SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

AULA 4

Prof. Douglas Eduardo Basso

CONVERSA INICIAL

Nesta aula vamos estudar conceitos relacionados aos ataques à segurança da informação, a identificação das várias formas de ataques cibernéticos, as classificações das ameaças, os tipos de *hackers*, quais são suas formas de ação e os interesses por trás dos ataques digitais. Vamos falar também sobre o ataque de engenharia social, as maneiras como esses ataques são feitos ao se utilizarem da autoconfiança, vaidades, responsabilidade, entre outros, como tudo isso é motivado. Serão abordados os conceitos de risco, ameaça e vulnerabilidade.

Ao longo desta aula vamos elencar os impactos relacionados aos ataques cibernéticos, quais são os principais códigos maliciosos e como criar medidas e contramedidas para se defender dessas ameaças. Outro tema abordado será o controle de acesso, os processos de autenticação, auditoria e contabilização, cenários de implementação de mecanismos de autenticação e, por fim, vamos falar sobre diversos aspectos relacionados à auditoria.

TEMA 1 – ATAQUES À SEGURANÇA

Os sistemas de informação são instrumentos fundamentais na gestão administrativa e estratégica de qualquer organização. São sistemas que trazem mais velocidade, versatilidade, agilidade e disponibilidade das informações, entretanto são sistemas que precisam garantir a tríade de segurança da informação (confidencialidade, integridade e disponibilidade) e gerir quem são os proprietários e utilizadores dos sistemas.

A área de tecnologia da informação deve trabalhar e contribuir efetivamente para que a organização aumente seus dividendos e minimize suas perdas e prejuízos. À medida que os especialistas em segurança da informação desenvolvem e evoluem as técnicas e tecnologias de segurança, tornando os sistemas e infraestruturas mais seguros e com menos vulnerabilidades, os criminosos e atacantes virtuais (cibernéticos) estão cada vez mais especializados na exploração de redes, infraestruturas e nos elementos humanos das organizações.

Para Galvão (2015), a área de segurança da informação deve proteger as informações dos mais diversos tipos de ameaças, com o objetivo de preservar o seu valor, fazendo-se necessária para:

- Garantir a continuidade dos negócios;
- Reduzir ao mínimo possível os riscos que podem surgir;
- Potencializar ao máximo os retornos dos investimentos feitos ao negócio;
- Gerar, cada vez mais, boas oportunidades à organização.

Segundo Donda (2020), sempre que falamos em ataques, é comum vir pensarmos nos *hackers*, e essa denominação ficou associada a algo sempre malicioso e ilegal. No entanto, um *hacker* vai além disso: ele é um indivíduo que se dedica a conhecer os mecanismos e a entendê-los profundamente, a fim de solucionar problemas, principalmente no meio cibernético.

Um *hacker* é qualquer pessoa capaz de acessar, criar ou modificar sistemas, a fim de alterar serviços, sistemas, dados e informações ou inserir novas funcionalidades que permitam seu acesso e sua manutenção. Existem diversas categorias de *hacker*. Vamos enumerar algumas delas:

- *Blue Hat* – é um *hacker* que tem a função de varrer e coletar vulnerabilidades em redes e sistemas, antes de um lançamento de produtos, *software*, serviço, *website* ou aplicativo;
- *Grey Hat* – nessa categoria, os *hackers* fazem a invasão de sistemas por diversão, geralmente sem causar nenhum tipo de dano nem modificar ou roubar dados. De qualquer forma, é bom lembrar que qualquer tipo de invasão ou ataque cibernético é considerado crime;
- *Black Hat* – sãos os *hackers* que utilizam seus conhecimentos para fins maliciosos e criminosos. Em algumas literaturas, são chamados de *crackers*, pois causam danos e prejuízos às organizações;
- *White Hat* – são os chamados *hackers* éticos, têm o foco no estudo e desenvolvimento da área de segurança da informação e se tornam especialistas em cibersegurança;
- *Hackers* governamentais – são *hackers* que acabam sendo contratados por agências de inteligência ou governos e utilizam seus conhecimentos para nações no cenário de guerra cibernética, espionagem etc.;
- Hacktivista – nessa categoria, os *hackers* empregam seus conhecimentos com o intuito de cooperar em causas sociais, ideológicas, religiosas, políticas, entre outras.

- *Insiders* – são utilizadores internos dos sistemas, funcionários legítimos de uma organização. São os que causam mais danos e prejuízos, utilizam seus acessos privilegiados para coletar dados e informações.

Os atacantes seguem uma linha e estrutura de ataque, iniciando com a coleta, enumeração, reconhecimento do alvo. Geralmente são realizados varreduras e escaneamento dos serviços, em busca de informações na internet, dados relacionados ao alvo, execução do ataque, acessos, manutenção de acessos, por fim, a limpeza de rastros, tentando evitar a identificação do ataque.

1.1 Engenharia social

Engenharia social é um termo utilizado para descrever um método de ataque em que alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou da confiança do usuário. É um conjunto de métodos e técnicas de manipulação psicológica de pessoas a fim de conseguir a execução de ações ou de modo que a pessoa consiga executar as ações ou de modo que a pessoa possa divulgar informações confidenciais (Donda, 2020).

A engenharia social é conhecida como a arte de manipular pessoas com a finalidade de coletar informações, seja pela internet, por telefone, correio eletrônico, correspondência tradicional, aplicativos de mensagens instantâneas, redes sociais ou até mesmo o contato direto. A engenharia social faz uso da exploração da ingenuidade dos recursos humanos. De modo geral, a engenharia social ocorre de algumas maneiras:

- Autoconfiança – transmite diálogos coletivos ou individuais, procura passar confiança, segurança, conhecimento, eficiência e saber, criando uma estrutura de comunicação favorável;
- Vaidades profissionais e pessoais – os recursos humanos costumam ser receptivos, com análises positivas, favoráveis, elogios. Nesse tipo de ataque, são utilizados argumentos pessoais e profissionais favoráveis;
- Utilidade – muitos se comportam de maneira proativa, com cortesia, com a intenção e vontade de ajudar, ser útil aos outros;
- Busca por novas amizades – quando são utilizadas técnicas de aproximação; quando da abertura de um diálogo, pessoas tentam se passar por amigos buscando coletar informações;

- Responsabilidade – quando os seres humanos se colocam responsáveis por um conjunto de atividades;
- Persuasão – é a maneira e a capacidade de persuadir pessoas na obtenção de dados e informações de uma forma mais específica. As pessoas possuem uma série de características de comportamento que as tornam vulneráveis.

Criminosos fazem da engenharia social uma ferramenta muito poderosa para conseguir o que desejam, o que envolve aplicar golpes, desde o funcionário de mais baixo cargo em uma empresa até funcionários do alto escalão (Fraga, 2019)

1.2 Motivos de ataques à segurança

Os ataques à segurança da informação geralmente tentam expor, destruir, adulterar, violar, alterar, inutilizar, roubar ou até mesmo ganhar acesso de maneira não autorizada, ou fazer utilização da informação de maneira ilegal. São ataques que exploram as vulnerabilidades e falhas de um sistema de informação, de uma rede de computadores, servidores, ou qualquer outro elemento da infraestrutura de tecnologia da informação. Existem também alguns ataques relacionados aos recursos humanos e que são geralmente nocivos para as organizações.

Para entender e combater os ataques à segurança da informação é essencial ter conhecimento dos diversos tipos de ataque para que, dessa maneira, seja possível montar medidas preventivas. Os ataques podem ser motivados por algumas finalidades, tais como:

- Adquirir e escalar privilégios de acesso a sistemas;
- Capturar dados e informações pessoais de usuários;
- Fazer o roubo de dados e informações corporativas, segredos industriais ou propriedades intelectuais;
- Buscar informações bancárias;
- Coletar informações de organizações;
- Tornar um sistema inoperante, dificultar o bom funcionamento de sistemas de informação;
- Estabelecer acesso a redes, computadores e sistemas de maneira não autorizada e criar um ataque a partir desse acesso;

- Utilizar os recursos da estrutura de tecnologia invadida para outros fins;
- Expor vulnerabilidades e colocar sistemas em risco.

1.3 Classificação dos ataques

Conhecer os ataques é uma maneira de identificar as ameaças. Para a adoção de medidas corretas, é necessário saber que existem vulnerabilidades e ameaças para que possamos pensar em uma boa segurança da informação. Os ataques podem ser classificados em quatro categorias:

1.3.1 Interrupção

Um ataque que atinge diretamente a disponibilidade das informações, tornando-a inacessível. Esse tipo de ataque tem o intuito de prejudicar o acesso dos usuários a serviços e informações.

1.3.2 Modificação

Esse ataque promove a alteração de mensagens que estão sendo transmitidas e interfere na integridade das informações.

1.3.3 Interceptação

Nesse tipo de ataque, os invasores conseguem ler, ter acesso e monitorar o tráfego de dados, conversações, antes mesmo que essa mensagem chegue a seu destino, afetando diretamente a confidencialidade.

1.3.4 Fabricação

Esse tipo de ataque tem relação com a autenticidade dos usuários e suas informações e ocorre quando um atacante se passa por um usuário do sistema, cria informações falsas com o intuito de coleta e transmissão de informações dentro da rede atacada.

Os ataques podem ainda ser classificados como *ativos* e *passivos*:

- Ataque passivo – faz a enumeração, captura, leitura e coleta de dados e informações de maneira não autorizada. Nada ocorre com o conteúdo das informações. Esse ataque passivo monitora os serviços e informações

sem que ocorra nenhuma percepção do alvo atacado e tem a finalidade de fazer o reconhecimento da rede e sistemas;

- Ataque ativo – nesse tipo de ataque, o invasor atinge de maneira contundente o seu alvo atacado, modificando informações, derrubando e degradando serviços de rede e sistemas com a intenção de danificar, causas danos, destruir os dados e a sua estrutura de rede. Nesse caso, são utilizadas as informações coletadas no ataque passivo. Assim, acessos não autorizados são realizados, e o sistema invadido acaba sendo infectado.

1.4 Riscos e ameaças

Para Cabral e Caprino (2015), o cenário de riscos está se ampliando e mudando rapidamente, e os desafios associados a eles continuam a evoluir. Além de preocupações com incertezas econômicas, o mercado financeiro, as exigências regulatórias, existem outros riscos enfrentados, como fraudes, fusões, aquisições, grandes projetos, lançamento de produtos e a continuidade de negócios. A tecnologia está presente em todo esse cenário e deve ser determinante em questões relacionadas à regulamentação, sigilo, segurança de dados, reputação, marca, fraudes, recursos humanos, grandes projetos e políticas governamentais. A Figura 1 a seguir mostra uma tabela com vários elementos que fazem parte desse cenário de risco:

Figura 1 – Elementos do cenário de riscos

Fonte: Cabral, 2015.

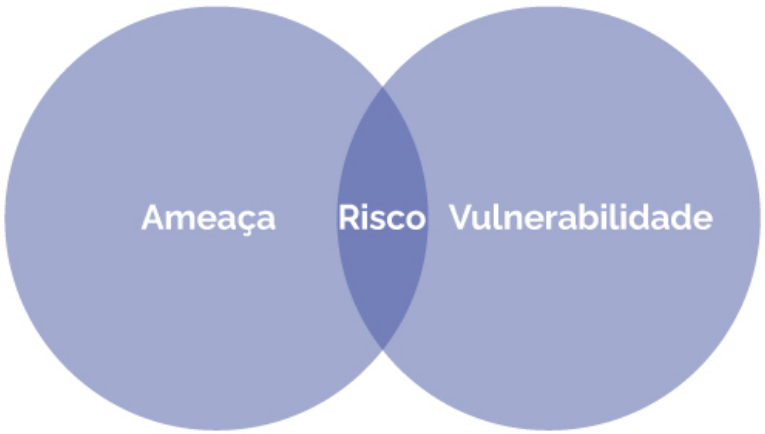
Para Galvão (2015), no cenário de riscos atual, em constante mudança, é preciso adotar uma mentalidade estratégica de reação aos riscos que ajudem a preparar a organização para novas ameaças e oportunidades.

Para entendermos melhor a questão, é preciso saber que uma ameaça é todo e qualquer fato capaz de causar, de forma eventual, um incidente ou problema que possa implicar algum tipo de dano ou prejuízo a uma organização. Podemos ainda considerar como uma ameaça as condições ou os agentes que, por meio de exploração de vulnerabilidades, criam incidentes e impactam a integridade, a confidencialidade e a disponibilidade das informações e outros ativos de tecnologia da informação, provocando perdas ou prejuízos aos processos de negócio.

Já o risco pode ser conceituado como uma possibilidade de determinada ameaça se consolidar em algum fato que afete e comprometa um serviço, um sistema, uma informação por meio de uma vulnerabilidade. Os riscos podem ser **naturais**, **involuntários** e **intencionais**. O risco é medido pela possibilidade de uma situação acontecer e de este produzir algum dano ou prejuízo.

A avaliação e a análise de riscos são muito importantes para dar visibilidade à situação dos ativos de uma organização, assim como priorizar os investimentos e proteger os ativos da melhor maneira possível. Conhecer o ambiente e o cenário de atuação da organização é fundamental. A análise de risco é um método de identificar vulnerabilidades e ameaças para avaliar possíveis impactos e determinar como elaborar controles de segurança da informação. Não existe risco se não há uma ameaça e uma vulnerabilidade associadas, conforme a Figura 2 a seguir (Donda, 2020].

Figura 2 – Ameaça, risco e vulnerabilidade



Fonte: Donda, 2020.

1.5 Vulnerabilidades

As vulnerabilidades são fragilidades que podem ser exploradas por algum tipo de ameaça que visa sempre estabelecer e concretizar um ataque. Essas fragilidades podem estar em processos, políticas de segurança, dispositivos eletrônicos, equipamentos de rede, servidores, sistemas operacionais e até mesmo nos recursos humanos. Com o advento da internet, esta se tornou o principal meio utilizado para invasões, pois o aumento de vulnerabilidades foi muito grande, e os ataques cibernéticos são, hoje, a principal fonte de danos e prejuízos das empresas.

Uma vulnerabilidade é uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Uma vulnerabilidade caracteriza a ausência ou a fraqueza de uma proteção que pode ser explorada. Essa vulnerabilidade pode ser um serviço rodando em um servidor, aplicações ou sistemas operacionais desatualizados, acesso irrestrito para entrada de chamadas em um equipamento de rede, uma porta de comunicação aberta no *firewall*, uma segurança física fraca que permita a qualquer pessoa entrar em uma sala de servidores ou a não aplicação de gestão de senhas em servidores e estações de trabalho (Baars; Hintzbergen; Hintzbergen, 2018].

Segundo Fraga (2019), o processo de identificação de análise de vulnerabilidades consiste em tarefas que vão desde a navegação no *site* em busca de páginas de erros e a exploração do código-fonte até o uso de ferramentas específicas, como varredores de rede a fim de obter versões de serviços e sistemas operacionais. Uma análise de vulnerabilidades não se aplica apenas a sistemas e serviços eletrônicos; ela engloba tudo que possa existir, desde uma simples caneta até pessoas, sendo possível aplicar engenharia social das mais diversas formas.

Para um melhor entendimento, é possível classificar as vulnerabilidades como:

1.5.1 Naturais

São as vulnerabilidades naturais tais como incêndios, inundações, terremotos, tempestades, furacões, entre outros.

1.5.2 Organizacionais

Referem-se a políticas, planos e procedimentos da organização e podem ser geradas pela ausência de política de segurança, pela falta de treinamento, por falhas, processos malconcebidos, deficiências em planos de contingência e redundância, recuperação de desastres e continuidade de negócios.

1.5.3 Físicas

Estão relacionadas com o ambiente: instalação realizada de maneira inadequada, falta de recursos para combate a incêndio, problemas elétricos, energia e conexões de rede, acesso descontrolado e desprotegido em locais críticos, problemas de vigilância e controle de acesso.

1.5.4 *Hardware*

São vulnerabilidades encontradas nos equipamentos de tecnologia da informação, podendo estar vinculadas à falta de atualização, configuração incorreta, conservação inadequada, *software* desatualizado, gerenciamento deficiente, entre outras causas.

1.5.5 *Software*

Aplicativos que apresentam pontos fracos, codificação incorreta, aplicativos sem camada de segurança, *softwares* obsoletos, instalação feita de maneira errada, entre outros.

1.5.6 Meios de armazenamento

Estão relacionadas aos meios de armazenamento como discos rígidos, dispositivos removíveis, discos ópticos (CD e DVD), disquetes, fitas magnéticas, sistemas de banco de dados, documentos impressos. Dentro dessa modalidade podemos elencar também questões como validade, utilização incorreta dos meios, falta de cópias de segurança, locais de armazenamento insalubres (umidade, estática, magnetismo, mofo), entre outros.

1.5.7 Humanas

Causam grande preocupação, pois é uma vulnerabilidade que tem sua origem na falta de capacitação técnica para o desempenho das funções, falta de consciência de segurança nas atividades, falhas, erros, omissões, desleixo, descontentamento na elaboração e no segredo com dados, informações, senhas, acessos no ambiente de trabalho, não utilização dos meios de segurança como: criptografia, cópias de segurança, antivírus, senhas fortes etc.

1.5.8 Comunicação

Estão incluídas nos processos de envio e recebimento de mensagens, no tráfego de informações, seja por qualquer meio de comunicação (fibra óptica, telefone, cabo, internet, rádio, *fax*, telefone, satélite), problemas com o tratamento, armazenamento, leitura das informações, ausência de sistemas criptográficos no transporte dos dados por meios inseguros (internet), escolha de equipamentos e sistemas de comunicação obsoletos, com protocolos de rede desatualizados, com falhas de segurança, falta de *firewall* e filtragem de acessos e informações, rede não segmentada, senhas fáceis.

O gerenciamento de vulnerabilidades é a prática que permite identificar, classificar, corrigir e mitigar vulnerabilidades. Esse processo envolve o conhecimento das tecnologias envolvidas e, em determinados casos, o uso de *softwares* especializados permite gerar um relatório de apoio ao gerenciamento de vulnerabilidades (Donda, 2020)

TEMA 2 – TÉCNICAS DE MITIGAÇÃO E CONTRAMEDIDAS DE SEGURANÇA

A revolução digital que temos presenciado atualmente está criando estímulos para que todas as organizações de qualquer porte se esforcem ao máximo para acompanhar esses avanços tecnológicos a fim de se alinhar e garantir seu crescimento, seja no ambiente físico ou digital. Dessa forma, isso exige um bom investimento na segurança de informações e sistemas.

Tendo em vista que já é possível entender questões relacionadas a riscos, ameaças e vulnerabilidades, é preciso empregar modelos, técnicas, modelos e mecanismos de segurança para que a organização fique livre de ataques, roubos, danos e prejuízos vinculados a invasões e ataques cibernéticos.

As técnicas de mitigação são mecanismos essenciais na área de segurança da informação. Trata-se de técnicas que visam minimizar e reduzir os impactos de ataques cibernéticos em organizações. As ferramentas utilizadas nessa etapa executam ações contínuas, acompanhando, notificando e classificando as ameaças existentes.

Uma contramedida é posta em prática para mitigar o risco em potencial. Ela pode ser uma configuração de *software*, um dispositivo de *hardware* ou um procedimento que elimine a vulnerabilidade ou reduza a probabilidade de um agente ameaçador ser capaz de explorar a vulnerabilidade. Existem várias contramedidas, como gestão de senhas fortes, um guarda de segurança, mecanismo de controle de acesso, treinamento de conscientização sobre segurança (Baars; Hintzbergen; Hintzbergen, 2018].

Os principais desafios que os especialistas de segurança encontram são a identificação de soluções, métodos e ferramentas que sejam capazes de ser utilizadas em cada camada de segurança computacional, garantindo que os dados e informações empresariais estejam completamente seguros. A segurança da informação é obtida pelo implemento de conjuntos adequados, incluindo as políticas, processos, normas, regras, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Esses controles precisam ser criados, elaborados, implementados, mantidos, monitorados, mantidos e avaliados para atingir os objetivos e a continuidade dos negócios.

Para Baars, Hintzbergen e Hintzbergen (2018), se uma empresa possui um *software* antivírus, mas não mantém as assinaturas dos vírus atualizadas, isso é vulnerabilidade, ou seja, a empresa está vulnerável a ataques de vírus. A ameaça é um vírus que aparece no ambiente e prejudica a produtividade. A probabilidade de um vírus surgir no ambiente e causar danos é o risco. Se um vírus se infiltrar no ambiente da empresa, então a vulnerabilidade foi explorada, e a empresa está exposta à perda. A contramedida nessa situação é prevenir-se contra um ataque de vírus instalando um *software* antivírus em todos os computadores e, é claro, mantendo as assinaturas dos antivírus atualizadas.

2.1 Incidentes e impactos

Ao avaliarmos as medidas a serem tomadas em relação a incidentes de segurança da informação, algumas pesquisas e estudos realizados em várias organizações e fontes de dados mostram quais são os principais impactos

causados pelos problemas e ameaças que permeiam o ambiente de tecnologia da informação. É preciso identificar esses impactos e mitigar esses problemas, tais como:

- Aumento de gastos com seguros;
- Fuga de clientes, contratos, fornecedores e colaboradores;
- Danos a reputação e imagem das pessoas ou organização;
- Diminuição de produtividade e desempenho;
- Multas e penalidades jurídicas;
- Prejuízos financeiros diversos;
- Gastos maiores com recuperação, retrabalho, reparação e recuperação de problemas.

Em outras pesquisas relacionadas à área de tecnologia sobre o mercado brasileiro, foram identificados os principais incidentes de segurança da informação. Ter o conhecimento dos incidentes mais comuns pode ajudar nos esforços e medidas para mitigá-los. Nesse aspecto, as maiores ocorrências foram:

- Vazamento de informações.
- Má utilização de recursos de tecnologia da informação.
- Exclusão de informações.
- Codificação maliciosa
- Problemas e falhas em equipamentos de tecnologia da informação.
- Iniciativas e tentativas de invasão.
- Ataques de engenharia social
- Acesso feito de forma indevida e não autorizada (acessos físicos e lógicos)

2.2 Códigos maliciosos e medidas de segurança

Código malicioso é um tipo de código para computadores ou *script* que se hospeda na internet e que é nocivo, tendo por finalidade estanciar vulnerabilidades em sistemas e gerar portas de acesso à comunicação, violações de segurança, roubo de dados e informações, além de outros danos e prejuízos possíveis a sistemas de informações, aplicativos, redes de

computadores e serviços. Vamos dar atenção especial a esses códigos maliciosos e elencar os principais:

2.2.1 Malware

É a combinação das palavras inglesas *malicious* e *software* e se refere a *softwares* indesejados, tais como vírus, *worms*, cavalos de Troia (*trojans*) e *spyware*. Uma medida padrão contra *malware* é usar antivírus e *firewalls*. Entretanto, está ficando cada vez mais claro que um antivírus sozinho não é suficiente para parar um *malware*. As principais razões são as ações humanas. Muitas vezes os equipamentos são infectados pela abertura de um anexo de *e-mail* malicioso; em alguns casos, parecem mensagens inofensivas (jogos, documentos, imagens), mas podem conter um vírus (Baars; Hintzbergen; Hintzbergen, 2018].

2.2.2 *Phising*

É uma espécie de fraude de internet. O golpe acontece quando uma vítima recebe uma mensagem eletrônica solicitando que este execute algo, confirme alguma informação, preencha algum formulário, entre outros. Essa fraude também migrou para aplicativos de mensagens instantâneas, e até mesmo golpes por telefone já foram registrados. É muito difícil identificar os autores dessas fraudes porque muitas mensagens como estas são enviadas por emissores forjados, ou contas anônimas. É necessário manter a vigilância e nunca responder a esse tipo de mensagem nem confirmar dados ou enviar informações, transferir dinheiro em hipótese nenhuma, senhas, códigos, número de cartões, entre outros.

2.2.3 *Spam*

É um termo utilizado para se referir a mensagens eletrônicas indesejadas, muitas delas originadas de campanhas publicitárias. Mensagens fraudulentas geram muito lixo eletrônico e acabam lotando a caixa de mensagens dos usuários. Filtros de mensagens são implementados para conter esse tipo de mensagens, mas existe uma série de regras para a criação e elaboração desses filtros, sendo recomendável, por exemplo, que as mensagens sejam excluídas, desativadas e denunciadas.

2.2.4 Vírus

É um tipo de *software* malicioso (*malware*) criado e programado para se autorreplicar e que faz cópias de si mesmo em qualquer unidade de armazenamento conectada ao seu computador. Um computador pode ser infectado por um vírus de três maneiras: mídias removíveis (*pendrives*, dispositivos USB), *downloads de internet* (softwares e aplicativos) e a *abertura de anexos* de uma mensagem eletrônica ou clicando em *links* suspeitos no corpo do *e-mail*. Como medidas contra os vírus, recomenda-se manter o sistema operacional e antivírus instalado com versões e definições atualizadas, sistemas *antispam* para o serviço de mensagens, elaborar campanhas de segurança da informação, boas práticas e políticas de segurança.

2.2.5 *Worm*

São programas maliciosos; um tipo de *malware* autônomo que se replica e se propaga por redes de comunicação, sem a interação de usuários. Os *worms* não precisam que um programa esteja sendo executado em um equipamento: uma vez o sistema infectado por um *worm*, este usa as conexões de rede para se propagar com muita velocidade. Como medidas preventivas estão as soluções de antivírus, sistemas operacionais atualizados e ferramentas de monitoramento de rede, pois é necessário gerenciar o tráfego de rede, uma vez que os *worms* consomem muita banda quando o sistema está infectado por eles.

2.2.6 Cavalo de Troia

Também chamado de *trojan*, é um *malware* que, além da função principal que está disposto a desempenhar, faz a condução de maneira proposital a outras atividades secundárias, acabando sendo imperceptíveis pelo utilizador do computador. Está disfarçado em um *software* legítimo, sendo utilizado por criminosos virtuais para a criação e obtenção de acesso a sistemas, espionagem, roubo de dados e danos de desempenho aos computadores e redes infectadas. Os *trojans* não conseguem se replicar. Como medida de segurança, é importante que o antivírus, além de instalado e atualizado, também tenha funções de varredura para que os *trojans* sejam detectados. A utilização de um *firewall* para fazer a detecção do tráfego suspeito de rede também é

importante, e o monitoramento de rede pode colaborar na descoberta de cavalos de Troia ativos na rede.

2.2.7 *Hoax*

Também chamado de *boato* ou *farsa*, é uma espécie de *spam*, que nada mais é que uma mensagem eletrônica que tenta convencer o receptor da mensagem de sua veracidade e depois tenta persuadir o usuário a efetivar determinada ação. As mensagens têm teor distorcido e duvidoso e são replicadas por seus leitores (diferente dos *spams*). Como medida de segurança, deve haver soluções de *antispam* atuando em conjunto com os servidores de *e-mail* e campanhas de conscientização em relação à segurança relacionada a mensagens eletrônicas.

2.2.8 Bomba lógica

É um código malicioso que infecta computadores de uma maneira parecida com vírus e é inserido de forma secreta em uma rede de computadores, aplicativo, *software* ou sistema operacional. São pequenos códigos inseridos em outros programas. Ele fica em espera até uma condição específica ocorrer. Tem como objetivo principal destruir dados e causar danos a discos rígidos. Como medida preventiva é necessária a revisão de códigos pelas equipes de desenvolvimento de *software* ou equipe de terceiros.

2.2.9 *Spyware*

É um *malware* que fica oculto enquanto coleta e registra secretamente os dados e informações de usuários (senhas, PINs, número de cartões, hábitos de navegação, *e-mails*), realizando o rastreamento das atividades e espionagem. Esses dados coletados são enviados para terceiros sem o conhecimento do usuário, afetam o desempenho do computador infectado, fazendo com que apareçam programas não instalados na tela. Barras de ferramentas novas nos navegadores de internet e janelas de navegação indesejadas são sinais de que o computador está infectado com esses *softwares* espiões. Medidas para conter os *spywares* são antivírus instalado e atualizado, utilização de ferramentas que inspecionem os registros do sistema operacional em busca de *software*

suspeitos, uso de um *firewall* para fazer a detecção de tráfego de rede suspeito, especialmente o tráfego de saída de dados.

2.2.10 *Botnets*

O termo foi criado da combinação das palavras *robot* e *network*, os *hackers* utilizam *trojans* para violar e ter acesso a vários equipamentos. Ao assumirem o controle de vários equipamentos, esses criminosos virtuais organizam esse grupo de máquinas infectadas para enviar *spams*, executar ataques de negação de serviço e espalhar *malwares* pela rede. Medidas para conter a *botnet* são sistemas operacionais e antivírus atualizados, ferramentas de varredura de registro de sistemas, soluções de segurança como *firewalls* e um bom monitoramento de rede para fazer a descoberta desses tráfegos maliciosos.

2.2.11 *Rootkit*

É um *malware* que possui uma coleção de *softwares* em sua estrutura, sendo utilizados pelo *hacker* para obter e manter o acesso a um sistema. Um *rootkit* consegue esconder a si mesmo em suas atividades, acaba se integrando ao sistema operacional e consegue fazer a interceptação de solicitações, sendo capaz de criar e ocultar arquivos (inclusive arquivos de sistema), conexões de rede, endereços de memória, alteração de processos. Pode permanecer por longos períodos no sistema infectado sem ser percebido. Medidas para conter os *rootkits* são antivírus e sistema operacional atualizado, ferramentas de inspeção de registro e processos do sistema operacional, utilização de *firewall*, ferramentas de monitoramento de tráfego de rede.

2.2.12 *Ransomware*

É um *malware* de extorsão que faz o bloqueio de computadores e depois solicita um resgate (*ransom*) para fazer o desbloqueio. O *ransomware,* após ganhar o acesso ao dispositivo, faz a criptografia de todo o sistema operacional ou arquivos específicos. Um resgaste é exigido do usuário que teve seu computador infectado. As medidas de segurança para evitar esse *malware* são sistemas operacionais atualizados, antivírus com funcionalidades de varredura,

sistema *antispam* e um plano de contingência pode ser criado, por exemplo, um *backup* de todos os dados deve ser feito periodicamente em local seguro.

2.3 Recuperação de desastres

O propósito de um plano de recuperação de desastres é minimizar as consequências de um desastre e tomar medidas necessárias para garantir que funcionários, ativos e processos de negócio estejam disponíveis novamente dentro de um tempo aceitável. O plano de recuperação de desastres é uma medida imediata após um desastre. O trabalho é focado em determinar os danos e fazer os sistemas e equipamentos funcionarem novamente (Baars; Hintzbergen; Hintzbergen, 2018).

Os analistas de tecnologia devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Segundo Donda (2020), de modo bem generalista, é necessário identificar quais ativos possuem maior dependência ao negócio e maior risco associado e entrar criar um plano de recuperação em caso de desastre para não afetar as operações comerciais e a segurança. Sistemas de recuperação contra desastres fazem uso de tecnologias de *backup*, replicação e redundância de *software* e *hardware*. Ao implementar ou verificar essas tecnologias, devemos ter atenção especial aos requisitos e às capacidades de proteção das informações.

Para Baars, Hintzbergen e Hintzbergen (2018), o propósito de fazer cópias de segurança (*backup*) é manter a integridade e a disponibilidade da informação e das instalações computacionais. As consequências da perda de informação dependem da idade da informação que pode ser recuperada a partir do *backup*. É importante considerar a rotina de *backup*: diário, semanal, mensal e os intervalos de tempo em que os *backups* são executados. As cópias de segurança devem ser testadas periodicamente.

TEMA 3 – CONTROLE DE ACESSO, AUTORIZAÇÃO E CONTABILIZAÇÃO (AAA)

Segundo Cabral e Caprino (2015), o controle de acesso compreende um conjunto de processos para gerenciar todo o ciclo de vida dos acessos dos usuários, internet ou externos, dentro de uma organização.

Uma política de controle de acesso deve ser estabelecida, documentada e revisada com base nos requisitos de negócio e de segurança da informação. Isso significa que o controle de acesso lógico também pretende prevenir que pessoas não autorizadas ganhem acesso lógico a qualquer coisa que tenha valor para a organização. Em organizações com políticas restritas de conformidade, as autorizações são normalmente concedidas pela pessoa responsável pelo ativo, aplicação ou informação, geralmente um gerente (Baars; Hintzbergen; Hintzbergen, 2018).

Os dados pessoais e os dados pessoais sensíveis podem estar armazenados em diversos locais, por isso é importante conceder o acesso de maneira a garantir que não haja mais acessos que o necessário. Existem muitos tipos específicos de atribuição de permissões de acesso a objetos como pastas, arquivos, banco de dados, computadores, serviços, entre outros (Donda, 2020).

Os controles de acesso são uma combinação de acessos lógicos, relacionados a sistemas de informação e acessos físicos. Dentre alguns tipos de acessos, podemos destacar uma lista com alguns deles:

- Acesso às informações;
- Acesso às aplicações de negócio;
- Acesso a equipamentos de tecnologia da informação;
- Acesso a redes e serviços.

Existem outras atividades dentro do controle de acesso que têm a função de prevenir os ativos de tecnologia da informação, garantindo sempre o acesso a pessoas autorizadas e reprimindo os acessos indevidos e não autorizados. É essencial estabelecer algumas premissas de gestão de acesso, as quais podemos elencar logo a seguir:

- Cadastro, registros, desligamentos e cancelamentos de acesso de usuários;
- Registros e controles de perfil de acesso dos usuários;

- Gestão de direitos para acesso de usuários avançados, administradores e privilegiados;
- Provisionamento de acesso, informações secretas, métodos de autenticação;
- Revisão periódica de direitos de acesso a usuários.

Para que o controle de acesso funcione, é fundamental que os usuários conheçam suas responsabilidades em termos de manter as informações e os ativos seguros e protegidos. Para conseguir isso, os usuários devem ser responsáveis por suas próprias informações de autenticação, salvaguardando essas informações. Isso significa que um usuário deve manter suas senhas seguras e não compartilhar com outros (Baars; Hintzbergen; Hintzbergen, 2018).

3.1 Autenticação

A partir da década de 1960, com a criação dos primeiros computadores multiusuários, surgiu a importância e a necessidade de fazer a identificação dos usuários que acessavam os sistemas e as informações. Dessa maneira, também foi necessário separar e filtrar o conteúdo de acesso de cada usuário. Com isso começavam a surgir os primeiros sistemas de autenticação que vêm evoluindo até os dias de hoje.

Com o advento da internet e o crescimento das redes de computadores, com maior largura de banda, latências menores, redes sem fio mais robustas, aumentaram também os índices de crimes cibernéticos, quebra de senhas, interceptação de mensagens, roubo de informações. Com os dados de outros usuários coletados, ficava fácil forjar mensagens, acessar sistemas com credenciais roubadas e executar acessos de maneira não autorizada.

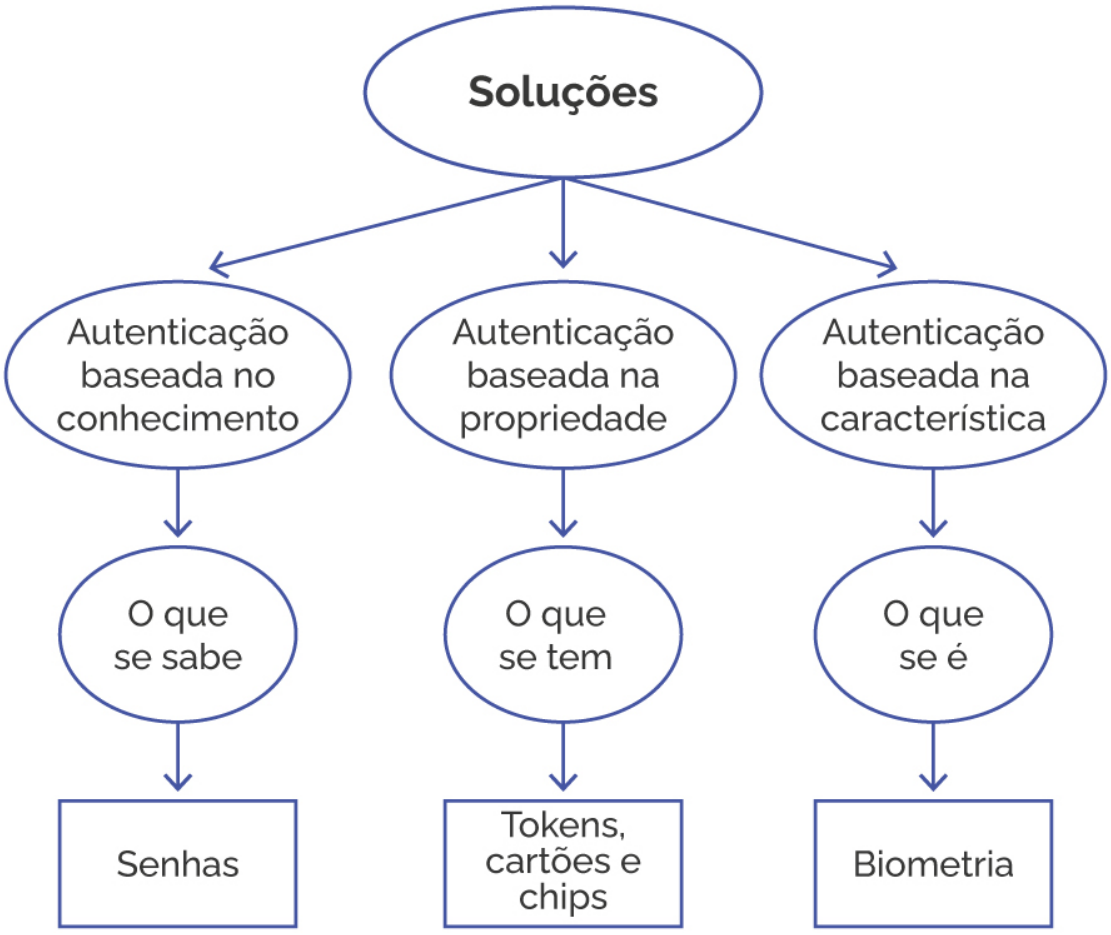
Dentro desse cenário, os meios utilizados para autenticação e identificação dos usuários se tornou algo primordial, a fim de garantir a segurança das informações. Para Galvão (2015), há três categorias de autenticação de usuário: *conhecimento*, *propriedade* e *característica*. Vamos descrevê-las a seguir:

- Autenticação por conhecimento – faz a utilização de informações que o usuário saiba. Destaca-se pelo uso senhas, segredos, chaves de criptografia e perguntas randômicas. É baseada no conhecimento que o usuário possa informar;

- Autenticação por propriedade – utiliza o que o usuário possui, como cartões inteligentes, chaves ou *tokens*, um objeto físico que o usuário tem. É uma espécie de prova de posse, autenticando um usuário baseado na posse de objetos físicos, artefatos, *tokens*, entre outros;
- Autenticação por característica – utiliza dados relacionados ao que o usuário é, como processo de reconhecimento de voz, identificação por biometria, rosto, impressão digital, padrão de íris, formato da mão e aspectos comportamentais ou até mesmo padrões de digitação. A autenticação é feita por meio de uma característica física ou comportamental.

A Figura 3 logo a seguir apresenta os três tipos de soluções de autenticação:

Figura 3 – Tipos de autenticação de usuários



Fonte: Galvão, 2015.

Independentemente de qualquer tipo de técnica utilizada, a autenticação precisa ser segura, mas ao mesmo tempo não pode criar nenhum tipo de

constrangimento. Além disso, os métodos biométricos são os mais caros e possuem etapas de autenticação um pouco mais complexas que as demais. Boas práticas relacionadas ao *login* de acesso, como exibir nomes padrões de usuários, mostrar mensagens de último *login* com êxito, tentativas malsucedidas de acesso, entre outras, podem ser úteis para a identificação do usuário, mas também podem ser pistas para os criminosos virtuais.

Ainda falando de autenticação, temos um conceito que envolve gestão de identidades chamados *single sign-on*, que é uma maneira de criar para o usuário uma autenticação única para que ela possa acessar uma série de recursos de tecnologia, sistemas, servidores, internet, entre outros, de uma maneira bem transparente. Sem que seja preciso passar por outros processos de autenticação, isso ajuda em questões relacionadas à eficiência operacional, gestão de riscos, sincronismo de senhas e o uso de diretório integrado para autenticação e sincronismo com outras bases de usuários.

Umas das melhores formas de ajudar a proteger os acessos é habilitar multifatores de autenticação. Em autenticação de sistemas, podemos utilizar senhas (algo que o usuário conhece), biometria (algo que o usuário é) e *tokens* (algo que o usuário tem). Esse método exige *hardware* específico, o que encarece a implementação, porém é muito seguro. Os *tokens* são muito utilizados pelas redes bancárias, podem usar *hardware* ou *software* e têm como função gerar um valor que deverá ser digitado para comprovar a autenticação (Donda, 2020).

3.2 Autorização

É de grande valia que o controle de acesso a sistemas e informações esteja alinhado com o modelo e norma de segurança adotado pela organização, seguindo uma política de segurança da informação. Mesmo que os utilizadores dos sistemas sejam devidamente identificados e autenticados, é necessário ainda verificar as questões de autorização, permissões de acesso de acordo com sua responsabilidade e nível hierárquico e funcional. Dessa maneira, é necessário que os sistemas tenham restrições de acesso em relação a dados, aplicações, arquivos, pastas, utilitários, entre outros.

A autorização de acesso pode ser implementada de algumas maneiras, vamos apresentar as principais:

3.2.1 Autorização de acesso mandatória

Na autorização de acesso mandatória, os acessos são provenientes de uma política. Os proprietários e utilizadores podem somente permitir acessos a outros colaboradores dentro das regras estipuladas por essa política, uma vez que a sua gestão geralmente é centralizada. Nessa política, deve conter as descrições de usuários, sistemas, aplicações, objetos, informações e os vínculos com cada sistema. Os atributos de acesso são correspondentes aos requisitos do usuário, e deve haver um sigilo de informações. Nesse modelo de autorização, os usuários não têm prerrogativas para alterar seus acessos e devem respeitar a política de segurança. Os administradores do sistema são os únicos que conseguem fornecer ou bloquear os acessos.

3.2.2 Autorização de acesso discricionária

Nesse modelo de autorização, os proprietários e utilizadores do sistema têm a capacidade de definição de acesso a seus dados e informação de uma maneira independente da política. Uma das vantagens desse modelo é a flexibilidade na esfera do usuário, entretanto manter um controle de acesso em ambientes em que sejam empregados requisitos de conformidade pode ser um pouco complicado, pois sistemas controlados dessa maneira acabam sendo mais difíceis de auditar. Pela característica flexível desse modelo, deve existir uma preocupação em relação ao cumprimento de políticas de segurança.

3.2.3 Autorização de acesso funcional

Nesse modelo temos algumas similaridades com o modelo mandatório, porém na autorização de acesso baseada na função, as autorizações não levam em conta os atributos. Aqui o critério utilizado é a função do usuário dentro da organização. Sempre deve haver mais usuários que funções, pois dessa maneira fica um pouco mais fácil gerenciar esses acessos e autorizações. Com base no papel de cada um dentro de um projeto, por exemplo, seria criado um perfil, mas existem algumas limitações desse método em relação às variações de configuração.

3.2.4 Autorização de acesso reivindicada

É um modelo de autorização em que os proprietários das informações ou sistemas criam um conjunto de reivindicações necessárias para fazer as concessões de acesso. Dessa maneira fica um pouco mais flexível a implementação, podendo-se usar como base a autorização de acesso funcional e depois, por meio de reivindicações, ajustar os controles esperados.

3.3 Contabilização e AAA

A contabilização é uma forma de monitorar o comportamento dos usuários relacionados aos sistemas e uma maneira de controlar o consumo de recursos computacionais (rede, impressão, armazenamento, entre outros). É muito útil nesse contexto de gerência de recursos, na cobrança por esses serviços, no planejamento de recursos, qual departamento precisa ser ajustado e melhorado.

É um processo em que equipamentos de redes, servidores, sistemas fazem o implemento de uma política de acesso, em que são coletadas todas as informações relacionadas à atividade do elemento autenticado e são enviadas ao servidor de autenticação e auditoria.

Quando utilizamos o triplo A (AAA), estamos querendo nos referir a uma espécie de *framework* que tem como objetivo o controle de acesso a recursos e serviços de redes e sistemas. Ele possui três funções, que são resumidas em *autenticação*, *autorização* e *auditoria* (ou *accounting*), por isso a sigla AAA.

TEMA 4 – IMPLEMENTAÇÃO DO AAA

Quando falamos em segurança da informação, a padronização AAA faz referência e está relacionada a processos de autenticação, autorização e contabilização. A autenticação atua na verificação da identidade digital do usuário. A autorização atua nas camadas de acesso a recursos que esse usuário autenticado pode ter, e a contabilização faz o complemento, realizando o registro e coleta das informações de acesso e utilização de recursos computacionais por parte do usuário.

O *framework* AAA (*Authentication, Authorization* e *Accounting*) apresenta algumas maneiras de autenticação a dispositivos e sistemas, realizando o controle em relação aos níveis de acesso dos usuários, aos recursos que estão disponíveis, às atribuições, ao que pode ser acessado e executado, além do

controle de todas as ações realizadas pelo usuário para contabilização e atividades de auditoria.

4.1 Radius

O protocolo de autenticação, autorização e auditoria Radius (*Remote Authentication Dial In User Service*) realiza todos os processos de identificação digital do usuário, autorizando os acessos que esse usuário pode ter e fazendo os registros desses acessos. Um servidor com o protocolo Radius consegue dar suporte a uma série de métodos e técnicas de autenticação. Entre esses métodos estão o PPP, PAP, CHAP ou UNIX *login*, e alguns outros mecanismos de autenticação.

Servidores Radius são empregados principalmente por provedores de acesso à internet para gerenciar seus usuários. Trata-se de um protocolo que protege uma rede habilitando a autenticação centralizada utilizando um banco de dados e o serviço de diretório LDAP (*Lightweight Directory Access Protocol*), que é um protocolo de aplicação aberto que fornece informações a diferentes sistemas e aplicativos.

4.2 Padrão IEEE 802.1X

O padrão IEEE 802.1X é um protocolo criado para controle de acesso a redes, faz o provimento de mecanismos de segurança para uma série de dispositivos (principalmente para redes locais e redes sem fio), fornecendo meios de autenticação a equipamentos que desejam se conectar a uma determinada rede.

Normalmente esse processo de autenticação 802.1X é utilizado como uma maneira de segurança avançada para redes com fio, mas alguns administradores de rede estão utilizando esses mecanismos para proteger suas conexões de rede sem fio também. As credenciais de acesso são validadas e depois dessa etapa os utilizadores conseguem acessar a intranet, internet e trafegar dados pelas redes com fio ou sem fio. O protocolo 802.1X é formado por três elementos:

- O usuário ou cliente que precisar ser autenticado no sistema é chamado de *suplicante*;

- O servidor atual que efetua o processo de autenticação. Geralmente esse servidor usa o protocolo RADIUS para prover a consulta em uma base de usuários e validar efetivamente a autenticação;
- O dispositivo entre os dois primeiros elementos pode ser um ponto de acesso sem fio ou um comutador (switch). Esse equipamento é chamado de *autenticador*.

4.3 LDAP

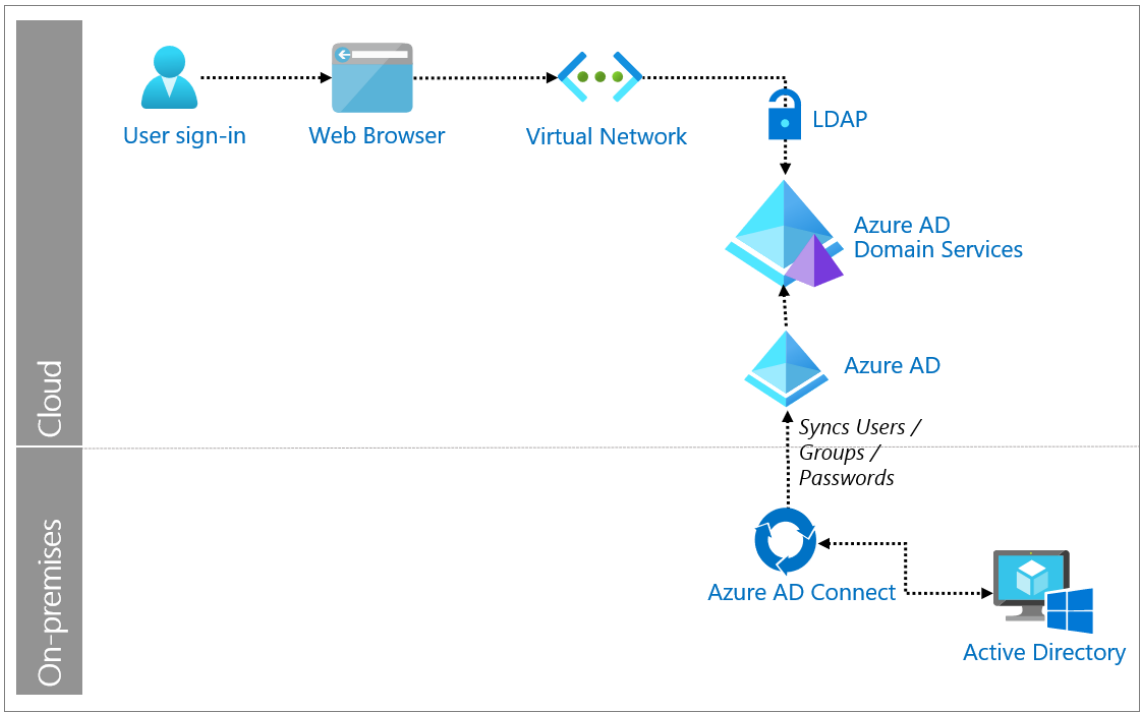
O *Lightweight Directory Access Protocol* (LDAP) é um protocolo para aplicativos utilizado para atuar com diversos serviços de diretório. Esses serviços fazem armazenamento de conta, usuários, senhas, objetos e vários outros elementos. Esse tipo de protocolo tem funções para compartilhamentos de informações para vários dispositivos de rede. Aplicações empresariais de várias áreas podem utilizar o LDAP para promover a autenticação, autorização e auditoria dos acessos, sistemas de mensagens, *e-mails*, sistemas de relacionamento com o cliente, aplicativos de recursos humanos, entre outros.

4.4 Cenários de uso do AAA

Existem alguns cenários em que os processos de autenticação utilizam os todos os componentes apresentados anteriormente. Um ambiente bem comum encontrado atualmente são as aplicações hospedadas na nuvem. Um exemplo disso é a plataforma *Microsoft Azure*, destinada à execução de aplicativos e serviços, baseada nos conceitos da computação em nuvem.

Na Figura 4, apresentamos um cenário de uso de autenticação utilizando o protocolo LDAP:

Figura 4 – Processo de autenticação LDAP



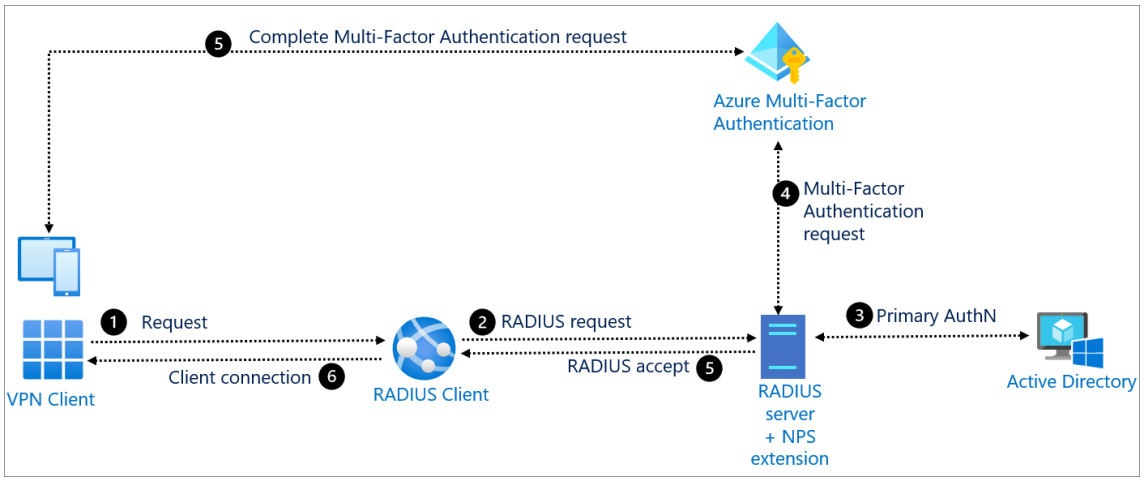
Fonte: Microsoft, 2021.

No cenário acima, temos alguns componentes que fazem parte desse sistema:

- Usuário – é o utilizador dos aplicativos que tem dependência de autenticação via navegador de internet com o protocolo LDAP;
- Navegador de internet – é a interface que o utilizador interage para acessar o endereço de acesso do aplicativo;
- Rede Virtual – é uma rede criada e utilizado pelo Microsoft Azure com qual o aplicativo faz o acesso e utiliza os recursos disponibilizados pelos serviços LDAP;
- Active Directory – o Active Directory é uma solução da Microsoft que utiliza o serviço de diretório no protocolo LDAP e faz o armazenamento de dados sobre objetos em rede de computadores e disponibiliza esses dados a usuários, grupos e administradores desta rede;
- Azure AD – O Azure AD faz todo o sincronismo de identidades de diretório local de uma organização;
- Azure AD Connect – é um recurso utilizado para fazer o sincronismo de dados de identidade local, dados de *logon* e componentes necessários para conexão do Microsoft Azure AD.

Existe um outro caso de uso utilizando o protocolo de autenticação Radius, muito utilizado em situações como acesso a VPN (*Virtual Private Network*), redes *wireless*, acessos remotos, entre outros. A figura a seguir apresenta um segundo cenário de implementação usando Radius:

Figura 5 – Processo de autenticação LDAP



Fonte: Microsoft, 2021.

No cenário acima, temos alguns componentes que fazem parte desse sistema:

- Aplicativo de cliente VPN – envia a solicitação de autenticação para o cliente Radius;
- Cliente Radius – faz a conversão das solicitações do aplicativo de cliente VPN e promove o envio ao servidor Radius, que possui a extensão NPS;
- Servidor Radius – faz a conexão com o servidor de Active Directory para efetuar a autenticação primária para a solicitação Radius. Caso a autenticação seja bem-sucedida, é disparada a solicitação da extensão NPS para a autenticação multifator do Azure AD;
- Extensão NPS – dispara solicitações para autenticação multifator do Azure AD para uma autenticação secundária. Também pode ser utilizado usando *tokens* de segurança;
- Autenticação multifator do Azure – faz a comunicação com o Azure Active Directory para resgatar os dados do usuário e efetua a autenticação secundária usando o método escolhido pelo usuário.

Com toda essa evolução digital e a utilização cada vez maior dos recursos de tecnologia por parte das organizações, surge a necessidade de melhorar os controles e as medidas de segurança de sistemas, por isso esses controles precisam ser avaliados e revisados periodicamente por meio de um processo de auditoria.

O objetivo da auditoria é encontrar as irregularidades que acontecem dentro da área de tecnologia da informação das empresas. Para isso, são utilizados alguns meios de avaliação, ajuste e adequação de sistemas e tecnologias utilizadas e são executadas revisões e avaliações de controles, desenvolvimento de sistemas, infraestrutura, serviços, operações, procedimentos, desempenho, conformidade e segurança da informação. Nesse aspecto, é possível fazer uma análise de riscos, falhas, erros, irregularidades, deficiências que podem estar ocorrendo ou que possam ocorrer, sendo levantadas recomendações de melhoria e correção de controles internos, em processos que têm o intuito de minimizar os riscos analisados.

Por muito tempo o termo *auditoria* foi ligado quase que exclusivamente à área contábil, entretanto muitos apontam que a auditoria pode ser vista de uma maneira mais ampla, englobando toda a organização, com seu raio de ação atingindo vários elementos como colaboradores, fornecedores, clientes, empresas públicas e privadas com quais a organização tem vínculo.

Dentro da área de tecnologia da informação, a auditoria pode ser entendida como um conjunto de procedimentos e técnicas que são utilizadas para controlar e avaliar um sistema de informação com o intuito de analisar se as atividades executadas pelos sistemas de informação estão corretas e em conformidade com os regulamentos de sua organização. É possível medir também a eficácia e a eficiência dos recursos computacionais, do controle dos dados e se estas têm apresentado a base para a tomada de decisões da empresa.

A auditoria é fundamental para garantir a segurança da informação, por isso acreditamos que a auditoria funcione muito bem como controle de segurança dissuasivo, pois usuários mal-intencionados não irão se arriscar e executar ações em ambientes nos quais eles sabem que estão sendo monitorados (Donda, 2020).

5.1 Elementos de auditoria de tecnologia da informação

A auditoria de sistemas ou de tecnologia é uma parte do processo geral de auditoria, que é um dos facilitadores e viabilizadores de governança corporativa. Não há uma definição universal para a auditoria de TI, mas uma definição aceitável seria

> o processo de obtenção e avaliação de evidências para determinar se um sistema de informação preserva os ativos, mantém a integridade dos dados, atinge as metas organizacionais e consome recursos de maneira eficiente. Os gestores em todos os níveis hierárquicos preocupam-se cada vez mais com os sistemas informatizados, apesar de muitas vezes não terem um completo entendimento de sua complexidade e, principalmente, de suas vulnerabilidades. (Galvão, 2015)

Nesse contexto, a auditoria tem como principal papel prover dados e informações, análises, correções, avaliações e recomendações para minimizar os riscos que se apresentam em todos os processos de negócios, sempre respeitando a tríade da segurança da informação: **integridade**, **confidencialidade** e **disponibilidade**.

A tecnologia da informação não é composta somente por computadores, uma vez que é um conjunto de vários elementos humanos, comportamentais, processuais, ambientes físicos e tecnológicos que fazem parte dessa composição e que são chamados de **soluções integradas de TI**. Dessa maneira, a auditoria de TI deve ser abordada de uma forma bem abrangente. Dentre os elementos que formam a auditoria, podemos destacar:

5.1.1 Revisão de administração de sistemas

Periodicamente é essencial avaliar os níveis de acesso dos usuários, principalmente os que têm perfil de administração ou controle total. É preciso também verificar os sistemas gerenciadores de banco de dados, processos relacionados à administração de sistemas de maneira geral e observar se as normas e regras estabelecidas estão sendo cumpridas em relação aos controles de acesso.

5.1.2 Avaliação de infraestrutura

É importante elaborar uma boa avaliação física dos ambientes críticos de tecnologia da informação, insumos, recursos de energia elétrica, ar-

condicionado, umidade, iluminação, eletrodutos e outros fatores que ambientais que possam impactar e comprometer a operação normal da infraestrutura;

5.2.3 Avaliação de aplicativos e sistemas de informação

Deve haver uma avaliação de aplicativos: os controles de sistemas em relação às atribuições de acesso, registro de atividades (*logs*), o tratamento de erros, integridade da informação, fluxo de dados, interfaces, análise minuciosa de procedimentos automatizados, aprovações prévias e segurança no desenvolvimento de aplicações, conformidade com as regras de negócios. Aplicações críticas como finanças, tesouraria, pagamentos, contas a pagar, entre outros requerem uma análise específica.

5.1.4 Avaliação de redes

Avaliar toda a conectividade de rede da organização, redes internas, redes externas, intranet, internet, os perímetros de segurança, *firewalls*, roteadores, sistemas de detecção de ataques, registros de conexões remotas, VPNs, acessos externos, servidores de rede, *websites* organizacionais, entre outros.

5.1.5 Avaliação de continuidade de negócios

Avaliar redundâncias, contingências, sistemas de tolerância falhas, alternativas em relação a *software* e *hardware*, sistemas de banco de dado, planos de recuperação de desastres, cópias de segurança, mitigação de riscos e soluções de contorno, deve ter o envolvimento de todas as áreas da organização.

Todos esses elementos devem ser avaliados na íntegra. Ao aplicar a auditoria de maneira adequada, fazer o levantamento de vulnerabilidades, de alterações não autorizadas, acompanhando os controles e acesso, problemas relacionados a infraestrutura, processos executados de maneira errada, percebe-se que o cenário de segurança é muito mais complexo e amplo. A auditoria deve ser uma maneira de avaliar todos esses componentes de segurança, o escopo da avaliação. É primordial também que essa auditoria tenha a participação de analistas de negócios para a avaliação de aplicações e dados de maneira mais coerente.

5.2 Auditoria de sistemas

A auditoria de sistemas de informações deve englobar todas as operações, processos, sistemas e responsabilidades de todos os integrantes da organização e principalmente da equipe de tecnologia de informação. Hoje a área de TI é considerada crítica e também recebe muitos investimentos. Dessa forma, a auditoria de sistemas tem a missão preventiva de garantir diversos requisitos, tais como integridade dos registros, veracidade das informações, confiabilidade e disponibilidade.

O objetivo dessa auditoria de sistemas é fazer a avaliação dos sistemas, desde a entrada de dados, os procedimentos, métodos utilizados, controles executados, arquivos gerados, segurança de dados e fontes de informações. Nessa avaliação, devem constar também questões relacionadas ao ambiente computacional, como os dispositivos, os equipamentos, os concentradores de tecnologia, *softwares*, processamentos de dados, entre outros elementos. Dentre esses objetivos, podemos elencar:

- Fazer uma avaliação dos meios físicos, das tecnologias utilizadas, e observar como são feitos os processamentos dos dados realizados durante a operação dos processos de negócio;
- Analisar os controles empregados e checar sua eficiência e eficácia;
- Promover a qualidade e utilidade das informações obtidas;
- Avaliar a adequação de todos os sistemas, procedimentos e sistemas de controle que garantam a segurança da tecnologia da informação e seu relacionamento direto com os componentes de TI (*software*, *hardware*, rede, entre outros).

Todos esses objetivos devem ser concretizados com a auditoria. Para isso, existem muitas metodologias específicas de cada área. Para atividades de auditoria, é primordial que o auditor possua conhecimento técnico sobre a área auditada e que apresente algumas habilidades comportamentais como a objetividade, honestidade, boa comunicação, clareza, capacidade de análise, síntese, flexibilidade, raciocínio lógico, compreensão rápida, entre outras aptidões.

A auditoria de sistemas deve apresentar ao menos quatro etapas:

- Planejamento e preparação;

- Execução da auditoria;
- Resultados e relatórios de auditoria;
- Planos de ação e correção.

Todas essas etapas geram diversos documentos e são de grande valor para as organizações. Dentro da auditoria são apontados os principais riscos encontrados, bem como a avaliação desses riscos, as vulnerabilidades, os controles que não estão em conformidade, correções de processos, recomendações de melhorias, entre outros. Todos esses documentos são mostrados para a alta administração e equipe de tecnologia da informação.

A auditoria também pode nortear a organização em relação aos caminhos a serem seguidos, investimentos a serem realizados, o que pode ser um guia estratégico e auxiliar a administração no planejamento no controle de novas ações.

5.3 Gerenciamento de *logs*

É importante registrar, por exemplo, todas a práticas e estratégias implementadas na empresa. Isso promove dois resultados importantes: primeiro, os funcionários podem consultar as informações sobre de que forma devem trabalhar, adequando-se às novas regras; segundo, o próprio analista de segurança pode avaliar se eventuais irregularidades são fruto de falhas no planejamento ou se alguém ainda não adotou as novas práticas estabelecidas. Parte desse trabalho é realizada por meio de auditoria interna, uma ferramenta essencial para momentos de mudanças operacionais como essa (Alves, 2021).

Segundo Donda (2020), o maior desafio no gerenciamento de eventos é superar a variedade de formato de *logs*. Em muitos ambientes, teremos diversos recursos gerando *logs*, como dispositivos de rede, roteadores, comutadores (switches), *firewalls*, soluções de antivírus, banco de dados, sistemas na web, servidores (Windows, Linux, Unix), seja de modo nativo ou por meio de *softwares*.

Ao analisar muitos arquivos de *logs* gerados por diversos sistemas, pode ser uma tarefa bem trabalhosa, pois milhares de eventos são gerados, por isso é necessário coletar e avaliar esses dados de várias fontes, sejam *logs* de sistemas locais, remotos ou na nuvem, sendo necessário combinar esses dados para que possam ser entendidos. Em casos de ataques cibernéticos, tentativas

de invasão, seja em rede local ou rede externa, a auditoria e o gerenciamento de *logs* precisam ter condições de identificar onde essa invasão ocorreu, que sistemas foram afetados. Assim, é essencial haver ferramentas e soluções que permitam a centralização e o gerenciamento dos eventos e *logs*, o que facilita muito a análise e o armazenamento.

Para Donda (2020), as funções primordiais de um gerenciamento de *logs* são as seguintes:

- Coletar e armazenar volumes massivos de dados;
- Processar e normalizar logs de diversas fontes;
- Armazenar e reter logs para longo prazo;
- Proteger os dados do registro de eventos contra adulteração ou destruição;
- Criar relatórios de *logs*;
- Analisar *logs*.

As soluções de gerenciamento de *logs* implicam a agregação de vários arquivos de *logs*, que são gerados por vários equipamentos, dispositivos de rede, servidores, sistemas de informação, entre outros. Isso facilita muito as atividades de análise de eventos e *logs*. Existem algumas ferramentas para fazer isso de uma forma mais eficiente. As soluções de *Security Information and Event Management* (SIEM) realizam funções de auditoria, segurança e monitoramento. Essas funcionalidades permitem que sejam feitas correlações de eventos, fornecendo uma combinação de gerenciamento e auditoria de segurança da informação. As soluções SIEM apresentam as seguintes funcionalidades:

- Apresenta um painel de informações com visualização de dados em tempo real;
- Possui mecanismos de alertas, de detecção e análise de ameaças;
- Tem uma gama completa de relatórios;
- Faz correlação entre eventos de diferentes fontes de dados;
- Possui uma inteligência em encontrar e classificar ameaças.

5.4 Estratégias de auditoria

Todo o levantamento de informações para a auditoria pode ser realizado de algumas maneiras, dependendo da estratégia a ser seguida. As informações

podem ser colhidas de várias fontes e forma, a escolha adequada da estratégia de auditoria é primordial, podemos destacar a seguir, algumas estratégias de auditoria:

5.4.1 Questionários

É uma técnica de levantamento formada por uma série ordenada de perguntas que podem ser respondidas sem a presença do auditor, com o intuito de checar determinado ponto de controle do ambiente computacional. Essas questões devem ser elaboradas de forma cuidadosa, baseando-se no conteúdo que se refere ao tema, e conter as especificidades de cada cenário de realização. O auditado deve ter um fácil entendimento das perguntas. Os questionários podem ser aplicados remotamente, a distância, e estão sujeitos sempre a interpretações subjetivas. Essa estratégia pode ser utilizada como primeira linha de ação e depois podem ser obtidos detalhes com a utilização de outra estratégia ou complementada com outro método.

5.4.2 Entrevistas

Nessa forma de coleta de informações, as questões são previamente escolhidas e preparadas, e o entrevistado, na presença do auditor, deve respondê-las. As entrevistas podem ser classificadas como **abertas** ou **fechadas**. A entrevista é o método ideal para coletar informações a respeito de controles internos, riscos, fraudes, entre outras. Dessa maneira, a entrevista apresenta vantagens na obtenção de dados em profundidade. É possível quantificar, classificar e qualificar os dados coletados. É possível também captar expressões corporais, tonalidade de voz e a sua ênfase em relação às respostas, uma vez que o entrevistado pode ser um não alfabetizado. Dentre as desvantagens, estão a falta de interesse do entrevistado em responder, a possibilidade de respostas falsas, a falta de capacidade do entrevistado para responder, aspectos pessoais relacionados à entrevista, o fato de o entrevistador ser inábil ao fazer a entrevista, os custos de realização das entrevistas (curso de treinamento a entrevistadores, aplicação de entrevistas com colaboradores em horário de expediente).

5.4.3 *Checklists*

Nessa modalidade é elaborado um conjunto de perguntas de maneira bem flexível, as quais moldam a condução da estratégia. São realizadas conversas informais, e o auditor pode fazer uma descrição de pontos fortes e fracos. Assim, os *checklists* podem fazer o complemento de um questionário e devem ser respondidos de maneira oral, fornecendo conteúdos de forma individualizada e com riqueza de detalhes.

A Figura 6 representa algumas estratégias adotadas para a auditoria:

Figura 6 – Processo de autenticação LDAP

Créditos: Drawlab19/Shutterstock.

5.5 Auditoria interna e externa

A auditoria pode ser realizada de duas maneiras: a primeira pela equipe interna, pelos próprios colaboradores da organização a passar pela auditoria; a segunda maneira é a realizada por consultores externos, normalmente de entidades que não têm vínculo com a organização auditada, empresas que têm dedicação exclusiva para a auditoria.

Na auditoria interna, a finalidade é ajudar a gestão a medir seu desempenho; já a auditoria externa é utilizada quando o intuito é uma maior objetividade, sendo a proximidade um fator fundamental. Na auditoria interna, existem alguns vínculos entre colaboradores; na externa, existe um distanciamento por parte de auditor e auditados.

Fazendo um comparativo, é possível elaborar algumas vantagens que a auditoria interna apresenta em relação à externa:

- Auditorias internas não menos perceptíveis aos colaboradores que uma auditoria externa;
- Apresenta um custo mais barato e os auditores já são familiarizados com a empresa e sistemas;
- Podem atuar de maneira mais rápidas em casos emergenciais;
- Por conhecerem a empresa, há várias fontes de coletas de informações;
- São o ponto de interligação e servem como base para auditorias externas.

Por mais que sejam apontadas as vantagens das auditorias internas, para muitos autores, a auditoria externa é considerada aquela que atinge os melhores resultados, pois não apresentam vínculos com colaboradores e com o ambiente da organização e pelo fato de estarem menos sujeitos à subjetividade. Assim, a postura dos auditores nas duas modalidades de auditoria deve ser imparcial, sem nenhum tipo de relacionamento interpessoal, para impedir que isso seja fator modificador de resultados do processo de auditoria.

5.6 Auditoria de segurança física

Os recursos físicos de uma organização devem ser auditados. É preciso avaliar a conformidade dos procedimentos, normas, medidas e princípios utilizados de segurança da informação; auditar as proteções físicas dos dados, mídias, discos, equipamentos de telecomunicações, servidores, unidades de armazenamento, condições de trabalho, ergonomia, medidas de combate a incêndio, áreas de evacuação, alarmes e saídas de emergência. Dentro desse contexto, é possível elencar algumas tarefas dessa auditoria de segurança física:

5.6.1 Avaliação de sistemas elétricos e energia

Essa atividade consiste em verificar os sistemas de alimentação elétrica, bem como suas proteções. Equipamentos críticos devem dispor de fontes

redundantes, sistemas de alimentação ininterrupta de energia elétrica para suportar falhas e falta de abastecimento por parte das concessionárias de energia. A utilização de estabilizadores também pode ser empregada em ambientes não críticos. Além disso, dependendo da missão da organização, é necessária também a implantação de geradores de energia.

5.6.2 Avaliação de condições ambientais

Fazer uma análise em torno do ambiente em que estão instalados os principais equipamentos de tecnologia da informação da empresa é fundamental para verificar questões relacionadas ao calor, umidade, ventilação, hidráulica e mitigar problemas relacionados a inundações, instalações malconcebidas em locais de risco.

5.6.3 Avaliação de controles de acesso físico

Avaliar concentradores de equipamento, centros de processamento de dados, salas de equipamentos de tecnologia da informação no sentido de haver controles físicos adequados, fazendo um filtro e permitindo acesso apenas à equipe autorizada, leitores biométricos, controles de acesso, entre outros.

5.6.4 Checagem de equipamentos e planos de emergência

Avaliar extintores, sistemas de alarme a intrusões e fogo, analisar se os equipamentos estão testados e dentro do prazo de validade.

5.6.5 Monitoramento físicos de instalações

Observar a utilização de sistemas de câmeras de segurança, controles de portas, sensores e sistemas de registros de entrada e saída de salas, portarias, entre outros. Avaliar também equipe de segurança, vigias e demais envolvidos com segurança.

5.6.6 Avaliação de cabeamento e montagem de equipamentos físicos

Em diversas áreas da organização é preciso avaliar a interligação de equipamentos de energia e de tecnologia da informação, checar o cabeamento elétrico e lógico, fibras ópticas, conectores, tomadas, identificar cabos,

certificando-se de que estão organizados e controlados para evitar qualquer tipo de falha de disponibilidade de sistemas e serviços.

5.7 Auditoria de segurança lógica

A maioria das invasões e ataques cibernéticos são realizados sobre aplicações e sistemas de informação. Assim, as avaliações devem ser periódicas, a manutenção da segurança lógica deve ser constante, a verificação dos controles, conformidade com as normas e regras estabelecidas na política de segurança, vários aspectos são levados em conta na auditoria de segurança lógica.

Um dos pontos de atenção é o controle de acesso. Para garantir a proteção dos dados, aplicações, programas e sistemas contra tentativas de acesso não autorizados, é essencial o controle de acesso, que permite registrar e minimizar falhas de acesso a recursos computacionais, utilizar ferramentas de gerenciamento de usuários, desativar senhas de ex-colaboradores, não gravar senhas em arquivos de *log*, desativar contas que não são utilizadas.

Nesse cenário, o auditor deve avaliar todas a contas de usuários dos sistemas e comparar com a lista de colaboradores que realmente precisam do acesso. A criação, a modificação e a exclusão de usuários devem respeitar os requisitos de segurança, senhas fortes, período de expiração, desativação em caso de várias tentativas erradas ou acessos indevidos.

Por mais que exista uma série de métodos de autenticação, autorização e auditoria e com o avanço de técnicas como biometria, *tokens*, duplos fatores de autenticação, é extremamente necessário existir uma boa definição de senhas, as quais não podem ser fáceis nem muito curtas. A presença de caracteres especiais, letras maiúsculas e minúsculas, números e um bom comprimento de senha fazem toda a diferença em uma grande estrutura com redes, diversos sistemas e demais elementos.

Para validar se um sistema consegue detectar tentativas de invasão e acessos não autorizados, é necessária a realização de testes de intrusão, que podem ser realizados dentro da rede local ou a partir da internet. O auditor pode usar o teste de invasão para avaliar a infraestrutura lógica, como servidores, equipamentos de rede, computadores, entre outros equipamentos. Esse teste vai gerar uma lista com uma série de vulnerabilidades a serem corrigidas e recomendações de melhoria.

A auditoria de segurança lógica deve percorrer todo o perímetro lógico da rede, serviços internos e externos, roteadores, *switches*, pontos de acesso, redes sem fio, servidores, as ligações com redes externas e internet. Existem muitos pontos vulneráveis quando são feitas análises desse modo, e há um conjunto de atividades que podem ser efetuadas pelos auditores em busca da localização de todos os dispositivos lógicos e que estão vulneráveis a uma possível invasão:

- Avaliação de equipamentos de rede como servidores, *switches*, roteadores, pontos de acesso, câmeras de segurança, centrais telefônicas, entre outros;
- Verificação das camadas de segurança, soluções de antivírus, *antispams*, *firewalls*, filtros de aplicações e conteúdo, alinhando essa checagem com as regras e normas organizacionais e se estão em conformidade;
- Localizar equipamentos ativos não mapeados na infraestrutura, um *modem* ou algum tipo de equipamento que não esteja autorizado, dispositivos que não estão devidamente identificados e registrado na rede.

As aplicações desenvolvidas pela organização devem atender a uma série de requisitos de segurança. As aplicações que compartilham dados devem ser avaliadas da melhor forma possível, impedindo que dados críticos possam ser acessados por usuários não autorizados.

As soluções de antivírus devem ser verificadas com o intuito de garantir a sua correta utilização, com atualizações automáticas, recursos de varredura a sistemas e dispositivos removíveis, atualizações de sistemas operacionais, aplicativos e demais componentes. As soluções de segurança devem estar rodando normalmente, cobrindo toda a infraestrutura de tecnologia da informação.

A auditoria ainda pode verificar o planejamento de continuidade das operações. Outro aspecto importante é avaliar planos de redundância e contingência, rotinas de cópias de segurança de dados, recuperação de arquivos, tolerância a falhas. Recursos computacionais vitais devem ter uma dupla abordagem de funcionamento. Deve haver a proteção e guarda dos dados, a recuperação de sistemas e a reposição de equipamentos em caso de falhas.

5.8 Auditoria de segurança de recursos humanos

O grande objetivo da segurança de recursos humanos é reduzir riscos de erros humanos, roubos, fraudes ou uso indevido das facilidades. Um dos ataques mais comuns a recursos humanos é a engenharia social. Assim, os auditores precisam testar os recursos humanos com o intuito de identificar um grau de vulnerabilidade da organização a ataques sociais, o que pode ser feito utilizando tentativas de coleta de informações por meio de ligações telefônicas, sistemas de mensagens, abordagens pessoais. Isso permite avaliar os aspectos de segurança da informação.

Outro ponto a ser avaliado é a formação e qualificação dos recursos humanos. Em muitos casos, uma formação deficiente, omissões e descuidos causam impactos para a segurança. Campanhas de conscientização, treinamentos e instruções podem ajudar minimizar os riscos com recursos humanos. Outro aspecto a ser analisado é quando administradores de sistemas acabam acumulando muitas funções, sobrecarga de responsabilidade que pode ser nociva à segurança. Uma solução para isso seria segregar funções a fim de minimizar qualquer possibilidade de fraude por parte de um colaborador, pois sem a segregação a organização acaba assumindo riscos como alterações impróprias, danos a recursos computacionais, operações e transações incorretas.

FINALIZANDO

Nesta aula, iniciamos elencando os principais ataques à segurança e detalhamos também a engenharia social, quais são os tipos de criminosos virtuais, as principais motivações para ataques virtuais, a classificação dos ataques, oferecendo um guia sobre riscos, ameaças e vulnerabilidades. Na sequência, destacamos as técnicas de mitigação e contramedidas de segurança, os incidentes de segurança, os impactos relacionados a esses incidentes. Destacamos as medidas de segurança confrontadas com as ameaças e, de maneira generalista, falamos sobre a recuperação de desastres e os planos de continuidade de negócio.

Em seguida, trouxemos detalhes sobre controles de acesso, autenticação, autorização, auditoria e contabilização, os modelos de autorização, os métodos de autenticação e observamos como esses processos ajudam no controle de

acessos das organizações. Depois apresentamos alguns cenários de aplicação de autenticação, autorização e auditoria (AAA). Falamos também sobre os protocolos Radius, LDAP e o padrão IEEE 802.1X. Por fim, argumentamos sobre auditoria, estratégias de auditoria, auditorias lógica, física e recursos humanos, além do gerenciamento de eventos e *logs*.

REFERÊNCIAS

ALVES, D.; PEIXOTO, M.; ROSA, T. **Internet das Coisas (IoT)**: segurança e privacidade de dados pessoais. Rio de Janeiro: Alta Books, 2021.

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.

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

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