SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

AULA 3

Prof. Douglas Eduardo Basso

TEMA 1 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança é um guia que apresenta uma série de princípios, valores, requisitos, diretrizes, premissas, compromissos, orientações e responsabilidades sobre o que pode ser realizado para que seja possível alcançar um bom padrão de proteção de informações. Esse documento é basicamente um manual de procedimentos que elenca e descreve como todos os recursos de tecnologia de informação devem ser blindados e protegidos, trazendo recomendações de utilização e boas práticas, como um alicerce da segurança da informação. Essas regras da política de segurança devem ser pré-estabelecidas, de modo a evitar inconsistências, para que a estrutura de tecnologia não apresente nenhuma vulnerabilidade.

Quando falamos sobre política de segurança, é preciso lembrar que ela deve estabelecer normas e regras de conduta, com o intuito de minimizar a probabilidade de ocorrência de incidentes de segurança, capazes de gerar, por exemplo, problemas de indisponibilidade de serviços, perda, furto ou extravio de informações. O processo de criação de uma política de segurança deve envolver a alta administração e os colaboradores da área de negócios, pois as necessidades do negócio devem orientar a política de segurança. Assim, a experiência dos colaboradores e dos gestores na elaboração da política de segurança é essencial.

Um dos pilares da política de segurança de informação é a definição de área de responsabilidade dos usuários. A gestão dos sistemas de informação e as redes de computadores devem refletir a realidade da organização, com adaptação de toda a estrutura para que a política de segurança seja implementada na direção certa.

A Política de Segurança da Informação (PSI) é um documento que tem como função estabelecer diretrizes sobre a proteção da informação. A PSI pode ser criada com base nas recomendações propostas pela norma ISO/IEC 27001. Ela deve conter regras e diretrizes capazes de orientar os funcionários sobre os padrões de segurança adotados, obrigatórios na empresa (em certas corporações, a PSI pode ser estendida a clientes e fornecedores). É muito importante que a política de segurança da informação seja criada com base no desenvolvimento de um comportamento ético e profissional, a fim de garantir a

manutenção da integridade, a confidencialidade e a disponibilidade das informações (Donda, 2020).

Uma política de segurança eficiente é dividida em três camadas:

- Estratégia: define todos os planos e diretrizes;
- Tática: define toda a padronização (normas);
- Operacional: define os procedimentos de todos os processos.

Segundo Galvão (2015), existem três tipos de políticas de segurança:

- Regulatória: política referente às necessidades legais impostas à empresa.
- Consultiva: política opcional, isto é, não obrigatória. Esse tipo de política indica quais ações devem ser realizadas e como isso deve acontecer para que determinada atividade seja efetuada.
- Informativa: especifica o que é desejado dos funcionários, porém não descreve as consequências para o descumprimento das normas estabelecidas. Esse tipo de política contém apenas informações adicionais.

1.1 Elementos da política de segurança

A compreensão e o entendimento da política de segurança devem ser facilitados para todos os colaboradores, sem exceção. As políticas de segurança não podem ser entendidas apenas pelos especialistas de tecnologia da informação, pois nesses casos corre-se o risco de a PSI não ser colocada em prática. A alta administração deve apoiar e aprovar a PSI para que os objetivos sejam alcançados. Deve apresentar um rigor no cumprimento da norma. Além disso, os funcionários devem respeitar as regras. As sanções podem ser criadas caso o funcionário viole as regras. Sem essas condições, podem surgir muitas exceções.

Uma série de normas são utilizadas para a definição de uma política de segurança. Entre elas, podemos destacar a BS 17799 (versão brasileira da norma criada pela British Standards Institution) e as ISOs da família 27000, que abordamos anteriormente, entre as quais se destaca a ISSO 27001, foi publicada em 2005.

A norma ISO 17799 está subdivida em 12 pontos, enumerados a seguir:

- Objetivo
- Termos e definições
- Política de segurança
- Segurança organizacional
- Classificação e controle dos ativos de informação
- Segurança de recursos humanos
- Segurança física e do ambiente
- Gerenciamento das operações e comunicações
- Controle de acessos
- Desenvolvimento e manutenção de sistemas de informação
- Gestão de continuidade de negócios
- Conformidade

Alguns elementos devem fazer parte da PSI, entre os quais podemos considerar:

- Utilização: os sistemas corporativos devem ser utilizados apenas para cumprir os seus objetivos.
- Integridade: as condições de todos os aplicativos devem ser íntegras, com as informações corretas, de maneira que sejam utilizadas de maneira segura e correta.
- Disponibilidade: todos os recursos de tecnologia devem estar disponíveis para os usuários quando da sua utilização. Dados e informações sensíveis, importantes e críticos devem estar sempre seguros e disponíveis, de maneira ininterrupta.
- Autenticidade: é essencial verificar a identidade, a autenticação, o controle e a auditoria dos usuários em sistemas. Essas condições são necessárias para avaliar a identificação dos usuários que utilizam os mais diversos sistemas.
- Confidencialidade: os dados de uma organização precisam ser classificados e disponibilizados somente para os proprietários dos dados e para os grupos relacionados com a sua utilização.

Dentro desse conjunto normativo, que estabelece controles administrativos, precisamos pensar nas interações entre tecnologia, processos e pessoas. Essa trinca é amplamente difundida para o alcance de uma boa segurança da informação.

1.2 Diretrizes da política de segurança

A política de segurança é um instrumento que materializa todas a intenções do que se deseja fazer em relação à política de segurança da informação, com a transformação de princípios, valores, compromissos, objetivos, requisitos e orientações de tudo que deve ser feito para alcançar um padrão. É preciso ainda considerar o escopo, a forma e os detalhes, aspectos que devem estar totalmente alinhados às atividades de negócio. A alta administração deve definir o nível adequado de segurança a ser empregado.

Segundo Cabral e Caprino (2015), as campanhas de conscientização em segurança da informação têm como objetivo principal mudar os hábitos das pessoas, incorporando precauções até então inexistentes ou deficientes à rotina. Essas precauções podem ser determinadas por políticas organizacionais, legislação e regulamentação, melhores práticas ou uma mistura de todos esses aspectos. Trata-se da situação mais comum. Os controles de segurança da informação, sejam eles lógicos (técnicos) ou físicos, são sempre desenhados para um contexto que envolve práticas e procedimentos.

É comum que um documento de políticas apresente uma estrutura hierárquica. Vários documentos de política são desenvolvidos com base em uma política de segurança corporativa de alto nível. Eles devem estar sempre em conformidade com a política corporativa, provendo diretrizes detalhadas para uma área específica (Baars; Hintzbergen; Hintzbergen; 2018).

Existem vários tipos de políticas, porém a norma ISO/IEC 27002, ao elencar as diretrizes de uma política de segurança da informação, deve apresentar certas diretrizes, entre as quais:

- A definição de segurança da informação, com suas metas globais, importância, escopo e premissas da segurança da informação, como um instrumento que habilita o compartilhamento de informação.
- Resolução e declaração da direção sobre o comprometimento, apoiando as metas e princípios da segurança da informação, ajustados com métricas e objetivos da estratégia de negócio.
- O estabelecimento e a estruturação de todos os componentes de controle, elencando corretamente todos os controles e estabelecendo um gerenciamento de riscos, bem como uma avaliação minuciosa de todos eles.

- Um guia que explane todas as políticas, normas, princípios e requisitos de apoiem a conformidade da segurança de tecnologia, com todas as especificações da organização.
- Apresenta uma definição de responsabilidades gerais e específicas de toda a gestão da segurança da informação, com a inclusão dos registros de incidentes e dos problemas relacionados à segurança de TI.
- Referenciar toda a documentação que possa servir como base, apoiando a política, os procedimentos técnicos mais detalhados e específicos de redes, além de sistemas, infraestruturas e demais regras e diretivas de segurança que todos os utilizadores devem seguir.

Segundo Baars, Hintzbergen e Hintzbergen (2018), a ISO/IEC 27002 estabelece que as políticas de segurança da informação devem ser revisadas em intervalos planejados, ou caso ocorram mudanças significativas, a fim de assegurar a sua contínua conformidade, adequação e eficácia. Cada política deve ter um encarregado, com responsabilidade gerencial aprovada para o desenvolvimento, a revisão e a avaliação de políticas. A revisão deve incluir a avaliação de oportunidades de melhoria de políticas da organização e a abordagem da gestão da segurança da informação, em resposta a mudanças no ambiente computacional, nas circunstâncias de negócio, nas condições legais ou no ambiente técnico. A revisão de políticas para a segurança da informação deve levar em conta os resultados das revisões gerenciais.

Um tema muito importante, que vamos discutir em conteúdo posterior, refere-se à utilização de equipamentos pessoais de tecnologia da informação (como notebooks, tablets e smartphones) dentro da organização, o chamado BYOD, que traz comodidade para os colaboradores. Assim, a produtividade e a mobilidade aumentam muito, mas a falta de segurança, a necessidade de aumento de infraestrutura, além da falta de separação entre dados pessoais e profissionais, causam uma certa desigualdade entre os colaboradores.

1.3 Gestão e políticas de senhas

Com as organizações atuando de maneira cada vez mais digital, aumentam as necessidades de criação de uma boa política de senhas. As senhas aumentam a segurança dos dados e atuam em conjunto com outros elementos, como controle de acesso e backup de dados.

Segundo Baars, Hintzbergen e Hintzbergen, um guia de melhores práticas para a política de senhas traria os seguintes aspectos:

- Sensibilização: senhas são pessoais e não devem ser compartilhadas, pois além de identificar individualmente as ações de uma pessoa, elas podem ser atacadas e usadas como ponto de entrada dos sistemas.
- Conhecimento: senhas precisam ter um número mínimo de caracteres, combinando letras e números. Também devem ser trocadas periodicamente. O ideal é que não sejam uma palavra conhecida.
- Entendimento: ataques contra senhas normalmente se pautam em adivinhação através de processos automatizados. Dessa forma, quanto maior a complexidade da senha, mais tempo é necessário para quebrá-la. Escolher uma palavra existente também simplifica o processo, pois há dicionários prontos que são usados nos ataques.
- Aplicação: configurar políticas de senhas em determinado sistema operacional, software ou aplicação.

Implantar uma boa gestão e uma boa política de senhas implica gerar várias camadas de proteção para dados, evitando problemas como ataques de *ransomware*, que podem gerar danos e prejuízos. Criar controles de acesso permite aos administradores de rede estabelecer um monitoramento de quando e onde são feitos esses acessos. Assim, é possível rastrear os logins quando há um problema de segurança da informação.

Vejamos mais algumas recomendações para a gestão e a política de senhas:

- Estabelecer senhas fortes
- Elaborar senhas longas e com complexidade
- Utilizar senhas únicas para cada conta de acesso
- Trocar as senhas periodicamente
- Implementar sistemas de bloqueio de contas
- Conscientizar os usuários

1.4 Tratamento de dados

Depois de uma revisão da política de segurança, é preciso inserir nesse documento uma área relacionada ao tratamento de dados pessoais. Esse

tratamento de dados deve ser revisado. Todos devem estar cientes das revisões, e também do fato de que existe uma nova legislação que se aplica ao tratamento de dados.

No dia 14 de agosto de 2018, foi promulgada a Lei n. 13.709, intitulada Lei Geral de Proteção de Dados Pessoais (LGPD), que altera a Lei n. 12.965, de 23 de abril de 2014, o Marco Civil da Internet. Devido à crise global provocada pela pandemia do Covid-19, a lei começou a entrar em vigor apenas em agosto de 2021. Ela é dividida em dez capítulos e seções.

O **capítulo I** é dedicado às disposições gerais, em que são encontrados os princípios que fundamentam a proteção de dados pessoais (art. 2º), o âmbito de aplicação territorial da lei (art. 3º) e os conceitos básicos (art. 5º). Destacamos aqui o art. 5º Para os fins da lei, considera-se:

- I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.
- II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, além de dado referente à saúde ou à vida sexual e dado genético ou biométrico, quando vinculado a uma pessoa natural.
- V - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- VIII - Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- IX - Agentes de tratamento: o controlador e o operador.
- X - Tratamento: toda operação realizada com dados pessoais, como as referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, além de modificação, comunicação, transferência, difusão ou extração.

No **capítulo II**, são apresentados os requisitos para o tratamento de dados pessoais, com dados pessoais sensíveis, dados pessoais de criança e de adolescente, além de hipóteses de término do tratamento de dados.

Os direitos dos titulares são apresentados no **capítulo III**, com a descrição dos prazos e das formas de atendimento das requisições dos titulares.

O **capítulo IV** é dedicado ao tratamento de dados pessoais pelo Poder Público, com responsabilização em caso de infração à LGPD.

O **capítulo V** trata da transferência internacional de dados, enquanto o **capítulo VI** se ocupa dos agentes de tratamento de dados pessoais, com a responsabilidade dos agentes e o ressarcimento dos danos.

O **capítulo VII** cuida da segurança e das boas práticas a serem adotadas no tratamento de dados pessoais, enquanto o **capítulo VIII** trata da fiscalização da proteção de dados pessoais, com destaque para o rol de sanções administrativas que podem ser aplicadas pela ANPD.

A Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República, e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, são especificados no **capítulo IX**.

Por fim, o **capítulo X** se dedica às disposições finais e transitórias. A política de segurança da informação traz esses pontos importantes da LGPD, definindo as responsabilidades dos envolvidos, os níveis de acesso aos dados, a utilização permitida das informações, e se os dados podem ser fornecidos a terceiros ou não. As campanhas e os treinamentos de conscientização fazem parte desse aprendizado.

TEMA 2 – SEGURANÇA DA INFRAESTRUTURA

A gestão de infraestrutura de tecnologia da informação acabou se tornando uma das principais atividades-chave no meio corporativo. Deve servir de apoio para as tomadas de decisão. A infraestrutura tem que ser sólida e segura. O crescimento estratégico dos negócios no mercado depende da área de tecnologia da informação.

A segurança da infraestrutura tem a responsabilidade de proteger todos os dados e informações armazenados em sistemas de informação. Essa segurança não pode incluir apenas softwares e equipamentos de tecnologia – a segurança é algo muito mais complexo, de modo que deve ter uma abrangência

bem maior, sendo necessário pensar na segurança física e lógica de todos os recursos presentes na organização. É essencial garantir proteção a equipamentos, que podem ser servidores, computadores, dispositivos de rede; prever de falhas; e criar mecanismos de cópia de segurança, contingências e redundâncias, para que seja possível manter a integridade e disponibilidade dos dados e sistemas.

Uma infraestrutura de tecnologia da informação é o alicerce tecnológico que possibilita o bom funcionamento de uma organização. Dessa forma, a infraestrutura de TI envolve todos os componentes, físicos, lógicos ou virtuais, que fazem parte de um conjunto que suporta as atividades e os processos de negócios, considerando a impressão de um contrato, o compartilhamento de arquivos e informações, os projetos, a comunicação, a mensageria, as redes internas e externas, a internet e todo o ciclo relacionado a clientes, colaboradores e parceiros de negócio.

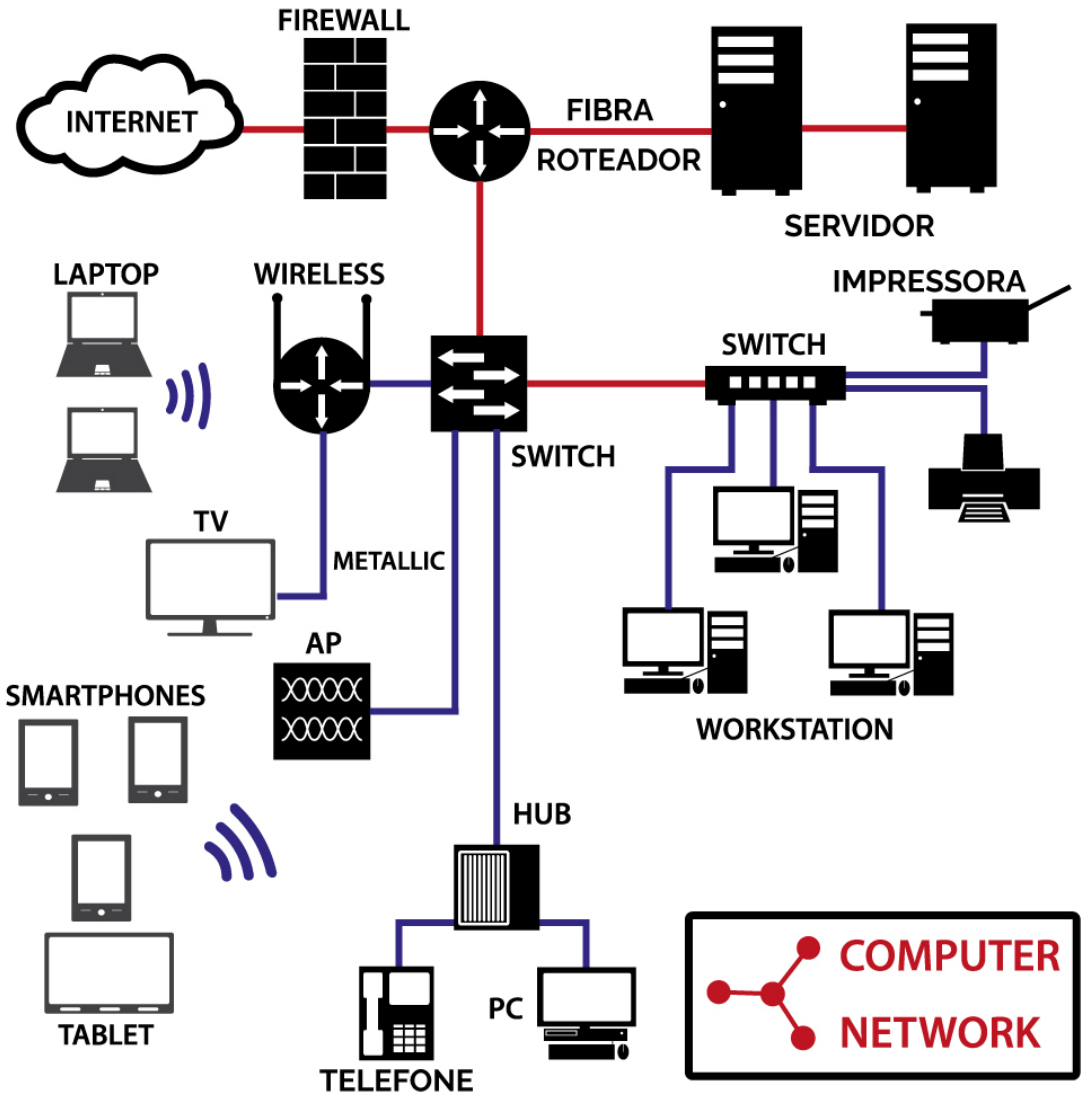
Dentre os principais elementos que fazem parte de uma infraestrutura de tecnologia, podemos elencar os seguintes:

- Computadores, notebooks, servidores de rede;
- Sistemas operacionais (Windows, Linux, Android, MacOS, entre outros);
- Impressoras, copiadoras, scanners;
- Softwares e aplicativos diversos;
- Equipamentos de redes de computadores (switches, firewalls, roteadores);
- Servidores de internet (serviços na nuvem);
- Unidades de armazenamento (storages);
- Equipamentos multimidia (câmeras, microfones, videoconferência)
- Sistemas gerenciadores de banco de dados.

A segurança de informação aplicada à infraestrutura deve ser projetada para detecção, prevenção ou até mesmo recuperação de um ataque de segurança. Deve ser responsável pela aplicação e concretização das políticas de segurança da informação. Os mecanismos utilizados para exercer esses controles físicos e lógicos são necessários para atender as propriedades de segurança e para manter a conformidade necessária ao negócio.

A Figura 1 apresenta os elementos de rede, dentro de um mapa de rede.

Figura 1 – Elementos de rede



Crédito: martin951/Shutterstock.

2.1 Controles físicos

Os controles físicos incluem uma série de medidas que devem ser aplicadas para respeitar a segurança, garantindo que um produto não seja alvo de roubo, furto, espionagem, sabotagem ou algum outro tipo de dano. Os controles físicos são barreiras que limitam o acesso ou o contato direto a uma informação, um dispositivo ou um componente da infraestrutura de TI, que garante o suporte a determinada informação.

No nível físico, é importante considerar outros tipos de ameaças físicas, dentre as quais podemos destacar:

- Ameaças naturais, terremotos, desastres, desmoronamentos, inundações, incêndios, problemas elétricos relacionados a tempestades, eventos climáticos de modo geral e outros sinistros.
- Ameaças vinculadas a elementos humanos, como tentativa de roubo e furto.
- Sabotagens internas e externas, distúrbios e acessos não autorizados.
- Problemas com temperatura e falta de energia elétrica.

Para minimizar e evitar as ameaças listadas, a segurança física deve levar em conta alguns aspectos:

- Proteção e gerência dos equipamentos: uma série de procedimentos devem ser utilizados para habilitar o gerenciamento de recursos, principalmente equipamentos que suportam as atividades críticas, em relação à segurança física de equipamentos que apresentam fontes de alimentação de energia redundantes, gerência de temperatura e componentes de segurança que emitem alertas em caso de pane.
- Controles de acesso: permitir acesso à sala de equipamentos, a datacenters e concentradores de rede a pessoas autorizadas, seja por crachá, biometria, senhas de acesso, fechadura eletrônica, utilização de câmeras de segurança, sistemas de gerenciamento de imagens. Ou seja, tais equipamentos podem ser implementados. Além disso, auditorias de acesso e outros mecanismos podem vir a garantir que somente a equipe autorizada tem acesso aos equipamentos de TI mais importantes da organização.
- Localização geográfica: as instalações dos datacenters ou do centro de informática devem levar em conta a localização. Locais próximos a caixas de água, banheiros e redes de esgoto devem ser passíveis de receber fácil monitoramento, com sistemas de combate a incêndios.
- Infraestrutura de datacenter: essas áreas precisam ser bem-estruturadas, com estrutura elétrica e lógica e temperatura controlada. A utilização de ar-condicionado é primordial. Como os equipamentos de climatização utilizam muitos recursos elétricos, e o próprio datacenter também consome muita eletricidade, é de suma importância que a infraestrutura de rede elétrica seja a melhor possível. Estabilizadores de energia, nobreaks, fontes redundantes, chaves reversoras, geradores de energia

e controles de temperatura são essenciais em tais cenários críticos. Fontes de energias redundantes, links de rede e internet de contingência são desejáveis.

É importante efetuar verificação periódica das medidas de controle físico, com a avaliação de aspectos técnicos, estado de conservação de equipamentos, rotinas de limpeza e manutenção preventiva e corretiva de instalações e dispositivos de segurança física. A finalidade de todos esses mecanismos de segurança física é evitar acessos não autorizados, evitando qualquer tipo de ataque presencial a equipamentos e estruturas, mantendo a disponibilidade dos sistemas de informação em caso de catástrofes naturais e interferências externas, falhas com a rede elétrica, entre outros fatores. A segurança de dados e informações é completada com controles lógicos.

Ao longo da disciplina, vamos falar sobre auditoria, planos de recuperação de desastres (DRP), planos de continuidade de negócios de segurança da informação e políticas de backup.

2.2 Controles Lógicos

Os controles lógicos estão relacionados com a segurança de softwares, programas, aplicativos, bancos de dados, servidores, computadores, sistemas de informação e redes de computadores. Visam garantir o acesso autorizado aos recursos de tecnologia. Sem a utilização da segurança lógica, todos os dados e informações das organizações estariam expostos a vários tipos de ataques. É necessário utilizar um conjunto de medidas que impeçam acessos indevidos, feitos local ou remotamente.

Dentre os controles lógicos, estes são os principais que devem ser levados em consideração:

- Controles de acesso: relaciona-se com a concessão ou negação de direitos de acesso a usuários de sistemas de informação. Definem quais atividades podem ser realizadas, gerando perfis de acesso. Esses controles devem prover autenticação, autorização e auditoria. Muitas aplicações usam a sigla (AAA) para processos relacionados ao controle de acesso lógico. A identificação pode ser feita de diversas maneiras. Nos próximos temas, vamos abordar o assunto mais a fundo. Também veremos em detalhes, em conteúdo posterior, os conceitos relacionados

com autenticação, autorização e auditoria, além dos protocolos Radius e LDAP, com cenários de aplicação.

- Combate a invasões e ataques: são dispositivos que se destinam a gerenciar e monitorar, filtrar e registrar acessos lógicos. Eles são colocados nos perímetros da infraestrutura de TI, com a missão de identificar e efetuar o tratamento de tentativas de ataque. São hardwares e softwares focados na proteção e no controle de acesso. Eles combatem de forma direta as tentativas de invasão e ataque.
- Firewalls: componente essencial da infraestrutura, com a responsabilidade de criar uma barreira de segurança no tráfego de dados entre redes internas e externas da organização. Efetuam o monitoramento dos acessos, com a função principal de criar uma proteção entre a internet e a rede privada. Em segurança de rede, veremos com mais detalhes os firewalls. Em estudo posterior, vamos apresentar detalhadamente o conceito de firewall, a filtragem de pacotes e as soluções de gerenciamento de ameaças integradas.
- Filtros de conteúdos e aplicações: é uma solução de segurança que faz a filtragem de acesso a páginas de internet e a aplicações. Faz a análise do conteúdo com uma filtragem, de acordo com as regras estabelecidas. Apresenta uma importante função no registro dos acessos para auditoria. No meio corporativo, muitas aplicações e conteúdos precisam ser bloqueados e filtrados, de modo a garantir melhor produtividade de colaboradores e parceiros.
- Sistemas de detecção de intrusão: os chamados IDS fazem a função de monitoria de atividades relativas a computadores e redes. Esses sistemas tentam reconhecer perfis de acessos e comportamentos nocivos, ou ainda ações intrusivas, por meio de uma análise das informações disponíveis em redes e sistemas de comunicação, geralmente criando alertas que são enviados aos administradores de rede. Em conteúdo futuro, vamos abordar em detalhes os conceitos de IDS e IPS (sistema de detecção de intrusos), com suas diferenças e similaridades.
- Antivírus: são softwares cuja função é proteger computadores e servidores de ameaças e modificações destrutivas de softwares. Apresentam a responsabilidade de impedir alterações nos sistemas operacionais, detectando a ameaça em tempo real e executando ações

para eliminá-la. Os antivírus utilizam um banco de dados com assinaturas, métodos e comportamentos mapeados de todas as ameaças já identificadas. É fundamental que sejam feitas as atualizações automáticas das soluções de antivírus.

- Criptografia: conjunto de técnicas que buscam assegurar o envio de mensagens e de informações por meio de um canal de comunicação público (até mesmo inseguro), como a internet.
- Assinatura digital: código digital que está anexado a uma mensagem eletrônica cuja função é identificar e validar a integridade do emissor e da sua mensagem.
- Certificado digital: nada mais é do que uma identificação eletrônica relacionada a empresas e pessoas. Garante autenticidade, confidencialidade e integridade, além de evitar repúdio em operações realizadas por meio da internet, com atribuições e validades jurídicas.
- Rede privada virtual: as chamadas VPNs são túneis criptográficos criados entre dois pontos autorizados. Podem ser criadas entre a internet e outras redes públicas para a transferência de informações de maneira segura. São usadas em redes corporativas e em acessos remotos, com mecanismos de troca de chaves para a cifragem dos dados. A VPN utiliza protocolos para a criação de túneis criptografados de comunicação, buscando manter as conexões seguras. Entre esses protocolos, destacamos:
    - IPsec: protocolo empregado de maneira dinâmica e flexível para garantir a segurança de transporte de dados entre duas pontas. Tem a função de autenticar e criptografar os pacotes IP de maneira individual em um processo de comunicação. O IPsec é utilizado em uma ampla gama de aplicações na camada da internet do conjunto de protocolos da Internet.
    - L2TP: um protocolo muito empregado no tunelamento, também para dar o suporte às redes virtuais privadas (VPNs), ou como componente integrante de serviços pelos provedores de serviços de internet.

2.3 Segurança de recursos humanos

Outro aspecto importante que deve ser levado em consideração são os recursos humanos, que estabelecem contato direto com todos os recursos tecnológicos e com sistemas de informação. Eles participam de todas as atividades de geração e de transformação de informações dentro das organizações.

A maior parte dos problemas de segurança da informação tem relação com colaboradores internos. Eles podem ser causados de maneira acidental ou intencional, por funcionários sem treinamento e formação adequada, ou ainda por falta de vivência ou experiência na função, negligência, ou até mesmo insatisfação com a organização. Boas práticas de recrutamento, seleção, formações desejadas e mensuração de responsabilidades são pontos de atenção na segurança de recursos humanos.

A segurança de recursos humanos deve iniciar por uma boa seleção de candidatos, com bons requisitos para as vagas ofertadas, a partir de exigências relacionadas à segurança de informações críticas. É preciso, no ato da contratação, apresentar as normas, regras e políticas de segurança da organização, o que é permitido e proibido fazer. Esses pontos devem ser acordados entre a empresa e o colaborador. A assinatura de termos e resoluções formaliza essa etapa.

A segurança dos recursos humanos deve atingir os seguintes objetivos:

- Reduzir riscos vinculados a erro humano, fraude, roubo, sabotagem e utilização indevida de qualquer informação da organização disponibilizada pelos sistemas de informação.
- Garantir que todos os colaboradores tenham conhecimento das políticas de segurança, estando cientes das ameaças à segurança e devidamente treinados e formados para o exercício de sua função de maneira normal e segura.
- Diminuir o impacto dos danos oriundos de incidentes de segurança e mau funcionamento de sistemas. O aprendizado contínuo dos colaboradores, nesse quesito de segurança, é essencial.

É interessante oferecer uma boa formação técnica para colaboradores que atuam em áreas que lidam com informações críticas. Outro fator complementar é estabelecer segregação de responsabilidades, evitando que

algumas atribuições vitais fiquem concentradas apenas em um colaborador. A concentração de atividades pode ser um risco às organizações. Falhas ou erros de um colaborador podem comprometer o processo de uma empresa. Dividir essa carga pode ser uma boa solução.

A gestão de segurança da informação deve contar com a participação de todos os colaboradores de uma empresa. A gestão também pode envolver outros atores, entre eles: terceiros, fornecedores, acionistas e clientes. Em alguns casos, é necessário criar um conselho especializado em segurança de tecnologia.

TEMA 3 – SEGURANÇA DE REDES

Segundo Baars, Hintzbergen e Hintzbergen (2018), as redes formam a espinha dorsal da maioria, senão de todos os sistemas de informação. Proteger essas redes ajuda a blindar as informações. A gestão de segurança de rede ajuda a manter os maus elementos longe dos ativos importantes.

Quando lidamos com informações altamente confidenciais, é importante lembrar que a maioria dos equipamentos conectados à rede, tais como impressoras, scanners, copiadoras, computadores e servidores, são equipados com discos rígidos. Tais discos armazenam as informações que são processadas.

Dentro desse cenário, é essencial estabelecer responsabilidades e procedimentos para a gestão segura da infraestrutura de rede. Vulnerabilidades podem aparecer inesperadamente em conexões de sistemas de comunicação, chamadas telefônicas, videoconferências, armazenamentos, dispositivos compartilhados e redes sem fio. Controlar o acesso a recursos e realizar verificações regulares sobre os utilizados dos sistemas pode ajudar nessa missão.

As redes de computadores se multiplicaram. Os sistemas operacionais estão ficando cada dia mais rápidos. Com todo esse crescimento, as redes e os sistemas começaram a sofrer ataques e invasões. Informações armazenadas pelas organizações passaram a ser violadas; além disso, dados confidenciais, principalmente de clientes, acabaram sendo expostos. Nesse momento, a segurança em redes de computadores e em sistemas operacionais tornou-se uma das maiores preocupações dos gestores de tecnologia da informação (Galvão, 2015).

3.1 Conceitos de redes

Uma rede consiste em dois ou mais computadores ligados entre si. Esses computadores compartilham dados, entre outros recursos, como impressoras, servidores e meios de comunicação de modo geral. As redes são classificadas de acordo com a sua extensão geográfica, de acordo com padrão, topologia ou meio de transmissão (Fraga, 2019).

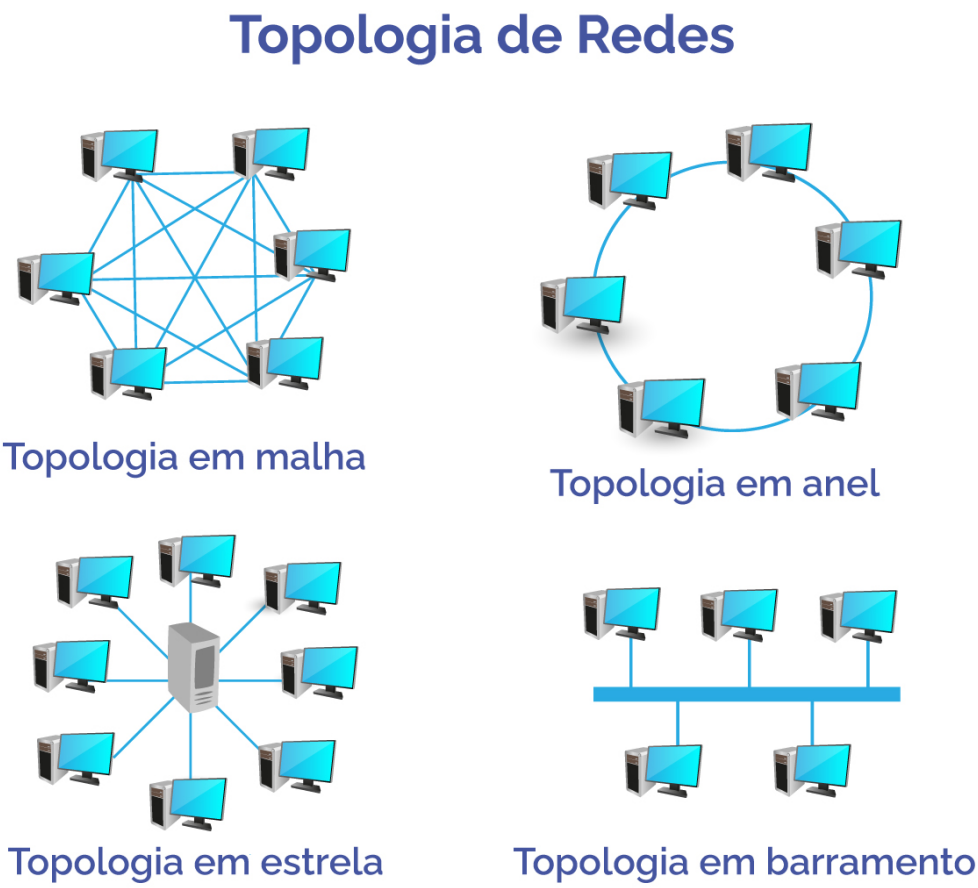
- Storage Area Network (SAN): redes utilizadas especificamente para armazenamento de dados, cópias de segurança, servidores de arquivos, entre outras funções.
- Local Area Network (LAN): redes de alcance local, que podem ser internas, de alcance curto ou médio. Podem chegar a aproximadamente 10 km, como a rede de um campus universitário.
- Metropolitan Area Network (MAN): redes que fazem a ligação de uma região metropolitana. As redes de operadoras de TV a cabo de uma determinada metrópole podem ser consideradas redes MAN.
- Wide Area Network (WAN): redes que atingem grandes extensões, de abrangência mundial, podendo interligar uma série de redes independentes – a que melhor retrata essa modalidade é a Internet.

Em relação à topologia, as redes podem ser definidas da seguinte forma:

- Topologia em Anel (Ring): todos os computadores são interligados em um único cabo, que passa pelos computadores em formato de anel. Um sinal faz o círculo por toda a estrutura. Caso um equipamento pare de funcionar, todos param.
- Topologia em Barramento (Bus): todos os computadores são interligados a uma única barra, que faz a transmissão dos dados. De modo similar à topologia de anel, se um equipamento para de funcionar, todos ficam fora da rede.
- Topologia em Estrela (Star): é a mais utilizada e eficiente. Todos os equipamentos são ligados a um concentrador de equipamentos. Apresenta facilidade para inserir e retirar equipamentos da rede a qualquer momento, sem interromper outras conexões.

- Topologia em Malha (Mesh): é uma topologia combinada, utilizada para redes redundantes e redes sem fio. A figura a seguir apresenta um layout dessas topologias.

Figura 2 – Topologias de redes



Crédito: TechnoVectors/Shutterstock.

Existem ainda outras topologias híbridas que fazem a combinação das topologias apresentadas anteriormente. Entre os meios de transmissão, vejamos elencar alguns dos mais utilizados:

- Redes de cabeamento coaxial;
- Redes de cabeamento de fibras ópticas;
- Redes de cabeamento de cobre com pares trançados;
- Redes sem fios que utilizam sinais infravermelhos, micro-ondas e rádio.

A arquitetura das redes pode ser:

- Cliente/servidor: um servidor hospeda os sistemas e informações e a máquina, na função de cliente, garante o acesso dos seus recursos ao servidor.
- Ponto a ponto (*peer to peer*): redes em que os computadores se conectam uns aos outros, com o compartilhamento de arquivos. Os computadores podem fazer as funções de cliente e de servidor.

Dentre os tipos de servidores que encontramos nas redes, os principais são:

- Servidores de arquivos: armazenam e compartilham informações.
- Servidores de impressão: fazem a gerência das filas de impressão e a comunicação com impressoras.
- Servidores de mensagens: fazem o gerenciamento de mensagens, e-mails, contatos, listas de distribuição e mensagens.
- Servidores de aplicação: hospedam os sistemas e aplicativos das organizações, as páginas web, entre outros.
- Servidores de comunicação: fazem o controle de acesso, encaminham requisições, além de filtro de conteúdo, roteamento, entre outras funções.

A comunicação dos dados executa um processo de transmissão entre um emissor, um recepto e um canal ou meio de comunicação. Entre os modos de operação dessa comunicação, temos três tipos:

- Simplex: utiliza apenas um canal de comunicação em apenas um sentido.
- Half-duplex: dois canais de comunicação (bidirecional), entretanto a comunicação não é simultânea.
- Full-duplex: dois canais de comunicação (bidirecional), com comunicação simultânea.

A comunicação em rede é feita utilizando protocolos, que são uma espécie de linguagem comum na comunicação entre os elementos de rede. São regras que visam garantir a comunicação entre emissor e receptor, bem como a utilização do canal de comunicação.

3.2 Controles de redes

Segundo Galvão (2015), a rede de uma empresa não consegue se manter ativa por muito tempo sem que um plano de segurança seja implementado.

Implementar métodos de controle e segurança de redes geralmente sai muito mais barato para a empresa do que a recuperação dos prejuízos causados por invasões ou ataques.

As redes atuam com elementos de hardware e software. Deve haver um alinhamento no gerenciamento ao acesso e no impedimento à instalação de diferentes ameaças na rede. Há um conjunto de camadas de defesa interligadas, desde a borda da rede, para permitir acesso somente a usuários autorizados, com bloqueio daqueles que apresentam potencial para executar ações indevidas, considerando ainda as redes e os dispositivos internos dentro da empresa.

Uma boa segurança de redes precisa colocar em prática algumas diretrizes para proteger os dados da organização, dentre as quais podemos destacar:

- Criar uma política de complexidade de senhas seguras e com uma estratégia definida, inclusive para as redes de acesso remoto, com conexões sem fio.
- Desenvolver uma prática de realização de cópias de segurança, com cronograma diário, mensal e semanal, executando testes periódicos de recuperação de dados.
- Fazer investimentos em soluções de segurança (como antivírus, firewalls, soluções de backup e sistemas antispam).
- Implantar uma lista de boas práticas e desenvolver uma cultura de segurança na empresa.
- Desenvolver um controle rígido em relação à instalação de softwares, combatendo a pirataria e a instalação de aplicações maliciosas.
- Definir diferentes níveis de acesso aos diferentes tipos de usuários e serviços de rede.
- Promover a atualização constante de sistemas de segurança, aplicações, sistemas operacionais e soluções de antivírus.

Para reagir às mudanças na segurança de rede, é importante conhecer o que acontece nas redes. Portanto, dependendo dos requisitos de segurança, é preciso projetar e implementar registros apropriados, com o monitoramento de redes e de serviços de rede. O objetivo do registro e do monitoramento é a detecção de violações de segurança. Também pode servir para examinar a

causa de incidentes e os problemas de segurança (Baars; Hintzbergen; Hintzbergen, 2018.

3.3 Serviços de redes

A segurança de redes tem a responsabilidade de controlar a largura de banda, coordenar a instalação de aplicativos, evitar que dispositivos conectados por usuários causem algum dano à rede, fiscalizar os usuários dos sistemas e colocar em prática a políticas de segurança. Existe uma camada na qual a segurança de redes deve atuar com muita atenção, estando integrada com todas as demais: a segurança dos serviços de rede.

Utilizar uma boa política de segurança na área de serviços permite que as organizações garantam a segurança e a eficiência necessárias para que todas as outras camadas de proteção funcionem. É importante estabelecer algumas definições em relação aos diversos serviços de rede em que a organização pode operar. Podemos elencar alguns pontos de atenção pertinentes aos serviços de rede:

- Implantar um bom controle de acesso;
- Instalar e manter soluções de antivírus e antimalware;
- Implementar a segurança nos diversos aplicativos;
- Fazer análises periódicas da rede de computadores, em sua utilização normal;
- Desenvolver prevenção de perda de dados (DLP);
- Promover a utilização segura dos serviços de e-mail e de mensagens instantâneas;
- Aperfeiçoar os filtros de acesso e o controle de aplicações, mantendo os firewalls;
- Manter sistemas de prevenção de intrusões;
- Implementar a segurança de dispositivos móveis;
- Elaborar a segmentação de rede;
- Gerenciar e monitorar as informações de segurança e o log de eventos;
- Utilizar as Rede Privadas Virtuais (VPN) no acesso remoto e na troca de informações pela internet;
- Blindar as aplicações corporativas acessadas pela web;
- Desenvolver um bom nível de segurança para aplicações e redes sem fio.

3.4 Segregação de redes

Na atualidade, as redes de dados crescem além dos limites tradicionais, em vários tipos de dispositivos móveis, com diversas aplicações, em sistemas que utilizam máquinas virtuais e sistemas hospedados na nuvem. Dessa forma, com o crescimento contínuo do volume de tráfego nas redes, novos dispositivos e aplicativos com perfis diferentes de segurança são interconectados todos os dias. As novas conexões mostram que, além de dispositivos móveis, uma série de novas aplicações com acesso à internet e acesso móvel ganham espaço: plataformas na nuvem, mídias sociais, novos navegadores e muitos acessos de computadores domésticos.

Esse crescimento em termos de conectividade aumenta a superfície de ataques à rede e cria falhas e brechas para que novos ataques ocorram. Eles podem começar pela invasão de um computador simples, depois migrar para ativos e dados mais críticos e valiosos. A busca por uma abordagem mais adequada de segmentação e segregação de recursos de rede faz com que os profissionais estabeleçam políticas que garantam somente aos colaboradores responsáveis o acesso a certos dados, informações, aplicações, servidores e recursos de rede.

A segmentação de rede, quando feita de maneira adequada, pode dificultar que um invasor localize e tenha acesso a informações valiosas da organização. A segregação é utilizada para disponibilizar controles lógicos e dinâmicos de contenção da invasão, mitigando possíveis danos e ajudando na identificação do ataque através de eventos e alertas de acesso não autorizado.

Os switches de rede apresentam uma funcionalidade chamada VLAN (Virtual Local Area Network). Esse recurso permite que um administrador de rede segmente a sua rede local, proporcionando uma divisão lógica que pode ser feita com base em departamentos, localização, finalidade de utilização, entre outras formas. Segmentar a rede ajuda em diversos aspectos: gestão, segurança, desempenho, escalabilidade e controle.

Vamos estudar os conceitos relacionados às VLANs em conteúdo posterior. A segmentação de redes IoT e as diversas camadas da computação em nuvem (acesso, neblina e nuvem) também serão um assunto importante ao longo da disciplina.

TEMA 4 – SEGURANÇA DE SOFTWARE

A segurança de software tem a missão de garantir a integridade, a confidencialidade e a disponibilidade dos recursos de informação, dando suporte à área de negócio das empresas.

Desde o primeiro momento em que a empresa considera comprar e desenvolver um sistema de informação, é recomendável que a segurança faça parte do projeto. A principal razão para isso é que adicionar segurança ao sistema de informação em uma fase posterior é mais caro do que fazer isso no projeto inicial. Projetar sistemas de informação seguros não é fácil, uma vez que eles normalmente são compostos por sistemas operacionais, infraestruturas, processos operacionais, produto pré-fabricados, serviços e aplicações (Baars; Hintzbergen; Hintzbergen, 2018).

Segundo Cabral e Caprino (2015), o software é parte fundamental da tecnologia da informação e de sistemas convencionais, tais como sistemas de transporte, militares, da área médica e financeiros. Se a presença de produtos de software em situações críticas é uma realidade, também são realidade as fragilidades de segurança a que eles estão expostos. Diversos estudos apontam que cerca de 90% das vulnerabilidades estão em software.

Nesse contexto, destaque para a ISO 15408, norma voltada para a segurança lógica das aplicações e para o desenvolvimento de aplicações seguras. Ela define métodos para a avaliação da segurança de ambientes de desenvolvimento de sistemas, estando intimamente ligada com a segurança de software. Em conteúdo posterior, também vamos abordar os *honeypots*, que são estruturas utilizadas para simular um ambiente computacional para o mapeamento de ataques cibernéticos.

4.1 Processo de desenvolvimento de software

É de grande importância para as organizações conhecer as vulnerabilidades de cada etapa e o processo da aquisição ou de desenvolvimento de software, para que as ameaças possam ser minimizadas ou removidas. É importante coletar dados e informações de cenários anteriores, fazendo o levantamento de riscos para evitar a entrega e a utilização de softwares mal estruturados e com problemas de segurança.

Segundo Cabral e Caprino (2015), os processos de desenvolvimento de software são um conjunto de atividades que cobrem todo o ciclo, desde a concepção de ideias até a descontinuação do software. Esse ciclo está estruturado em cinco processos fundamentais:

- Processo de aquisição: definição da necessidade de adquirir um produto de software. Continua com a preparação, a emissão do pedido de proposta e a seleção de fornecedor e gerência do processo de aquisição, através da aceitação do produto ou do serviço de software.
- Processo de fornecimento: pode ser iniciado tanto pela decisão de preparar uma proposta para responder a um pedido de um adquirente como pela assinatura e celebração de um contrato para fornecer o produto de software. Continua com a determinação dos procedimentos e com os recursos necessários para gerenciar e garantir o projeto, incluindo o desenvolvimento e a execução dos planos de projetos até a entrega.
- Processo de desenvolvimento: contém as atividades para a análise de requisitos, projeto, codificação, integração, testes, instalação e aceitação, relacionados aos produtos de software. Pode conter atividades relacionadas ao sistema, caso estipulado em contrato. O desenvolvedor executa ou apoia as atividades ao longo do processo, de acordo com o contrato.
- Processo de operação: contém as atividades do operador. O processo cobre a operação do produto de software e o suporte operacional aos usuários. Como essa operação está integrada à operação do sistema, as atividades e tarefas desse processo se referem ao sistema.
- Processo de manutenção: esse processo é ativado quando o produto de software é submetido a modificações no código e na documentação, devido a um problema ou à necessidade de melhoria ou adaptação. O objetivo é modificar um software existente, preservando a sua integridade. O processo inclui a migração e a descontinuação.

Com base nesses cinco processos, é possível criar, elaborar, desenvolver e entregar produtos de software a todos os segmentos de mercado, até mesmo em soluções empregadas em cenários de missão crítica.

4.2 Princípios da segurança de software

O conhecimento de alguns princípios e fundamentos básicos de segurança de softwares pode ajudar na implementação da segurança. Controles sólidos diminuem os riscos. Vejamos alguns desses princípios:

- Segurança por padrão: apresenta controles de segurança que devem ser empregados por padrão, sem nenhum tipo de configuração adicional.
- Menor privilégio: define que o software vai funcionar utilizando o privilégio mínimo necessário.
- Defesa em profundidade: combinar várias camadas de proteção sem depender exclusivamente de um único método. Todos os níveis devem ser utilizados, incluindo sistema operacional, rede e código de aplicação.
- Controles de acesso: controlar os recursos de software de forma identificada, autenticada e autorizada.
- Validação de dados: funcionalidades de checagem de dados e informações em softwares ajudam na interação do usuário com os softwares, com a validação de formatos, como data, documentos numéricos, códigos, endereços e tipos específicos de dados essenciais na segurança dos softwares.
- Proteção de dados sensíveis: o cuidado com dados e informações valiosas e sensíveis tem que ser muito maior. O armazenamento, o transporte e a apresentação desses ativos são pontos de atenção na segurança de software.
- Garantias de integridade: buscar atender a integridade, desde a origem de acesso a recursos, nos aspectos de comunicação e armazenamento, garantindo que a informação é fidedigna.
- Tolerância a falhas: elaborar mecanismos de redundância e contingência em caso de panes, garantindo a integridade dos dados e sistemas mesmo em caso de falhas.
- Auditoria: estabelecer uma estrutura para auditoria e consulta de eventos de segurança, fornecendo consultas em relação aos processos de negócios e aos usuários dos sistemas de informação.

A utilização desses princípios visa minimizar a probabilidade de que ameaças associadas a sistemas e softwares causem danos e prejuízos às organizações.

4.3 Boas práticas no desenvolvimento de software

Desenvolver um software seguro é uma das obrigações dos desenvolvedores de software. Para que essa premissa seja cumprida, é essencial analisar o ciclo de vida do desenvolvimento de software, com a identificação de vulnerabilidades e erros, o que diminui a probabilidade de problemas futuros. Uma metodologia de desenvolvimento segura, com padrões de códigos, regras e normas de codificação, pode mitigar as falhas de segurança no desenvolvimento de software.

Dentre as boas práticas relacionadas ao desenvolvimento de software, podemos destacar as seguintes:

- Gerenciamento de código-fonte: a utilização de ferramentas de gerenciamento de código-fonte possibilita a organização, o versionamento e a interação entre a equipe de desenvolvimento, mantendo a integridade e promovendo versões de código, de modo a evitar erros em versões de softwares mal concebidas, colocadas em produção de maneira equivocada.
- Realização de testes: ambientes de testes são essenciais. Desde os pequenos protótipos, até uma avaliação geral de software, são etapas essenciais para a validação do sistema e a identificação de erros e falhas, com possíveis melhorias na usabilidade do software. A realização de testes deve ser baseada no conceito Sandbox, que será abordado em conteúdo posterior, calcado em plataformas utilizadas para testes de aplicações.
- Correção de erros: o emprego de utilitários e ferramentas que permitem registrar os erros e as falhas no ambiente de teste ajuda os envolvidos no desenvolvimento do sistema a resolver possíveis bugs.
- Integração contínua: recomenda-se a prática de buscar a qualidade dos softwares com a integração a outros sistemas e aplicativos. Automatizar as verificações e garantir a compatibilidade e a portabilidade de um software são pontos positivos no desenvolvimento.

- Documentação do software: com a rotatividade cada vez maior dos recursos humanos, é importante ter uma documentação bem elaborada e clara de toda a arquitetura. Os códigos-fonte buscam impulsionar a qualidade do software desenvolvido. Desenvolver uma documentação coesa, objetiva e bem estruturada é fundamental para que o software seja criado, desenvolvido e expandido de forma segura e sustentável.
- Padrões de códigos seguros: trata-se de elencar listas de códigos seguros para o desenvolvimento, seguindo as boas práticas de acordo com a linguagem da programação adotada e com a plataforma onde o software é hospedado e desenvolvido. Recomenda-se ainda o emprego de checklists para avaliar e analisar as principais funcionalidades e ações durante o desenvolvimento do software, com revisões nos quesitos de segurança.

No ambiente de desenvolvimento, é essencial que os desenvolvedores criem novos softwares, ou ainda que atuem na mudança de softwares existentes, utilizando esquemas de versionamento. Esse requisito de segurança deve ser aplicado.

Segundo Baars, Hintzbergen e Hintzbergen (2018), a fim de garantir que as mudanças não sejam implementadas de forma descontrolada, também é recomendável estabelecer ambientes de desenvolvimento, testes, além de aceitação e produção dos sistemas de informação. O ambiente de teste serve para determinar se o desenvolvimento atende aos requisitos gerais e, mais especificamente, aos requisitos de segurança.

A figura a seguir apresenta algumas boas práticas relacionadas ao desenvolvimento de softwares.

Figura 3 – Boas práticas em desenvolvimento de software

Crédito: limeart/ Shutterstock.

4.4 Responsabilidades com a segurança de software

Para que as práticas de segurança de softwares sejam adequadamente implantadas, é preciso elencar as responsabilidades e classificar os papéis de cada um dos membros da equipe dentro das atividades de desenvolvimento de software seguro. Dentre os principais envolvidos, podemos elencar os seguintes:

- Administradores de sistemas: principais responsáveis pelos processos de operação, suporte e disponibilidade do produto de software para usuários e clientes.
- Gestores de negócio: sua função é fazer o elo entre as necessidade e expectativas de negócio e o desenvolvimento do software.
- Auditores de segurança: têm a responsabilidade de efetuar os testes mais específicos e detalhados em relação à segurança da informação.
- Testadores: fazem a validação e os testes relacionados a casos de uso, analisando requisitos estabelecidos, simulações e operação do sistema.
- Gerentes: têm a responsabilidade de coordenar as ações e as atividades executadas pelos times de desenvolvimento e pelos demais envolvidos.
- Arquitetos: fazem definições em relação à plataforma de desenvolvimento, considerando ainda arquitetura utilizada, normas, padrões e convenções técnicas de produção de software.

- Desenvolvedores: são os principais atores do processo, atuando como responsáveis por implementar e codificar os requisitos e as regras dos negócios estabelecidos no software.

4.5 Segurança em modelos de desenvolvimento

No desenvolvimento de sistemas, existem modelos e metodologias que se constituem como práticas calcadas em técnicas e rotinas criadas para melhorar a produtividade e garantir coesão e coerência para o desenvolvimento de software. Entre esses, modelos podemos destacar os seguintes métodos:

- RAD (Rapid Application Development): traduzido como Desenvolvimento Rápido de Aplicação, é um modelo de desenvolvimento de software incremental, tendo sido foi registrado por James Martin em 1991. É um processo de desenvolvimento de aplicações. Funciona de maneira rápida, com objetivos bem definidos e uma análise de requisitos bem alinhada. Esse modelo reforça o uso de um ciclo curto, com a finalidade de garantir um desenvolvimento melhor e mais rápido.
- RUP (Rational Unified Process) – traduzido como Processo Unificado Rational, foi criado pela Rational Software Corporation. Em 2003, foi adquirido pela IBM. Faz uso de uma abordagem de orientação a objetos. Seu conceito é projetado e documentado com a utilização de UML para ilustrar os processos. Entre suas principais características, destaque para o fato de que é incremental e iterativo.

Em relação à segurança, verificamos que esses modelos de processo de softwares foram desenvolvidos muito antes disseminação da internet. Foram criados e elaborados quando o ambiente tecnológico ainda não tinha uma preocupação generalizada com as vulnerabilidades e com a segurança da informação, em decorrência da exposição de aplicações computacionais às redes abertas de internet.

TEMA 5 – SEGURANÇA DE DADOS

A gestão da segurança da informação estabelece uma base para um programa de segurança abrangente, a fim de garantir a proteção dos ativos de

informação da organização. Hoje, as organizações estão altamente interligadas através da internet. Praticamente nenhuma organização pode alegar que tem sistemas de computadores isolados (Baars; Hintzbergen; Hintzbergen, 2018).

Um banco de dados é um grupo lógico de arquivos que se relacionam, armazenando dados e associações entre eles. Trata-se de um conjunto integrado de elementos de dados relacionados logicamente. As tarefas pertinentes ao armazenamento, à recuperação, ao gerenciamento e à segurança dos dados são de responsabilidade dos sistemas de gerenciamento de banco de dados (Kolbe Junior, 2017)

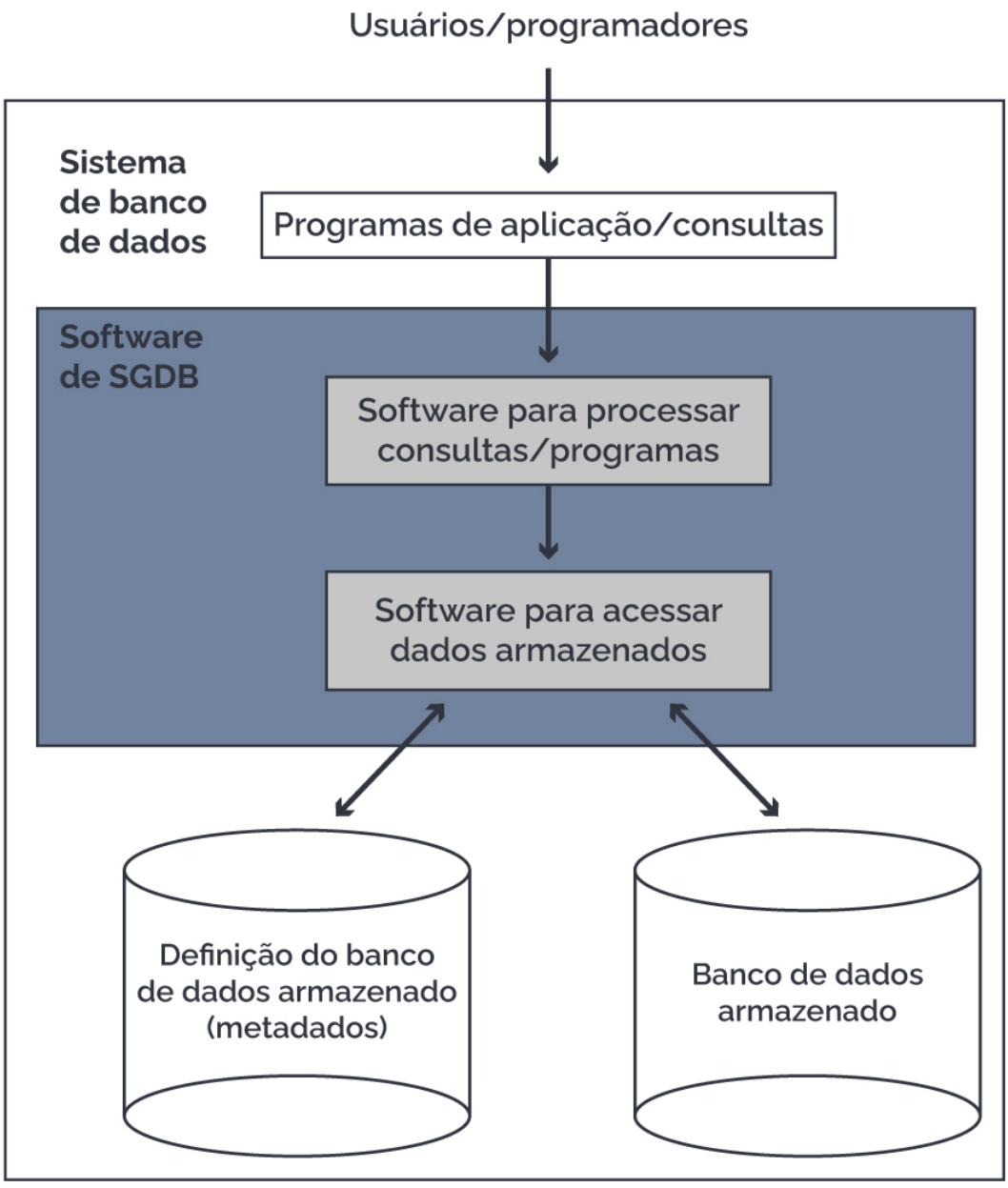
Segundo Galvão (2015), um banco de dados é um conjunto de informações relacionadas entre si, armazenadas de maneira estruturada, de preferência com o mínimo de redundância. Os dados armazenados por um banco de dados devem ficar disponíveis para que sejam acessados por diferentes programas e usuários, incluindo os mais diferentes sistemas computacionais que tiverem permissão para tal acesso.

Para que um banco de dados seja eficaz e eficiente, são necessárias algumas características e princípios:

- Redundância: ao longo da utilização dos sistemas, o armazenamento de dados das organizações acaba aumentando muito. Os dados acabam sendo gravados de maneira redundante, principalmente quando departamentos e setores organizacionais fazem uso dos dados de maneira simultânea, o que resulta em aumento dos custos de armazenamento e dificulta a gestão e a gerência dos dados pelos sistemas de informação.
- Inconsistência: os dados podem estar armazenados de maneira errada – podem estar desatualizados e incompletos. A inconsistência pode levar a tomadas de decisões equivocadas. Alterações e atualizações constantes na base de dados podem produzir inconsistência. A redundância, somada com a inconsistência, pode acarretar problemas relacionados com a atualização e com dados em locais e setores diferentes da base de dados.
- Integração: como há um compartilhamento intensivo entre as bases de dados e os mais diversos sistemas que operam sobre esses dados, existe a necessidade de promover integração, estabelecendo níveis de controle em relação à consolidação, à atualização e à comunicação desses dados entre os departamentos e os setores corporativos.

A figura a seguir apresenta um diagrama simplificado de um ambiente de sistema de banco de dados.

Figura 4 – Diagrama de ambiente banco de dados



Fonte: Elmasri; Navathe, 2018.

5.1 Ciclo de vida dos dados

Entender e documentar o ciclo de dados na sua empresa é vital para o desenvolvimento do processo de adequação. Trata-se de acompanhar e entender tudo o que acontece com os dados, desde a sua criação e recebimento até a sua exclusão. O ciclo de vida dos dados envolve as atividades de coleta,

produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação e modificação (Donda, 2020).

A figura a seguir traz algumas etapas do ciclo de vida dos dados.

Figura 5 – Ciclo de vida dos dados

Crédito: Ashalatha/Shutterstock.

Com a nova lei de proteção geral de dados (LGPD), o ciclo de vida e o tratamento dos dados ganhou mais importância. Nas etapas de coleta, processamento e compartilhamento, é preciso ter atenção quanto aos princípios e responsabilidades. Em muitos casos, é preciso ter o consentimento específico do proprietário das informações.

Ainda com relação ao ciclo de vida dos dados, com o entendimento dessas etapas é possível identificar quais dados podem ser eliminados, considerando que as organizações não têm mais propósito para armazená-los.

5.2 Classificação e mapeamento de dados

A classificação e o mapeamento dos dados auxiliam na operação e na manutenção das principais características da informação. Algumas normas, como a ISO 27002, recomendam que os dados pertinentes às informações de uma organização sejam classificados e mapeados com base em características como valor, criticidade, sensibilidade e requisitos legais. Essa prática atende algumas premissas da segurança da informação:

- Confidencialidade: os dados podem ser confidenciais, reservados ou públicos.
- Disponibilidade: os dados devem estar disponíveis em minutos, semanas ou meses. Além disso, é necessário elencar dados cuja falta possa impactar a organização.
- Integridade: pode ser vinculada à alta, média e baixa exigência em relação à integridade.
- Autenticidade: recai sobre as exigências de checagem de validade, veracidade e autenticidade de dados e informações. É importante saber a procedência e confirmar a utilização.
- Outros fatores: a classificação pode estar focada em aspectos como criticidade, sensibilidade, ou ainda se os dados são vitais.

Uma das etapas mais difíceis e complexas da segurança de dados é elaborar o mapa de todos os dados da organização. Com o advento da Internet, da computação em nuvem e da computação distribuída de maneira geral, fica praticamente impossível que os gestores de tecnologia façam esse controle. Assim, existem softwares que podem ajudar com a descoberta dos dados (*data discovery*), com os controles de prevenção de perda dos dados (*data loss prevention*) e com a classificação dos dados (*data classification*):

- *Data discovery*: os softwares de descoberta de dados identificam, analisam e classificam, de maneira automática, dados que contêm informações pessoais, como nomes, endereços, documentos, contas bancárias e telefones.
- *Data loss prevention* (DLP): têm a finalidade de auxiliar na busca de informações e na classificação de informações, com base em criticidade e importância. Softwares de DLP conseguem detectar e impedir violações

de dados, transferência não autorizadas, ou ainda descarte indesejado de informações confidenciais. Fazem a proteção dos dados em repouso ou mesmo em movimento, na nuvem ou em qualquer estação de trabalho de usuários.

- *Data classification* – atuam no rastreamento e na proteção das informações. É possível utilizar os softwares de classificação com base em parâmetros de conteúdo dos arquivos, de maneira automatizada ou manual. Existem ferramentas que implementam essa classificação por níveis: secreto, confidencial, público etc. A classificação deve acontecer antes da utilização do DLP. A classificação auxilia os gestores nas tomadas de decisão.

5.3 Recursos de segurança de dados

Segundo Galvão (2015), um banco de dados é um conjunto de informações relacionadas entre si, armazenadas de maneira estruturada, de preferência com o mínimo de redundância possível. Os dados armazenados por um banco de dados devem ficar disponíveis para que sejam acessados por diferentes programas e usuários, incluindo diferentes sistemas computacionais que tiverem permissão para esse acesso.

A segurança das informações armazenadas em bancos de dados está baseada em alguns recursos que podem ser utilizados para diminuir as probabilidades de ocorrência de incidentes de segurança:

- Acesso de administração: limitar a poucos colaboradores o acesso privilegiado a serviços de dados. O controle e o gerenciamento desses acessos são atividades essenciais.
- Segurança local e física: impedir o acesso físico a servidores locais que possuam bases de dados é uma prática excelente. Recomenda-se evitar cópias de dados e informações não autorizada dos servidores, risco que acaba sendo minimizado sem um acesso físico aos equipamentos.
- Blindagem de servidores: minimizar a área de ataque de um servidor é uma boa medida de proteção. A blindagem de servidor elimina serviços e recursos que não sejam realmente necessários dentro dos servidores. Os administradores dos bancos de dados são peças fundamentais para a blindagem dos servidores.

- Criptografia: a cifragem dos dados também é muito utilizada em bases de dados e no seu transporte. Diversos sistemas de gerenciamento de banco de dados apresentam funcionalidades ligadas com criptografia e segurança.
- Auditoria e gerência de eventos: monitorar todos os eventos e atividades dentro da base de dados faz parte de uma boa auditoria. Ações suspeitas, tentativas de ataque e acessos não autorizados estão vinculados geralmente ao acesso e à ação de algum usuário no banco de dados. A documentação e a utilização de ferramentas avançadas de auditoria permitem a criação e a elaboração de alertas de atividades. Recomenda-se a revisão de arquivos que guardam as informações dos eventos (logs). Em sistemas grandes, milhares de acessos a bancos de dados são realizados diariamente, de modo que o histórico desses acessos é importante.
- Cópias de segurança: a realização de cópias de segurança (backup) é uma medida primordial para a segurança dos bancos de dados. A recuperação dos dados e a sua restauração, em caso de falhas, é uma necessidade bem comum. Existem ainda questões relacionadas com a retenção de informações em virtude de novas legislações (LGPD), considerando ataques virtuais de sequestro de dados. As rotinas de backup devem ser diárias, semanais e mensais. Validação e testes de recuperação devem ser feitos periodicamente.

FINALIZANDO

Nesta aula, abordamos os principais temas relacionados às políticas de segurança da informação, seus elementos e definições, e também o tratamento de dados. Além disso, observamos a estrutura da nova lei geral de proteção de dados (LGPD). Estudamos ainda as premissas de segurança de informação, com enfoque na infraestrutura, nos sistemas e nas redes. Nosso objetivo foi oferecer uma visão geral de como é possível montar uma boa política de segurança; quais são as normas, regras e procedimentos a serem utilizado; além dos elementos que fazem parte da estrutura de segurança de informação de uma organização.

REFERÊNCIAS

BAARS, H.; HINTZBERGEN, K.; HINTZBERGEN, J. **Foundations of information security**: based on ISO 27001 and 27002 Rio de Janeiro: Brasport, 2018.

CABRAL, C.; CAPRINO, W. **Trilhas em segurança da informação**: caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.

DONDA, D. **Guia prático de implementação da LGPD**: conheça estratégias e soluções para adequar sua empresa em conformidade com a Lei. São Paulo: Labrador, 2020.

ELMASRI, R.; NAVATHE, R. E. **Sistemas de banco de dados** 7. ed. São Paulo: Pearson Education do Brasil, 2018.

FRAGA, B. **Técnicas de invasão**: aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Labrador, 2019.

GALVÃO, M. da C. **Fundamentos em segurança da informação**. São Paulo: Pearson Education do Brasil, 2015.

KOLBE JUNIOR, A. **Sistemas de segurança da informação na era do conhecimento**. Curitiba: InterSaberes, 2017.