiz Y, consequentemente todas as ACs abaixo dessas cadeias confiam entre si.

Para abordar as questões de gestão dos certificados não tratadas pelas ACs, pode-se recorrer a uma ICP (infraestrutura de chaves públicas), que deve combinar o uso de software, hardware, protocolos, padrões e processos.

Uma ICP é um conjunto de tecnologias e processos desenhados para prover serviços de segurança. Entre seus componentes básicos, encontram-se usuários, aplicações, ACs, certificados digitais, ARs (autoridades registradoras) e diretórios/repositórios de dados.

O objetivo das autoridades registradoras é interagir com o usuário e repassar, por exemplo, pedidos de emissão ou renovação de certificados digitais para o processamento das ACs, garantindo assim a proteção destas contra ações externas.

Quanto aos diretórios/repositórios de dados, eles fornecem um local de fácil acesso para que terceiros verifiquem os certificados emitidos pelas ACs.

A legislação sobre ICP tem por finalidade validar legalmente os mecanismos criptográficos utilizados. Em 24 de agosto de 2001, foi editada a Medida Provisória n° 2.200-2, que instituiu a ICP-Brasil, com o objetivo de "garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras" (BRASIL, 2001).

Saiba mais

Leia a respeito da ICP-Brasil em:

BRASIL. Instituto Nacional de Tecnologia da Informação. *ICP-Brasil*. Brasília, 2017. Disponível em: <http://www.iti.gov.br/icp-brasil>. Acesso em: 5 jul. 2018.

Essa medida provisória também estabeleceu um comitê gestor, cuja missão é "adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil" (BRASIL, 2001). Foram instituídas ainda a AC raiz (a primeira entidade da cadeia de certificação da ICP-Brasil), as demais ACs e as ARs, em conformidade com as normas do comitê gestor.

Resumo

Nesta unidade, consideramos algumas ferramentas para a proteção das redes coorporativas. Tratamos primeiro da segurança física. Esta, além de se encarregar de todas as instalações físicas (internas e externas) da organização, cuida da proteção dos ativos quando estão em transporte.

Destacamos depois as variadas estratégias de segurança existentes, como as de confiança, privilégio mínimo, defesa em profundidade, ponto de estrangulamento, elo fraco, fail-safe, participação universal e simplicidade. A união de estratégias é um procedimento recomendado para aumentar a segurança.

Também discutimos a criptografia, que, apesar de muito antiga, ainda é a principal ferramenta de proteção. Vimos o conceito de criptografia simétrica, em que uma mesma chave é usada tanto para codificar como para decodificar as mensagens, e o de criptografia assimétrica, em que se usam duas chaves, uma pública e outra privada.

Abordamos, por último, os certificados digitais, fornecidos pelas autoridades certificadoras, as quais são responsáveis por verificar a identidade do proprietário de uma chave pública, assinando digitalmente sua comprovação.