

SEGURANÇA E AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

Ver anotações

Deseja ouvir este material?

Áudio disponível no material digital.

CONHECENDO A DISCIPLINA

Seja bem-vindo ao fascinante e cada vez mais importante mundo da segurança da informação. Com a transformação digital e a informação fluindo em uma velocidade cada vez maior, a inovação tecnológica cria uma série de oportunidades. Diante disso, também é preciso entender o seu lado obscuro, composto por ameaças cibernéticas. Toda empresa tem que tratar, em diferentes níveis, da prevenção, da detecção e da resposta a incidentes de segurança.

Como um ataque de um cracker, por exemplo, faz com que uma ameaça se torne um incidente de segurança? O que ele pode explorar para causar impactos para as empresas, seja em suas operações, seja na criação de novos produtos, no desenvolvimento de novas tecnologias ou na otimização de processos de negócios?

Nesta disciplina, você entrará em contato com os principais aspectos envolvidos com a segurança e auditoria de sistemas, que são primordiais para o bom funcionamento de qualquer empresa, de qualquer natureza.

Esta jornada inclui aspectos técnicos, como o conhecimento e a compreensão das redes de computadores seguras, além do entendimento dos diferentes tipos de ataque e as possíveis medidas de segurança. Além disso, ela envolve, ainda, aspectos humanos e processuais, como a compreensão de culturas de segurança e a gestão de políticas de segurança e provedores de serviços em redes seguras.

Você conhecerá e compreenderá a auditoria de sistemas, fundamental para manter a conformidade com as normas vigentes de segurança e privacidade. Serão quatro unidades de assuntos relevantes.

A **Unidade 1** tratará de segurança da informação e redes. Serão abordados os principais conceitos, como os princípios de segurança da informação, mecanismos de defesa e riscos em segurança da informação. Além disso, a segurança de redes, com as vulnerabilidades, as ameaças, os ataques e os mecanismos de proteção, será abordada conjuntamente aos pontos mais importantes sobre criptografia.

A **Unidade 2**, por sua vez, tratará da gestão e das políticas de segurança com foco na família de normas de segurança (a ISO 27.000) e a Lei Geral de Proteção de Dados Pessoais (LGPD). Além disso, a unidade abordará a cultura de segurança com questões operacionais e legais, o armazenamento de dados, incluindo o uso de técnicas de acesso e anonimização de dados, principalmente em ambientes de nuvem.

Já a **Unidade 3** tratará da segurança na internet, com discussão de elementos importantes para as pessoas e as empresas, como a privacidade e os golpes cibernéticos. A unidade abordará, ainda, elementos de proteção para dispositivos móveis, bem como a análise de vulnerabilidades e *pentest*, que faz parte das atividades de times de segurança das empresas.

Esta disciplina, por fim, será finalizada na **Unidade 4**, que focará a auditoria de sistemas e segurança, abordando os seus fundamentos, os controles de segurança que são auditados e as principais técnicas e ferramentas para o auditor realizar as suas atividades.

O tema desta disciplina se aplica tanto ao seu universo pessoal quanto ao universo organizacional ou corporativo. Vivenciamos constantemente incidentes de segurança relevantes, e alguns deles serão discutidos ao longo desta disciplina. Vamos explorar o mundo da segurança da informação, o que fará grande diferença em sua vida pessoal e na forma como você atuará profissionalmente, com a formação de um *mindset* que resultará em operações, serviços, produtos, tecnologias e processos mais seguros, mais resilientes e mais confiáveis.

Bons estudos!

NÃO PODE FALTAR

INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Emilio Tissato Nakamura

QUAIS SÃO OS PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO?

Os três princípios da segurança da informação são confidencialidade, integridade e disponibilidade.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

CONVITE AO ESTUDO

Temos visto uma série de incidentes de segurança relacionados ao vazamento de informações que podem trazer uma série de problemas. Com base nisso, podemos refletir: por que é necessário investir em segurança da informação e redes? O que deve ser protegido? Por quê? Como? Essas são algumas questões que podem ser respondidas com elementos essenciais que o acompanharão durante esta disciplina e, o mais importante, durante a sua vida pessoal e profissional.

Há ataques que modificam informações e/ou levam serviços a pararem de funcionar. Esses ataques estão relacionados com os princípios de segurança que devemos assegurar: confidencialidade, integridade e disponibilidade. Além disso, eles são complementados com o conhecimento dos elementos do risco, que guiam a segurança: probabilidade, impacto, ativo, agente de ameaça, ameaça, vulnerabilidade e controles. Assim, nesta unidade você conhecerá e compreenderá redes de computadores seguras, que são definidas e implementadas com a aplicação de controles de segurança, que, por sua vez, são definidos a partir de uma visão de riscos.

A estratégia de segurança deve ser definida a partir da avaliação de riscos, que prioriza as ações de acordo com o cálculo da probabilidade e do impacto envolvido no caso de um agente de ameaça explorar vulnerabilidades de ativos. O objetivo deve ser evitar que os riscos sejam uma possibilidade, com a ameaça se tornando um incidente de segurança, o que resulta em impactos.

Além da compreensão dos princípios de segurança e dos elementos de risco, uma estratégia de segurança que funcione dependerá do seu entendimento, da diferenciação e da aplicação de técnicas de segurança em redes de computadores.

A Seção 1 será dedicada à introdução à segurança da informação, em que serão abordados os princípios da segurança da informação e a abrangência da proteção, com discussões sobre mecanismos de defesa

e a relação com os riscos em segurança da informação. Na Seção 2, você entenderá os principais aspectos da segurança de redes, envolvendo as vulnerabilidades, as ameaças, os ataques e os controles que protegem os ativos. A Seção 3 tratará de um dos principais controles de segurança: a criptografia. Conceitos importantes como os tipos de algoritmos, o tamanho das chaves criptográficas, os principais algoritmos existentes e as aplicações mais comuns serão elucidados, e você ficará surpreso quanto à extensão da presença da criptografia em seu dia a dia.

o

Ver anotações

PRATICAR PARA APRENDER

Você já parou para pensar na quantidade de informações, principalmente digitais, que passam por seus dispositivos pessoais e que se misturam com as informações corporativas? Sejam elas estratégicas, operacionais ou técnicas, as informações corporativas fazem toda a diferença para a sua empresa. Mas e se essas informações caírem em mãos erradas, como as de um concorrente, ou se forem divulgadas em redes sociais e tornarem-se públicas, o que acontecerá com a sua empresa? E como isso pode acontecer? São as respostas a essas perguntas que você obterá ao entender como um ataque cibernético ocorre, o que pode ser comprometido da informação e como a segurança da informação pode evitar que isso aconteça em sua empresa.

Seu primeiro passo é consolidar os principais conceitos envolvidos com os princípios da segurança da informação (confidencialidade, integridade, disponibilidade), elementos do risco (ativos, vulnerabilidades, agentes de ameaça, ameaças, vulnerabilidades, probabilidade, impacto) e os mecanismos de defesa, controles de segurança e técnicas de segurança de redes.

Esse entendimento inicial fará toda a diferença em sua jornada para ajudar a sua empresa com a segurança da informação. Você poderá atuar em prevenção, detecção e resposta, realizando ações em

segurança cibernética considerando a identificação, a proteção, a detecção, a resposta e a recuperação.

Você é o responsável pela segurança da informação de uma empresa do setor químico onde trabalham os maiores cientistas brasileiros. Tal empresa possui unidades em São Paulo, Rio de Janeiro e Salvador, e conta com a cooperação internacional de duas empresas, uma chinesa e outra suíça, bem como de grandes investidores que financiam seus projetos.

A sua atividade está focada em um grande projeto em andamento que já chegou a grandes resultados. Os cientistas descobriram um novo composto que será utilizado na indústria agrícola. Diante disso, você está preocupado com a forma como os resultados do desenvolvimento estão sendo protegidos. O impacto pode ser gigantesco em caso de incidentes de segurança, principalmente com a concorrência também mobilizando grandes equipes para colocar no mercado os avanços para o setor.

Frente a essas informações, pense no que pode acontecer com o projeto do novo produto e a estratégia de marketing. Considere que a segurança da informação envolve identificação, proteção, detecção, resposta e recuperação.

Prepare uma **apresentação** para a diretoria executiva da empresa com a sua visão sobre a necessidade de se tomar ações para a segurança do projeto.

Quais são os ataques e os ativos que precisam ser protegidos?

Nessa apresentação, a diretoria executiva precisa conhecer a CID, correspondente à confidencialidade, integridade e disponibilidade. Mostre que o projeto está em execução pelas pessoas, que têm as ideias, e que essas informações vão de forma digital do *notebook* até o servidor da empresa, passando pela rede. Nesse caminho, as informações podem ser vazadas, alteradas ou destruídas (CID). Esclareça que isso pode ocorrer por meio de um ataque cibernético motivado pelo valor dos ativos. Mostre que há ameaças que podem causar a perda de investimento na empresa. Dê um exemplo de

ameaça, como a destruição dos dados do servidor no caso de um *cracker* explorar uma vulnerabilidade utilizando um *exploit* próprio.

Apresente os elementos do risco para a diretoria executiva.

Com essa apresentação, você conseguirá expor suas considerações para que a diretoria executiva possa tomar as devidas providências e patrocinar devidamente a segurança da informação.

Esse primeiro passo é para chamar a atenção da diretoria, fazer com que compreenda a necessidade de proteger o projeto e a estratégia da empresa contra vazamentos e acessos não autorizados (confidencialidade), bem como alterações maliciosas de informações, como os elementos químicos do composto (integridade). Além disso, os diretores devem compreender que é preciso garantir que essas informações estejam sempre acessíveis às equipes responsáveis (disponibilidade).

Para finalizar, apresente um resumo sobre os controles de segurança sugeridos para a prevenção. Com a apresentação, você iniciará a evolução do nível de maturidade em segurança da informação, principalmente com uma resposta inicial para a pergunta: “segurança da informação para quê?”

Vamos juntos iniciar esta jornada em segurança da informação e auditoria de sistemas. Você estudará conteúdos que o ajudarão não somente na profissão, mas que também serão úteis em sua vida pessoal, que também necessita de segurança e privacidade.

CONCEITO-CHAVE

Uma questão inicial que surge quando falamos sobre segurança da informação é: por onde começar? Pelos ataques? Pelos controles, como a criptografia? Pela confidencialidade da informação? Pelas pessoas?

Para que respostas diferentes não apareçam e provoquem confusão, vamos entender e diferenciar os principais conceitos envolvidos, a fim de que a aplicação mais efetiva seja feita por você.

O primeiro conceito importante que você precisa compreender é que a segurança da informação envolve identificação, proteção, detecção, resposta e recuperação (NIST, 2020), como pode ser visto na Figura 1.1.

Figura 1.1 | Segurança da informação envolve mais do que proteção



Fonte: adaptada de NIST (2020).

Esses processos possuem relação com aquela frase que você já deve ter escutado ou falado para alguém: “não existe nada 100% seguro”. Exatamente: riscos podem virar incidentes de segurança quando crackers atacam uma base de dados, por exemplo, e você precisa gerenciar esses riscos com a proteção adequada, utilizando controles de segurança, mecanismos de segurança e técnicas de segurança de redes.

Além disso, uma vez protegido, você precisa ter a capacidade de detectar ataques em andamento, responder a esses ataques e ser capaz de recuperar o seu ambiente.

Nada é totalmente seguro, porque os elementos do risco são dinâmicos, seja quando novas vulnerabilidades surgem, seja quando o ambiente muda com novos ativos ou quando a motivação de um agente de ameaça alcança níveis que aumentam a chance de sucesso de um ataque.

Assim, o que é seguro, hoje, pode não ser amanhã. Além disso, pontos de ataques envolvem ativos tecnológicos, humanos e processuais (NAKAMURA, 2016).

REFLITA

Segurança da informação envolve identificação, proteção, detecção, resposta e recuperação (NIST, 2020). Como você executa essas funções e quais aspectos estão envolvidos?

Pense que a informação existe em meios físicos (como o papel), em meios digitais (como no dispositivo móvel) ou na cabeça das pessoas. Como trabalhar nesse mundo de complexidade?

Vamos organizar os conceitos mais importantes desta seção em três partes. Na primeira parte, o objetivo é entender os princípios da segurança da informação: confidencialidade, integridade e disponibilidade. Na segunda parte, serão apresentados os elementos do risco: ativos, vulnerabilidades, agentes de ameaça, ameaças, vulnerabilidades, probabilidade e impacto. Já na terceira parte, o objetivo é entender, diferenciar e aplicar mecanismos de defesa, controles de segurança e técnicas de segurança de redes.

■ CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE

A segurança da informação é formada por um pilar, composta pela tríade CID: confidencialidade, integridade e disponibilidade. Todas as ações de identificação, proteção, detecção, resposta e recuperação

Para visualizar o objeto, acesse seu material digital.

Imagine que a sua empresa desenvolveu um produto inovador no setor químico. Toda a fórmula deve ser protegida adequadamente, porque não pode cair em mãos erradas, causando grandes impactos. A informação — a fórmula — deve ser protegida, e o princípio da segurança da informação relacionado é a **confidencialidade**.

EXEMPLIFICANDO

Um caso emblemático que mostra que os princípios da segurança podem ser comprometidos é o que ocorreu com uma cadeia de lojas norte-americana, a TJX. Ela teve mais de 45 milhões de dados de cartões roubados, mas só percebeu o incidente de segurança após 18 meses de roubo das informações, a partir da invasão de uma rede Wi-Fi. O ataque ao TJX é considerado um dos casos mais emblemáticos de segurança da informação. Com prejuízos estimados em mais de US\$ 1 bilhão, o ataque foi feito a partir de redes sem fio que utilizavam um protocolo reconhecidamente vulnerável de acesso à rede, o WEP.

Saiba mais sobre o ataque e as consequências desse caso em:

- OU, George. **TJX's failure to secure Wi-Fi could cost \$1B.**
ZD NET, 2007.

O segundo princípio da segurança da informação é a **integridade**. As informações devem permanecer íntegras, ou seja, não podem sofrer qualquer tipo de modificação. Um exemplo de incidente de segurança

relacionado à perda de integridade é um ataque a um sistema de viagens de uma empresa, em que o destino de uma viagem é alterado, ocasionando prejuízos e violação de normas internas.

Para completar a tríade CID, há o princípio da **disponibilidade**, que possui como característica a sua rápida percepção em caso de comprometimento. Os usuários e os administradores de sistemas identificam rapidamente quando um recurso se torna indisponível, já que suas atividades ficam imediatamente paralisadas. Já no caso da confidencialidade ou da integridade, o incidente de segurança é percebido, normalmente, quando a empresa perde clientes ou quando é passada para trás pela concorrência (NAKAMURA, 2016).

Os ataques clássicos que comprometem a disponibilidade são os de **negação de serviço**, como o **DoS (Denial of Service)** e o **DDoS (Distributed Denial of Service)** (OLIVEIRA, 2017). Segundo Nakamura e Geus (2007), os ataques de negação de serviços (*Denial-of-Service Attack*, DoS) fazem com que recursos sejam explorados de maneira agressiva, de modo que usuários legítimos ficam impossibilitados de utilizar esses recursos. Nesses ataques, que podem ocorrer com a aplicação de diversas técnicas, que vão desde o nível de rede ao nível de aplicação, os serviços tornam-se indisponíveis e o acesso à informação é comprometido.

REFLITA

Será que é apenas a CID que devemos garantir para a segurança da informação? Há, ainda, outras propriedades importantes, como a autenticidade, que faz com que a CID vire CIDA (Confidencialidade, Integridade, Disponibilidade e Autenticidade). A norma ABNT NBR ISO/IEC 27001 (2013) cita, ainda, outras propriedades importantes, como a responsabilidade, o não repúdio e a confiabilidade. Já a norma ISO/IEC 13335-1 (2004), sobre conceitos e modelos para segurança de TI, cita a confidencialidade, integridade,

disponibilidade, contabilidade, autenticidade e confiabilidade como sendo os objetivos a serem definidos, alcançados e mantidos pela segurança de TI.

0

ELEMENTOS DO RISCO

Há uma grande complementariedade entre a gestão de riscos, a gestão de segurança da informação e a gestão de continuidade de negócios.

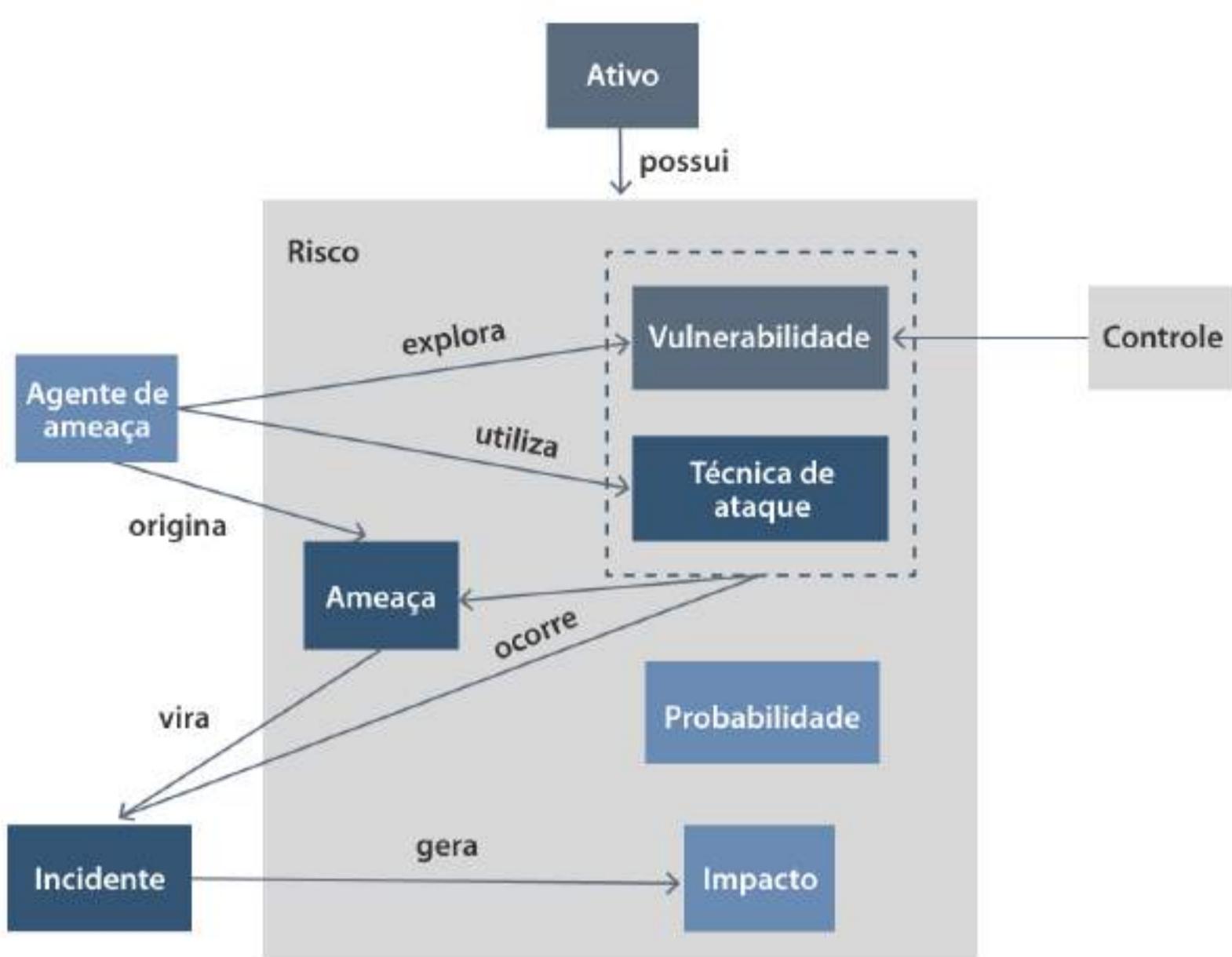
Todas elas apresentam diferentes aspectos, incluindo os de segurança da informação. Apesar de agregar diferentes elementos, a ideia é simples: riscos representam eventos que podem ocorrer, e precisamos conhecê-los para prover a devida segurança com a implementação de controles. Porém, como há riscos aceitos, riscos residuais e novos riscos não identificados ou emergentes, é preciso estar preparado para eventuais incidentes de segurança.

Ver anotações

O risco de segurança da informação é a probabilidade de um agente de ameaça explorar vulnerabilidade(s) de ativo(s), fazendo com que uma ameaça se torne um incidente de segurança, provocando impactos e danos a um ativo ou a um grupo de ativos da empresa.

Essa relação está ilustrada na Figura 1.2.

Figura 1.2 | Fluxo com componentes de risco de segurança da informação



Fonte: elaborada pelo autor.

Dessa forma, a identificação de riscos envolve a identificação de todos estes elementos: ativos, vulnerabilidades, ameaças, agentes de ameaças. A análise e a avaliação de riscos são feitas com o cálculo da probabilidade e do impacto de cada um dos eventos identificados, formando-se uma matriz de riscos. É a partir desse ponto que os controles de segurança ou mecanismos de defesa são definidos e implementados no tratamento dos riscos. Você pode observar na Figura 1.3 uma matriz contendo 3 níveis de probabilidade (baixo, médio e alto) e 4 níveis de impacto (baixo, médio, alto e extremo). O cálculo da matriz, neste caso, levou a 5 níveis de risco: insignificante, baixo, médio, alto e extremo.

Figura 1.3 | Matriz de Riscos (R), considerando a probabilidade (P) e o Impacto (I)

Probabilidade Impacto		1	2	3
		B	M	A
1	B	1	2	3
2	M	2	4	6
3	A	3	6	9
4	E	4	8	12

Risco (P x I)	1	Insignificante
	2 e 3	Baixo
	4 e 6	Médio
	8 e 9	Alto
	12	Extremo

Fonte: elaborada pelo autor.

SAIBA MAIS

Diferentes tipos de riscos existem e devem ser considerados. Danos à reputação ou à marca, crime cibernético, risco político e terrorismo são alguns dos riscos que as organizações privadas e públicas de todos os tipos e tamanhos do mundo devem enfrentar cada vez mais. Há uma norma de gestão de riscos, a ABNT NBR ISO 31000:2018, que abrange riscos de forma mais ampla, e, em segurança da informação, há uma norma específica, a ABNT NBR ISO/IEC 27005:2019. Isso reforça a importância da visão de riscos para que possamos trabalhar com segurança da informação, pois é a partir da identificação dos riscos que a proteção pode ser realizada.

A informação que precisa ter a confidencialidade, a integridade e a disponibilidade preservadas com controles de segurança passa por uma série de elementos ou ativos. Em uma empresa, há pessoas que estão trabalhando nos projetos de novos produtos ou no plano de marketing, nos softwares utilizados nos trabalhos e nos hardwares que armazenam, processam ou transmitem essas informações, e qualquer um desses pontos pode ser alvo de vazamento ou ataques cibernéticos. Assim, a informação, que existe em diferentes formas (físico, digital, na cabeça das pessoas), pode ser considerada o ativo principal a ser protegido; ela pode sofrer um incidente de segurança a partir de ataques em ativos da empresa, que podem ser humanos, físicos, processos ou tecnológicos.

Os ativos, por sua vez, possuem vulnerabilidades. São essas fraquezas existentes em ativos que os agentes de ameaça exploram em seus ataques. Um exemplo é um *cracker* (agente de ameaça) explorando uma autenticação fraca do usuário (vulnerabilidade) na aplicação *Web* (ativo). Esse ataque (ameaça) pode tornar-se um incidente de segurança e ser, ainda, lançado em diferentes níveis. Há possibilidades de ataques ao *notebook* com um *malware*, ao servidor com um ataque que explora vulnerabilidades no sistema operacional ou ao banco de dados com o sistema sendo atacado por falha na autenticação do administrador. Além disso, há a possibilidade de invasões físicas ao *datacenter* ou golpes que explorem a inocência de algum funcionário.

Assim, os elementos a serem protegidos são os ativos, que começam na informação e passam pelas pessoas, pela rede e pelos dispositivos, equipamentos e locais físicos. Há ainda os ativos tecnológicos, compostos pelos softwares, compreendendo *firmwares*, sistemas operacionais, aplicações, aplicativos, plataformas, *middlewares*, banco de dados, protocolos.

As vulnerabilidades estão relacionadas aos ativos, e esse conceito é importante em segurança da informação, por se tratar do elemento que é explorado em ataques (NAKAMURA, 2016). Uma **vulnerabilidade** é um ponto fraco que, uma vez explorado, resulta em um incidente de segurança. Segundo a ISO/IEC 13335-1 (2004), ela inclui fraquezas de um ativo ou grupo de ativos que podem ser explorados (ISO 13335-1, 2004). Quanto maiores as vulnerabilidades, maiores as fraquezas exploradas em ataques.

No caso de sua empresa, você precisa, então, conhecer essas vulnerabilidades para que possam ser eliminadas. Há um conceito bastante relevante sobre a segurança da informação: a segurança de um ativo ou de uma empresa é tão forte quanto o seu elo mais fraco da corrente, ou seja, se houver um ponto fraco (vulnerabilidade), é por lá que o ataque ocorrerá. É por isso que precisamos conhecer todas as

vulnerabilidades de todo o ambiente da empresa, para fazermos todo o tratamento necessário. Já para o atacante, basta encontrar e explorar uma única vulnerabilidade para atacar a empresa (NAKAMURA, 2016).

o

ASSIMILE

Um ataque só acontece porque vulnerabilidades são exploradas pelos atacantes. Temos que eliminar todos os pontos fracos de nosso ambiente, em todos os níveis. Em segurança da informação, vulnerabilidades existem em todas as camadas: humano, físico, *hardware*, protocolo, sistema operacional, aplicação, rede, arquitetura, entre outros. Para complicar, a integração entre diferentes componentes de um ambiente insere complexidade que, como consequência, pode resultar em novas vulnerabilidades. Lembre-se da vulnerabilidade no WEP, protocolo usado em redes Wi-Fi, que foi utilizada para ataques ao TJX (OU, 2007).

Ver anotações

Segundo Nakamura (2016), a exploração de vulnerabilidades pelos atacantes é feita com o uso de métodos, técnicas e ferramentas próprias para cada tipo de vulnerabilidade existente. Se há, por exemplo, um ponto fraco na entrada do centro de dados e o atacante vê que pode acessar fisicamente o servidor e roubá-lo por inteiro, ele explorará essa vulnerabilidade. Para as vulnerabilidades tecnológicas, o ataque é feito com os *exploits*, que são *softwares* que utilizam dados ou códigos próprios que exploram as fraquezas de ativos.

Há *exploits* variados, como aqueles para serviços e aplicações remotas, para aplicações web, para escalada de privilégios e para negação de serviço; além desses, temos os *Shellcodes*, que consistem em códigos a serem executados para explorar vulnerabilidades (NAKAMURA, 2016).

É importante que você entenda que há diferenças entre ameaça e vulnerabilidade. Além disso, é preciso diferenciar, ainda, o ataque de um risco e do agente de ameaça. Ameaça é algo que pode acontecer, é algo que possui potencial de se concretizar. Você pode pensar no mundo físico e imaginar um exemplo de ameaça, que pode ser um golpe, como o da loteria, que só acontece (o golpe) se um golpista (agente de ameaça) explora, com sua conversa fiada (ataque), um indivíduo ingênuo e precisando de dinheiro (vulnerabilidade). A verdade é que a ameaça de golpe sempre existirá, porém ela só se tornará um incidente quando um agente de ameaça explorar uma vulnerabilidade de um ativo, concretizando aquele potencial.

•
Ver anotações

REFLITA

Você usaria *exploits* em seu trabalho como profissional de segurança? *Exploits* são utilizados em ataques, mas também são usados para o aprendizado de problemas de segurança, que levam ao conhecimento de vulnerabilidades e, consequentemente, definição, implementação e manutenção de controles de segurança. Há uma série de websites que disponibilizam *exploits*, como o Exploit Database. Há, ainda, o CVE (*Common Vulnerabilities and Exposures*), que é um dicionário público de vulnerabilidades que pode ser utilizado com o objetivo de proteger a sua empresa.

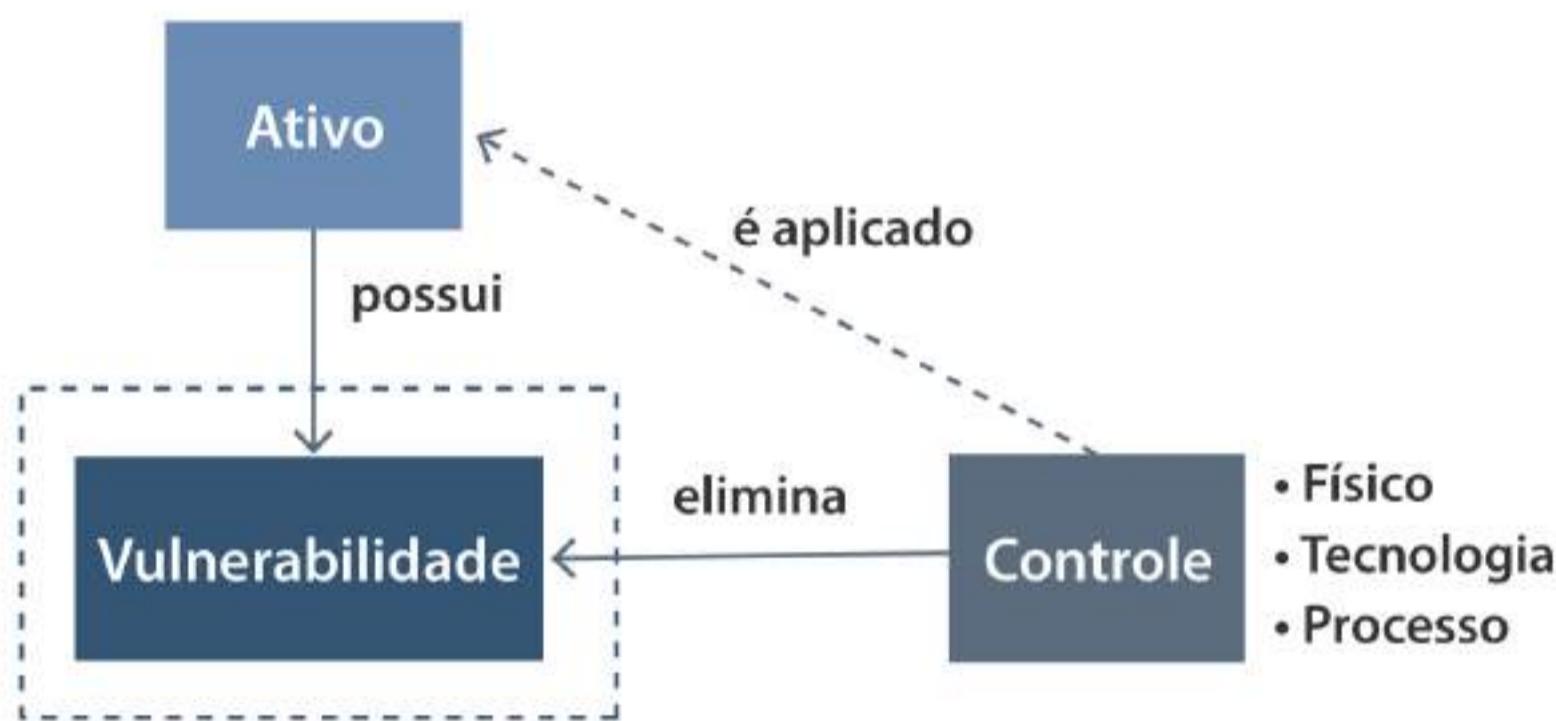
Assim, em segurança da informação, a ameaça é primordial para o entendimento dos riscos que sua empresa corre. Estes são alguns exemplos de **ameaças** para sua empresa:

- Vazamento de projeto de novo produto ou de estratégia de marketing.
- Acesso não autorizado às informações confidenciais.
- Negação de serviço aos sistemas de TI da empresa.
- Alteração de informações-chave da estratégia de marketing.

A proteção, que visa à prevenção contra os riscos identificados, analisados e avaliados, é feita pela definição e implementação de controles de segurança, que englobam mecanismos de defesa e uso de medidas e técnicas de segurança de redes. Os controles de segurança podem ser físicos, tecnológicos ou de processos e são aplicados nos ativos para remover as vulnerabilidades.

O fluxo de controle pode ser visto na Figura 1.4.

Figura 1.4 | Fluxo de controle de segurança



Fonte: elaborada pelo autor.

O conjunto de controles de segurança faz parte da estratégia de segurança para a prevenção e pode ser composto por processos, como a **gestão de identidades e acessos**, que envolve o gerenciamento de contas e senhas dos usuários. Trata-se de um controle essencial, principalmente porque muitos incidentes de segurança visam à obtenção das credenciais de acesso dos usuários.

Um controle de segurança de tecnologia tradicional é o **antivírus**, que é aplicado em servidores e dispositivos dos usuários. Outros mecanismos de defesa tecnológicos são: *firewalls*, controle de acesso lógico, criptografia e monitoramento de redes.

Já um exemplo de controle de segurança processual e humano é a **conscientização de segurança e privacidade** realizada na admissão de funcionários e realizado anualmente.

Para finalizarmos a introdução aos controles de segurança, sob o ponto de vista da segurança de redes, consideramos que as **configurações de equipamentos** de rede, incluindo a arquitetura de redes segura, devem ser feitas de forma conjunta com as outras áreas da empresa, como as de sistemas e negócio.

PESQUISE MAIS

A Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada pelo Decreto 10.222, de 5 de fevereiro de 2020, foi elaborada com o objetivo principal de apresentar, para a sociedade brasileira, os rumos que o Governo Federal considera essenciais para que o país, a sociedade e suas instituições tornem-se seguros e resilientes no uso do espaço cibernético.

- BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020.
Aprova a estratégia nacional de segurança cibernética.

Diário Oficial da União, Brasília, DF, 2020.

Esse decreto apresenta uma série de informações relevantes que serão muito úteis para esta disciplina.

- BRASIL. Segurança da Informação. Gabinete de Segurança Institucional da Presidência da República. **Estratégia Nacional de segurança cibernética / e-ciber.** [s.d.].

Assim, chegamos ao final desta importante seção, em que foram apresentados os principais conceitos que o acompanharão durante toda sua jornada em segurança da informação. Lembre-se sempre de que a segurança da informação envolve identificação, proteção, detecção, resposta e recuperação. Um desejo importante é que a segurança da

informação seja vista como uma área parceira e viabilizadora dos negócios da empresa e menos como uma área que coloca obstáculos e compromete a usabilidade dos usuários.

FAÇA VALER A PENA

Questão 1

Um dos ataques cibernéticos que mais afetam as empresas é o *Denial of Service* (DoS) ou a negação de serviço. Há uma série de técnicas desse ataque, desde o nível de redes até o nível de aplicação. Quando esse ataque ocorre, clientes e funcionários ficam impedidos de acessar os sistemas.

Assinale a alternativa que apresenta o princípio da segurança da informação atacado.

a. Confidencialidade.

b. Integridade.

c. Disponibilidade.

d. Vulnerabilidade.

e. Ameaça.

Questão 2

Em um ataque recente contra um famoso sistema operacional, um *malware* ou código malicioso infectou todas as máquinas que utilizavam determinada versão do sistema. Essa infecção alterou funções importantes do sistema, incluindo, em cada dispositivo infectado, uma função que monitora tudo o que o usuário digita. Com isso, quando o usuário acessa o banco para pagar um boleto, esses dados são alterados para um boleto falso e a transação é fraudulenta. O usuário foi vítima de uma fraude com boleto bancário.

Há um conjunto de conceitos de segurança envolvido nessa situação; há o *malware*, o sistema operacional, o dispositivo, o usuário, o boleto falso e a fraude bancária. Os conceitos de segurança da informação que

estão relacionados com a fraude bancária e o resultado dela são:

a. Confidencialidade e ameaça.

b. Integridade e ameaça.

c. Disponibilidade e ameaça.

d. Ameaça e integridade.

e. Vulnerabilidade e ameaça.

Questão 3

Um cliente de uma instituição financeira foi vítima de um ataque cibernético e teve os recursos de sua conta transferidos para um desconhecido. Ele ficou sabendo do ataque quando percebeu que não estava conseguindo realizar uma compra, já que sua conta estava negativa. Como especialista em segurança da informação da instituição financeira, você identificou que o ataque ocorreu internamente, ou seja, algum funcionário acessou indevidamente o sistema e realizou as transações.

Assinale a alternativa que contém os elementos da segurança da informação que você identificou no contexto apresentado.

a. Risco e vulnerabilidade.

b. Incidente de segurança e agente de ameaça.

c. Vulnerabilidade e confidencialidade.

d. Agente de ameaça e risco.

e. Controle de segurança e ameaça.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉNICAS. **ABNT NBR ISO/IEC 27001:2013.** Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2013.

27002:2013. Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

BEAHM, G. **O mundo segundo Steve Jobs.** Rio de Janeiro: Editora Campus.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a estratégia nacional de segurança cibernética. **Diário Oficial da União, Brasília, DF.** 2020. Disponível em: <https://bit.ly/3jcx6uB>. Acesso em: 23 out. 2020.

BRASIL. Segurança da Informação. Gabinete de Segurança Institucional da Presidência da República. **Estratégia Nacional de segurança cibernética / e-ciber.** [s.d.]. Disponível em: <https://bit.ly/3rd0xzG>. Acesso em: 23 out. 2020.

NAKAMURA, E. T.; GEUS, P. L. de. **Segurança de redes em ambientes cooperativos.** São Paulo: Editora Novatec, 2007.

NAKAMURA, E. T. **Segurança da informação e de redes.** São Paulo: Editora e Distribuidora Educacional S.A. 2016.

NIST. **The Five Functions.** 2018. Disponível em: <https://bit.ly/3pHlItl>. Acesso em: 23 out. 2020.

OFFENSIVE SECURITY. **Exploit Database.** 2020. Disponível em: <https://www.exploit-db.com>. Acesso em: 23 out. 2020.

OLIVEIRA, R. C. Q. **Segurança em redes de computadores.** São Paulo: Editora Senac, 2017. Disponível em: <https://bit.ly/36AOCDU>. Acesso em: 23 out. 2020.

OU G. **TJX's failure to secure Wi-Fi could cost \$1B.** 2007. Disponível em: <https://zd.net/3ap56Ad>. Acesso em: 23 out. 2020.

THE MITRE CORPORATION. **Common vulnerabilities and exposures.** 2020. Disponível em: <https://cve.mitre.org>. Acesso em: 23 out. 2020.

FOCO NO MERCADO DE TRABALHO

INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Emilio Tissato Nakamura

Ver anotações

SEGURANÇA DA INFORMAÇÃO PARA QUÊ?

Entenda na prática por que é necessário investir em segurança da informação.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Você é o responsável pela segurança da informação de uma empresa do setor químico e iniciará um trabalho que começará com uma visão organizada de todos os principais conceitos da segurança da informação:

- A segurança da informação envolve identificação, proteção, detecção, resposta e recuperação.
- É preciso garantir os princípios da segurança da informação: confidencialidade, integridade, disponibilidade.
- É preciso trabalhar com os elementos do risco: ativos, vulnerabilidades, agentes de ameaça, ameaças, vulnerabilidades, probabilidade, impacto.
- A aplicação de mecanismos de defesa, de controles de segurança e de técnicas de segurança de redes é definida a partir de uma visão de riscos.

Essa visão organizada é fundamental para que uma cultura de segurança se inicie e possibilite uma evolução constante do nível de maturidade da empresa, começando pela diretoria executiva. Ao final da apresentação, ficará mais claro para todos tudo o que envolve a questão “segurança da informação para quê?”.

Sugestão de estrutura da apresentação:

1. Faça um resumo do projeto da empresa.
2. Apresente os ativos envolvidos no projeto, não se esquecendo de que eles podem ser as pessoas, os equipamentos, os artefatos físicos, os processos, os sistemas e as tecnologias. Não é necessário citar todos, mas uma boa representatividade é importante.
3. Considere *crackers* e concorrentes como agentes de ameaça. Cite uma ameaça de cada tipo que afeta confidencialidade, integridade e disponibilidade.
4. Justifique que os ativos podem ter vulnerabilidades e explique-as.
5. Disserte sobre impactos em caso de uma ameaça tornar-se um incidente de segurança. Considere a tríade CID e descreva impactos incrementais, que iniciam com a equipe e incluem o projeto, indo até a empresa e as perdas financeiras de mercado e de reputação, por exemplo.
6. Faça uma relação entre os elementos do risco, unindo as informações anteriores.
7. Defina uma proposta de implementação de controles de segurança, mecanismos de defesa e técnicas de segurança de redes e aponte quais são eles.

Atenção para os princípios da segurança da informação:
confidencialidade, integridade e disponibilidade — são eles que precisam ser protegidos. Uma falha comum é focar apenas um dos

aspectos da segurança da informação, negligenciando os outros. Há muitas ameaças rondando o ambiente da empresa, e as vulnerabilidades precisam ser identificadas.

Com a sua apresentação, você responderá a uma série de questões:

- No caso de um ataque cibernético contra a empresa, quais princípios de segurança da informação podem ser comprometidos?
- O que pode ser atacado, por que e por quem?
- O que pode acontecer em caso de um incidente de segurança?
- O que pode ser implementado para a segurança da informação?

EVITANDO VAZAMENTO DE INFORMAÇÕES

Devemos, como profissionais de segurança da informação, garantir a confidencialidade da informação, ou seja, permitir que somente pessoas autorizadas tenham acesso àquelas informações. O grande desafio da segurança da informação é, além de entender esse princípio, fazer com que ele seja cumprido. Como garantir a confidencialidade da informação? Como permitir que somente pessoas autorizadas tenham acesso às informações? Como evitar acessos não autorizados às informações? Como impedir vazamentos ou ataques cibernéticos que comprometem a confidencialidade?

De forma complementar, a disponibilidade também é um requisito primordial para a sua empresa, principalmente ao se tratar de uma plataforma de *marketplace* imobiliário. Sem o acesso a essas informações, o andamento dos negócios sofre prejuízos. No caso mais simples, a perda de disponibilidade temporária resulta em perda de tempo. Já nos casos mais complexos, a perda total das informações resulta em prejuízos bem maiores, que inviabilizam todo o andamento da empresa. Como tratar a segurança da informação nesse caso?

RESOLUÇÃO



Inicie a resolução considerando os diferentes tipos de ativos existentes: humanos, físicos, tecnológicos; explore as vulnerabilidades típicas existentes em cada um desses tipos de ativo. Por exemplo, humanos podem ser fonte de vazamento de informações em caso de suborno e um serviço na nuvem pode ser explorado a partir de uma vulnerabilidade da aplicação, que não é de responsabilidade do provedor de nuvem. Frente a isso, explore os possíveis controles de segurança que podem ser aplicados nos ativos para tratar as vulnerabilidades.

NÃO PODE FALTAR

SEGURANÇA DE REDES

Emilio Tissato Nakamura

Ver anotações 0

CONTROLE DE SEGURANÇA

O controle de segurança mais famoso é o *firewall*, que é o responsável pelo controle de acesso de rede.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

PRATICAR PARA APRENDER

Nesta seção, você reforçará e aprofundará o entendimento dos princípios da segurança da informação (confidencialidade, integridade e disponibilidade), dos elementos do risco (ativos, vulnerabilidades,

agentes de ameaça, ameaças, probabilidade e impacto) e dos relacionamentos com mecanismos de defesa, controles de segurança e técnicas de segurança de redes.

Para os profissionais de segurança da informação que buscam prevenção, detecção e resposta, é preciso entender onde, por que e como os ataques acontecem. Nesta seção, vamos detalhar alguns desses ataques e conhecer alguns controles de segurança que podem ser utilizados para a prevenção e detecção.

Para você alcançar a melhor estratégia de segurança, é importante entender que os elementos que compõem o risco de segurança se inter-relacionam o tempo todo. Por exemplo, ataques de negação de serviço (*Denial of Service, DoS*) afetam a disponibilidade e podem ser realizados por crackers que exploram vulnerabilidades em protocolos de rede. Há, ainda, outras variáveis que devem ser entendidas sobre os ataques DoS e tudo o que está envolvido, desde os pontos de ataques até os controles de segurança que podem ser aplicados.

Lembre-se de que os controles de segurança atuam sobre as vulnerabilidades que existem em ativos, e os agentes de ameaça exploram essas vulnerabilidades existentes em ativos. Quando isso acontece, uma ameaça se torna um incidente de segurança, o que causa impactos para a empresa.

Você é o responsável pela segurança da informação de uma empresa do setor químico que conta com os maiores cientistas brasileiros e possui unidades em São Paulo, Rio de Janeiro e Salvador. Além disso, ela tem acordo de cooperação internacional com uma empresa chinesa e outra suíça, bem como tem parceria com grandes investidores para o financiamento de seus projetos.

A sua atividade será focada em um grande projeto em andamento que já chegou a grandes resultados, uma vez que os cientistas descobriram um novo composto que será utilizado na indústria agrícola. Você, no

entanto, está preocupado com a forma como os resultados do desenvolvimento estão sendo protegidos. O impacto pode ser gigantesco em caso de incidentes de segurança, principalmente com a concorrência também mobilizando grandes equipes para colocar no mercado os avanços para o setor.

Nesta disciplina, você já sensibilizou a diretoria executiva da empresa quanto à necessidade de ações para a segurança do projeto. Você fez uma apresentação envolvendo, conceitualmente, elementos do risco, como ativos, agentes de ameaça, vulnerabilidades, ameaças, impactos e controles de segurança, fazendo uma conexão com os princípios da segurança da informação (confidencialidade, integridade e disponibilidade).

Nesta segunda rodada de apresentação para a diretoria executiva, você detalhará os seguintes elementos:

- Pontos de ataques, representados por sistemas compostos por diferentes aspectos, que possuem vulnerabilidades: *hardware*, *software*, protocolos, aplicações.
- Pontos de ataques indicando os ativos humanos e físicos envolvidos.
- Agentes de ameaça, ameaças e técnicas de ataques.
- Controles de segurança para a autenticação dos usuários.
- Controles de segurança de rede.

Considere que o projeto está em execução pelas pessoas que têm as ideias e que essas informações vão, de forma digital, do *notebook* até o servidor da empresa, passando pela rede, e que nesse caminho as informações podem ser vazadas, alteradas ou destruídas (CID).

Você pode **fazer um diagrama ou relacionar todos os elementos em uma lista**, bem como fazer um **breve resumo** de cada caso ou situação presente nela. Por exemplo: uma situação que os diretores executivos precisam saber é que um *cracker* (agente de ameaça) pode explorar uma vulnerabilidade do sistema operacional do servidor (ativo) para

contaminar o sistema com um *exploit* (técnica de ataque) e roubar (ameça) as informações do novo composto químico (ativo). Apresente as situações envolvendo DoS, DDoS, ataque de força bruta e ataque do homem do meio.

0

Ver anotações

No final da apresentação, **apresente uma sugestão de conjunto de controles de segurança**, indicando quais situações cada um deles mitiga. A diretoria executiva, então, saberá que há diversos pontos de ataques e diferentes situações de segurança que podem ser resolvidos com a sua proposta de estratégia de segurança contendo um conjunto de controles.

Vamos, agora, explorar o mundo dos ataques que viraram notícias no mundo da segurança e que tanto afetam as empresas. É o entendimento dos assuntos desta seção que fará você compreender melhor o mercado de trabalho de segurança da informação, que sofre transformações constantes em linha com as evoluções dos ataques cibernéticos, dos novos negócios, das novas tecnologias e das novas ameaças.

CONCEITO-CHAVE

INCIDENTES DE SEGURANÇA

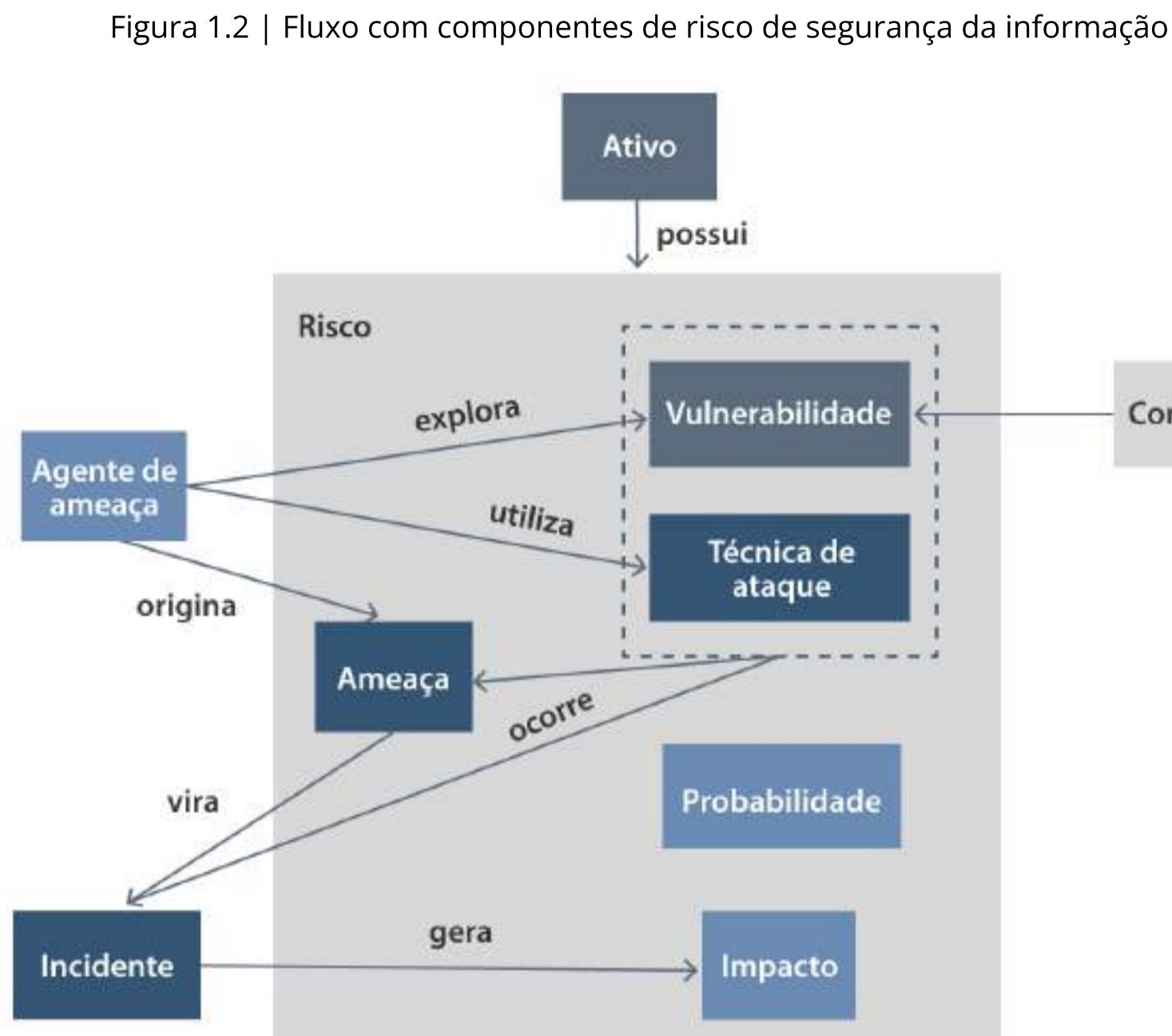
Em agosto de 2020, a bolsa de valores da Nova Zelândia sofreu paralisação de suas operações em virtude de ataques de negação de serviços por quatro dias (CPOM, 2020). Ataques de *ransomware*, que sequestram dados de servidores e usuários com a finalidade de resgates, continuam fazendo vítimas em todo o mundo (CRN, 2020).

Esses dois casos mostram que os ataques de crackers ou ataques cibernéticos continuam acontecendo e evoluindo numa alta velocidade, atingindo desde pequenos negócios até infraestruturas críticas de países.

O que há de comum entre os dois ataques citados é que eles podem ter sido causados pelos mesmos agentes de ameaça, os *crackers*, e resultaram em grandes impactos para as suas vítimas. Há, no entanto, um conjunto de elementos diferentes, que vai desde a ameaça até a técnica de ataque utilizada, a vulnerabilidade explorada, o princípio da segurança da informação atingido e o ponto de ataque ou ativo

explorado, e são esses elementos que serão discutidos nesta seção, de modo que você possa entender a complexidade e as possibilidades de ataques existentes.

A Figura 1.2 mostra os elementos do risco. Agentes de ameaça exploram, com técnicas de ataques, as vulnerabilidades de ativos, e, quando isso ocorre, uma ameaça se torna um incidente de segurança. Como profissional de segurança, você deve conhecer esses elementos e, a partir do cálculo do risco (probabilidade e impacto), estabelecer uma estratégia de segurança com os controles de segurança a serem implementados.

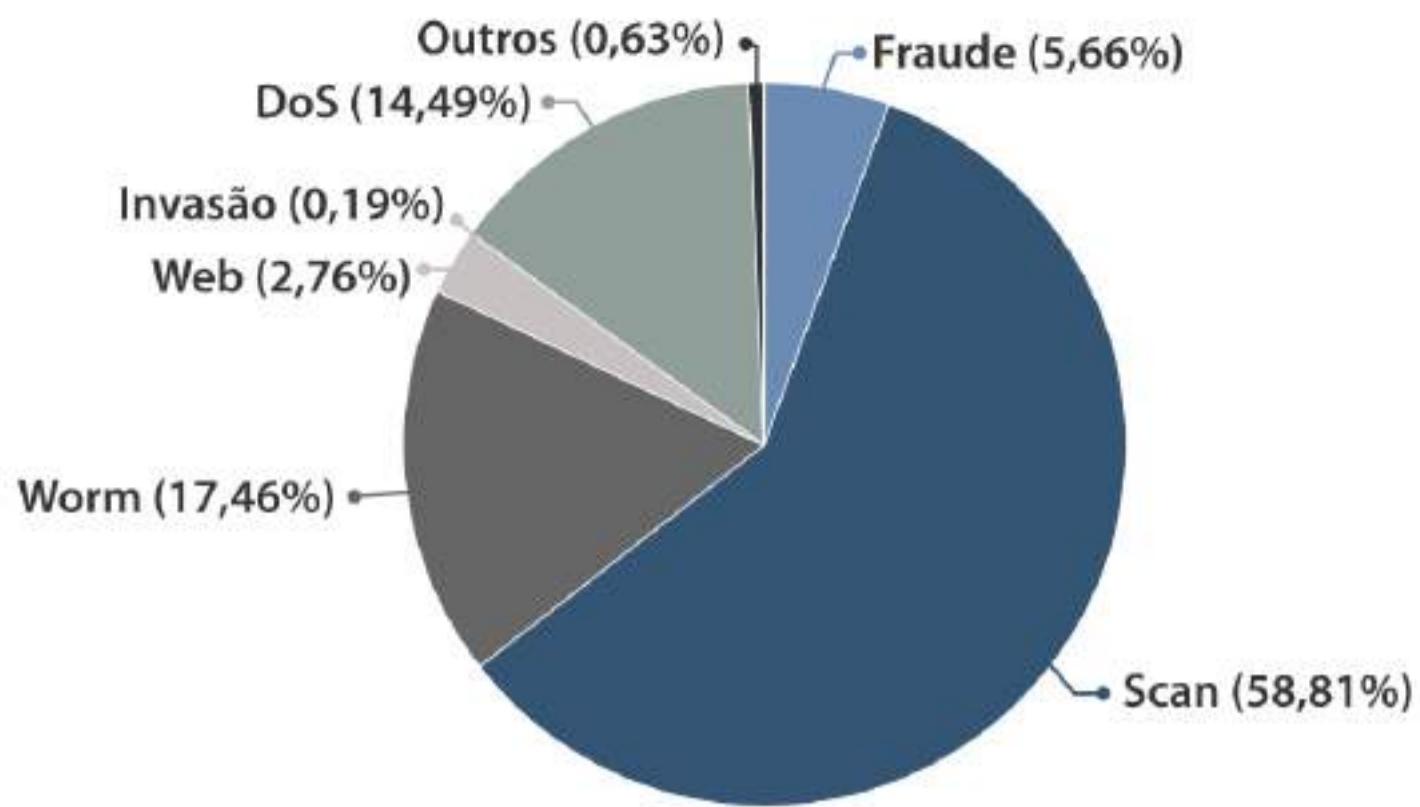


Fonte: elaborada pelo autor.

O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. Ele é responsável por tratar incidentes de segurança em computadores que envolvem redes conectadas à Internet no Brasil. A Figura 1.5 apresenta os incidentes de segurança reportados ao CERT.br de janeiro a junho de 2020, enquanto o Quadro 1.1 apresenta os ataques que fazem parte da estatística (CERT, 2020).

Figura 1.5 | Incidentes de segurança reportados ao CERT.br (janeiro a junho de 2020)

Tipos de ataque



Fonte: adaptada de: CERT.br.

Quadro 1.1 | Definição para os incidentes de segurança reportados ao CERT.br

<i>worm</i>	Notificações de atividades maliciosas relacionadas ao processo automatizado de propagação de códigos maliciosos na rede.
DoS	Notificações de ataques de negação de serviço, em que o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, um computador ou uma rede.
invasão	Um ataque bem sucedido que resulta no acesso não autorizado a um computador ou rede.
<i>Web</i>	Um caso particular de ataque visando especificamente ao comprometimento de servidores Web ou desfigurações de páginas na Internet.
<i>scan</i>	Notificações de varreduras em redes de computadores com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
fraude	Segundo Houaiss (2001, p. 1388), é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Essa categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de se obter vantagem.
outros	Notificações de incidentes que não se enquadram nas categorias anteriores.

A partir desse entendimento da dinâmica dos ataques, você pode definir a melhor estratégia de segurança da informação, composta pelos elementos do risco para justificar as definições, e os controles de segurança a serem implementados.

VOCABULÁRIO

Hackers ou *crackers*? Segundo Nakamura e Geus (2007), os *hackers*, por sua definição original, são aqueles que utilizam seus conhecimentos para invadir sistemas, não com o intuito de causar danos à vítima, mas sim como um desafio às suas habilidades. Eles invadem os sistemas, capturam ou modificam arquivos para provar a sua capacidade e compartilham a sua proeza com seus colegas, demonstrando que conhecimento é poder. Exímios programadores e conhecedores dos segredos que envolvem as redes e os computadores geralmente não gostam de ser confundidos com *crackers*. Com o advento da Internet, os diversos ataques pelo mundo foram atribuídos a *hackers*, mas eles refutam essa ideia, dizendo que hacker não é *cracker*.

Crackers são elementos que invadem sistemas para roubar informações e causar danos à vítima. *Crackers* também é uma denominação utilizada para aqueles que quebram códigos e proteções de *softwares*. Com o crescimento da Internet e a consequente facilidade em se obter informações e ferramentas de ataques, a definição de *hacker* mudou. A própria imprensa mundial tratou de mudar esse conceito. Muitas vezes, um incidente de segurança é atribuído a *hackers*, em seu sentido genérico (NAKAMURA; GEUS, 2007).

OS PONTOS DE ATAQUES

Ativos são atacados pelos agentes de ameaça, que exploram as suas fraquezas ou pontos fracos ou vulnerabilidades. Em segurança da informação, a definição da estratégia de segurança é desafiadora justamente porque um *cracker* pode concretizar o seu ataque explorando uma única vulnerabilidade de um único componente ou ativo de um sistema. Por outro lado, você, como profissional de segurança, deve ser capaz de enxergar todas essas possibilidades, definir e implementar os controles de segurança que protegem a sua empresa. Isso deve ser feito de acordo com uma visão de riscos, ou seja, você deve definir os controles de acordo com as prioridades que resultam da avaliação da probabilidade e do impacto envolvido com cada ameaça existente.

E os pontos de ataques são muitos em um sistema (LIMA, 2017). Imagine que sua empresa disponibiliza um portal de fornecedores; nesse cenário, quais são os pontos de ataques que devem ser considerados?

REFLITA

A segurança da informação visa garantir os princípios da confidencialidade, integridade e disponibilidade da informação.

A informação possui diferentes dimensões:

- Ela pode estar na cabeça das pessoas.
- Ela pode estar em um meio físico, como em um pedaço de papel ou cunhado na parede de uma caverna.
- Ela pode estar em um meio digital, como em um *smartphone*, em um servidor, na nuvem ou sendo transmitido pelo ar, por meio de ondas de rádio, por exemplo.

Isso faz com que tenhamos que pensar em controles de segurança que vão além dos aspectos tecnológicos, tais como a conscientização de usuários e o controle de acesso físico. Os controles de segurança devem, assim, ser utilizados em conjunto, formando uma defesa em camadas.

No caso do portal de fornecedores, há um conjunto de elementos ou ativos que fazem parte do sistema e que podem, assim, conter vulnerabilidades que são visadas pelos agentes de ameaça. Há, no portal de fornecedores, além da aplicação, o banco de dados, o *middleware*, o sistema operacional, o servidor, a comunicação ou a rede e os administradores que possuem o acesso a esses componentes. Todos eles representam pontos de ataques que podem levar à perda de confidencialidade, integridade ou disponibilidade.

Há, nesse exemplo, potenciais vulnerabilidades de *hardware* (servidor, disco rígido), *software* (aplicação, *middleware*, banco de dados, sistema operacional), protocolos (TCP/IP ou outro utilizado pela aplicação). Como tudo passa pela rede e a aplicação está na camada 7 da pilha de protocolos TCP/IP, o portal de fornecedores está sujeito às vulnerabilidades de rede e de *hardware*.

Além disso, não podemos deixar de lado as vulnerabilidades humanas, relacionadas aos administradores de sistemas, e as vulnerabilidades físicas, relacionadas ao *datacenter*.

Os pontos de ataques também devem ser avaliados de acordo com o estado da informação. A informação pode estar em processamento, também conhecido como Data-In-Use (DIU), ou em transmissão, conhecido como *Data-In-Motion* (DIM). Quando a informação está armazenada, o estado é conhecido como *Data-At-Rest* (DAR).

Com a **Lei Geral de Proteção de Dados Pessoais** (LGPD), os dados pessoais devem ser protegidos para a garantia da privacidade. Ataques podem ser realizados para que dados pessoais sejam vazados e a privacidade seja comprometida, bem como podem ocorrer com dados em processamento (DIU), dados em transmissão (DIM) ou dados armazenados (DAR). Ataques a banco de dados visam aos dados armazenados, enquanto ataques à rede visam aos dados em transmissão. Já os dados em processamento podem sofrer ataques mais sofisticados.

■ AGENTES DE AMEAÇA, AMEAÇAS E TÉCNICAS DE ATAQUES

Os agentes de ameaça são elementos importantes para o entendimento dos riscos e da segurança; os mais comuns são as pessoas, que possuem facetas diferentes, de acordo com o ambiente em avaliação.

Por exemplo, os **crackers**, a depender do contexto, são pessoas maliciosas que atacam sistemas de informação, mas há outras pessoas que também podem comprometer a sua empresa. Será que um funcionário mal-intencionado também não pode atacar a sua empresa?

Fraudadores também são pessoas que podem atacar a sua empresa, explorando vulnerabilidades de funcionários desatentos, por exemplo. E há, ainda, os **agentes de ameaça naturais**, que podem comprometer a disponibilidade da informação em caso de uma inundação de datacenter, por exemplo.

Um agente de ameaça bastante crítico, que pode ser considerado também uma ameaça, é o **malware** ou o código malicioso. *Malwares* são programas desenvolvidos com o objetivo de gerar alguma ação danosa ou maliciosa em um computador. Existem diversos tipos de *malware* e cada um age de uma maneira; vírus e *worm* são exemplos.

VOCÊ SABE A DIFERENÇA ENTRE UM VÍRUS E UM WORM?

Vírus é um código malicioso que contamina um sistema a partir de uma ação do usuário. Por exemplo: um clique em um link contaminado, que contém um vírus que explora uma vulnerabilidade do sistema, ou a instalação de um *software* suspeito, tornando-se parte de outros programas e arquivos. Já aquele código malicioso que se propaga automaticamente nas redes em busca de uma vulnerabilidade do sistema operacional, por exemplo, contaminando e se espalhando sem a necessidade de ação humana, é chamado de **worm**.

0

Ver anotações

Outro exemplo de *malware* é o **cavalo de Troia**, que o usuário instala em seu sistema imaginando que o *software* executa somente aquela função que ele buscava, mas que, na realidade, realiza ações maliciosas, como o *keylogger*, para capturar o que o usuário digita ou a gravação e o envio de arquivos para o *cracker*.

EXEMPLIFICANDO

Um ataque bastante comum que visa ao roubo de credenciais de acesso a bancos é o uso de *keylogger*. Quando o equipamento do usuário é contaminado com esse *malware*, tudo o que é digitado, como a senha bancária, é enviado ao *cracker*.

Outro tipo de *malware* é o **Backdoor**. Esse código malicioso possibilita que o invasor realize acessos remotos não autorizados ao sistema sem que, muitas vezes, seja percebido. O *Backdoor* explora vulnerabilidades no sistema, por exemplo, *softwares* ou *firewall* desatualizados, pela abertura de portas, por exemplo, servidor, do roteador e *firewall*.

Há ainda, casos em que *backdoors* são inseridos por fabricantes de programas de forma proposital, com a justificativa de administração do sistema (CERT.BR, 2020).

PESQUISE MAIS

Para entender melhor os *malwares*, tais como os vírus, *worm*, *bot* e *botnet*, *spyware*, *backdoor*, cavalo de Troia (*trojan*) e *rootkit*, acesse a Cartilha de Segurança do CERT.BR.

- CERT.br. **Cartilha de Segurança para internet.** [s.d.].

Um *malware* crítico é o ***ransomware***: ele sequestra informações com o uso de criptografia. O criminoso cifra os arquivos ou o disco e exige o pagamento de um resgate em troca da chave criptográfica que decifra as informações originais.

REFLITA

Em meados de 2017, um *ransomware* chamado *WannaCry* trouxe sérios transtornos para muitas instituições, inclusive no Brasil. O cibercriminoso bloqueia o acesso a recursos por meio de criptografia e a vítima só consegue descriptografá-los após o pagamento de um resgate. Qual princípio da segurança da informação você considera que foi violado: confidencialidade ou integridade dos dados? O que pode ser feito para evitar ou minimizar os impactos desse tipo de ataque?

Agora, vamos discutir outro tipo de **ataque que afeta a disponibilidade da informação**. A informação pode existir em diferentes estados (DIM, DIU, DAR), e entender o fluxo dela do servidor para o usuário é importante para identificar como a disponibilidade pode ser afetada.

De forma geral, uma informação que está em um banco de dados (DAR) pode ser acessada por um usuário, e o fluxo passa pela aplicação, que pode fazer um processamento (DIU) antes de ser enviado pela rede (DIM), mas não sem antes passar pelo sistema operacional, e esses são os pontos em que a informação pode ser atacada.

No caso da disponibilidade, o ataque mais tradicional é a **negação de serviço ou Denial-of-Service (DoS)**, que pode ser direcionado para qualquer um desses pontos de ataque. Imagine uma quantidade tão grande de requisições que uma aplicação não é mais capaz de atender. Não precisa nem mesmo ser um ataque, já que, em muitas ocasiões, o acesso a determinado serviço pode se tornar impossível quando há muitos acessos simultâneos, como para a compra online de ingressos ou o envio de documentos obrigatórios no final do prazo por todos os brasileiros. Quando há uma coordenação para que as requisições sejam enviadas simultaneamente, a partir de diferentes pontos, o ataque é conhecido como **Distributed Denial-of-Service (DDoS)**.

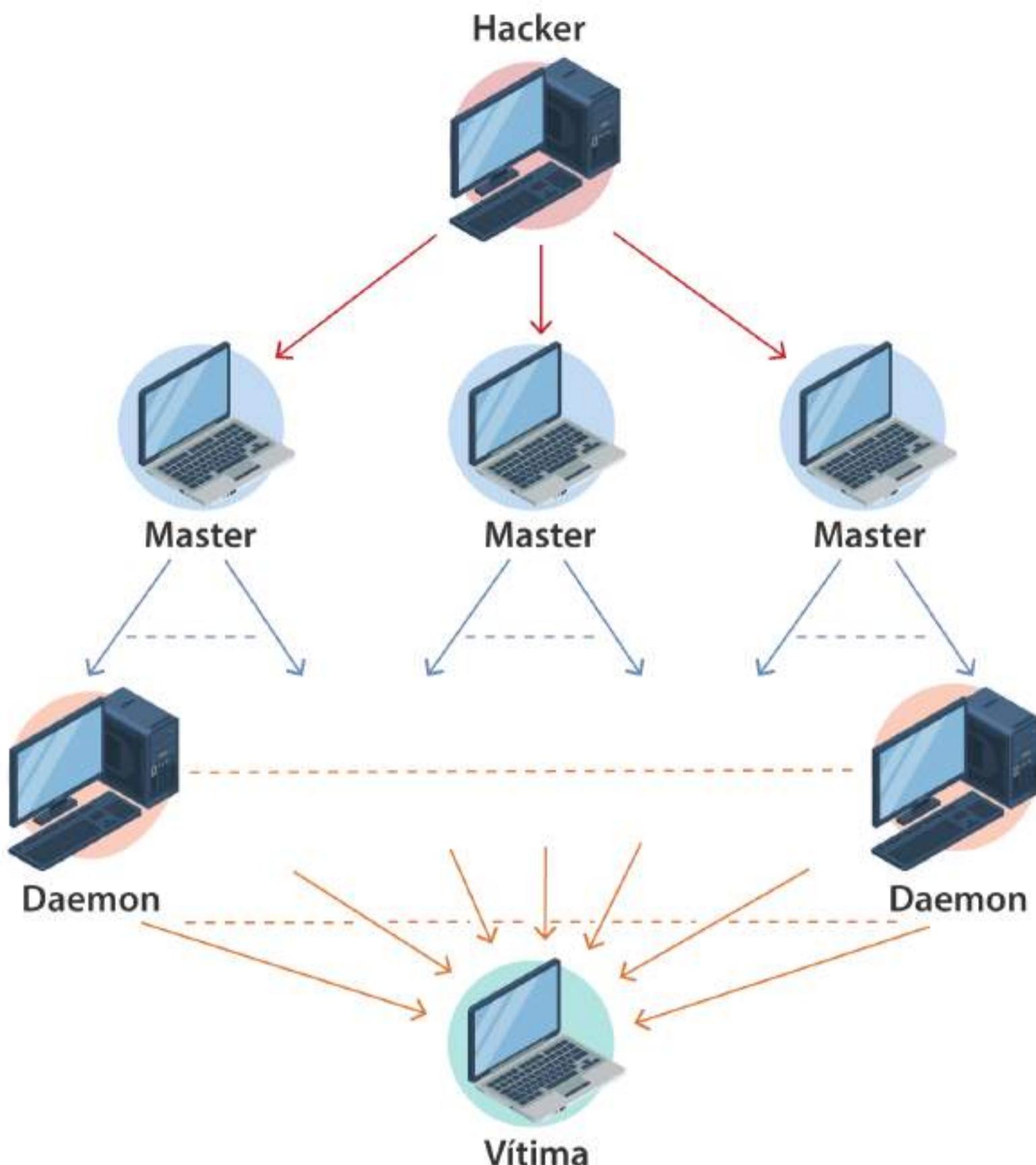
SAIBA MAIS

Há uma série de ataques de negação de serviço (DoS ou DDoS) que valem a pena ser conhecidos. Há o *SYN Flooding*, fragmentação de pacotes IP, *Smurf* e *Fraggle* e DDoS com distribuição e coordenação com o uso de *master*, *zombies* e *daemons*.

A Figura 1.6 apresenta um ataque DDoS, em que o atacante utiliza *masters* e *daemons* para o ataque distribuído e coordenado à vítima. Os *masters* são máquinas controladas diretamente pelo atacante, enquanto os *daemons* são controlados pelos *masters*. Os *daemons* realizam efetivamente o ataque à vítima.

Figura 1.6 | Ataque de DDoS

Ver anotações



Fonte: elaborada pelo autor.

Os ataques DoS e DDoS podem tirar proveito também do próprio protocolo TCP com a manipulação das mensagens de conexão envolvendo o SYN (OLIVEIRA, 2017).

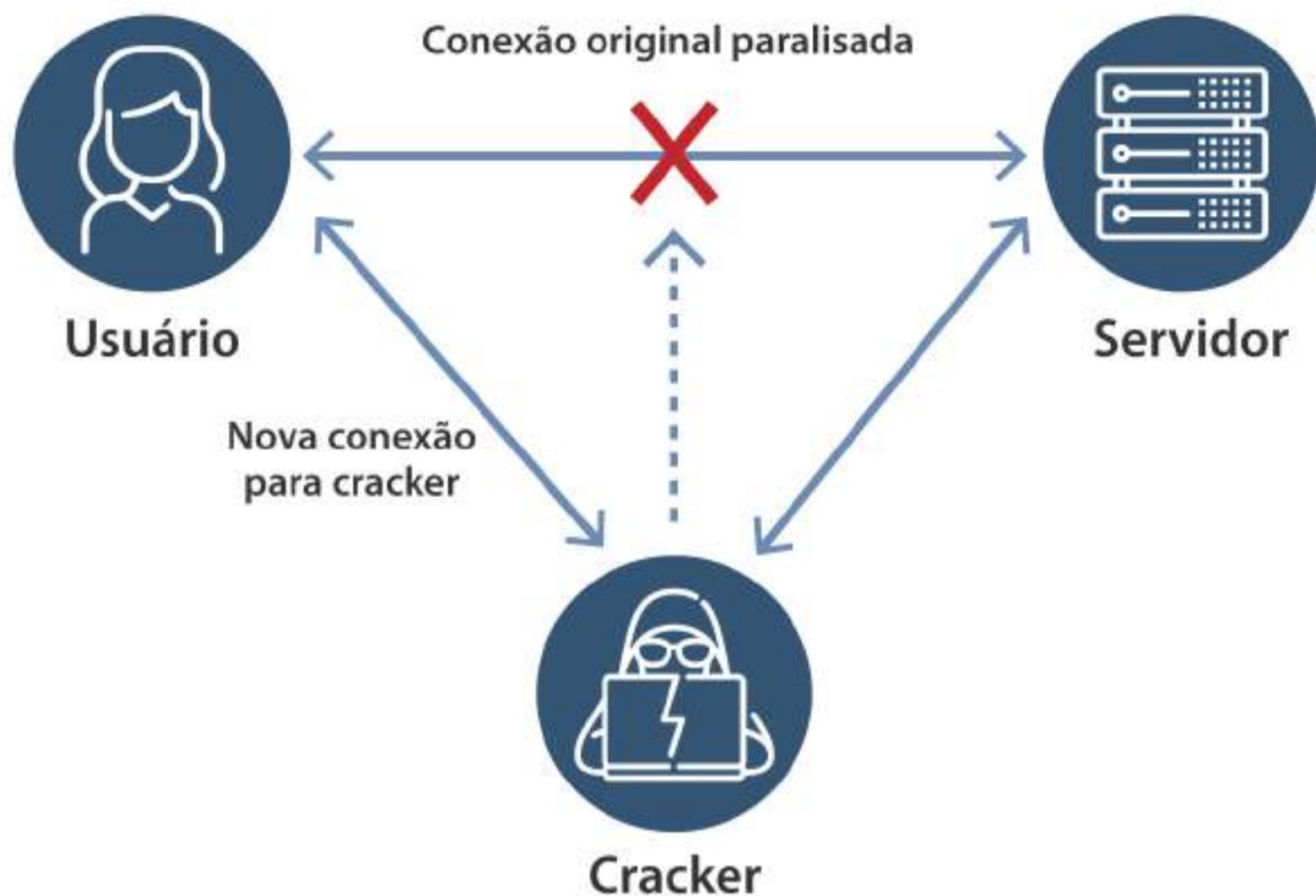
EXEMPLIFICANDO

Uma técnica típica de DoS é o *SYN Flooding*, que causa o *overflow* da pilha de memória por meio do envio de grande número de pedidos de conexão TCP, que não podem ser totalmente completados e manipulados. Essa técnica foi uma das utilizadas por Kevin Mitnick em um dos ataques mais

conhecidos da internet (LUONG, 2007). Além desse ataque, outros ataques DoS e DDoS continuam acontecendo, comprometendo bancos, especialistas em segurança, provedores de serviços e de nuvem, entre outros (JUNQUEIRA, 2020).

Outro ataque importante é **o ataque do homem do meio ou *Man-In-The-Middle* (MITM)**, que pode ser visto na Figura 1.7.

Figura 1.7 | Ataque do homem do meio com redirecionamento de tráfego



Fonte: elaborada pelo autor.

Esse ataque é conhecido também como sequestro de conexões e é ativo, ou seja, a manipulação ocorre em tempo real, com o agente de ameaça tendo o controle dela, redirecionando as conexões TCP para determinada máquina.

Além da injeção de tráfego, permite, ainda, driblar proteções geradas por protocolos de autenticação, comprometendo, assim, a confidencialidade (tendo acesso às informações em trânsito), a integridade (alterando ou injetando informações na conexão) e mesmo a disponibilidade (descartando informações que deixam de chegar ao seu destino) (NAKAMURA; GEUS, 2007). Malenkivich (2013) cita alguns exemplos de ataques do homem do meio ou MITM.

Outro problema relacionado à autenticação dos usuários é que uma senha pode ser adivinhada (*password guessing*) ou descoberta com o uso de técnicas como o **ataque do dicionário**, em que palavras de dicionários são testadas, ou o **ataque de força bruta**, em que diferentes combinações de caracteres são testadas em busca do acesso.

Assim, um dos mecanismos de segurança que podem ser utilizados é a trava de tentativas de acessos após determinado número de tentativas inválidas de senhas.

ASSIMILE

DoS e DDoS comprometem a disponibilidade da informação com a exploração de diferentes componentes de um sistema, como a rede ou a aplicação; já ataques envolvendo *malware* ou o ataque do homem do meio podem comprometer, além da disponibilidade, a confidencialidade e a integridade da informação.

CONTROLES DE SEGURANÇA E PROTEÇÃO

Já vimos os principais pontos de ataques e as relações entre agentes de ameaça, ameaças e as principais técnicas de ataques utilizadas. Agora, vamos complementar o entendimento com os controles de segurança e proteção, começando com a proteção à rede. Após uma discussão sobre *firewall*, *Intrusion Prevention System* (IPS) e *antimalware*, apresentaremos algumas das principais ferramentas de proteção de informações.

A proteção à rede considera que, no fluxo da informação, todo acesso passa pela rede, sendo este, portanto, um bom local para controles de segurança. De fato, uma boa estratégia de segurança deve levar em consideração a rede, com uma **arquitetura de redes segura, considerando segmentação, uso de zonas desmilitarizadas (DeMilitarized Zone, DMZ), controle de acesso de rede e detecção de ataques** (OLIVEIRA, 2017).

ASSIMILE

Em uma rede segura, a criação de uma zona desmilitarizada ou *DeMilitarized Zone* (DMZ) é uma técnica importante. Uma DMZ é uma rede específica que fica entre uma rede pública, como a Internet, e a rede interna. Com essa segmentação, a

rede interna conta com uma camada adicional de proteção, pois os acessos são permitidos para os serviços disponibilizados na DMZ, mas não para a rede interna.

O controle de segurança mais famoso é o **firewall**, que é o responsável pelo controle de acesso de rede. Na realidade, o *firewall* começou funcionando na camada de rede e, atualmente, ele atua também na camada de aplicação, realizando a proteção contra ataques que vão além de ataques de rede, com o **Web Application Firewall** (WAF).

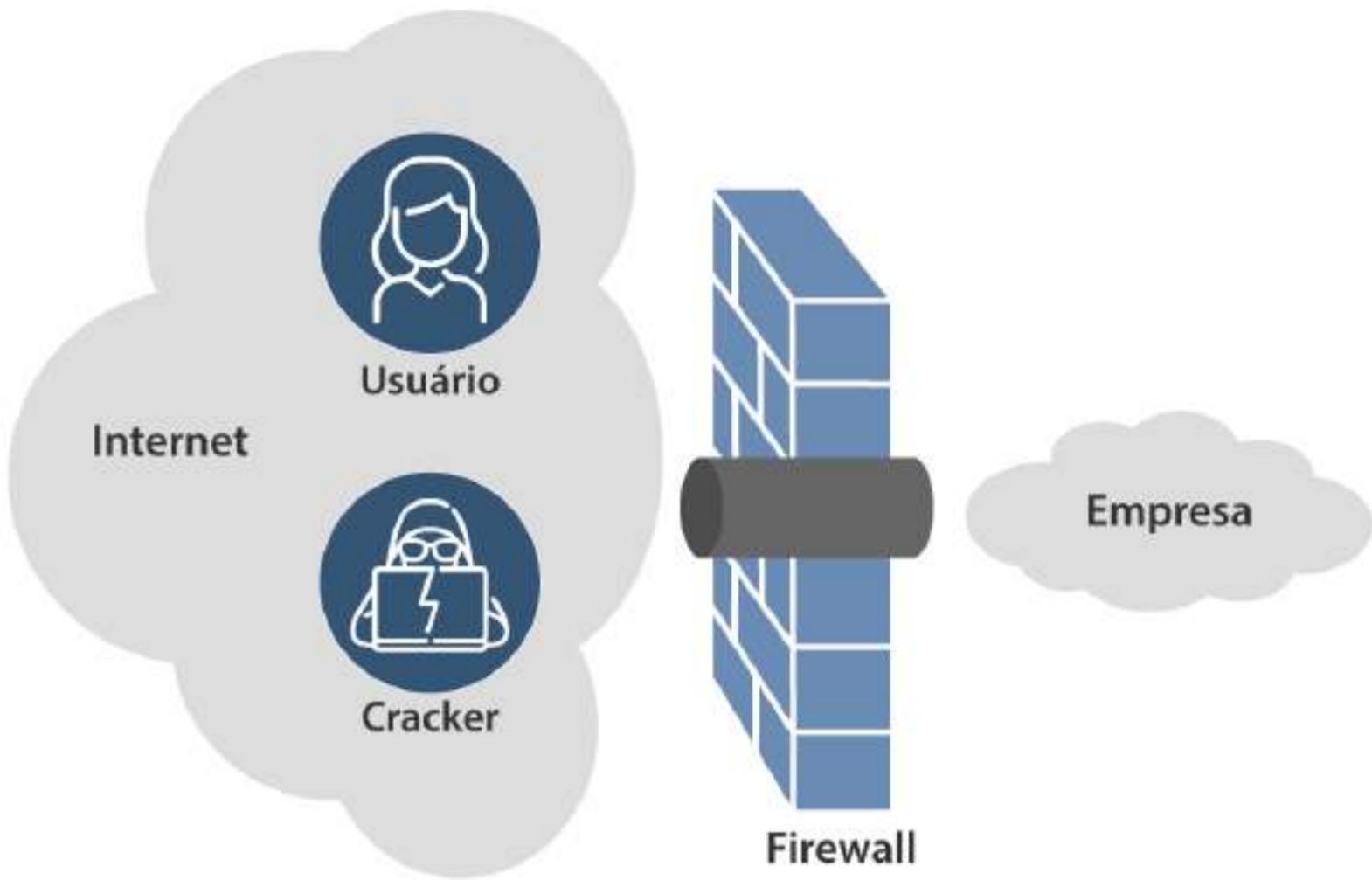
ASSIMILE

Um controle de segurança importante para proteger as aplicações é o *firewall* de aplicação web ou *Web Application Firewall* (WAF). Enquanto um *firewall* faz a filtragem do tráfego de rede baseado nos cabeçalhos dos pacotes, o WAF faz o filtro e monitora o tráfego entre os usuários e a aplicação Web na camada de aplicação HTTP.

Um *firewall* tradicional funciona como um avaliador de pacotes de rede, filtrando as conexões de acordo com os cabeçalhos dos pacotes e as regras definidas. Dessa forma, um dos principais desafios do uso do *firewall* é a sua configuração, composta por regras que consideram, pelo menos, os diferentes segmentos de rede, os serviços disponibilizados pela empresa e os serviços que podem ser acessados pelos usuários internos. A complexidade dessas regras pode fazer com que conexões que não devem passar pelo *firewall* consigam o acesso a recursos.

Na Figura 1.8, o *firewall* é configurado com regras que possibilitam algumas conexões para a empresa e que são utilizadas pelos usuários, mas que também podem ser utilizadas por um cracker para os ataques.

Figura 1.8 | *Firewall* possibilita algumas conexões com as regras



Fonte: elaborada pelo autor.

EXEMPLIFICANDO

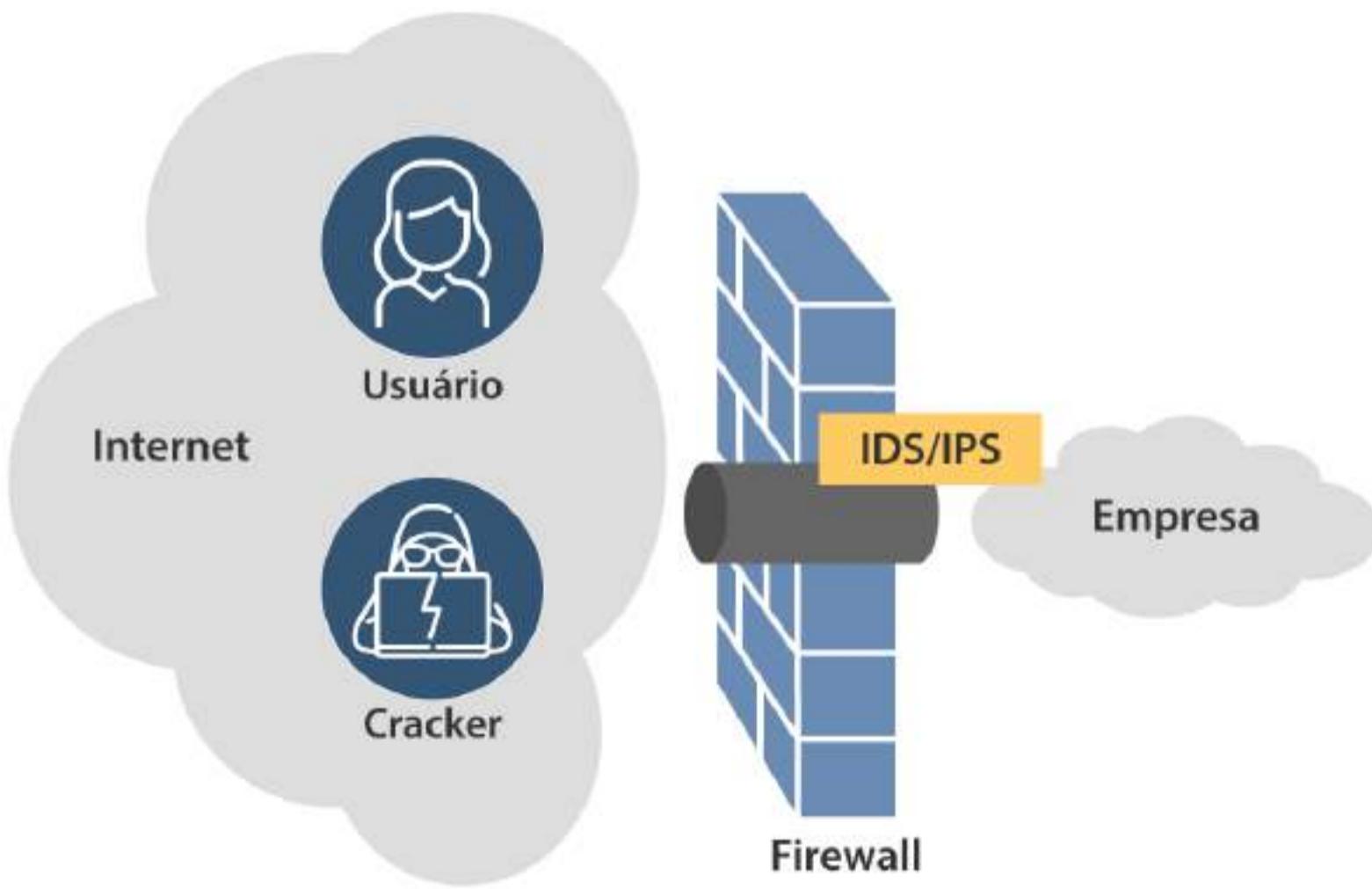
Um exemplo de aplicação é o *Microsoft Terminal Services*, cujo **Remote Desktop Protocol (RDP)** é um serviço disponibilizado pelo *Windows* para acesso remoto. O acesso remoto possibilita que acessos externos sejam feitos a equipamentos que, muitas vezes, estão na rede interna da empresa. Isso facilita atividades como administração remota ou suporte remoto, porém abre uma brecha significativa, que pode ser explorada em ataques. O *firewall* tem que liberar a porta TCP 3389 para que o RDP funcione, e, já que o *firewall* possibilita essas conexões, os ataques passam diretamente pelo *firewall*.

O *scan* de portas é uma técnica que possibilita a identificação de computadores ativos e a coleta de informações sobre os programas instalados e serviços existentes na empresa ou em determinada faixa de endereços IP. O *scan* de portas permite a descoberta de serviços como o RDP.

Assim, é importante que você saiba que a existência de um *firewall* na empresa é uma das principais fontes da falsa sensação de segurança, já que o papel dele é filtrar tudo aquilo que não é permitido. É como se um muro protegesse a sua empresa, mas uma série de portas ou furos existisse nesse muro para permitir as conexões necessárias para a sua empresa. Com isso, ataques aos serviços não podem ser protegidos por um *firewall* tradicional, já que as conexões, inclusive dos ataques direcionados àquele serviço, passam livremente pelo controle, uma vez que as regras permitem.

Reforçando a importância da defesa em camadas, o controle complementar ideal para o *firewall* é o sistema de detecção de intrusão ou ***Intrusion Detection System (IDS)***. Esse controle de segurança analisa diferentes informações, como as conexões, os logs e os fluxos de dados para detectar ataques em andamento, em tempo real (Figura 1.9).

Figura 1.9 | IDS / IPS monitorando as conexões que passam pelo *firewall*



Fonte: elaborada pelo autor.

O **Intrusion Prevention System (IPS)** é uma evolução do IDS, funcionando não somente com a detecção de ataques, mas também tomando ações automáticas de contenção dos ataques em tempo real. Há vários aspectos a serem considerados na tecnologia, como a possibilidade de ataques que visam justamente à paralisação dos acessos aos serviços da empresa com o envio de mensagens que ativam o IPS, que, acreditando haver um ataque em andamento, fecha as conexões e impossibilita o acesso legítimo.

Os avanços tecnológicos continuam e os sistemas de detecção e prevenção de intrusão atuais incorporam técnicas de inteligência artificial para diminuir a quantidade de falsos positivos (alarmes falsos) e falsos negativos (ataques não detectados).

Um ponto importante a considerar é que o contexto da segurança da informação continua a sua evolução com o uso de nuvem (LIMA, 2017) e os perímetros das empresas alterando-se rapidamente, de modo que o ambiente corporativo atual vai além do perímetro físico da empresa e alcança os parceiros de negócios e a residência dos funcionários.

Aliados à transformação digital, aspectos de segurança ganham ainda mais importância; com isso, os controles de segurança são essenciais também nos próprios dispositivos, constituindo, assim, a segurança de ponta ou segurança de *endpoint*. Os próprios *firewall*, IPS e *antimalware* fazem parte do arsenal de defesa dos *endpoints* ou dispositivos, complementando a segurança de redes.

Antimalware busca códigos maliciosos e, basicamente, funciona com a verificação de assinaturas ou códigos que identificam um *malware* já identificado anteriormente e que possui vacina específica. Se, por um lado, os códigos maliciosos podem alterar seu próprio código ou gerar polimorfismo para não serem detectados pelo *antimalware*, do outro lado, o controle de segurança adota, cada vez mais, a inteligência artificial para detectar comportamentos anômalos que podem representar perigo para as empresas.

Dessa forma, os controles de segurança de rede atuam não somente nos pontos de ataque de rede, mas também nos dispositivos dos usuários.

Outro conjunto de controles de segurança visa ao controle de acesso, tanto de usuários quanto de conteúdo. A **autenticação** é um dos principais controles de segurança ao validar a identidade dos usuários, a fim de que possam ter acesso aos recursos. Já vimos que o ataque de força bruta busca a descoberta da senha, que representa um fator de autenticação baseado em alguma coisa que o usuário sabe. Como há outros ataques, como a adivinhação de senhas ou o furto com o uso de *malwares* ou engenharia social, é importante considerar o uso de outros fatores de autenticação. Há possibilidade de usar códigos ou *Tokens* em dispositivos móveis, como os enviados via SMS (alguma coisa que o usuário possui) ou mesmo a biometria (alguma coisa que o usuário é). Quando dois fatores diferentes de autenticação, como a senha e o SMS, são utilizados, a autenticação é de duplo fator ou de múltiplo fator.

o

Ver anotações

REFLITA

Em segurança, é preciso considerar aspectos de usabilidade e o nível de segurança requeridos para cada caso. No caso da autenticação, há três fatores utilizados tradicionalmente para a validação da identidade: algo que o usuário sabe, algo que o usuário possui e algo que o usuário é. Cada método de autenticação possui suas características tecnológicas que se somam aos aspectos de segurança e usabilidade. Por exemplo: o uso de SMS exige que o usuário esteja com a posse do dispositivo móvel no momento do acesso, mas a mensagem nem sempre chega para ele. Já as senhas precisam ser memorizadas, e a repetição de senhas não é recomendada, visto o número de incidentes de segurança envolvendo o vazamento de senhas de acesso de variados serviços, que acabam comprometendo outros. No caso da

biometria, acessos públicos por meio da impressão digital, por exemplo, possuem reflexos na privacidade e em questões de higiene. Assim, cada tipo de acesso deve levar em consideração o nível de risco e os tipos de ataques existentes, bem como os aspectos de segurança e usabilidade envolvidos.

o

Ver anotações

Para finalizar, o **controle de conteúdo** faz parte dos controles de segurança das empresas ao filtrar o acesso a conteúdos impróprios ou que levam à perda de produtividade de seus funcionários.

Normalmente, atuando em conjunto com o *firewall*, o filtro de conteúdo pode ser baseado em endereços web ou em palavras-chave.

Chegamos, assim, ao final desta seção, em que você pôde se aprofundar em aspectos fundamentais para a concepção da melhor estratégia de segurança para a sua empresa. Você viu que diferentes pontos de ataque podem ser explorados pelos agentes de ameaça: da aplicação ao sistema operacional, passando pelo *datacenter*, pela rede e pelos próprios funcionários, entre outros. Você viu, ainda, que há uma série de técnicas de ataques que pode ser utilizada pelos agentes de ameaça e que essas técnicas são variadas, passando de ataques de rede até ataques de aplicação, existindo, ainda, ataques aos próprios controles de segurança, como os ataques que comprometem a autenticação dos usuários. Tudo isso é importante para que você defina os controles de segurança mais condizentes com a sua empresa.

FAÇA VALER A PENA

Questão 1

Você é o analista de segurança de uma grande empresa do setor de energia. Durante uma avaliação de segurança periódica, você avalia os riscos, incluindo as vulnerabilidades. Considere um servidor de arquivos no *datacenter* com documentos confidenciais sobre salários de todos os empregados da empresa.

Os controles de segurança devem ser implementados

- a. Somente no servidor de arquivos, porque não pode haver vulnerabilidades no *datacenter*.
- b. Somente no *datacenter*, porque não pode haver vulnerabilidades no servidor de arquivos.
- c. No servidor de arquivos e no *datacenter*, porque todas as vulnerabilidades devem ser eliminadas.
- d. Somente no servidor de arquivos, porque não pode haver ataques ao *datacenter*.
- e. Somente no *datacenter*, porque não pode haver ataques ao servidor de arquivos.

Questão 2

Um *cracker* pode utilizar uma série de técnicas de ataques em diferentes pontos. Uma dessas técnicas é o DoS, que visa “derrubar” um servidor, impedindo os acessos legítimos, o que compromete a disponibilidade daquela informação.

Assinale a alternativa que corresponde ao caso de ataque de DoS referente ao exposto.

- a. Cracker utilizou o DoS para roubar informações do servidor.
- b. Cracker invadiu um banco de dados utilizando o DoS.
- c. Cracker explorou um ataque de força bruta para “derrubar” o servidor.
- d. Cracker explorou grande número de conexões para paralisar o servidor.
- e. Cracker acessou uma informação invadindo um ponto de ataque do servidor.

Questão 3

Um *malware* bastante crítico é o *ransomware*, em que o criminoso cifra os arquivos ou o disco e exige o pagamento de um resgate em troca da chave criptográfica que decifra as informações originais.

Assinale a alternativa que apresenta o princípio da segurança da informação comprometido pelo *ransomware* e um possível controle de segurança para se lidar com o *malware*.

- a. Disponibilidade e *firewall*.

REFERÊNCIAS

CERT.BR. **Cartilha de Segurança para Internet.** [s.d.]. Disponível em: <https://cartilha.cert.br/malware/>. Acesso em: 1 dez. 2020.

CERT.BR. **Incidentes reportados ao CERT.br -- janeiro a junho de 2020.** 2020. Disponível em: <https://bit.ly/39KCd2a>. Acesso em: 1 dez. 2020.

HOPE, A. **New Zealand stock exchange shut down by DDoS cyber attack.** 2020. Disponível em: <https://bit.ly/2YIFRDk>. Acesso em: 1 dez. 2020.

HOUAISS, A. **Grande dicionário Houaiss da Língua Portuguesa.** 1 ed. Rio de Janeiro: Ed. Objetiva, 2001.

LIMA, A. C. de. **Segurança na computação em nuvem.** São Paulo: Editora Senac, 2017.

MALENKOVICH, S. **O que é um Ataque Man-in-the-Middle?** 2013. Disponível em: <https://bit.ly/2MUb5Vi>. Acesso em: 1 dez. 2020.

NAKAMURA, E. T.; GEUS, P. L de. **Segurança de redes em ambientes cooperativos.** São Paulo: Editora Novatec, 2007.

NOVINSON, J. **The 11 Biggest Ransomware Attacks Of 2020 (So Far).** 2020. Disponível em: <https://bit.ly/3at60vA>. Acesso em: 1 dez. 2020.

OLHAR DIGITAL. **Confira 5 dos maiores ataques DDoS dos últimos anos.** 2020. Disponível em: <https://bit.ly/3jfjiiZ>. Acesso em: 1 dez. 2020.

OLIVEIRA, R. C. Q. **Segurança em redes de computadores.** São Paulo: Editora Senac, 2017.

b. Integridade e firewall.

c. Confidencialidade e firewall.

d. Confidencialidade e backup.

e. Disponibilidade e backup.

SOUZA, R. de. **Relatório aponta aumento no número de ataques DDoS no segundo trimestre de 2020.** 2020. Disponível em:

<https://bit.ly/3rjlboY>. Acesso em: 1 dez. 2020.

THE HACK. **The hack.** 2020. Disponível em: <https://thehack.com.br>.

Acesso em: 1 dez. 2020.

FOCO NO MERCADO DE TRABALHO

SEGURANÇA DE REDES

Emilio Tissato Nakamura

Ver anotações 0

PONTOS DE ATAQUE

Ações de tratamento dos riscos podem ser executadas para que incidentes de segurança sejam evitados.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você, como responsável pela segurança da empresa em que trabalha, deve preparar um relatório que complemente a primeira apresentação realizada para a diretoria executiva e que teve sucesso para chamar a atenção para os riscos de forma mais conceitual.

O seu relatório e sua apresentação devem focar o grande projeto em andamento que já chegou a grandes resultados, com os cientistas tendo descoberto um novo composto que será utilizado na indústria agrícola.

O cenário que você deve considerar é a proteção do projeto que está em execução pelas pessoas, que possuem as ideias, e que essas informações vão de forma digital do *notebook* até o servidor da empresa, passando pela rede.

Comece **elencando os pontos** de ataque que envolvem o fluxo da informação, que começa nas pessoas. O que surge delas passa para o *notebook*, que pode estar em diferentes localidades e em transporte. Do *notebook*, as informações vão para o servidor da empresa, passando pela rede. No *notebook* há, além do *hardware*, aplicações e sistema operacional. No servidor da empresa há, além do *hardware*, aplicações, sistema operacional, banco de dados e *middleware*.

Pense nos **controles de segurança**. Entre o *notebook* e o servidor da empresa há, além da rede, controles de segurança como *firewall* e IPS. No *notebook* podem existir controles de segurança como *antimalware* e *firewall*; no servidor, também podem existir controles de segurança como *firewall* de aplicação (WAF).

Considere as **ameaças e as técnicas de ataques** relacionadas com as ameaças. A ameaça de vazamento do projeto pode se tornar realidade (um incidente de segurança) no caso de um *cracker* (agente de ameaça) realizar um ataque do homem do meio durante a conexão entre o *notebook* do funcionário com o servidor da empresa. Há uma série de outras possibilidades de ataques ligadas à ameaça de vazamento do projeto; uma delas é a contaminação do *notebook* do funcionário por um *malware* ou a descoberta da senha do funcionário. Explore as

possibilidades de ataques que resultam em roubo do projeto e relate os controles de segurança correspondentes. Por exemplo: para o caso do *malware*, o controle de segurança é o *antimalware*.

Avance nas situações de segurança explorando as **ameaças de negação de serviço**, indicando as técnicas de ataque relacionadas, bem como os controles de segurança recomendados.

Pense em ameaças que levam à **perda da integridade do projeto** com alterações de informações e não se esqueça de que há vários pontos de ataques.

Dê uma atenção especial para a autenticação dos usuários, indicando para a diretoria executiva os aspectos relacionados aos fatores de autenticação e os problemas de segurança existentes em cada abordagem.

Ao final da apresentação, a diretoria executiva da empresa estará, ao mesmo tempo, preocupada pelos riscos existentes que podem causar grandes impactos, mas aliviada por ter tido acesso a informações valiosas sobre os riscos. O ponto fundamental é que os riscos representam o futuro, ou seja, são situações que podem ocorrer, tornando-se incidentes de segurança. Com isso, ações de tratamento dos riscos podem ser executadas, de modo a se evitar incidentes de segurança.

AVANÇANDO NA PRÁTICA

SEGURANÇA EM CAMADAS: CONTROLES DE SEGURANÇA, *FIREWALL – IDS, IPS, ANTIMALWARE, ENDPOINT E CORRELAÇÃO DE EVENTOS*

Você, enquanto profissional de segurança, deve ter uma visão sobre como controles de segurança podem ser violados. Isso vem do entendimento de como os controles de segurança funcionam e também das técnicas de ataques. Considere que você também é o dono de uma

loja virtual de materiais preciosos e está usando um *datacenter* próprio com o objetivo de fazer a proteção do servidor que está hospedado nele.

A partir disso, vá construindo a sua estratégia de segurança para proteger o servidor e **apresente a razão de este controle não ser suficiente, indicando, logo a seguir, outro controle de segurança capaz de criar uma camada adicional de segurança.**

Considere os seguintes controles de segurança: *firewall*, IDS, IPS e correlação de eventos, que trata de forma integrada e correlacionada diferentes logs de vários ativos, tais como o *firewall*, os equipamentos de rede como roteador, servidor de aplicação ou *middleware*, além da aplicação e das autenticações.

Caso queira ir adiante, você pode considerar, ainda, a autenticação duplo fator dos clientes de sua loja e o *firewall* de aplicação.

RESOLUÇÃO



Pense sempre nos pontos de ataque. No caso da loja virtual, você não possui controle sobre os dispositivos de seus clientes ou os *endpoints*; logo, o que resta a você é partir para a arquitetura de rede segura, que começa com a segmentação de rede. O servidor deve estar em uma DMZ para proteger a sua rede interna, que deve estar isolada; a segmentação e o controle de acesso de rede podem ser feitos pelo *firewall*, que bloqueia tentativas de ataques a portas filtradas. Porém, em portas liberadas pelo *firewall*, necessárias para que os clientes cheguem ao servidor, ataques podem ocorrer. O controle adicional sugerido é o IDS, que faz a detecção de ataques. Para que as detecções reflitam ações como o encerramento das conexões dos ataques, um IPS deve ser utilizado. O problema do IPS é que ele atua na rede, e ataques com construções de pacotes de rede, que são mais difíceis de serem detectados, podem ser feitos contra a sua empresa. Nesse caso, a correlação de eventos, que considera logs de ativos como o servidor de aplicação ou

middleware, além da aplicação e das autenticações, pode ser correlacionada às informações da camada de rede, resultando em detecções mais assertivas.

Você pode, ainda, explorar novas tecnologias de detecção que utilizam técnicas de inteligência artificial e detectam situações como desvios de padrão.

NÃO PODE FALTAR

CRIPTOGRAFIA

Emilio Tissato Nakamura

0
Ver anotações

HISTÓRIA DA CRIPTOGRAFIA

Conhecer a história da criptografia, sua constante evolução e as nuances que existem nos algoritmos vai ajudá-lo na definição de controles de segurança para a proteção da informação, incluindo dados pessoais.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

PRATICAR PARA APRENDER

Nesta seção, vamos entrar no mundo da criptografia, um assunto que faz mais parte da sua vida do que você imagina. As informações de seu dispositivo móvel estão protegidas por criptografia, bem como as do seu notebook. Sua comunicação com familiares e amigos também está protegida com a criptografia, de modo que as escutas não levarão ao conteúdo.

Aliás, você sabia que a criptografia não visa esconder a mensagem ou a informação, mas, sim, torná-la sem valor, mesmo sendo interceptada? Mas há uma tecnologia que visa esconder a mensagem ou a informação: a **esteganografia**. Com ela, você pode estar olhando para uma foto, mas ela pode trazer informações codificadas escondidas.

Há diferentes tipos de criptografia. Se no início a criptografia foi criada para proteger as mensagens, a evolução levou a novas possibilidades, como a de verificar a integridade da informação ou a de garantir a autenticidade da origem. Com isso, você deve pensar na criptografia como um conjunto de controles de segurança que vai além da proteção da confidencialidade. E a evolução da criptografia levou às criptomoedas e continua evoluindo. Pense na computação quântica. O que será da criptografia com o poder computacional que facilita ataques de força bruta? Há estudos em criptografia pós-quântica que visam proteger a informação no mundo da computação quântica. Assim, a evolução continua incluindo ainda a computação leve, destinada a dispositivos de Internet das Coisas, ou *Internet of Things* (IoT), que apresentam limitações que comprometem o uso da criptografia.

Você é o responsável pela segurança da informação de uma empresa do setor químico, a qual conta com os maiores cientistas brasileiros. A empresa tem unidades em São Paulo, Rio de Janeiro e Salvador. Além disso, tem cooperação internacional com uma empresa chinesa e outra suíça. A empresa tem grandes investidores financiando seus projetos.

A sua atividade será focada em um grande projeto em andamento que já chegou a grandes resultados, com os cientistas tendo descoberto um novo composto que será utilizado na indústria agrícola. Você está preocupado com a forma como os resultados do desenvolvimento estão sendo protegidos. O impacto pode ser gigantesco em caso de incidentes de segurança, principalmente com a concorrência também mobilizando grandes equipes para colocar no mercado os avanços para o setor.

Prepare uma **apresentação** para a diretoria executiva da empresa com uma **estratégia de segurança** que considera as seguintes situações:

- A documentação com os resultados do projeto é armazenada no servidor de arquivos, que está na nuvem.
- O desenvolvimento do projeto é colaborativo, na própria nuvem, entre brasileiros, chineses e suíços.
- Alguns cientistas gravam o documento em seus equipamentos para trabalharem no fim de semana na fazenda, onde há limitações de conectividade.
- Outros cientistas gravam os documentos em *pendrives* para *backup*.
- Quando um cientista vai de Salvador para Pequim, ele leva a documentação em seu *notebook* e também em um *pendrive*.
- Resultados intermediários são discutidos entre São Paulo, Rio de Janeiro e Salvador, e, às vezes, com os parceiros chineses e suíços, com troca de documentos anexados em e-mails e uso de serviço de troca de arquivos como o *Dropbox*.

Na apresentação, faça uma **correlação dos controles de segurança propostos com a ameaça correspondente**, como o vazamento do projeto, a invasão seguida de alteração dos resultados e a inserção de documentos fraudulentos nos arquivos do projeto.

Não esqueça de inserir em sua apresentação uma explicação breve para a diretoria executiva sobre os **algoritmos criptográficos propostos para cada caso**.

Conhecer a história da criptografia, a sua constante evolução e as nuances que existem nos algoritmos vai ajudá-lo na definição de controles de segurança para a proteção da informação, incluindo dados pessoais. Como profissional de segurança, é preciso conhecer e entender as possibilidades da criptografia para que a sua estratégia de segurança tenha ainda mais sucesso.

Ver anotações

CONCEITO-CHAVE

Em 2016, o *Federal Bureau of Investigation* (FBI) dos Estados Unidos tentou de tudo, sem sucesso, para ter acesso às informações de um dispositivo móvel do principal suspeito de um tiroteio que vitimou 14 pessoas em dezembro de 2015 em San Bernardino (KAHNEY, 2019). Esta história mostra o poder de um dos principais controles de segurança: a criptografia. Este caso ilustra também que a segurança em camadas é fundamental, já que a criptografia foi utilizada em conjunto com outros controles de segurança, como a autenticação, para proteger os dados do legítimo dono.

Da origem para ocultar o significado de uma mensagem até o uso em aplicações como *WhatsApp* e acesso a *websites*, passando pelo uso em guerras e por agentes secretos, a criptografia evoluiu de uma arte para uma ciência e, atualmente, faz parte de nossas vidas, incluindo os objetivos de autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicas, além de dinheiro digital (NAKAMURA, 2016).

REFLITA

A criptografia surgiu para proteger as mensagens há séculos, envolvendo histórias de amor, guerras e traições. Atualmente ela é considerada um controle de segurança da informação, junto de uma série de outros controles que surgiram no mundo digital. Será que existe um controle de segurança tão amplo no seu uso, tão antigo e que seja de conhecimento da grande maioria das pessoas?

A criptografia deriva de duas palavras gregas: *kryptos*, que significa oculto, e *graphien*, que significa escrever. O Dicionário Oxford define criptografia como a arte de escrever ou resolver códigos. Estas definições podem ser consideradas um reflexo do seu objetivo original, que era ocultar o significado das mensagens. Note que o objetivo não é esconder a existência da mensagem, de modo que ela pode cair nas mãos de um intruso, mas fazer com que essa pessoa não consiga compreendê-la. Com a criptografia, apenas o remetente e o destinatário, em princípio, com um acordo preestabelecido (as chaves), têm acesso ao significado da mensagem (NAKAMURA, 2016).

ASSIMILE

O termo criptografia é usado muitas vezes como sinônimo de criptologia, abrangendo assim a criptanálise, que tem por função descobrir os segredos, ou quebrar a confidencialidade entre emissor e receptor (FIARRESGA, 2010).

Com o advento científico, em especial da matemática, a criptografia também evoluiu. Uma definição mais recente do termo se refere ao estudo de técnicas matemáticas relacionadas a aspectos da segurança da informação, tais como confidencialidade, integridade, autenticação de entidade e autenticação de origem de dados (MENEZES; OORSCHOT; VANSTONE 2001). As aplicações atuais da criptografia incluem os seguintes objetivos (KATZ; LINDELL, 2007; FIARRESGA, 2010):

- **Sigilo:** proteção dos dados contra divulgação não autorizada.
- **Autenticação:** garantia que a entidade se comunicando é aquela que ela afirma ser.
- **Integridade:** garantia que os dados recebidos estão exatamente como foram enviados por uma entidade autorizada.
- **Não repúdio:** garantia que não se pode negar a autoria de uma mensagem.

- **Anonimato:** garantia de não rastreabilidade de origem de uma mensagem.

REFLITA

A criptografia é apresentada em cursos de segurança da informação, de ciência da computação, mas também de matemática. Você sabia que os grandes inventores dos algoritmos criptográficos são matemáticos? E que a matemática possibilita a proteção da confidencialidade, além de permitir que você autentique entidades, verifique se uma informação foi modificada, garanta que quem enviou uma mensagem só pode ser a própria pessoa e ainda possibilita o anonimato? Sobre esse último ponto, veja o *bitcoin*, que utiliza vários conceitos criptográficos para transações anônimas.

0

Ver anotações

| CRIPTOGRAFIA AO LONGO DA HISTÓRIA

A criptografia é um dos principais controles de segurança da informação e tem uma história fascinante, que envolve o seu uso inicial por governos, militares e acadêmicos. Esta história tem início no Egito, em 1900 a.C., com o uso de hieróglifos, os quais têm origem grega e significado de inscrição sagrada. Um dos modelos de hieróglifos eram estruturados na forma de pictogramas, que consiste em um conjunto de imagens de objetos, pessoas ou animais que funcionavam como uma palavra. A Figura 1.10 ilustra um exemplo de hieróglifos egípcios.

Figura 1.10 | Hieróglifos egípcios



Fonte: Pixabay.

CIFRA DE CÉSAR

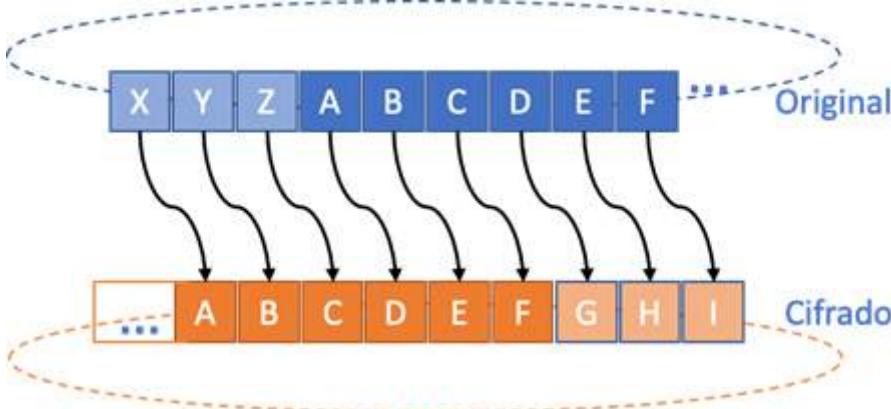
Entre 600 a.C. e 500 a.C. surgiu a Cifra de César criada por Júlio César. Ela consiste na substituição simples de letras do alfabeto por letras avançando algumas letras na sequência, e uso de 25 combinações possíveis com o objetivo de parecer sem significado ao ser interceptada. Essa sigla foi utilizada por vários militares ao longo dos anos.

Vamos exemplificar a Cifra de César: imagine que você deseja enviar a mensagem “INTERNET” com uma chave 3, e para isso foi gerada uma mensagem cifrada “L Q W H U Q H W”.

Para decifrarmos a mensagem e chegarmos à mensagem original, fazemos o processo inverso, retornando 3 letras. Assim, “L” se torna “I”, “Q” se torna “N”, “W” se torna “T, e assim por diante, formando a mensagem original “I N T E R N E T”.

Observe a Figura 1.11 com as possíveis substituições para o alfabeto considerando chave 3.

Figura 1.11 | Cifra de César e as substituições feitas com uma chave 3



Fonte: elaborada pelo autor.

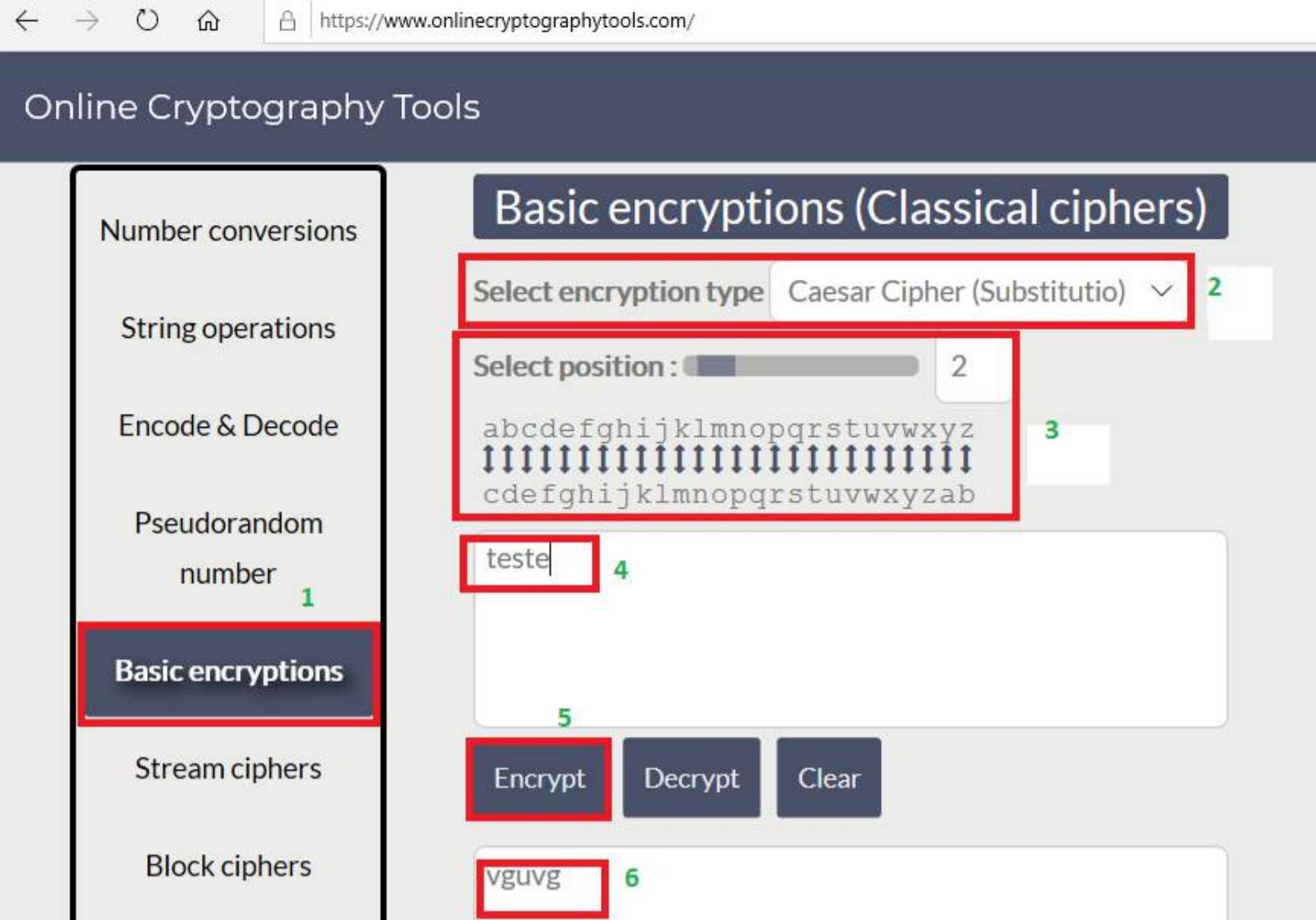
PESQUISE MAIS

Você pode testar alguns algoritmos de criptografia em uma ferramenta online chamada **Online Cryptography Tools**, disponível em: <https://www.onlinecryptographytols.com>. Acesso em: 2 nov. 2020.

Essa ferramenta contém exemplos de cifras simples, como a cifra de César, a criptografia de chave simétrica e *hash*.

A ferramenta contém exemplos decifras simples, como a cifra de César, a criptografia de chave simétrica e *hash*. Observe a Figura 1.12, em que temos um exemplo de aplicação da Cifra de César. Vamos utilizar como senha a palavra “teste” e substituir cada letra da palavra avançando duas letras no alfabeto. Por exemplo, a letra “t” vamos substituir por “v”, a letra “e” será alterada para letra “g” e a letra “s” pela letra “u”. Para testar o exemplo, siga os passos enumerados na imagem:

Figura 1.12 | Cifra de César e as substituições feitas com uma chave 3 na palavra teste



Fonte: elaborada pelo autor.

Passo 1: Ao acessar o site, vá em Basic encryptions.

Passo 2: Em “Select encryption type”, selecione a Caesar Cipher (Cifra de César).

Passo 3: Em “Select Position”, selecione o número de posições que será avançado no alfabeto para a substituição das letras. No caso, foi selecionado 2. Observe que a letra “a” será trocada por “c”, “b” por “d”, conforme podemos visualizar no passo 3.

Passo 4: Incluímos a palavra “teste”.

Passo 5: Ao clicar em “Encrypt”, a palavra será criptografada.

Passo 6: É gerada a palavra correspondente “vguvvg”.

Teste outros exemplos e selecione mais posições a serem avançadas no alfabeto.

A partir daí, a criptografia continua evoluindo, como mostra o advento da criptografia pós-quântica e das criptomoedas e *blockchain* hoje (MARTIN, 2019; PRADO, 2017).

Desde 2015, um padrão para a criptografia pós-quântica tem sido estudado. O objetivo é proteger as informações quando o ataque teórico ao RSA se tornar prática com a computação quântica. A criptografia quântica é diferente da criptografia pós-quântica e é também conhecida como comunicação quântica ou segurança quântica. Ela provê uma solução teórica para a distribuição de chaves, com a *Quantum Key Distribution* (QKD) (RICE, 2020).

| CRIPTOGRAFIA E SUAS TÉCNICAS

| ESTEGANOGRÁFIA

A esteganografia tem origem nos termos gregos *steganos*, que significa “coberta, escondida ou protegida”, com *graphein*, que significa “escrita”. É o uso de técnicas para ocultar informações ou mensagens dentro de outra fonte (mensagem). A diferença entre a criptografia e esteganografia é que a criptografia oculta o significado da mensagem, enquanto a esteganografia oculta a existência da mensagem (SIMON, 1999). Além disso, os esquemas de codificação da esteganografia dependem de segredos como dicionários que decodificam as informações. E, uma vez revelado o dicionário, o sistema de codificação é permanentemente comprometido. Com isso, o risco de exposição aumenta conforme aumenta o número de usuários que conhecem o segredo.

EXEMPLIFICANDO

Você pode testar a esteganografia com a ferramenta **Steghide**, disponível em: <https://steghide.sourceforge.net>.

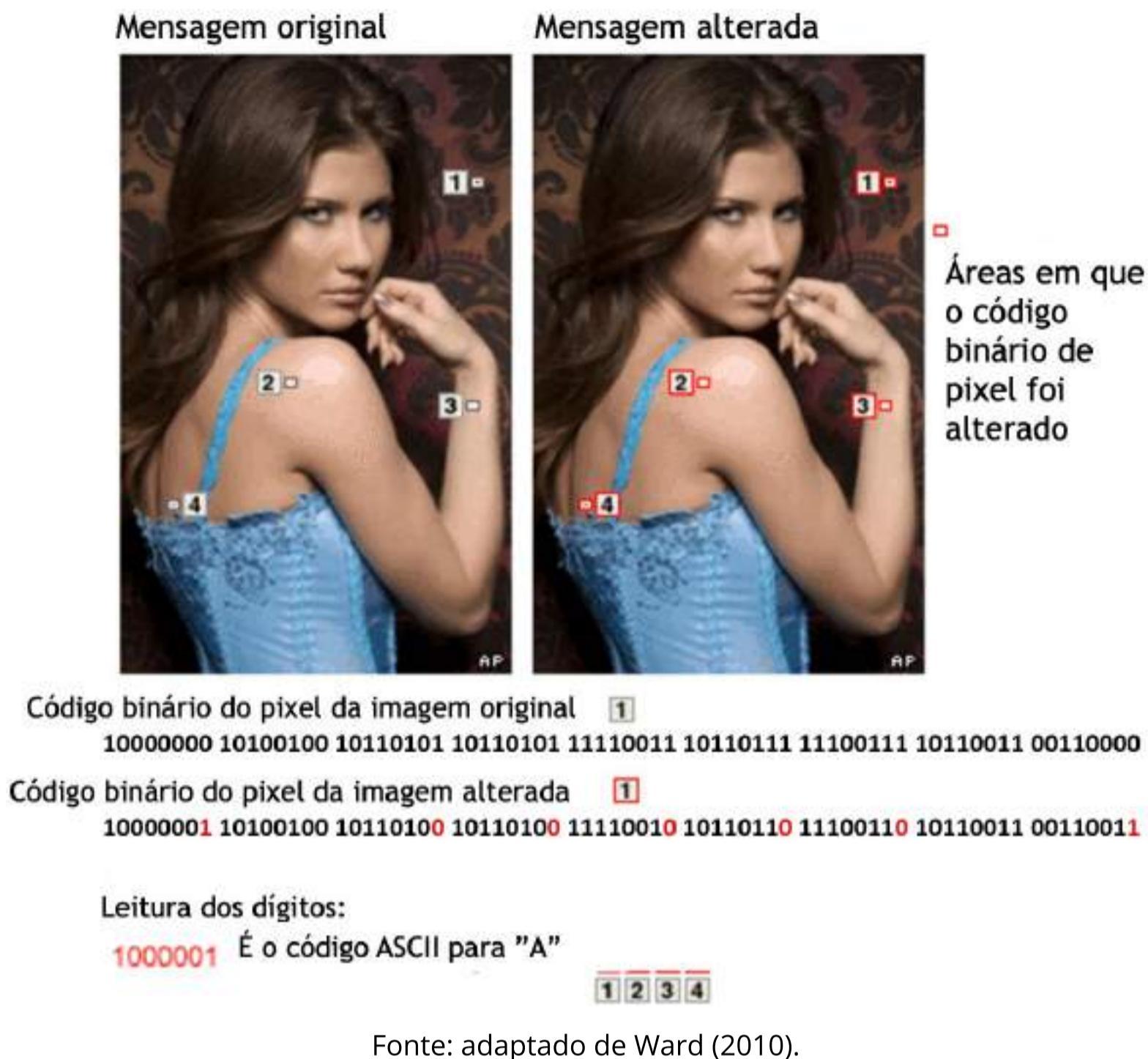
Acesso em: 2 nov. 2020. A ferramenta possibilita a inserção de dados em arquivos de imagem e de áudio.

Outra ferramenta é a **OpenPuff**, disponível em:
<https://bit.ly/2MTGMy1>. Acesso em: 13 nov. 2020.

De acordo com Nakamura (2016), alguns exemplos de uso da esteganografia são:

- Uso de tintas invisíveis.
- Mensagens escondidas no corpo do mensageiro, como na cabeça raspada, que era depois escondida após o crescimento dos cabelos.
- Código Morse costurado na roupa do mensageiro.
- Mensagens escritas nos envelopes nas áreas dos selos.
- Inserção de mensagens nos *bits* menos significativos de áudios ou imagens (Figura 1.13).
- Inserção de mensagens em seções de arquivos.
- Uso de caracteres Unicode que se parecem com conjunto de caracteres ASCII padrão.

Figura 1.13 | Exemplo de esteganografia



REFLITA

Você sabia que vários hackers estão utilizando a técnica de esteganografia para esconder códigos maliciosos, como vírus em arquivos de imagens e áudios? Muitos desses arquivos são os famosos “memes”. Portanto, fique atento ao receber uma imagem. Existem vários casos da inclusão de códigos maliciosos em imagens e áudios. Mas como se proteger desse tipo de ameaça?

| CRIPTOGRAFIA DE CHAVE PRIVADA OU SIMÉTRICA

A função mais conhecida da criptografia é proteger a confidencialidade ou o sigilo da informação, fazendo com que a informação chegue ao seu destino sem que qualquer pessoa não autorizada tenha acesso ao seu conteúdo. Nakamura (2016) apresenta o exemplo de Alice e Beto, que

trocaram mensagens por um canal, normalmente inseguro, tornando possível que um atacante escute a mensagem, afetando assim a privacidade e a confidencialidade da comunicação.

0

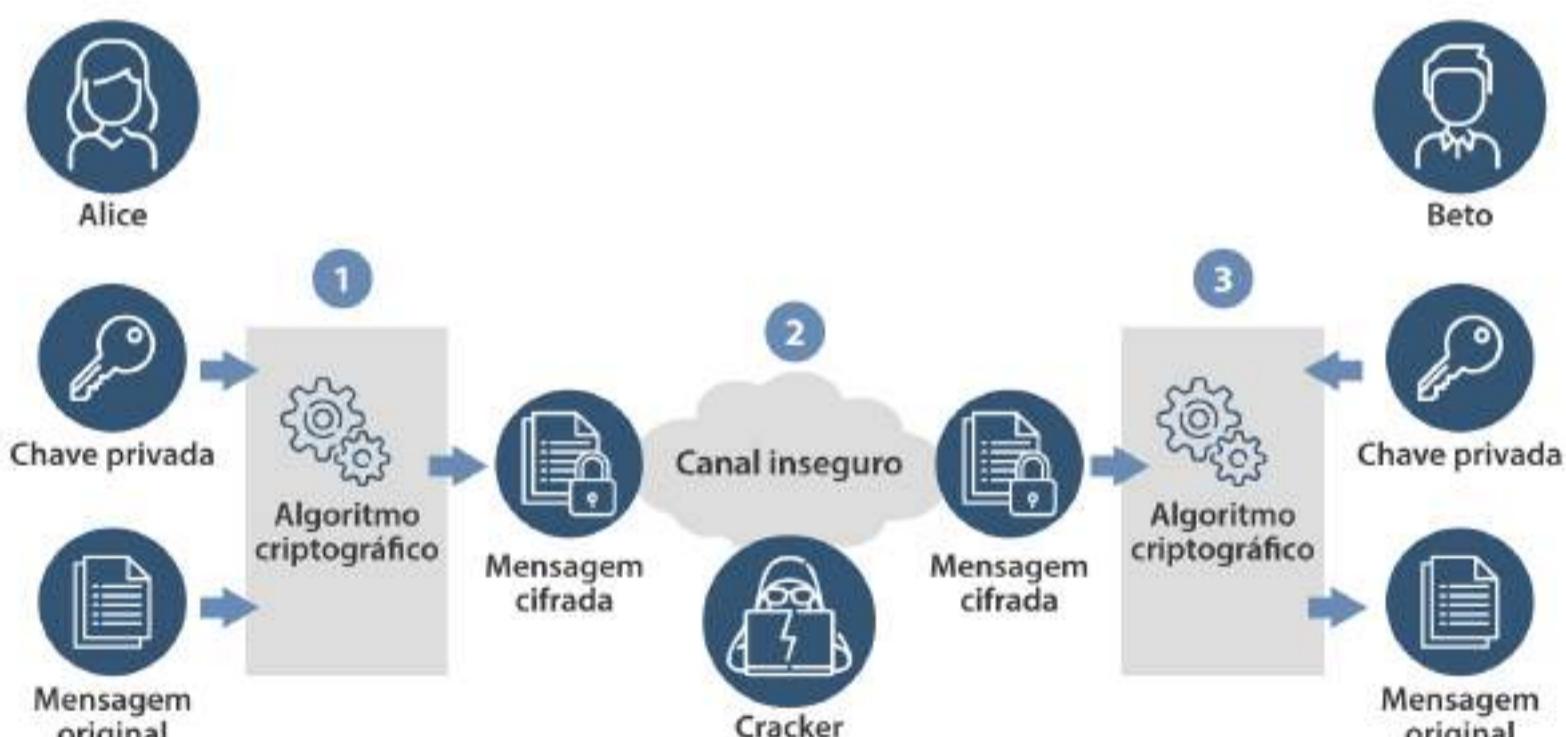
REFLITA

Na criptografia de chave privada ou simétrica, a chave criptográfica é a mesma para cifrar e decifrar a informação. Ela também precisa ser compartilhada entre o remetente e o destinatário. Como você faz para trocar esta chave privada com o seu interlocutor? Você utiliza o mesmo canal inseguro pelo qual vai enviar a mensagem cifrada ou usa um canal alternativo?

Ver anotações

A Figura 1.14 mostra a comunicação entre Alice e Beto com o uso da criptografia. Alice utiliza um algoritmo criptográfico e uma chave secreta privada para cifrar a mensagem original. O resultado é um texto incomprensível para o atacante. Beto recebe a mensagem cifrada e utiliza a mesma chave secreta (compartilhada com Alice) ou simétrica para decifrar a mensagem e retornar ao conteúdo original.

Figura 1.14 | Alice e Beto utilizam criptografia para a troca de mensagem



- 1 Alice utiliza a chave privada para cifrar a mensagem original, gerando a mensagem cifrada.
- 2 A mensagem cifrada passa pelo canal inseguro, infestada por crackers.
- 3 Beto recebe a mensagem cifrada e utiliza a chave privada para abrir a mensagem, recuperando a mensagem original.

Os processos de cifragem e decifragem são realizados via uso de algoritmos com funções matemáticas que transformam os textos claros, que podem ser lidos, em textos cifrados, que são inteligíveis, e vice-versa.

Estes algoritmos podem ser baseados em cifras de fluxo, em que a cifragem é feita a cada dígito (byte), ou em cifras de blocos, em que um conjunto de *bits* da mensagem é agrupado em blocos, que então são cifrados (NAKAMURA, 2016).

EXEMPLIFICANDO

O algoritmo padrão de criptografia de chave privada ou simétrica é o *Advanced Encryption Standard* (AES), também conhecido por Rijndael, que é uma cifra e blocos de 128 bits. O AES substituiu o *Data Encryption Standard* (DES), que teve sua efetividade invalidada em 1997, quando uma mensagem cifrada com o algoritmo foi quebrada pela primeira vez. Em 1998, um equipamento com custo de US\$ 250 mil quebrou uma chave de 56 bits em aproximadamente 2 dias, mostrando a redução dos custos de equipamentos para os ataques de força bruta, assim como do tempo para a quebra (NOMIYA, 2010).

KEY ESCROW

O acesso a informações protegidas por criptografia é uma discussão grande, que reflete em aspectos de privacidade e de segurança nacional. Apesar de polêmica, há mecanismos para que o acesso seja possível. Um desses mecanismos é a **custódia de chaves ou caução de chaves**, ou *key escrow*, que faz com que cópias de chaves criptográficas existam para o acesso a informações cifradas no caso de ordens judiciais, por exemplo. Com este mecanismo, o sistema criptográfico cria

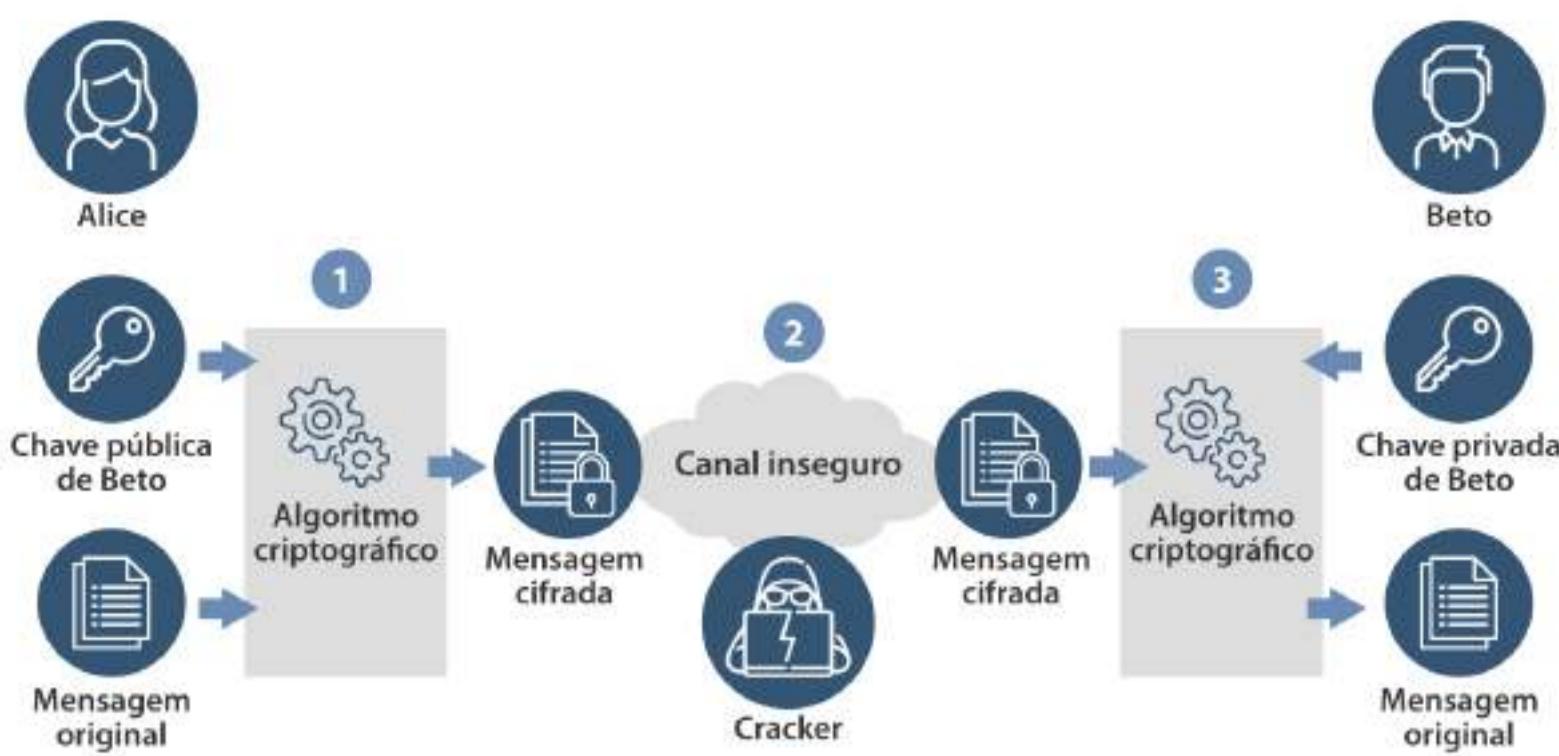
múltiplas chaves que dão acesso às informações. A justiça, neste caso, seria um custo diante de uma das múltiplas chaves, e teria uma cópia das chaves para acessar as informações em caso de necessidade (NAKAMURA, 2016).

CRIPTOGRAFIA DE CHAVE PÚBLICA OU ASSIMÉTRICA

Uma característica que você precisa saber sobre a criptografia de chave privada ou simétrica é que ela apresenta o desafio da troca de chaves (GOYA, 2006; NAKAMURA; GEUS, 2007), porém é rápida de ser executada, em termos de processamento computacional. Já a criptografia de chave pública ou assimétrica é computacionalmente mais pesada, porém é adequada para ser utilizada na troca de chaves.

A criptografia de chave pública ou assimétrica utiliza um par de chaves (pública e privada) que são utilizado em conjunto para a cifragem (com a chave pública) e decifragem (com a chave privada). Na Figura 1.15, Alice cifra a mensagem utilizando a chave pública de Beto, que pode ser compartilhada. Para abrir a mensagem, somente a chave equivalente é utilizada, que é a chave privada de Beto, que não é compartilhada e fica sempre de posse do dono.

Figura 1.15 | Alice e Beto utilizam criptografia de chave pública para a troca de mensagem



- 1 Alice utiliza a chave pública de Beto para cifrar a mensagem original, gerando a mensagem cifrada.
- 2 A mensagem cifrada passa pelo canal inseguro, infestada por crackers.
- 3 Beto recebe a mensagem cifrada e utiliza a chave privada para abrir a mensagem, recuperando a mensagem original.

Fonte: Nakamura (2016).

EXEMPLIFICANDO

O RSA, publicado em 1978 por Ron Rivest, Adi Shamir e Leonard Adleman, é composto pela geração de chaves pública e privada, cifragem e decifragem. O algoritmo faz uso da exponenciação modular do produto de dois números primos muito grandes, para cifragem e decifragem, além da assinatura digital. A quebra da chave privada, que é utilizada na decifragem, é considerada improvável, já que não há algoritmos eficientes para realizar a operação matemática envolvida, que no caso é a fatoração de inteiros em fatores primos, principalmente quando o número de algarismos é 100 ou maior. O tempo de cifragem de uma mensagem é desprezível, porém o tempo de decifragem pode tornar o processo inviável (SILVA, 2006).

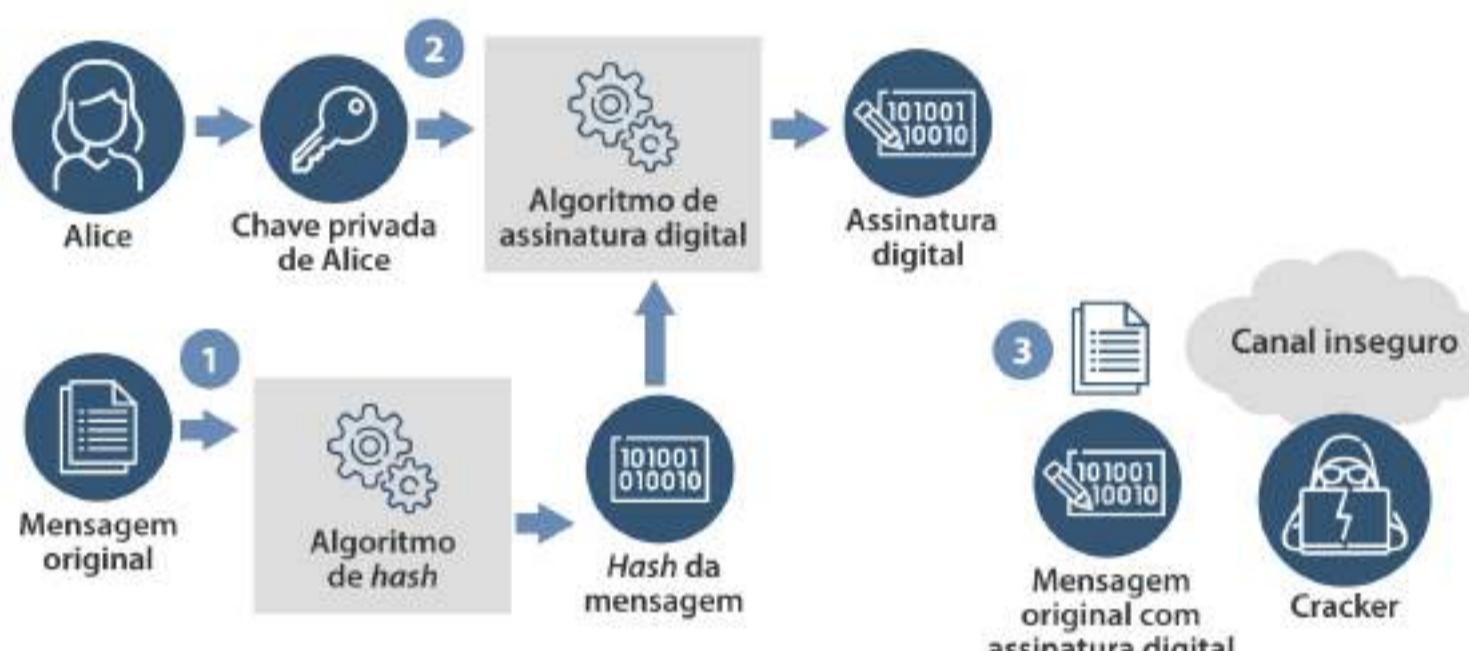
ASSINATURA DIGITAL

O par de chaves pública e privada de cada entidade é utilizado na criptografia de chave pública ou assimétrica. Para cifrar uma mensagem, é utilizada a chave pública do destinatário, enquanto a decifragem é

realizada com o uso da chave privada correspondente. Além da cifragem, a criptografia de chave pública pode ser utilizada para validar a origem de uma mensagem.

A Figura 1.16 ilustra Alice assinando digitalmente uma mensagem. Neste processo, Alice utiliza sua chave privada para “cifrar” o *hash* da mensagem. O *hash* é o resultado de um cálculo matemático em uma via, ou seja, não é possível a sua reversão, ou seja, não é possível chegar à mensagem original a partir de um *hash*.

Figura 1.16 | Alice assina digitalmente uma mensagem



- 1 Um *hash* da mensagem original é gerado.
- 2 Alice utiliza a sua chave privada para assinar digitalmente o *hash* da mensagem original.
- 3 A assinatura digital é enviada para Beto, junto com a mensagem original.

Fonte: Nakamura (2016).

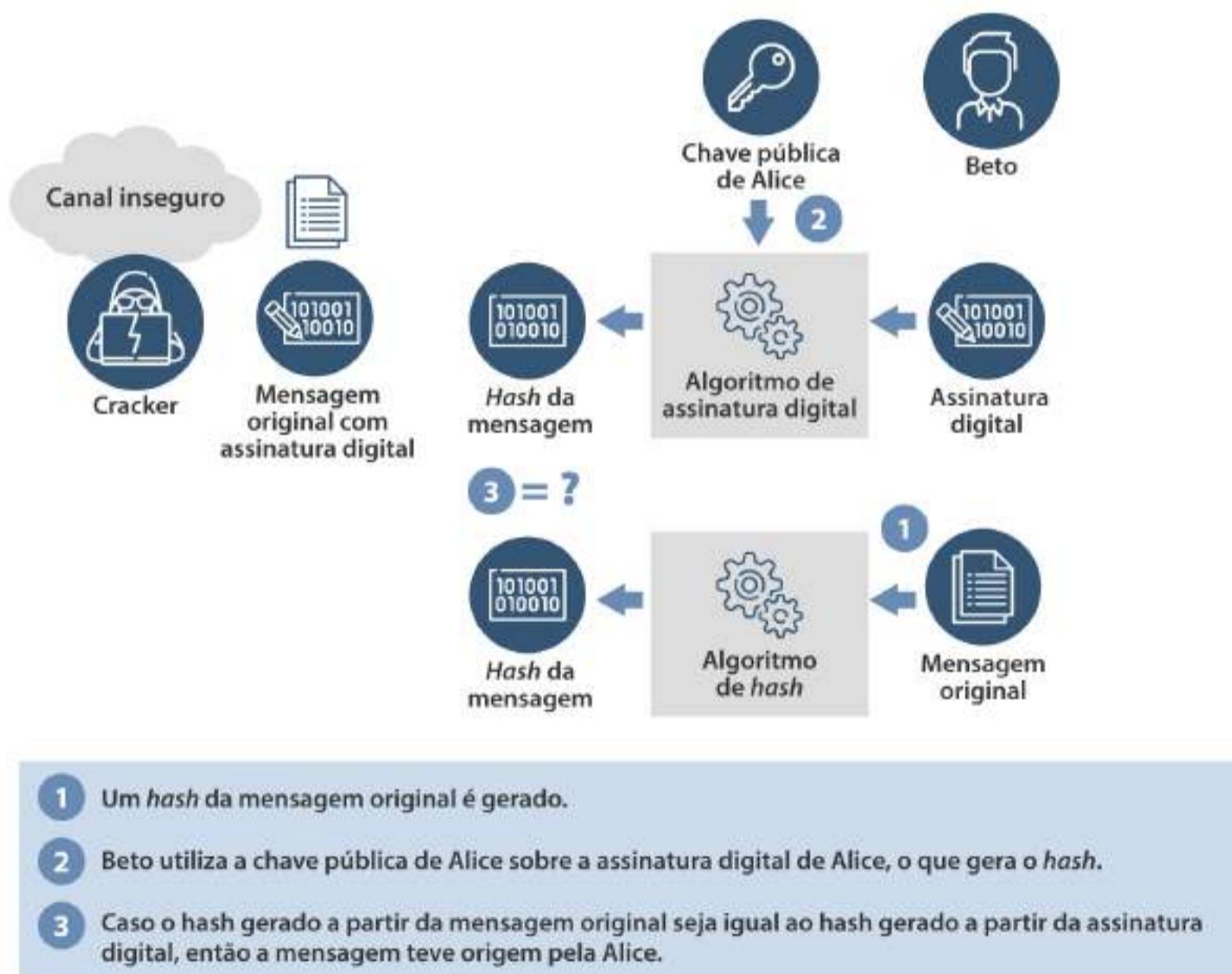
EXEMPLIFICANDO

Funções de *hash* são utilizadas para a verificação da integridade. Estes algoritmos realizam um cálculo matemático nas mensagens ou nos documentos. O receptor recebe a mensagem juntamente com o *hash* e utiliza o mesmo algoritmo para calcular o *hash* da mensagem recebida. O *hash* recebido e o *hash* calculado devem ser comparados, e devem ser iguais, o que garante a integridade da mensagem ou do documento. Alguns exemplos de funções de *hash* são o MD5 e a família SHA (SHA-1, SHA-256 e

SHA-512). É importante ressaltar que o MD5 e o SHA-1 não devem mais ser utilizados na prática, pois são suscetíveis a ataques de colisão. Neste ataque, mensagens diferentes podem gerar o mesmo *hash*, impossibilitando a validação da integridade.

Beto recebe e “decifra” o *hash* da mensagem utilizando a chave pública correspondente, de Alice. Na Figura 1.17, Beto ainda calcula o *hash* da mensagem, o compara com o *hash* decifrado vindo de Alice. Os dois *hashes* devem ser idênticos, o que comprova que foi mesmo Alice quem assinou digitalmente a mensagem, já que somente ela possui a chave privada.

Figura 1.17 | Beto verifica a assinatura digital de Alice



Fonte: Nakamura (2016).

REFLITA

E se algum impostor se passar por Alice, divulgando uma chave pública como se fosse ela? Este é o cenário para o certificado digital e a autoridade certificadora, que têm a

função de publicar os certificados digitais, que são as chaves públicas com alguns atributos adicionais. Além disso, a autoridade certificadora valida os certificados digitais, estabelecendo uma relação de confiança.

TROCA DE CHAVES CRIPTOGRÁFICAS

Você já viu que a criptografia de chave privada é rápida, mas há o desafio da troca de chaves. E a criptografia de chave pública é mais lenta, com a vantagem de não ser preciso trocar chaves. Desta forma, usar criptografia de chave pública em toda comunicação pode não ser muito eficiente. Então, por que não utilizar a criptografia de chave pública para a troca da chave privada da criptografia simétrica, que seria utilizada na comunicação?

Além do desafio da troca de chaves, é fundamental o seu gerenciamento, envolvendo parâmetros como o tempo de validade, armazenamento, geração, uso e substituição. O uso em conjunto da criptografia de chave pública e a de chave privada é tradicionalmente utilizado para a criação de um canal seguro, que por sua vez pode ser utilizado para a troca de chaves privadas.

Um exemplo é o *Secure Sockets Layer* (SSL), utilizado para proteger comunicações *Web*, que implementa em conjunto mecanismos de gerenciamento de chaves criptográficas.

Outro exemplo é o Diffie-Hellman, criado em 1976 por Whitfield Diffie e Martin Hellman e utilizado até hoje. Ele foi o primeiro método criptográfico para troca de chaves, que permite que duas entidades que não possuem conhecimento prévio uma da outra possam compartilhar uma chave secreta mesmo com o uso de um canal inseguro.

Matematicamente, o Diffie-Hellman utiliza o cálculo de logaritmos discretos em um campo infinito para gerar e estabelecer uma chave secreta compartilhada, a partir de uma informação prévia comum que

não é crítica no caso de ser comprometida. Assim, com o Diffie-Hellman, uma chave secreta compartilhada é gerada pelas entidades, sem que sejam transmitidas em um canal de comunicação (NAKAMURA, 2016).

SEGURANÇA DOS SISTEMAS CRIPTOGRÁFICOS

Você sabia que a segurança de um sistema criptográfico está no tamanho das chaves, e não no algoritmo criptográfico? Os algoritmos criptográficos mais utilizados são públicos, tendo sido avaliados por toda a comunidade científica. Porém, a segurança não pode ser medida somente pelo tamanho da chave utilizada, sendo necessário conhecer o algoritmo e a matemática envolvida no processo de codificação de dados.

Um atacante pode fazer o ataque explorando o algoritmo ou tentando descobrir a chave secreta. Deste modo, um algoritmo que utiliza chaves de 256 bits não significa que seja necessariamente mais seguro do que outros algoritmos, como o DES de 128 bits, caso existam falhas no algoritmo ou em sua implementação. A segurança de sistemas criptográficos depende de uma série de fatores, tais como (NAKAMURA; GEUS, 2007):

- **Geração de chaves:** sem uma geração aleatória de chaves, o algoritmo utilizado pode revelar padrões que diminuem o espaço de escolha das chaves, o que facilita a sua descoberta.
- **Mecanismo de troca de chaves:** as chaves precisam ser distribuídas e trocadas para o estabelecimento das comunicações seguras, e, para tanto, protocolos como o Diffie-Hellman são utilizados.
- **Taxa de troca das chaves:** quanto maior a frequência de troca automática das chaves, maior será a segurança, pois isso diminui a janela de oportunidade de ataques, pois, caso uma chave seja quebrada, em pouco tempo ela já não é mais útil para a comunicação.

- **Tamanho da chave:** são diferentes para a criptografia de chave privada ou simétrica e para a criptografia de chaves públicas ou assimétricas.

SAIBA MAIS

Sistemas criptográficos já apresentaram problemas de segurança, o que demonstra que a criptografia deve ser considerada uma das camadas de segurança. Um dos problemas mais conhecidos foi o do algoritmo de chave privada RC4, que foi o pivô de problemas no WEP (*Wired Equivant Privacy*), protocolo de segurança utilizado em redes Wi-Fi, em 2001. Atualmente o WEP não pode ser utilizado devido a este problema com o RC4. Nos últimos anos, o protocolo SSL foi alvo de diferentes ataques, o que culminou na recomendação pela não utilização do SSL e na expansão do uso da nova versão do TLS. Alguns ataques relacionados são o ataque de renegociação do protocolo (2009), BEAST (2011), CRIME, BREACH, Truncation (2013), Heartbleed, BERserk, Cloudfare, FREAK, PODDLE (2014), Logjam (2015), DROWN, Unholy PAC (2016).

■ APLICAÇÕES DE CRIPTOGRAFIA

A criptografia de chave privada e a criptografia de chave pública têm uma série cada vez maior de aplicações. Algumas delas são:

- **Proteção da comunicação:** autenticação de entidades, integridade e confidencialidade em mensagens pessoais como os do aplicativo *WhatsApp*, em comunicação de voz como o do *Skype*, em e-mails com o uso de sistemas como o *Pretty Good Privacy* (PGP), ou em acesso remoto por *Virtual Private Network* (VPN).
- **Proteção de dados armazenados:** confidencialidade de dados em dispositivos móveis, em notebooks e desktops diretamente pelo sistema operacional ou por sistema específico, ou na nuvem.

- **Proteção de transações:** autenticação de entidades, integridade e confidencialidade no uso de cartões, em transações bancárias, em compras online.

Um dos principais protocolos de segurança para transações é o *Hyper Text Transfer Protocol Secure* (HTTPS), que é um *Uniform Resource Identifier* (URI) para o uso do *Hyper Text Transfer Protocol* (HTTP) sobre uma sessão *Secured Socket Layer* (SSL) ou *Transport Layer Security* (TLS).

Este conjunto de protocolos é utilizado para transações Web com a criação de um túnel seguro por onde trafegam as informações. Além de garantir a **confidencialidade** (dados cifrados com chave simétrica de sessão), eles podem visar também a **integridade dos dados** (uso de *Message Authentication Code*, MAC) e a **autenticidade das partes** (as entidades podem ser autenticadas com o uso de criptografia de chave pública).

De forma geral, o SSL evoluiu para o TLS, de modo que o SSL 3.1 é o TLS 1.0. Já o HTTPS é o HTTP dentro do SSL/TLS. O túnel bidirecional do HTTP é criado entre duas entidades, e quando este túnel é seguro por uma conexão SSL/TLS, então o conjunto é conhecido como HTTPS. No HTTPS, a conexão SSL/TLS é estabelecida antes, e os dados HTTP são trocados sobre essa conexão SSL/TLS (NAKAMURA, 2016).

O funcionamento é:

1. Cliente se conecta a um servidor com TLS, requisitando uma conexão segura, apresentando uma lista de algoritmos suportados.
2. O servidor escolhe um algoritmo simétrico e de *hash* que ele também suporta e notifica o cliente.
3. O servidor envia sua identificação como um certificado digital, com nome, autoridade certificadora (CA) e a chave pública.
4. O cliente confirma a validade do certificado antes de prosseguir.

5. Para gerar a chave de sessão, o cliente cifra um número aleatório com a chave pública do servidor e envia o número cifrado para o servidor.

6. Como somente o servidor consegue abrir o número aleatório, os dois podem gerar uma chave de sessão única a partir dele.

7. Diffie-Hellman é utilizado para gerar uma chave de sessão única.

Outra aplicação importante de criptografia para as comunicações é a rede privada virtual ou **Virtual Private Network (VPN)**. A criptografia possibilita o tunelamento das comunicações, como o uso de protocolos como o IPSec ou TLS, de modo que entidades em uma rede pública ou compartilhada accessem uma rede privada como se estivessem nela. O acesso pode ser individual, como no caso de um acesso remoto, ou pode ser de uma rede para outra (*gateway-to-gateway* VPN) (NAKAMURA; GEUS, 2007).

A criptografia tem um papel importante para a proteção de dados armazenados, ainda mais em um mundo em que as informações estão distribuídas em *datacenters* de empresas, dispositivos de usuários e nuvem. São diferentes níveis de proteção, que vão desde a cifragem de dados diretamente no banco de dados até o cifragem de arquivos ou disco rígido de notebooks que utilizam o Windows, com o BitLocker.

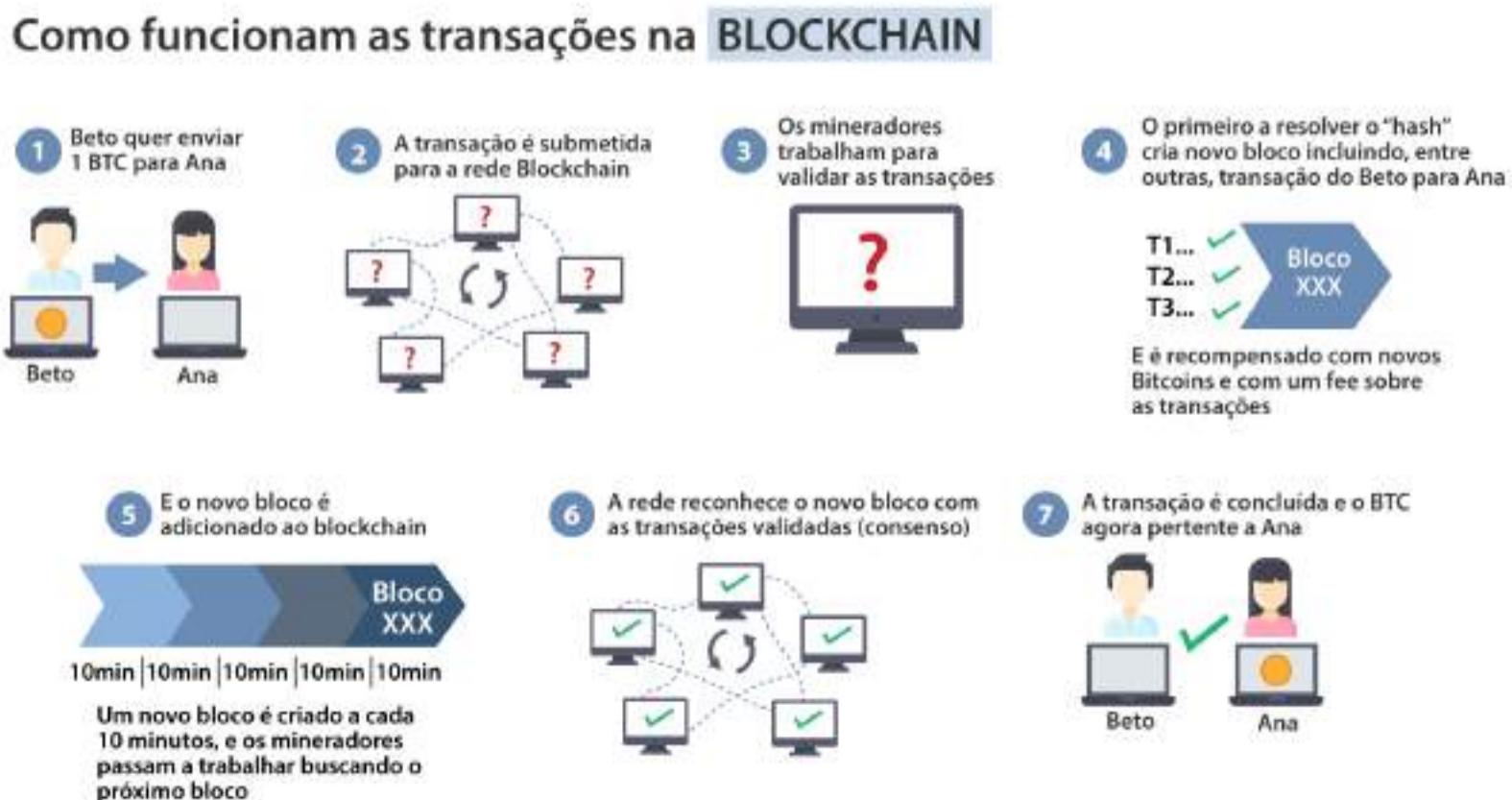
Quando pensamos no nosso cotidiano online, há ainda uma série de aplicações da criptografia. Quando realizamos uma compra pela Internet, por exemplo, temos que ter a tranquilidade de saber que os dados de nosso cartão do banco estão sendo transferidos de forma segura até a loja. Além disso, uma vez que a transferência dos dados de cartão foi feita de forma segura, estes dados devem estar protegidos no banco de dados e no servidor da loja virtual.

Para completar o entendimento de que a criptografia faz parte de nossas vidas, podemos contar com a segurança em nossas comunicações quando utilizamos aplicativos como o *WhatsApp*, *Skype* ou outros similares. Alguns utilizam criptografia fim-a-fim, o que garante que ninguém no meio do caminho tenha acesso ao conteúdo e à troca de chaves, que ocorre de forma transparente para os usuários. Já o dispositivo móvel também já conta com a criptografia dos dados armazenados. Além disso, o acesso Web, tanto de aplicações de redes sociais quanto de negócios, financeiros e de comércio online, conta com o HTTPS, e até mesmo uma camada adicional específica de criptografia em alguns casos. E os dados que partem de nós trafegam pela rede e chegam às empresas são protegidos também por criptografia no armazenamento.

Outra aplicação que utiliza conceitos de criptografia que tem sido muito explorada nos últimos anos é a tecnologia ***blockchain***. *Blockchain* é a tecnologia por trás do *bitcoin* e utiliza, de forma conjunta, uma série de algoritmos computacionais que incluem criptografia e sistemas distribuídos, criando um ambiente de confiança distribuído.

Figura 1.18 ilustra como uma transação é feita usando a *blockchain* (JUNGES, 2018).

Figura 1.18 | Uma transação utilizando *blockchain*



Fonte: adaptada de Junges (2018).

No exemplo, Beto quer enviar 1 BTC, que é a unidade da criptomoeda *bitcoin* para Ana. A carteira digital de Ana é baseada na criptografia de chave pública, e Beto utiliza a chave pública de Ana para realizar a transação. Esta chave pública pode ser representada por meio de um código QR, que indica ainda o endereço *bitcoin* de Ana. Você deve lembrar que somente Ana consegue abrir a sua carteira digital, pois somente ela possui a chave privada correspondente. A transação é enviada para a *blockchain*, que é uma rede distribuída em que os nós tentam validar a transação com a mineração. A mineração, neste exemplo, é a resolução do *hash* envolvido com a transação, que consome muitos recursos computacionais. O primeiro que resolver o desafio do *hash* valida a transação e é recompensado. A transação, assim, passa a fazer parte de um bloco da *blockchain*, e será usada para validar outras transações. E Ana possa a ter o BTC transacionado por Beto e validado pela rede (JUNGES, 2018).

PESQUISE MAIS

O livro de Stallings (2015) traz uma série de elementos de criptografia, focando também nas teorias matemáticas e nos cálculos realizados (STALLINGS, 2015). Na parte 1 do livro são tratadas as cifras simétricas, com técnicas clássicas de encriptação, cifras de bloco e DES, conceitos básicos de teoria dos números e corpos finitos, AES, operação de cifra de blocos e geração de número pseudoaleatório e cifras de fluxo. Já a parte 2 trata de cifras assimétricas, com mais teoria dos números, criptografia de chave pública e RSA, além de outros criptossistemas de chave pública. Já na parte 3 são tratados os algoritmos criptográficos para integridade dos dados, incluindo funções de *hash* criptográficas, códigos de autenticação de mensagem, assinaturas digitais, gerenciamento e distribuição de chaves.

STALLINGS, W. Criptografia e Segurança de Redes:

Princípios e Práticas. 6. ed. São Paulo: Pearson, 2015.

Assim, finalizamos esta seção, em que discutimos aspectos que mostram a razão de a criptografia ser considerada um dos principais controles de segurança, a qual vem sendo utilizada desde muito antes de a informação passar a ser digital. Em seus projetos de segurança, nunca se esqueça de proteger a confidencialidade dos dados que trafegam e que são armazenados, cuidando ainda da integridade e da autenticidade.

FAÇA VALER A PENA

Questão 1

A criptografia é um dos principais controles de segurança da informação, sendo utilizada para uma série de necessidades, como para garantir a confidencialidade, integridade ou autenticidade. Para cada uma dessas necessidades, há algoritmos específicos.

Assinale a alternativa que apresenta a função do algoritmo Diffie-Hellman.

a. Para cifrar mensagens.

b. Para assinar mensagens.

c. Para a troca de chaves criptográficas.

d. Para verificar a segurança.

e. Para enviar mensagens seguras.

Questão 2

Um cliente deseja enviar uma mensagem ao seu advogado. Apesar de ele ser uma figura pública, o cliente quer preservar a confidencialidade desta mensagem, de modo que somente o advogado tenha acesso a ela. O cliente não deseja, inclusive, que ninguém além do advogado saiba desta mensagem, ou seja, a mensagem deve passar despercebida por todos.

Dante ao exposto, assinale a alternativa que apresenta técnica, tecnologia ou algoritmo que o cliente deve utilizar para enviar a mensagem para o advogado.

a. AES.

b. RSA.

c. Diffie-Hellman.

d. Hash criptográfico.

e. Esteganografia.

Questão 3

O serviço de mensagens *WhatsApp* utiliza criptografia em todas as suas comunicações, incluindo mensagens de voz e outros arquivos, entre seus usuários. Com o que chamam de "criptografia de ponta a ponta", as mensagens são cifradas ao deixar o dispositivo móvel da pessoa que as envia e só conseguem ser decodificadas no dispositivo móvel de quem as recebe. Segundo um comunicado da empresa, Quando você manda uma mensagem, a única pessoa que pode lê-la é a pessoa ou grupo para quem você a enviou. Ninguém pode olhar dentro da mensagem. Nem cibercriminosos. Nem *hackers*. Nem regimes opressores. Nem mesmo nós. Com a criptografia de ponta a ponta, um canal seguro é estabelecido entre o remetente e o destinatário, com a criptografia de chave pública. Este canal seguro é utilizado para trocar uma chave privada do algoritmo de criptografia simétrica entre as duas entidades, que é efetivamente utilizado para cifrar as mensagens.

Assinale a alternativa que apresenta as chaves criptográficas utilizadas neste processo, primeiro para o estabelecimento do canal seguro e depois a cifragem das mensagens.

a. Esteganografia.

b. Chave privada compartilhada entre remetente e destinatário, e chave pública do remetente.

c. Chave privada compartilhada entre remetente e destinatário, e chave pública do destinatário.

d. Par de chaves do remetente e destinatário, e chave privada compartilhada.

e. Par de chaves do destinatário, e chave privada compartilhada.

REFERÊNCIAS

ANCHISESLANDIA –Brazilian Security Blogger. **[Segurança] A Cifra Macônica.** 12 de julho de 2017. Disponível em: <https://bit.ly/3oNuHla>. Acesso em: 7 out. 2020.

COPELAND, B. J. Britannica. **Ultra – Allied intelligence project.** Disponível em: <https://bit.ly/3pRCLJd>. Acesso em: 8 out. 2020.

CRYPTO Corner. **Vigenère Cipher.** Disponível em: <https://bit.ly/3jdMGq4>. Acesso em: 7 out. 2020.

FIARRESGA, V. M. C. **Criptografia e Matemática.** Dissertação (Mestrado em Matemática para Professores) – Faculdade de Ciências, Universidade de Lisboa. Lisboa, 2010. Disponível em: <https://bit.ly/2O5hbmC>. Acesso em: 7 out. 2020.

GRABBE, O. J. **The DES Algorithm Illustrated.** Disponível em: <https://bit.ly/3oPMluR>. Acesso em: 8 out. 2020.

JUNGES, F. **Blockchain descomplicado.** Livecoins. Disponível em: <https://bit.ly/2MUyZAk>. 4 de abril de 2018. Acesso em: 26 out. 2020.

KAHNEY, L. The FBI Wanted a Back Door to the iPhone. Tim Cook Said No. **Wired**, 16 abr. 2019. Disponível em: <https://bit.ly/2Ms1Pbs>. Acesso em: 7 out. 2020.

KATZ, J.; LINDELL, Y. L. **Introduction to Modern Cryptography.** Flórida: CRC Press, 2007.

MARSH, A. The Hidden Figures Behind Bletchley Park's Code-Breaking Colossus. **IEEE Spectrum**, 31 dez. 2019. Disponível em: <https://bit.ly/3aArNkS>. Acesso em: 8 out. 2020.

LOEFFLER, J. How Peter Shor's Algorithm Dooms RSA Encryption to Failure. **Interesting Engineering**, 2 maio 2019. Disponível em: <https://bit.ly/36GiO0t>. Acesso em: 2 nov. 2020.

MARR, B. F. What Is Homomorphic Encryption? And Why Is It So Transformative?. **Forbes**, 15 nov. 2019. Disponível em: <https://bit.ly/3oNc4US>. Acesso em: 2 nov. 2020.

MARTIN, G. Explainer: What is post-quantum cryptography? **MIT Technology Review**, 12 jul. 2019. Disponível em: <https://bit.ly/36GHzK6>. Acesso em: 7 out. 2020.

MCCULLOUGH, M. Making sense of an Enigma. **Ingenium**. Canada's Museums of Science and Innovation. 24 out. 2018. Disponível em: <https://bit.ly/3jgxBnD>. Acesso em: 8 out. 2020.

MEDEIROS, F. Uma breve história sobre Criptografia. **CryptID**, 6 jul. 2015. Disponível em: <https://bit.ly/36F29du>. Acesso em: 20 out. 2020.

MENEZES, A. J.; OORSCHOT, P. C. van. VANSTONE, S. A. **Handbook of Applied Cryptography**, ago. 2020 Disponível em: <https://cacr.uwaterloo.ca/hac/>. Acesso em: 6 out. 2020.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. **Bitcoin.Org**. 31 out. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 2 nov. 2020.

NAKAMURA, E. T., GEUS, P. L. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

NAKAMURA, E. T. **Segurança da informação e de redes**. Londrina: Editora e Distribuidora Educacional, 2016.

NIST. National Institute of Standards and Technology. U.S. Department of Commerce. Computer Security Division. Applied Cybersecurity Division. **Lightweight Cryptography**. Disponível em: <https://bit.ly/3pO9PBH>. Acesso em: 2 nov. 2020.

Disponível em: <https://bit.ly/3rgSGks>. Acesso em: 7 out. 2020.

RICE, D. What Is the Difference Between Quantum Cryptography and Post-Quantum Cryptography? **FedTech**, 4 mar. 2020. Disponível em: <https://bit.ly/3ttZBZu>. Acesso em: 2 nov. 2020.

SIMON, S. **O livro dos códigos**. Rio de Janeiro: Record, 2010.

TOWSEND Security. AES vs. DES Encryption: Why Advanced Encryption Standard (AES) has replaced DES, 3DES and TDEA. **Preciserly**, 1 jun. 2020. Disponível em: <https://bit.ly/3tt5GFC>. Acesso em: 8 out. 2020.

WARD, M. **The ancient art of hidden writing**. BBC News, 2 jul. 2010.

Disponível em: <https://bbc.in/3rmYHw2>. Acesso em: 8 out. 2020.

FOCO NO MERCADO DE TRABALHO

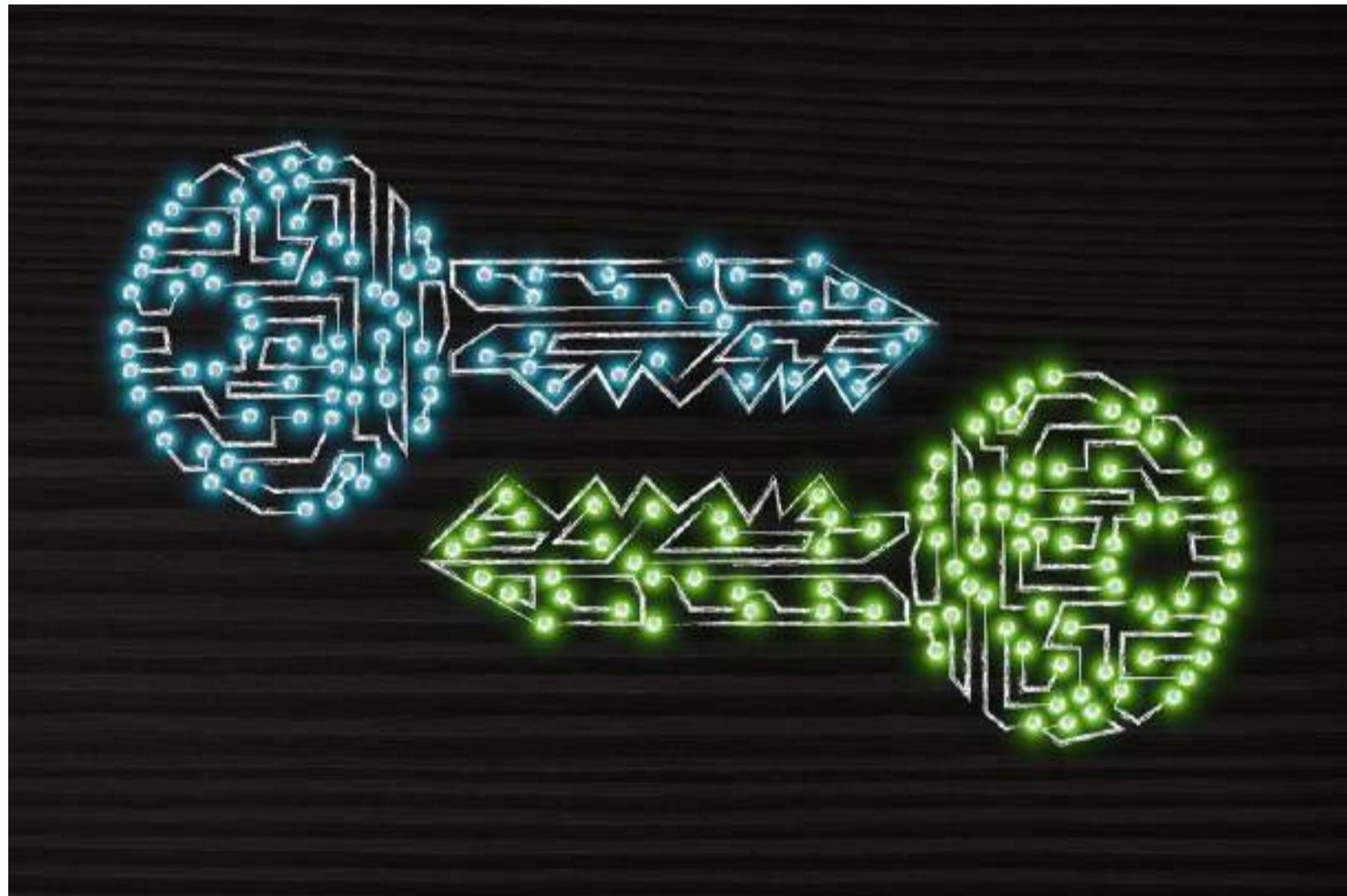
CRIPTOGRAFIA

Emilio Tissato Nakamura

0
Ver anotações

APLICAÇÕES DA CRIPTOGRAFIA

A criptografia de chave privada e a criptografia de chave pública têm uma série cada vez maior de aplicações.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você é o responsável pela segurança da informação de uma empresa química e sua apresentação para a diretoria executiva com a estratégia de segurança para as situações relatadas deve, ao mesmo tempo, mostrar que há riscos envolvidos e que você sabe como fazer a empresa avançar.

Comece a apresentação contextualizando o projeto de desenvolvimento do composto químico para o agronegócio e a forma como as equipes estão trabalhando nas três localidades do Brasil (São Paulo, Rio de Janeiro e Salvador), em conjunto com os parceiros chineses e suíços.

A partir do entendimento de como as equipes estão trabalhando, inclua as plataformas, os sistemas e aplicativos utilizados.

Incorpore as ameaças relacionadas com a criptografia para cada uma dessas situações, que envolvem as pessoas, as necessidades e as plataformas, os sistemas e aplicativos. Um direcionamento pode ser:

- **Situação 1:** armazenamento de resultados do projeto no servidor de arquivos na nuvem. Servidor de arquivos ou o provedor de nuvem pode ser atacado e a documentação pode ser vazada ou alterada. Envolve confidencialidade e integridade.
- **Situação 2:** armazenamento de resultados do projeto no serviço de troca de arquivos. Serviço pode sofrer um incidente de segurança e resultar em acesso não autorizado. Envolve confidencialidade e integridade.
- **Situação 3:** armazenamento de documentação em notebooks e pendrives. Equipamentos e dispositivos podem ser roubados, perdidos ou acessados indevidamente. Envolve confidencialidade no caso de roubo, perda ou acesso indevido, e integridade no caso de acesso indevido.
- **Situação 4:** dados do projeto trafegam pela Internet quando são trabalhados de forma colaborativa, quando são armazenados no servidor de arquivos e quando são enviados entre as equipes, via e-

mail e serviço de troca de arquivos. Dados podem ser expostos e alterados durante a transmissão. Envolve confidencialidade e integridade.

- **Situação 5:** dados do projeto trocados via e-mail permanecem nestes servidores, que podem ser atacados. Envolve confidencialidade e integridade.
- **Situação 6:** origem dos documentos pode ser alterada, de modo que informações falsas podem ser inseridas na empresa. Envolve integridade e, mais especificamente, autenticidade de origem.

A estratégia de segurança envolvendo a criptografia pode ser definida desta forma:

- Criptografia de chave privada ou simétrica: situações 1, 2, 3, 4, 5 e 6.
- *Hash* criptográfico: situações 1, 2, 3, 4, 5 e 6.
- Criptografia de chave pública ou assimétrica com assinatura digital: situação 6.

Não se esqueça de incluir um *overview* sobre os tipos de criptografia na apresentação para a diretoria executiva.

AVANÇANDO NA PRÁTICA

UM DOCUMENTO SECRETO PARA 30

Você é o especialista de segurança de um conglomerado de agentes secretos, com uma série de atividades, e sua função é proteger a comunicação entre eles. Esses agentes secretos estão espalhados pelo Brasil, e o diretor do conglomerado precisa enviar um comunicado importante, sensível e secreto para 30 do total de 31 agentes secretos. Qual é a sua estratégia para que os 30 agentes secretos, e somente eles, recebam o comunicado?

RESOLUÇÃO



Você poderia propor o uso de criptografia para proteger o comunicado. Sim, a criptografia faz sentido, mas o de chave privada ou simétrica traz alguns desafios. Como você faria a distribuição desta chave privada para os 30 agentes secretos, mais o diretor? E, se a chave privada deve chegar de forma secreta para cada um dos 30 agentes secretos, por que já não enviar o comunicado? Eles já estão espalhados pelo Brasil, e um encontro físico e real poderia resolver o problema das chaves, mas neste caso também a criptografia seria desnecessária, já que o próprio comunicado poderia ser entregue pessoalmente.

Outro ponto importante da criptografia de chave privada é que, em caso de comprometimento da chave privada, todos estarão inseguros, com uma nova chave privada tendo de ser definida. Neste caso de muitas entidades (30 agentes secretos), a criptografia de chave privada apresenta limitações.

A melhor solução é o uso da criptografia de chave pública. O diretor e cada um dos 31 agentes secretos poderiam ter um par de chaves. Para o comunicado, o diretor pode utilizar as chaves públicas dos 30 agentes secretos com quem ele precisa se comunicar. Cada um deles, assim, recebe o pacote cifrado e é o único que pode decifrá-lo, já que somente ele possui a chave privada correspondente.

NÃO PODE FALTAR

GESTÃO E POLÍTICAS DE SEGURANÇA

Emilio Tissato Nakamura

Ver anotações

O QUE É LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) é uma lei que visa proteger os direitos fundamentais de privacidade dos dados dos cidadãos brasileiros.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

CONVITE AO ESTUDO

Caro aluno, nesta unidade serão apresentados aspectos normativos e de cultura da segurança da informação, que tratam, de uma forma integrada, de processos, pessoas e tecnologias.

Muitos casos de incidentes de segurança são resultados de exploração de vulnerabilidades nestas três frentes, o que exige que as empresas tenham que tratá-las de uma forma integrada. Em 2008, houve a exploração de falhas de sistemas internos de um banco europeu, causando prejuízo de US\$ 7 bilhões (SPAMFIGHTER, 2008). Este exemplo reforça a importância de controles de segurança que considerem os aspectos de processos, pessoas e tecnologias. No caso do banco, o funcionário que fez a exploração tinha acesso a sistemas internos e se aproveitou da falta de segurança que poderia ser tratada com processos que envolvessem, por exemplo, limites e aprovações de instâncias superiores. Para que ele não explorasse os sistemas internos de uma forma ilícita, uma política de segurança clara também seria fundamental. E, para complementar, os sistemas internos deveriam ser protegidos com controles de segurança envolvendo monitoramento, controle de acesso e desenvolvimento seguro, por exemplo.

Este caso mostra também a importância da cultura de segurança, que é particular de cada organização, construída com medidas e comportamentos de todos os funcionários, e no relacionamento com clientes, parceiros e fornecedores. É por meio da soma das ações de todos que uma cultura de segurança da informação é construída, de modo que é fundamental a representatividade e a formalização de instrumentos importantes, como um Sistema de Gestão de Segurança da Informação (SGSI). Discutiremos a cultura de segurança e a construção de um SGSI, juntamente com a política de segurança da informação, que é um dos controles primordiais das empresas, e um dos pontos iniciais para a consolidação de uma cultura de segurança da informação forte.

Há um conjunto de *frameworks* e normas que guiam as ações de segurança da informação, como as da família NBR ISO/IEC 27000 (ABNT, 2020), que você deve conhecer para organizar e otimizar sua estratégia de segurança da informação. Você terá uma abordagem da família NBR ISO/IEC 27.000 e verá que há outras fontes relevantes, como o *Cybersecurity Framework do National Institute of Standards and Technology* (NIST) (NIST, 2018) e o CIS Controls, do Center for Internet Security (CIS) (CIS, 2020).

Não podemos esquecer que, na Era da Informação, reforçada pela transformação digital, a proteção dos princípios da segurança da informação (confidencialidade, integridade e disponibilidade) deve fazer parte direta dos negócios, seja para proteger transações, dados pessoais, documentos confidenciais, processos de negócios em que o fluxo de dados envolve diferentes áreas da empresa, ou dados que trafegam por equipamentos de fábricas.

A segurança da informação é, assim, direcionada por aspectos de negócios e cada organização com a sua missão e seus valores. E a segurança da informação é direcionada também por aspectos legais, regulatórios e contratuais, como os do setor médico, de telecomunicações ou financeiro.

No Brasil, a Lei nº. 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2020), a Lei Nº 12.965, o Marco Civil da Internet (BRASIL, 2014) e a Lei Nº 12.737, a Lei Carolina Dieckmann (BRASIL, 2012) também reforçam a necessidade de segurança da informação.

A política e cultura de segurança devem tratar de todos os aspectos de sua empresa, incluindo desde a forma e as responsabilidades de funcionários que recebem equipamentos, até as necessidades de proteção nas relações com parceiros e fornecedores, passando pela

forma como os acessos físicos e lógicos são gerenciados. Além disso, é importante também que a aquisição e o desenvolvimento de sistemas considerem aspectos de segurança da informação.

Você deve considerar que as empresas estão em constante evolução, assim como os riscos de segurança da informação, o que resulta em uma natural evolução da própria área de segurança da informação, que deve ser sempre acompanhada. Iremos discutir nesta unidade algumas tendências em segurança da informação que moldarão o seu futuro.

Nesta unidade também discutiremos aspectos importantes de segurança da informação envolvidos com o uso de nuvem computacional e iremos nos aprofundar um pouco mais nos dados que têm o seu ciclo de vida e precisam ser seguros, envolvendo o uso de criptografia e técnicas como anonimização e pseudonomização, importantes principalmente para a conformidade com a LGPD.

Bons estudos!

PRATICAR PARA APRENDER

Caro aluno, nesta seção será abordado um dos aspectos mais complexos da segurança da informação: como trabalhar com segurança da informação integrando aspectos relacionados a pessoas, processos e tecnologias. Uma cultura de segurança da informação forte é construída

pelas pessoas, com seus hábitos do dia a dia nas empresas, e um dos principais instrumentos para esta construção é a Política de Segurança. Muitos tratam as pessoas como o elo mais fraco da segurança da

informação das empresas. Você já passou por aquela situação em que os usuários questionam sobre o que é permitido ou não, e onde isto está escrito?

Porém, a Política de Segurança da Informação é apenas um dos controles de segurança necessários nas empresas. Para uma proteção plena da confidencialidade, integridade e disponibilidade das informações, é preciso tratar a segurança da informação de uma forma

holística, que engloba a necessidade de um conjunto de diferentes controles de segurança. E a complexidade aumenta com a constante evolução das ameaças, dos negócios e das leis e regulamentações.

O estabelecimento de um Sistema de Gestão de Segurança da Informação (SGSI) é, assim, um ponto importante para uma atuação holística em segurança da informação.

Para a sua orientação, há um conjunto de frameworks e normas que guiam as ações de segurança da informação, como as da família NBR ISO/IEC 27.000 (ABNT, 2020), o *Cybersecurity Framework do National Institute of Standards and Technology* (NIST) (NIST, 2018) e o *CIS Controls, do Center for Internet Security* (CIS) (CIS, 2020).

Você pode certificar o SGSI de sua empresa de acordo com a norma ABNT NBR ISO/IEC 27001, enquanto a ABNT NBR ISO/IEC 27002 foca nos objetivos de controles de segurança. O *Cybersecurity Framework* tem uma abordagem integrada de diferentes aspectos de segurança importantes, enquanto o *CIS Controls* estabelece uma forma mais prática de trabalho.

Nesta seção ainda discutiremos sobre a privacidade, que exige a proteção de dados pessoais, o que é regido pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 (BRASIL, 2020).

Uma empresa é composta por uma matriz em Natal, no Rio Grande do Norte, e filial em Belo Horizonte, em Minas Gerais. Com foco em energias renováveis, o desenvolvimento de novas tecnologias é feito por também por uma equipe que fica em Santiago, no Chile. Há laboratórios conectados em Belo Horizonte e Santiago. A empresa tem projetos com militares argentinos, o que exige um alto nível de segurança, já que envolve aspectos de segurança nacional.

A empresa tem um diretor de segurança da informação, que é o responsável por uma estrutura que inclui uma gerência de governança de segurança, uma gerência de tecnologias de segurança e outra gerência de processos de segurança. Você é o gerente de processos de segurança e deve trabalhar em sinergia com os outros dois gerentes para alinhar os planos e atividades de segurança da informação da empresa.

O diretor de segurança da informação da empresa solicitou um status dos aspectos normativos da empresa e você deve preparar uma apresentação com esse material. É preciso fazer um alinhamento com o

gerente de governança de segurança e o gerente de tecnologias de segurança.

Estruture uma apresentação descrevendo os tópicos com detalhes. Os tópicos a ser abordados são listados a seguir:

- *Frameworks* de segurança disponíveis e qual a empresa segue.
- Aspectos de negócios, legais, normativos e contratuais que devem ser considerados pela empresa.
- Controles de segurança da empresa: quais são e como são definidos.
- Estrutura normativa, considerando políticas, normas, diretrizes, procedimentos, guias.

Nesta seção, você terá acesso a instrumentos que farão a diferença em sua jornada em segurança da informação, ao integrar aspectos de pessoas, processos e tecnologias, com a possibilidade de aplicar normas e frameworks importantes como a família ISO 27000, *Cybersecurity Framework* do NIST e o CIS *Controls* do CIS.

Boa aula!

CONCEITO-CHAVE

Um dos principais instrumentos para a aplicação de segurança da informação nas empresas são as normas e *frameworks*, os quais apresentam uma visão mais abrangente das necessidades e implementações de segurança da informação, e devem ser seguidos, na medida do possível.

Um dos principais desafios da segurança da informação é o tratamento dos variados riscos, que englobam aspectos de pessoas, processos e tecnologias. Eles devem ser tratados de uma forma integrada, todas as pessoas devem conhecer os elementos de segurança da informação das empresas onde trabalham, criando assim uma cultura de segurança da informação que guie e influencie diretamente os negócios e dite o dia a dia das atividades de todos.

A Política de Segurança da Informação é um dos principais e fundamentais controles de segurança necessários nas organizações, independentemente de sua natureza. Ela faz parte de normas e frameworks de segurança da informação, como as descritas a seguir.

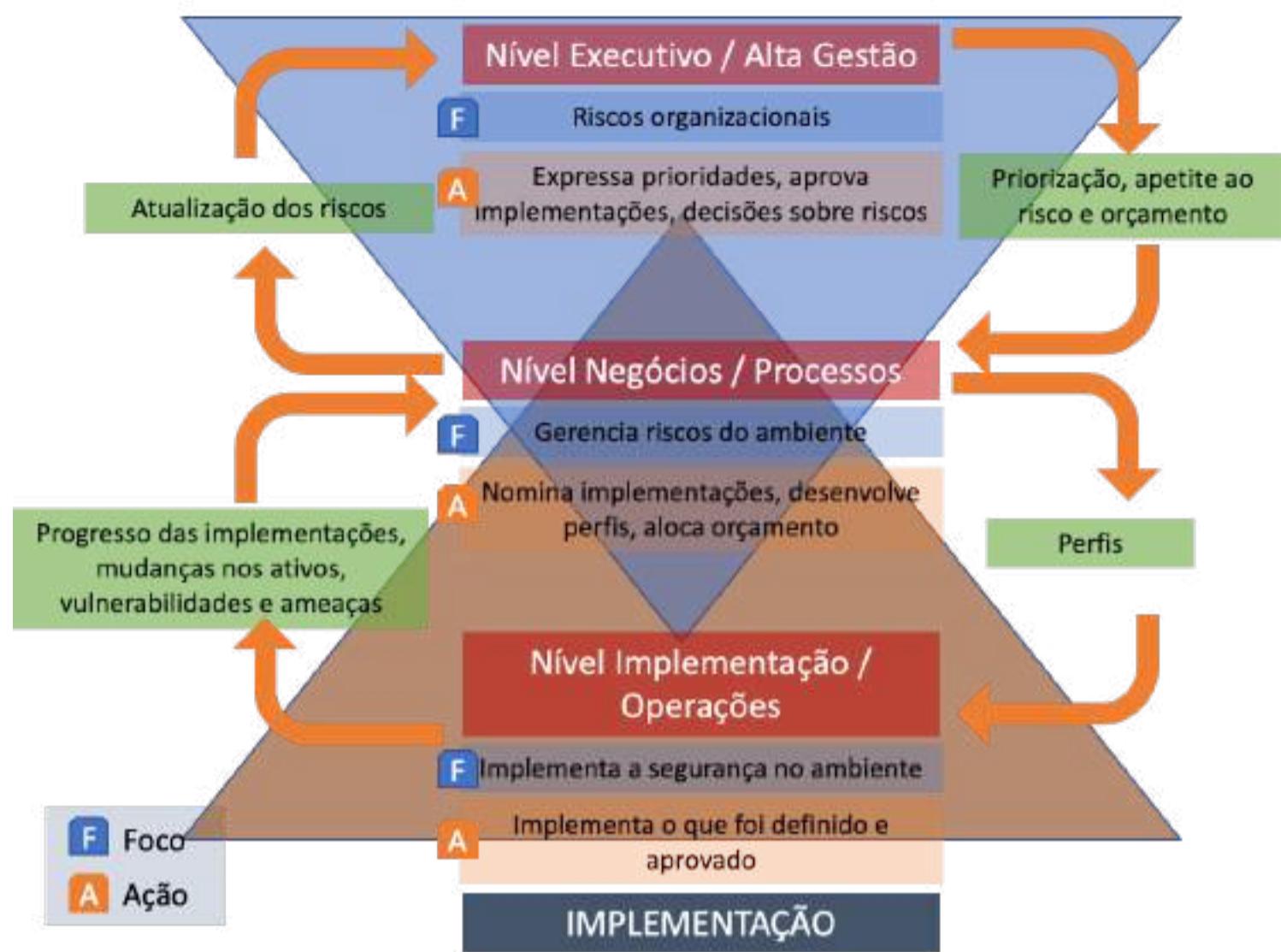
o

Ver anotações

| CYBERSECURITY FRAMEWORK, DO NIST

O *Cybersecurity Framework do National Institute of Standards and Technology* (NIST) (NIST, 2018) organiza diferentes elementos da segurança da informação, focando no uso de direcionadores de negócios para guiar atividades de segurança cibernética, considerando os riscos de segurança da informação. O *framework* faz a ponte entre o nível executivo com o operacional (Figura 2.1) e provê uma taxonomia e determinados mecanismos para as organizações alcançarem variados objetivos de segurança da informação (Figura 2.2). O nível executivo tem foco nos riscos organizacionais, enquanto o nível de negócios e processos faz o gerenciamento dos riscos do ambiente, com o nível de implementação e operações implementando a segurança. O *framework* trabalha com os elementos importantes para as atividades destes três níveis, incluindo objetivos, priorizações, orçamentos, métricas e comunicação.

Figura 2.1 | Integração entre visões e os riscos de segurança da informação



Fonte: adaptada de NIST (2020).

Figura 2.2 | Objetivos do *Cybersecurity Framework* do NIST



Fonte: adaptado de NIST (2018).

As três partes do *Cybersecurity Framework* são:

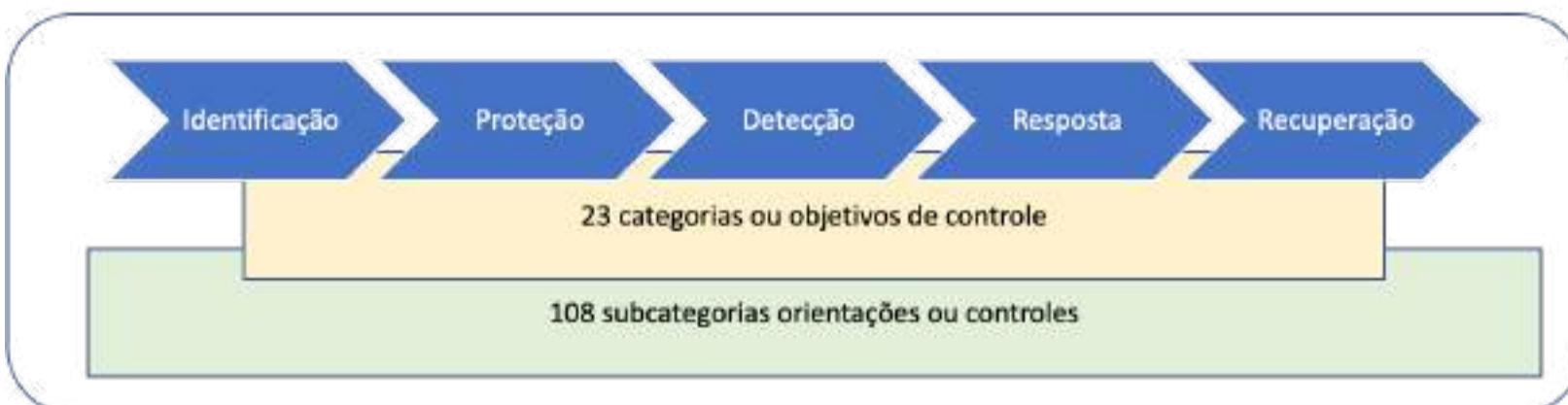
- **Núcleo (*Framework Core*)**, com guias detalhadas para desenvolver perfis organizacionais, que prioriza as atividades de segurança de

acordo com requisitos de negócios, missão, tolerância a riscos e recursos disponíveis. Envolve as cinco funções (identificar, proteger, detectar, responder e recuperar) (Figura 2.3), que provê uma visão estratégica do ciclo de vida dos riscos de segurança da informação.

As funções têm categorias (23 no total), abrangendo resultados cibernéticos, físicos, pessoais e comerciais. Há ainda 108 subcategorias, divididas nas 23 categorias, que são orientações para criar ou melhorar um programa de segurança cibernética, com referências a outros padrões de segurança da informação, como a ABNT NBR ISO/IEC 27001 (ISO 27001, 2013), COBIT (COBIT, 2020), NIST SP 800-53 (NIST, 2020), ANSI/ISA-62443 (ISA, 2020) e CIS *Controls* (CIS, 2020);

- **Camadas de implementação**, que proveem um mecanismo para ver e entender as características da abordagem para o gerenciamento de riscos da organização, para priorizar e alcançar os objetivos de segurança da informação. As camadas vão de parcial (*Tier 1*) a adaptativo (*Tier 4*), refletindo as respostas informais e reativas iniciais até a agilidade e a resposta formal baseada na visão de riscos;
- **Perfis**, que são os alinhamentos de padrões, guias e práticas em um cenário de implementação. Os perfis podem identificar as oportunidades de melhoria da postura de segurança, comparando um perfil atual ("as is") com um perfil alvo ("to be").

Figura 2.3 | As cinco funções do *Cybersecurity Framework*



Fonte: adaptado de NIST (2018).

O CIS *Controls* é um conjunto priorizado de ações que, de uma forma integrada, estabelecem a defesa em camadas para mitigar os ataques mais comuns contra sistemas e redes. Com objetivo de melhorar o estado de segurança, o CIS *Controls* muda a discussão de “o que minha empresa faz?” para “o que devemos todos fazer?” para melhorar a segurança e fortalecer uma cultura de segurança da informação (CIS, 2020). Ele foi desenvolvido pela comunidade de segurança da informação e tem as seguintes características:

- **O ofensivo direciona a defesa:** uso de controles para atuar sobre ataques reais;
- **Priorização:** investe primeiramente em controles que proveem a maior redução do risco e proteção contra as ameaças mais perigosas;
- **Medidas e métricas:** estabelece uma linguagem comum para executivos, especialistas de TI, auditores e profissionais de segurança para medir a eficiência das medidas de segurança, de modo a identificar e implementar rapidamente os ajustes necessários;
- **Diagnóstico e mitigação contínua:** mede continuamente a efetividade das medidas de segurança atuais para direcionar a priorização das próximas etapas;
- **Automação:** automatiza defesas para que a organização alcance confiabilidade, escalabilidade e medição contínua da aderência dos controles e métricas.

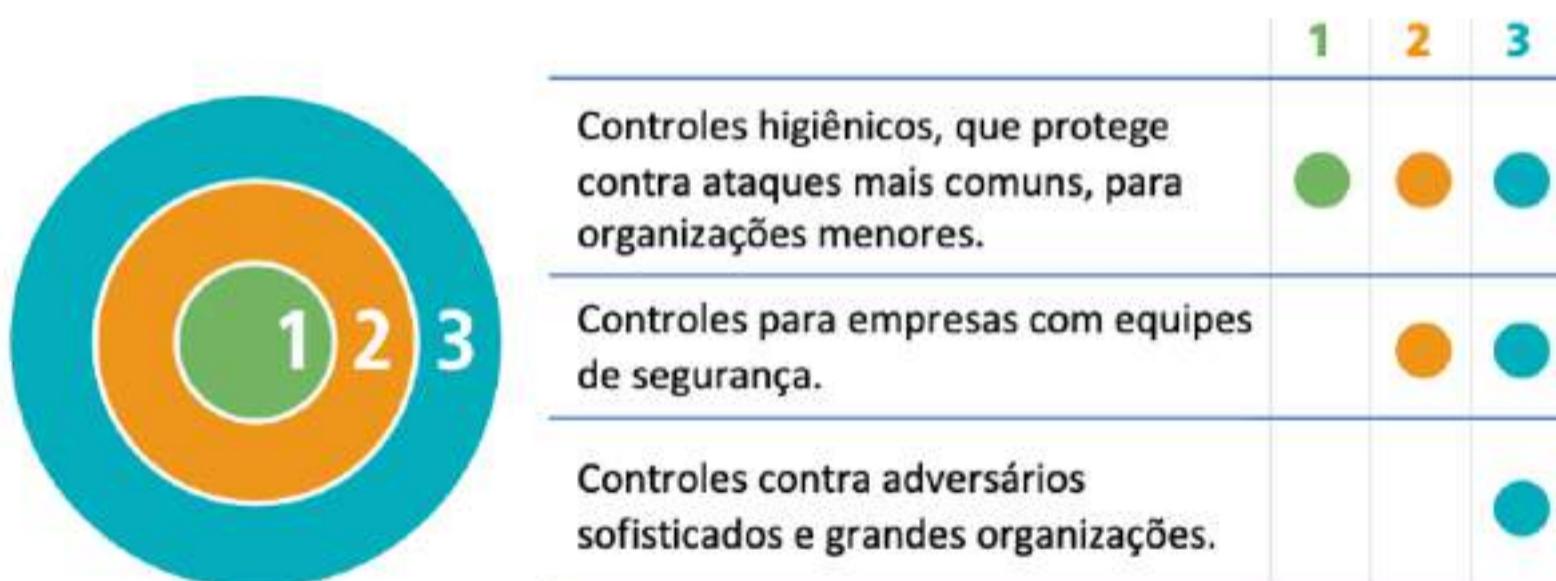
O CIS *Controls* define um conjunto de seis controles considerados básicos ou higiênicos:

- Inventário e controle de ativos de *hardware*.
- Inventário e controle de ativos de *software*.

- Gestão de vulnerabilidades.
- Uso controlado de privilégios administrativos.
- Configuração segura para *hardware* e *software* de dispositivos móveis, laptops, *workstations* e servidores.
- Manutenção, monitoramento e análise de logs de auditoria.

Porém, considerando que estes controles podem ser difíceis de serem implementados por organizações com recursos limitados, a base para as priorizações são os grupos de implementação (*CIS Controls Implementation Groups, IGs*), que são categorias de avaliação própria a partir de alguns atributos relevantes de segurança da informação. A Figura 2.4 apresenta os 3 grupos de implementação, com o IG1 focando nos dados críticos e sendo considerados os controles higiênicos, capazes de proteger contra os ataques mais comuns. O IG2 foca em organizações com equipes de segurança, enquanto o IG3 busca a proteção contra adversários sofisticados. Eles são complementares, ou seja, IG1 deve ser implementado, depois IG2 e depois o IG3.

Figura 2.4 | CIS *Controls Implementation Groups, IGs*



Fonte: adaptado de CIS(2020).

Um exemplo de classificação como IG1 são empresas familiares com 10 funcionários. Já uma organização regional provendo um serviço poderia ser classificada como IG2, e uma grande corporação com milhares de funcionários pode ser classificado como IG3 (CIS, 2020).

O conjunto de controles de segurança do CIS *Controls* pode ser visto na Figura 2.5.

o

Figura 2.5 | Controles de segurança do CIS *Controls*

Básico	Fundamental	Organizacional
Inventário e controle de ativos de hardware	Proteção de e-mail e web browser	Programa de conscientização e treinamento em segurança
Inventário e controle de ativos de software	Proteção contra malware	Segurança de aplicações
Gestão de vulnerabilidades	Controle de portas, protocolos e serviços de rede	Gestão e resposta a incidentes
Controle do uso de privilégios administrativos	Capacidade de recuperação de dados	Testes de segurança
Configuração segura para hardware e software em dispositivos móveis, laptops, workstations e servidores	Configuração segura de dispositivos de rede	Defesa de borda
Manutenção, monitoramento e análise de logs	Proteção de dados	Controle de acesso baseado no <i>need to know</i>

Ver anotações

Controle de

acesso sem fio

Monitoramento e

controle de contas

Fonte: adaptado de CIS (2020).

I FAMÍLIA ISO 27000

Quando falamos sobre segurança da informação, devemos conhecer a família de normas da ISO 27000. Estas normas abarcam ainda a certificação de segurança da informação, realizada por auditores líderes ISO 27001.

ASSIMILE

Certificação em segurança da informação pode ser concedida para uma organização que segue a norma ABNT NBR ISO/IEC 27001 (ISO 27001, 2013), que trata dos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI). O auditor líder faz a auditoria de certificação (BSI, 2020).

A certificação é sobre o Sistema de Gestão de Segurança da Informação (SGSI), tratado pela ABNT NBR ISO/IEC 27001. Os auditores líderes fazem a auditoria do SGSI, em um escopo bem definido da organização. Há ainda auditoria interna, que prepara a organização para a auditoria externa, realizada por um auditor líder certificado, que ao final do processo certifica a organização em ISO 27001 naquele escopo definido.

O SGSI é composto por elementos-chave da ABNT NBR ISO/IEC 27001, estabelecendo uma abordagem organizacional para proteger a informação e seus critérios de confidencialidade, integridade e disponibilidade. Ele será discutido mais adiante.

REFLITA

Os sistemas de gestão não são tecnológicos ou, necessariamente, sistemas automatizados. O sistema é no seu sentido mais amplo, com o SGSI incluindo estratégias, planos, políticas, medidas, controles e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Ver anotações

A ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) é uma norma importante para os profissionais de segurança da informação, ao definir o código de prática para controles de segurança da informação. De uma forma geral, a ABNT NBR ISO/IEC 27001 se relaciona com a ABNT NBR ISO/IEC 27002 da seguinte forma:

- Escopo da aplicação da ABNT NBR ISO/IEC 27001 é definido.
- Análise de riscos é realizado.
- Aplicabilidade dos controles de segurança é formalizado.
- Controles de segurança são implementados, com base na ABNT NBR ISO/IEC 27002.

Os controles de segurança apropriados devem ser selecionados e implementados para que os riscos da organização sejam reduzidos a um nível aceitável, a partir dos requisitos de segurança da informação e da estratégia de tratamento dos riscos. A Figura 2.6 mostra os objetivos de controle definidos na ABNT NBR ISO/IEC 27002.

Figura 2.6 | Objetivos de controles de segurança da informação da ABNT NBR ISO/IEC 27002



Fonte: adaptado de ISO 27002 (2013).

0

Além das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, a família conta com outras normas importantes, sintetizadas no Quadro 2.1. Algumas normas não foram traduzidas para o português, como é o caso da ISO/IEC 27000, que trata do vocabulário.

Quadro 2.1 | Normas da família ISO 27000

Normas da família ISO 27000	
ISO/IEC 27000:2018	<i>Information technology — Security techniques — Information security management systems - Overview and vocabulary</i>
ABNT NBR ISO/IEC 27001:2013	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002:2013	Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação
ABNT NBR ISO/IEC 27003:2020	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações

Ver anotações

Normas da família ISO 27000

ABNT NBR ISO/IEC 27004:2017	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação
ABNT NBR ISO/IEC 27005:2019	Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação
ISO/IEC 27006:2015	<i>Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems</i>
ABNT NBR ISO/IEC 27007:2018	Tecnologia da informação — Técnicas de segurança — Diretrizes para auditoria de sistemas de gestão da segurança da informação
ISO/IEC TS 27008:2019	<i>Information technology — Security techniques — Guidelines for the assessment of information security Controls</i>
ISO/IEC 27009:2020	<i>Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 – Requirements</i>
ISO/IEC 27010:2015	<i>Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications</i>

[Ver anotações](#)

Normas da família ISO 27000

ISO/IEC 27011:2016	<i>Information technology — Security techniques — Code of practice for Information security Controls based on ISO/IEC 27002 for telecommunications organizations</i>
ISO/IEC 27013:2015	<i>Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1</i>
ABNT NBR ISO/IEC 27014:2013	Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação
ISO/IEC TR 27016:2014	<i>Information technology — Security techniques — Information security management — Organizational economics</i>
ABNT NBR ISO/IEC 27017:2016	Tecnologia da informação - Técnicas de segurança — Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem
ABNT NBR ISO/IEC 27018:2018	Tecnologia da informação — Técnicas de segurança — Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII
ISO/IEC 27019:2017	<i>Information technology — Security techniques — Information security Controls for the energy utility industry</i>

Ver anotações

Normas da família ISO 27000

ISO/IEC 27031:2011	<i>Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity</i>
ABNT NBR ISO/IEC 27032:2015	Tecnologia da Informação — Técnicas de segurança — Diretrizes para segurança cibernética
ISO/IEC 27033-1:2015	<i>Information technology — Security techniques — Network security — Part 1: Overview and concepts</i>
ISO/IEC 27033-2:2012	<i>Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security</i>
ISO/IEC 27033-3:2010	<i>Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues</i>
ISO/IEC 27033-4:2014	<i>Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways</i>
ISO/IEC 27033-5:2013	<i>Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)</i>

[Ver anotações](#)

Normas da família ISO 27000

ISO/IEC 27033-6:2016	<i>Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access</i>
ISO/IEC 27034-1:2011/Cor 1:2014	<i>Information technology — Security techniques — Application security — Part 1: Overview and concepts — Technical Corrigendum 1</i>
ISO/IEC 27034-2:2015	<i>Information technology — Security techniques — Application security — Part 2: Organization normative framework</i>
ISO/IEC 27034-3:2018	<i>Information technology — Application security — Part 3: Application security management process</i>
ISO/IEC 27034-5:2017	<i>Information technology — Security techniques — Application security — Part 5: Protocols and application security Controls data structure</i>
ISO/IEC TS 27034-5-1:2018	<i>Information technology — Application security — Part 5-1: Protocols and application security Controls data structure, XML schemas</i>
ISO/IEC 27034-6:2016	<i>Information technology — Security techniques — Application security — Part 6: Case studies</i>
ISO/IEC 27034-7:2018	<i>Information technology — Application security — Part 7: Assurance prediction framework</i>
ISO/IEC 27035-1:2016	<i>Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management</i>

Normas da família ISO 27000

ISO/IEC 27035-2:2016	<i>Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response</i>
ISO/IEC 27035-3:2020	<i>Information technology -- Information security incident management — Part 3: Guidelines for ICT incident response operations</i>
ISO/IEC 27036-1:2014	<i>Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts</i>
ISO/IEC 27036-2:2014	<i>Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements</i>
ISO/IEC 27036-3:2013	<i>Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security</i>
ISO/IEC 27036-4:2016	<i>Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services</i>
ABNT NBR ISO/IEC 27037:2013	Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital

Normas da família ISO 27000

ABNT NBR ISO/IEC 27038:2014	Tecnologia da informação — Técnicas de segurança — Especificação para redação digital
ISO/IEC 27039:2015	<i>Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)I</i>
ISO/IEC 27040:2015	<i>Information technology — Security techniques — Storage security</i>
ISO/IEC 27041:2015	<i>Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method</i>
ISO/IEC 27042:2015	<i>Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence</i>
ISO/IEC 27043:2015	<i>Information technology — Security techniques — Incident investigation principles and processes</i>
ISO/IEC 27050-1:2019	<i>Information technology — Electronic discovery — Part 1: Overview and concept</i>
ISO/IEC 27050-2:2018	<i>Information technology — Electronic discovery — Part 2: Guidance for governance and management of electronic discovery</i>
ISO/IEC 27050-3:2020	<i>Information technology — Electronic discovery — Part 3: Code of practice for electronic discovery</i>

Ver anotações

Normas da família ISO 27000

ABNT NBR ISO/IEC 27701:2019 Versão Corrigida:2020	Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes
ABNT NBR ISO 27799:2019	Informática em saúde — Gestão de segurança da informação em saúde utilizando a ISO/IEC 27002

Fonte: ABNT (2020).

EXEMPLIFICANDO

Algumas normas ainda estão sendo trabalhadas, como para forense digital e segurança cibernética. E há casos curiosos, como a norma ABNT NBR ISO 27020:2014 ser da área de odontologia e a ISO 27048 ser da área de radiação.

Além das normas da família ISO 27000, que focam na segurança da informação, há outras normas que tratam de diferentes aspectos de segurança, como classificação da informação, segurança na área de saúde e privacidade. O Quadro 2.2 apresenta algumas dessas normas.

Quadro 2.2 | Normas que envolvem aspectos de segurança da informação

Normas que envolvem aspectos de segurança da informação	
ABNT NBR 16167:2013	Segurança da Informação — Diretrizes para classificação, rotulação e tratamento da informação
ABNT NBR 16386:2015	Tecnologia da informação — Diretrizes para o processamento de interceptação telemática judicial

Normas que envolvem aspectos de segurança da informação

ABNT ISO/TR 18638:2019	Informática em saúde — Orientações sobre educação da privacidade das informações em saúde em organizações de assistência à saúde
ABNT ISO/TS 21547:2016	Informática em saúde — Requisitos de segurança para arquivamento de registros eletrônicos de saúde — Princípios
ABNT NBR ISO 25237:2020	Informática em saúde — Pseudonimização
ABNT NBR ISO/IEC 29100:2020	Tecnologia da informação — Técnicas de segurança — Estrutura de Privacidade

Fonte: ABNT (2020).

Ver anotações

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

O SGSI é um elemento-chave para o fortalecimento da cultura de segurança da informação das organizações. E você pode, uma vez estabelecido um SGSI, certificar a sua empresa na ISO 27001. A norma ABNT NBR ISO/IEC 27001 estabelece os requisitos para o estabelecimento de um sistema de gestão de segurança da informação (ISO 27001, 2013).

O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

É importante que um sistema de gestão da segurança da informação seja parte e esteja integrado com os processos da organização e com a estrutura de administração global e que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles (ISO 27001, 2013).

Você deve especificar e implementar o SGSI de acordo com as características específicas da sua organização, que apresenta necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização. Como estes fatores evoluem com o tempo, é preciso estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta é uma das características principais dos sistemas de gestão, o processo de melhoria contínua, ou PDCA (Plan, Do, Check, Act), que pode ser visto na Figura 2.7.

0

Ver anotações

Figura 2.7 | Melhoria contínua e PDCA do SGSI



Fonte: Palma (2016).

A Figura 2.8 mostra alguns requisitos de um SGSI que formam os fatores críticos de sucesso:

- **Contexto da organização**, incluindo questões internas e externas relevantes para o seu propósito, os requisitos das partes interessadas, incluindo requisitos legais, regulatórios e contratuais.
- Escopo do SGSI.
- **Liderança**, com comprometimento da alta direção, estabelecimento de uma política de segurança da informação e atribuição de papéis, autoridades e responsabilidades.
- **Planejamento**, com ações para contemplar riscos e oportunidades, avaliação de riscos de segurança da informação, tratamento de riscos de segurança da informação e estabelecimento de objetivos de segurança da informação para as funções e níveis relevantes.
- **Apoio**, com provimento de recursos, criação de competências, conscientização e comunicação.
- **Operação**, com planejamento operacional e controle, avaliação de riscos de segurança da informação, tratamento de riscos de segurança da informação.
- **Avaliação de desempenho**, com monitoramento, medição, análise e avaliação, além de auditoria interna e análise crítica pela direção,
- **Melhoria**, com tratamento de não conformidades e ação corretiva, além de melhoria contínua.

Figura 2.8 | Requisitos de um SGSI



Fonte: elaborada pelo autor.

O contexto da organização está relacionado com as evoluções que ocorrem no ambiente de negócio, tecnológico e operacional.

| LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A LGPD (BRASIL, 2020) é uma lei que entrou em vigor no Brasil em setembro de 2020, visando proteger os direitos fundamentais de privacidade dos cidadãos brasileiros. A lei estabelece medidas para que haja a transparência na coleta e no tratamento de dados pessoais pelas organizações, que deve então prover a proteção adequada destes dados para garantir a privacidade dos seus usuários.

No Capítulo I, Art. 5º da LGPD define alguns elementos importantes (Planalto, 2018):

- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável.
- **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, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- **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).
- **Agentes de tratamento:** o controlador e o operador.
- **Tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação,

utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O que devemos pensar é que, de acordo com a LGPD, os dados pessoais podem ser coletados mediante finalidade e base legal. O titular dos dados pessoais tem direitos, e a empresa que faz o tratamento dos dados pessoais passa a ser a responsável pelos dados pessoais coletados. E essa responsabilidade envolve, principalmente, a proteção, já que qualquer uso irregular, incluindo o seu vazamento, afeta a privacidade do titular. As empresas devem, assim, implementar controles de segurança da informação para evitar incidentes de segurança que podem levar ao vazamento de dados pessoais.

o

Ver anotações

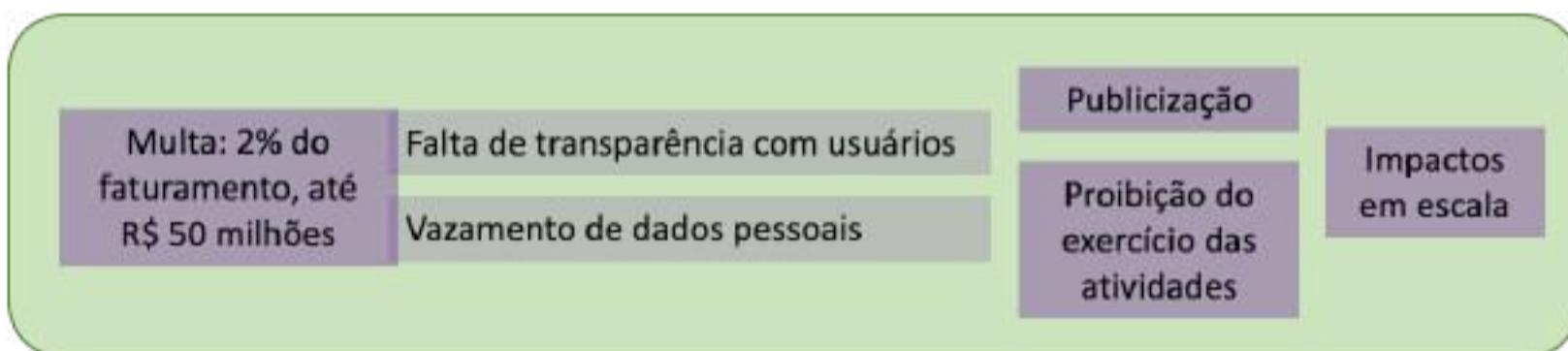
EXEMPLIFICANDO

Uma empresa que coleta dados de uma pessoa, como nome e CPF, deve dizer de uma forma explícita a finalidade daquela coleta, incluindo a forma como aqueles dados coletados serão protegidos, por quanto tempo, e se haverá compartilhamento com terceiros. A pessoa pode ou não aceitar estes termos, e terá direito a revisões dos dados sendo tratados pela empresa, podendo solicitar a remoção do banco da empresa. Há casos, como em hotéis, em que há a coleta de dados pessoais no momento do check-in, como número de documentos e endereço. A coleta deve obedecer à finalidade relacionada à hospedagem, de acordo com a legislação do setor. No caso de uso destes dados para outros fins, como o compartilhamento para um parceiro comercial do hotel, o hóspede deve ser informado sobre ele e dar um consentimento explícito. Além deste aspecto de transparência nas relações com as pessoas, o hotel deve

proteger todas os dados coletados. Em caso de vazamento destes dados, sejam eles em papel ou em meio digital, o hotel estará sujeito às sanções previstas na lei.

A lei estabelece sanções para quaisquer organizações, sejam elas grandes ou pequenas empresas, que não cumpram os requisitos estabelecidos, envolvendo a transparência nas relações com as pessoas, e vazamentos de dados pessoais, que comprometem a privacidade das pessoas (Figura 2.9).

Figura 2.9 | Sanções previstas na LGPD



Fonte: elaborada pelo autor.

A Figura 2.10 ilustra uma visão do que é necessário para a proteção dos dados pessoais. A visão de riscos é importante para guiar as ações de segurança da informação. Um ponto adicional da LGPD é que a sua adequação é obrigatória, envolvendo fortemente aspecto de conformidade. Do nosso ponto de vista, a de segurança da informação, devemos implementar os controles de segurança para proteção de vazamentos, que podem ser decorrentes de ataques cibernéticos. Há uma estratégia possível de ser adotada para a adequação à LGPD, como a descrita em Garcia (2020).

Figura 2.10 | Visão integrada da privacidade e da proteção de dados pessoais



Fonte: elaborada pelo autor.

REFLITA

A LGPD trata da privacidade e da proteção de dados pessoais. Do ponto de vista da segurança, qual é o princípio que deve ser trabalhado, considerando a tríade CID (confidencialidade, integridade, disponibilidade)? Privacidade tem relação com a confidencialidade. Assim, empresas já com nível de maturidade mais alto em segurança da informação já têm maior aderência com a lei, já que tratam as informações em todos os princípios da CID. Alguns exemplos de controles de segurança são a criptografia e o controle de acesso a sistemas e banco de dados. Outro ponto importante da LGPD é que os dados pessoais devem ser protegidos, logo, esses dados devem ser primeiramente mapeados. Já os Dados confidenciais e dados corporativos não fazem parte do escopo da LGPD.

SAIBA MAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD) foca na proteção da privacidade dos cidadãos brasileiros, que passam a ter direitos sobre seus próprios dados. As empresas devem estabelecer uma relação de transparência

para a coleta dos dados pessoais, com princípios importantes como a minimização para a coleta somente dos dados estritamente necessários, e a finalidade para definir a razão daquela coleta. Além disso, as organizações estarão sujeitas a sanções que vão de multas à paralização das atividades em caso de vazamento de dados pessoais. Para evitar os vazamentos e proteger os dados pessoais, as empresas precisam de controles de segurança da informação.

MARCO CIVIL DA INTERNET

A Lei nº 12.965, o Marco Civil da Internet (BRASIL, 2014) é a lei que regula o uso da internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

O Marco Civil da Internet trata de temas como neutralidade da rede, privacidade e retenção de dados, além de impor obrigações de responsabilidade civil aos usuários e provedores.

A lei ainda trata, ainda, da confidencialidade das comunicações privadas, e dá especial atenção aos dados de registros de acesso, como endereços de IP e *logins*.

LEI CAROLINA DIECKMANN

A Lei nº 12.737, também conhecida como Lei Carolina Dieckmann (BRASIL, 2012), altera o código penal brasileiro, tornando crime a invasão de aparelhos eletrônicos para obtenção de dados particulares, a interrupção de serviço telemático ou de informática de utilidade pública. Os exemplos de crime, penalidade e agravante podem ser observados nos Quadros 2.3 e 2.4.

Crime	Pena	Exemplo
Invasão de um dispositivo. Pode estar conectado ou não a rede, mediante a violação de segurança com o objetivo de obtenção de informações sem autorização.	Detenção de 3 meses a 1 ano e multa.	Invasão de um computador para roubar informações, sem consentimento do proprietário.

Fonte: elaborado pelo autor.

Quadro 2.4 | Lei Carolina Dieckmann: agravantes

Agravante	Pena	Exemplo
Roubo de informação causando prejuízo econômico.	Aumenta a pena de detenção de 3 meses a 1 ano e 4 meses.	Cibercriminoso rouba conteúdo sigiloso de uma pessoa e apaga a informação, causando perda financeira.
Obtenção de conteúdo de comunicações privadas de forma não autorizada.	Aumenta a pena de detenção de 6 meses a 2 anos.	Roubo de conteúdos sigilosos de e-mails ou controle de computadores, tornando-os “zumbis”.
Divulgação e comercialização de conteúdo roubado de dispositivo.	Reclusão de 8 meses a 3 anos e 4 meses.	Roubo de informações sigilosas e venda ou divulgação na internet.

Fonte: adaptado de UOL (2013).

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

As políticas de segurança da informação constituem um dos principais controles de segurança da informação. Com a definição de elementos como regras, orientações, diretrizes, responsabilidades e sanções, as políticas de segurança da informação guiam as ações de todos da organização, incluindo os terceiros, prestadores de serviços, parceiros e fornecedores.

As políticas de segurança da informação devem tratar de todos os aspectos cotidianos da organização, incluindo os relacionados às pessoas, aos processos e às tecnologias.

EXEMPLIFICANDO

Quando um funcionário é contratado por uma empresa, ele deve saber quais são seus papéis e responsabilidades quanto à segurança da informação. Os aspectos de segurança envolvidos, por exemplo, com acessos remotos usando dispositivos da própria empresa devem estar bem definidos, claros e comunicados adequadamente. O mesmo para acessos remotos a partir de dispositivos pessoais. E quanto ao uso de aplicações de nuvem, aqueles não homologados pela área de segurança da empresa podem ser utilizados? Todas as informações referentes às políticas de segurança devem ser informadas para todos da empresa de maneira clara e no que diz respeito a qualquer tipo de aplicações e dispositivos etc.

Você deve construir as políticas de segurança com o apoio da alta direção da empresa. A própria norma ABNT NBR ISO/IEC 27001 (ISO 27001, 2013) diz que a alta direção deve estabelecer uma política de segurança da informação que:

- Seja apropriada ao propósito da organização.

- Inclua os objetivos de segurança da informação ou forneça a estrutura para estabelecer os objetivos de segurança da informação.
- Inclua um comprometimento para satisfazer os requisitos aplicáveis, relacionados com segurança da informação.
- E inclua um comprometimento para a melhoria contínua do sistema de gestão da segurança da informação.

Outro ponto importante que a norma ABNT NBR ISO/IEC 27001 estabelece é que a política de segurança da informação deve:

- Estar disponível como informação documentada.
- Ser comunicada dentro da organização.
- E estar disponível para as partes interessadas conforme apropriado.

Já a ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) define como objetivo das políticas de segurança da informação o provimento de orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes, com dois controles:

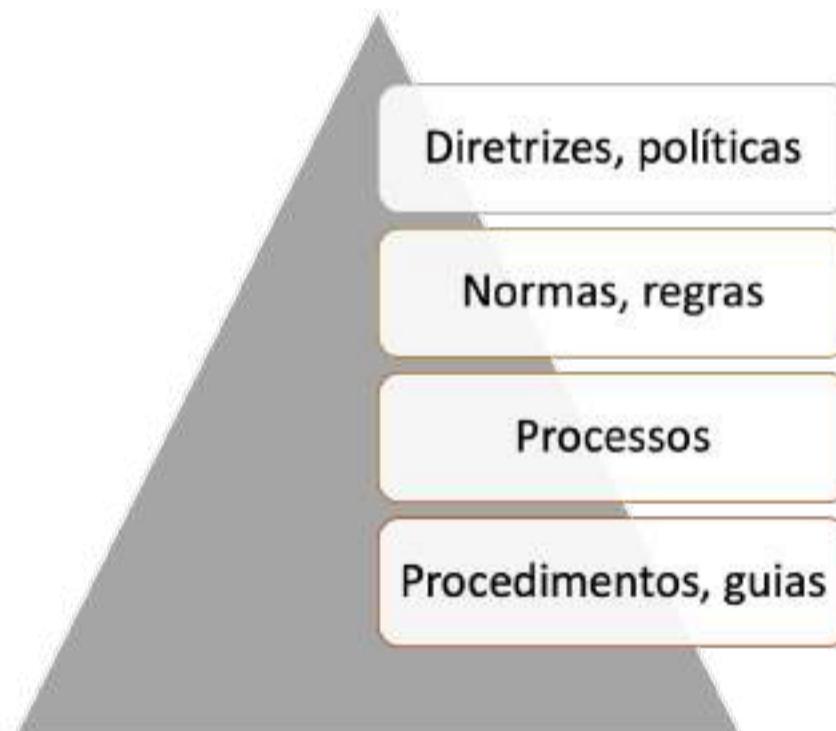
- **Políticas para segurança da informação:** um conjunto de políticas de segurança da informação deve ser definido, aprovado pela direção, publicado e comunicado para os funcionários e partes externas relevantes.
- **Análise crítica das políticas para segurança da informação:** as políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Uma definição que irá ajudar você na definição, aprovação e publicação de políticas de segurança é o entendimento de que elas constituem um conjunto de documentos com regras, papéis e responsabilidades que devem ser seguidos por todos os funcionários e partes externas

relevantes. Este conjunto de documentos pode ser definido em partes, pensando em quem irá ler. Por exemplo, uma política de senhas pode apresentar as regras para a definição de senhas de usuários para acesso aos serviços corporativos. Mas e as senhas administrativas, utilizadas pelos administradores de sistemas que possuem acesso privilegiado? Nesse caso, para acessos privilegiados, seria melhor ficar em uma mesma política, ou seria melhor uma política de senhas diferenciada? Esta definição depende de cada empresa, e daí a importância do SGSI.

Outra questão aparece quanto à forma de cumprimento das políticas de segurança pelos funcionários. Muitas vezes há a necessidade de procedimentos específicos, que dizem, além “do que” deve ser feito, o “como” deve ser feito. Assim, a estrutura de documentos que constitui as políticas de segurança da informação das empresas poderia ser como a Figura 2.11.

Figura 2.11 | Árvore de documentos que formam a política de segurança da informação



Fonte: elaborada pelo autor.

Assim, uma política de segurança poderia ser um documento mais diretrivo, que coloca os aspectos gerais da segurança da informação, com os assuntos relativos desmembrados em normas. Um exemplo importante diz respeito às senhas, com normas e as regras de escolha e renovação. Destas regras há desdobramentos para os usuários, que

podem seguir os processos para a escolha de senhas, junto dos guias. E, para os administradores de sistemas, os processos de configuração dos serviços devem seguir as regras definidas na norma.

TECNOLOGIAS DE SEGURANÇA DA INFORMAÇÃO

Os controles de segurança da informação devem ser definidos de acordo com uma avaliação de riscos, que leva em consideração aspectos próprios de cada organização. Os frameworks de segurança e a família ISO 27000 são de extrema importância para a definição destes controles de segurança, os quais podem ser físicos, tecnológicos ou processuais, e uma fonte importante para você seguir é a norma ABNT NBR ISO/IEC 27002 (ISO 27002, 2013), com os objetivos de controle de controle e os controles de segurança da informação.

Para visualizar o objeto, acesse seu material digital.

Fonte: adaptado de ISO 27002 (2013).

PESQUISE MAIS

Vale a pena você ler a Lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2020). Há no texto elementos importantes para a sua evolução como profissional de segurança da informação, e o que está na lei será aplicado por você tanto como pessoa física quanto como profissional da área.

- BRASIL. Lei Geral de Proteção de Dados Pessoais. Presidência da República – Secretaria-Geral – Subchefia para Assuntos Jurídicos. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD).

Chegamos ao final desta seção, que tratou da gestão de segurança da informação e da integração entre visões que levam em consideração os contextos particulares de cada organização. O conhecimento de *frameworks* e normas de segurança da informação é importante para a sua formação como profissional da área, principalmente porque direciona as ações e possibilita uma visão holística dos aspectos da segurança da informação que precisam ser compreendidos.

FAÇA VALER A PENA

Questão 1

A família ISO 27000 é composta por um conjunto de normas que trata de segurança da informação, incluindo assuntos como sistema de gestão de segurança da informação, controles de segurança, segurança na área de saúde, segurança em comunicações, segurança de redes, resposta a incidentes, segurança de aplicações e privacidades, entre outros.

Assinale as normas que certificam uma empresa em segurança da informação.

a. ABNT NBR ISO/IEC 27001.

b. ABNT NBR ISO/IEC 27002.

c. ABNT NBR ISO/IEC 27003.

d. ABNT NBR ISO/IEC 27004.

e. ABNT NBR ISO/IEC 27005.

Questão 2

Sobre as políticas e os controles de segurança da informação, analise as afirmativas a seguir:

- I. O contexto da organização, como seus objetivos de negócios, não influencia na segurança da informação.
- II. Os controles de segurança da informação podem tratar de aspectos relacionados às pessoas, aos processos e às tecnologias.

III. A família ISO 27000 trata de segurança da informação, sendo

composta por uma série de normas como a ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 27003.

É correto o que se afirma em:

a. I e II, apenas.

b. I e III, apenas.

c. II, apenas.

d. II e III, apenas.

e. III, apenas.

Questão 3

A Lei Geral de Proteção de Dados Pessoais (LGPD) visa a privacidade dos cidadãos brasileiros, com as organizações públicas e privadas tendo que estabelecer relações transparentes para a coleta e o tratamento de dados pessoais, e a proteção destes dados pessoais.

Assinale a alternativa que corresponde ao princípio de segurança da informação envolvido com a LGPD, com o motivo que a segurança da informação é necessária.

a. Integridade e controles de segurança para evitar vazamentos.

b. Disponibilidade e controles de segurança para evitar vazamentos.

c. Confidencialidade e controles de segurança para evitar vazamentos.

d. Integridade e controles de segurança para evitar privacidade.

e. Confidencialidade e controles de segurança para evitar privacidade.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **ABNT**

Catálogo. Disponível em: <https://bit.ly/3b9isIE>. Acesso em: 25 out. 2020.

ABNT – Associação Brasileira de Normas Técnicas. **NBR ISO/IEC**

27001:2013 Tecnologia da informação — Técnicas de segurança —

Sistemas de gestão da segurança da informação — Requisitos.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC**

27002:2013 Tecnologia da informação — Técnicas de segurança —

Código de prática para controles de segurança da informação.

AGUILERA-FERNANDES, E. **Padrões, Normas e Políticas de Segurança**

da Informação. São Paulo: Senac São Paulo, 2017. Disponível em:

<https://bit.ly/2O2o3kR>. Acesso em: 13 out. 2020.

BRASIL. Lei Carolina Dieckmann. Presidência da República – Casa Civil –

Subchefia para Assuntos Jurídicos. **Lei nº 12.737, de 30 de novembro**

de 2012. Disponível em: <https://bit.ly/3uOC32d>. Acesso em: 8 nov. 2020.

BRASIL. Marco Civil da Internet. Presidência da República – Casa Civil –

Subchefia para Assuntos Jurídicos. **Lei nº 12.965, de 23 de abril de**

2014. Disponível em: <https://bit.ly/3bWwEgV>. Acesso em: 8 nov. 2020.

BRASIL. Lei Geral de Proteção de Dados Pessoais. Presidência da

República – Secretaria-Geral – Subchefia para Assuntos Jurídicos. **Lei nº**

13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados

Pessoais (LGPD). Disponível em: <https://bit.ly/2NXlssx>. Acesso em: 25

out. 2020.

BSI – British Standards Institution. **Formação de Auditor Líder em**

Sistema de Gestão de Segurança da Informação ISO/IEC 27001:2013

- IRCA. Disponível em: <https://bit.ly/2MJx41L>. Acesso em: 24 out. 2020.

CIS – Center for Internet Security. **CIS Controls.** Disponível em:

<https://bit.ly/30cBNMx>. Acesso em: 24 out. 2020.

COBIT. COBIT 5. **ISACA.** Disponível em: <https://bit.ly/2NQCBEP>. Acesso

em: 25 out. 2020.

GARCIA, L. R.; AGUILERA-FERNANDES, E.; GONÇALVES, R. A. M.; PEREIRA-

BARRETO, M. R. **Lei Geral de Proteção de Dados Pessoais (LGPD) –**

Guia de Implantação. São Paulo: Editora Edgard Blücher Ltda., 2020.

Disponível em: <https://bit.ly/3uOGlqp>. Acesso em: 8 nov. 2020.

ISA – International Society of Automation. **ANSI/ISA-62443**: Security for industrial automation and control systems. Disponível em: <https://bit.ly/3baMMfA>. Acesso em: 25 out. 2020.

NIST – National Institute of Standards and Technology. **Framework for Improving Critical Infrastructure Cybersecurity**. Version 1.1, 16 abr, 2018. Disponível em: <https://bit.ly/2Oo9zeT>. Acesso em: 24 out. 2020.

NIST – National Institute of Standards and Technology. **SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations**, set. 2020. Disponível em: <https://bit.ly/2NXISPD>. Acesso em: 25 out. 2020.

PALMA, F. Sistema de Gestão de Segurança da Informação (SGSI). **Portal GSTI**. Disponível em: <https://bit.ly/38oO05p>. Acesso em: 24 out. 2020.

SPAMFighter. Societe Generale Employee Confesses to Trading through Hacked Systems, **News**, 5 fev. 2008. Disponível em: <https://bit.ly/3kOxznJ>. Acesso em: 24 out. 2020.

UOL. "Lei Carolina Dieckmann" sobre crimes na internet entra em vigor. **Tilt**, 2 abr. 2013. Disponível em: <https://bit.ly/3rdJo9z>. Acesso em: 8 nov. 2020.

FOCO NO MERCADO DE TRABALHO

GESTÃO E POLÍTICAS DE SEGURANÇA

Emilio Tissato Nakamura

Ver anotações

O QUE É SGSI?

O Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de políticas, processos e procedimentos, entre outros controles, para definir e prover segurança da informação em uma empresa.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Você, como especialista em segurança e privacidade de uma plataforma digital, tem grandes responsabilidades. O planejamento dos principais aspectos que a empresa deve considerar para a segurança e privacidade é importante para direcionar a estratégia da empresa. O foco deste planejamento está na segurança em transações *web*, que complementa a segurança da informação da plataforma digital em si. Como a plataforma digital está em um provedor de nuvem, há vários aspectos como a arquitetura segura, desenvolvimento seguro, gestão de vulnerabilidades e gestão de continuidade de negócios, por exemplo.

Para a segurança em transações *web*, você pode começar o seu planejamento considerando os seguintes aspectos, os quais devem ser detalhados e desenvolvidos:

- Transação parte do usuário, que utiliza dispositivos e possui instalados aplicativos ou aplicações.
- Transação trafega pela internet, passando pelo provedor de internet.
- Transação chega à empresa e os dados são processados e armazenados.
- Há ameaças no ambiente do usuário, do provedor de internet e da empresa.
- Se o usuário for comprometido, a empresa também pode ser.
- O que pode ser feito para que o usuário não seja comprometido.
- O que deve ser feito pela empresa após receber os dados pessoais e transacionais.

O ponto central a ser planejado é que, além dos controles de segurança para proteger a transmissão dos dados dos clientes para a sua empresa, usando HTTPS/TLS/SSL, os clientes são parte central da segurança e privacidade, pois transações fraudulentas podem chegar à empresa a partir deles.

Mostre que pode haver o furto de identidade, a captura da senha, a captura da senha de transação, a modificação da transação e a interrupção do acesso. Essas ameaças existem no ambiente do cliente, no ambiente de internet e no próprio ambiente da empresa, que utiliza um provedor de nuvem.

Mostre que, no ambiente do cliente, os golpes na internet potencializam as ameaças, aumentando o nível de risco. E, como é o ambiente com menor controle, o desafio é maior nos clientes. Apresente os principais golpes na internet que podem comprometer a empresa, com destaque para o *phishing* e o *pharming*.

Defina a partir deste mapeamento um plano de conscientização para os clientes, minimizando as probabilidades deles caírem em fraudes na *internet*, e também de serem vítimas de *malwares*. Dentre as dicas, podem ser inclusos pontos como não clicar em *links* recebidos por e-mails e SMS, além de verificar sempre se uma conexão segura está estabelecida com a empresa, verificando os dados do certificado digital.

Um outro ponto importante para aumentar o nível de segurança é o uso de autenticação de duplo fator. Com este controle de segurança, em caso de furto de identidade, ainda é necessário o dispositivo móvel para o acesso aos serviços da empresa, o que torna o acesso indevido mais difícil.

Com relação à privacidade e proteção de dados pessoais, o planejamento deve incluir os avisos de privacidade na coleta das informações dos clientes. Além disso, a proteção destes dados pela empresa é parte da estratégia de segurança e privacidade, com o reforço de que há sanções previstas na LGPD.

Outro ponto importante a ser planejado são os processos e mecanismos para o atendimento às solicitações dos clientes, que podem consultar e solicitar a remoção dos seus dados pessoais.

Assim, com o tratamento destes principais aspectos, a empresa poderá operar com a necessária segurança e privacidade, minimizando os problemas de acessos a partir de clientes falsos, resultando em melhores resultados.

0

Ver anotações

AVANÇANDO NA PRÁTICA

AUMENTANDO A SEGURANÇA NO ACESSO PELO NAVEGADOR

Os clientes de sua empresa virtual fazem o acesso pelo navegador, digitando o *link*. Você já implementou a segurança do servidor e envia constantemente mensagens para seus clientes para que eles aumentem o nível de conscientização e não caiam em golpes que podem levar ao furto de identidade, que no final resulta em prejuízos para a sua empresa. Cite os pontos que podem levar à contaminação do ambiente do cliente e por que evitar o furto de identidade é crucial para a sua empresa. Além disso, cite algumas possibilidades para você aumentar a segurança no acesso do cliente pelo navegador.

RESOLUÇÃO



A empresa deve evitar as transações maliciosas, que podem chegar de duas formas principais: a partir de um criminoso que furtou a identidade do cliente e faz as transações como se fosse ele, utilizando recursos financeiros também de terceiros; e a partir de transações modificadas que partem do cliente legítimo, mas com os dados alterados para beneficiar o criminoso. A identidade pode ser furtada com a instalação de *malwares* que capturam os dados, os quais podem contaminar os clientes com o uso de *phishing* ou *pharming* como principal vetor, além de poder ser pela exploração de vulnerabilidades em diferentes componentes do dispositivo do cliente. Com o *phishing*, o cliente pode clicar em um *link* que leva para um site falso que coleta os dados de acesso e dados pessoais, incluindo o nome de usuário e senha. O *phishing* também pode fazer com que *malwares* sejam instalados quando executados pelos clientes. Os *malwares* podem também modificar os dados das transações na saída do ambiente do cliente e a empresa recebe essas transações adulteradas.

Uma vez com as credenciais do cliente, o agente de ameaça pode fazer as transações como se fosse ele, porém em benefício próprio.

Um mecanismo tradicional de se utilizar para evitar o uso de identidades furtadas é o uso de autenticação de dois passos ou de duplo fator. Em autenticação, os fatores são algo que o usuário sabe (como senhas), algo que o usuário possui (como tokens ou dispositivos móveis) ou algo que o usuário é (como a biometria).

Com o uso de autenticação de duplo fator, é necessário, além da senha, um outro elemento, como um código único temporário enviado ao dispositivo móvel do usuário via SMS.

Há ainda a possibilidade de utilizar mecanismos de segurança que fazem uma proteção contra *malwares* para evitar a contaminação pelos usuários. Estes mecanismos devem ser instalados e fazem a proteção contra *malwares*, mas apresentam pontos negativos, como o uso de recursos computacionais dos dispositivos dos usuários, bem como a interferência na usabilidade.

Assim, como profissional de segurança, você deve adotar a abordagem em camadas, podendo utilizar ainda controles de segurança como processos de validação de transações ou uso de plataformas antifraude. Uma visão de riscos é fundamental, já que os controles de segurança podem afetar tanto a usabilidade dos clientes quanto a própria operação, que pode ficar mais complexa com as validações. Uma forma de flexibilizar as validações é a adoção de níveis, com base, por exemplo, em valores das transações. Deste modo, transações maiores teriam validações mais estruturadas, enquanto as menores teriam validações mais automatizadas, por exemplo. Isto deve ser definido com uma visão de riscos, e deve ser dinâmica, com atualizações constantes.

NÃO PODE FALTAR

CULTURA DE SEGURANÇA

Emilio Tissato Nakamura

Ver anotações

COMO É FORMADA A CULTURA DE SEGURANÇA E PRIVACIDADE?

Ela é formada pelo conjunto de hábitos, crenças e conhecimentos em segurança e privacidade, através de ações que busquem reforçar estes elementos em todos da empresa.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Caro aluno, nesta seção reforçaremos os aspectos que fortalecem uma cultura de segurança e privacidade, complementando as informações que estudamos na seção anterior.

A segurança da informação é feita a partir de uma visão de riscos, e as políticas de segurança direcionam a forma como a empresa protege a confidencialidade, integridade e disponibilidade de suas informações, tendo um papel importante no fortalecimento da cultura de segurança.

Neste contexto, os termos e contratos, como os de ciência, de uso ou de confidencialidade, fazem parte das necessidades das empresas, ao formalizar entre as partes as necessidades de segurança e privacidade.

Em conjunto com as políticas de segurança, eles explicitam para todas as partes as responsabilidades e obrigações de segurança e privacidade.

As pessoas declaram que conhecem as políticas de segurança e privacidade, e as empresas declaram que há regras e responsabilidades.

Esta importância é reforçada pela necessidade de proteção de dados pessoais oriundos da Lei Geral de Proteção de Dados Pessoais (LGPD).

Discutiremos ainda outros pontos essenciais que ajudam a fazer com que uma cultura de segurança seja fortalecida. Além disso, discutiremos alguns elementos para que as políticas de segurança e privacidade possam ser criadas de modo que cumpram de fato o seu objetivo, chegando ao seu público-alvo, para que assim possam ser seguidas por todos.

Os aspectos de segurança da informação no desenvolvimento de sistemas também serão discutidos nesta seção. São aspectos importantes para profissionais de TI e de segurança, independente do modelo de desenvolvimento adotado pela empresa. Iremos discutir, ainda, pontos como o gerenciamento de segurança de sistemas, e os aspectos operacionais, éticos e legais que devem fazer parte da segurança de sistemas. Além disso, o desenvolvimento de sistemas exige uma preocupação com o ambiente de desenvolvimento seguro, que apresenta uma série de elementos essenciais.

Para finalizar a seção, discutiremos alguns assuntos que direcionam a segurança da informação, com as tendências e o futuro que moldarão as atividades dos profissionais de segurança e privacidade.

Uma empresa com foco em energias renováveis é composta por uma matriz em Natal, no Rio Grande do Norte, e filial em Belo Horizonte, em Minas Gerais. O desenvolvimento de novas tecnologias é feito por uma equipe que fica em Santiago, no Chile. Há laboratórios conectados em Belo Horizonte e Santiago. A empresa tem projetos com militares argentinos, o que exige um alto nível de segurança, já que envolve aspectos de segurança nacional.

A empresa tem um diretor de segurança da informação, que é o responsável por uma estrutura que inclui uma gerência de governança de segurança, uma gerência de tecnologias de segurança e outra gerência de processos de segurança. Você é o gerente de processos de segurança e deve trabalhar em sinergia com os outros dois gerentes para alinhar os planos e atividades de segurança da informação da empresa.

O diretor de segurança da informação da empresa solicitou um *status* de alguns aspectos normativos da empresa, para complementar a apresentação anterior, e você deve preparar uma apresentação para tal. É preciso fazer um alinhamento com o gerente de governança de segurança e o gerente de tecnologias de segurança

Estruture sua apresentação descrevendo os seguintes tópicos:

1. Cultura de segurança e privacidade.
2. Como a segurança é tratada pelos agentes externos.
3. Como a segurança é tratada para os usuários e para os administradores de sistemas.
4. Segurança no desenvolvimento de sistemas.

O fortalecimento da cultura de segurança e privacidade das empresas depende de um conjunto de elementos. Nesta seção, você compreenderá estes elementos e poderá adotá-los na sua jornada em segurança da informação. Para o desenvolvimento seguro de software, há também informações importantes para você.

Boa aula!

CONCEITO-CHAVE

Caro aluno, a cultura de segurança e privacidade é fundamental para as empresas protegerem os seus ativos. Ela é formada pelo conjunto de comportamentos das pessoas no dia a dia das empresas em questões que refletem na proteção das informações e, consequentemente, dos negócios. Um ponto fundamental é que a cultura de segurança e privacidade de uma empresa é única, constituída por um conjunto de hábitos, crenças e conhecimentos de todos. Ela envolve, ainda, a forma como a segurança e privacidade são tratadas pelos funcionários, prestadores de serviços e fornecedores quando as atividades da empresa são exercidas.

CULTURA DE SEGURANÇA E PRIVACIDADE

Toda empresa tem a sua própria cultura de segurança e privacidade (COACHMAN, 2010). O objetivo é que esta cultura seja fortalecida constantemente, principalmente porque cada vez mais a segurança da informação influencia na resiliência das empresas. O grande desafio é que, como toda cultura, a de segurança e privacidade se torna mais

forte com ações da empresa que engajem todas as pessoas, dos funcionários aos fornecedores. Formada pelo conjunto de hábitos, crenças e conhecimentos em segurança e privacidade (Figura 2.12), as ações devem buscar reforçar estes elementos em todos da empresa.

Figura 2.12 | Cultura de segurança e privacidade



Fonte: elaborada pelo autor.

EXEMPLIFICANDO

Um exemplo da influência da cultura de segurança e privacidade no comportamento das pessoas é o caso em que um *pendrive* USB é encontrado no estacionamento da empresa. O que um funcionário que encontrasse o *pendrive* faria? Será que ele reportaria o achado como um incidente de segurança? Ou ele inseriria o dispositivo em seu notebook para ver o seu conteúdo? Ele sabe que *pendrives* são um dos vetores de contaminação por *malware* mais perigosos? Como ele poderia saber que não ele não pode inserir um *pendrive* em equipamentos da empresa?

Dispositivos USB são a principal fonte de *malware* para sistemas de controle industrial. Esta técnica já foi utilizada para contaminar, por exemplo, uma usina nuclear que tinha uma rede isolada. O perigo dos dispositivos USB, que vão além de *pendrives*, é que o USB é

utilizado para conectar e carregar outros dispositivos, e também para injetar malwares, executar programas para criar ou criar conexões externas (PEREKALIN, 2019).

E você, como profissional de segurança e privacidade, o que faria para proteger a sua empresa contra este risco relacionado ao *pendrive*? O bloqueio das portas USB dos equipamentos da empresa pode servir como um controle de segurança técnico. Neste caso, você estaria implantando um controle de segurança técnico. Porém, esta medida de segurança deve ser bem avaliada, de acordo com o seu nível de risco, já que pode comprometer a produtividade da empresa.

Vale destacar que a segurança da informação é feita em camadas, com um conjunto de controles de segurança utilizados de uma forma integrada. O raciocínio aqui é que um controle de segurança pode funcionar para tratar um grande percentual dos riscos, porém para o pequeno percentual em que este controle de segurança possa falhar, outro controle de segurança o complementa.

No caso do *pendrive*, a principal camada de segurança poderia ser a conscientização dos usuários, com o intuito de prover aos usuários o conhecimento sobre os perigos do uso de dispositivos não autorizados. A crença do perigo real que um *pendrive* inserido em equipamentos da empresa pode ser incorporada no dia a dia da empresa neste processo de treinamento e conscientização, com técnicas que podem envolver vídeos ou campanhas que envolvem até mesmo representações teatrais. Todos devem entender que a empresa tem regras definidas na política de segurança que restringe o uso de *pendrive* e todos devem acreditar que os motivos são legítimos.

O hábito deve ser criado com a diligência da própria pessoa, mas também de todos que se encontram ao seu redor, lembrando-as dos perigos existentes em determinados comportamentos, criando assim uma atitude de segurança.

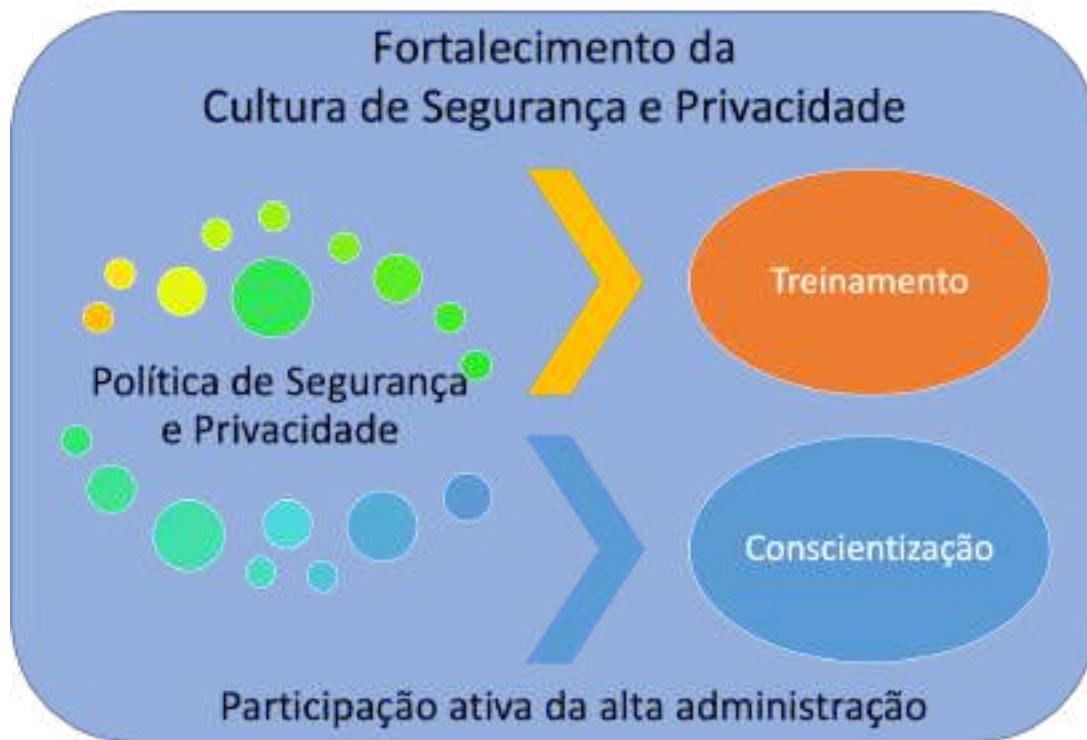
Um exemplo de criação de hábito e de consolidação de conhecimento de segurança é a simulação. Muito utilizado no caso de *phishing*, a simulação pode ser feita também espalhando-se pendrives com mensagens sobre a importância de se seguir a política de segurança da empresa.

O uso de *pendrives* deve estar definido na política de segurança da empresa e, com treinamentos e programas de conscientização, deve ser de conhecimento e deve ser aplicado por todos. O bloqueio USB dos equipamentos da empresa pode constituir uma camada adicional de segurança.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Um dos elementos primordiais para fortalecer uma cultura de segurança e privacidade é a política de segurança da informação e privacidade (AGUILERA-FERNADES, 2017). Com a definição formal de como a empresa enxerga e trata a segurança e privacidade, com base no seu contexto que inclui os riscos, a política de segurança e privacidade direciona a cultura da empresa. O que constrói a crença, o conhecimento e o hábito necessários é fazer com que as definições da política de segurança cheguem a todos. E o que reforça esta crença é a participação ativa da alta administração. Assim, a política de segurança, treinamentos e conscientização dos usuários são importantes para o fortalecimento da cultura de segurança e privacidade, como mostra a Figura 2.13.

Figura 2.13 | Fortalecimento da cultura de segurança e privacidade



Fonte: elaborada pelo autor.

Um passo importante para o sucesso da política de segurança e privacidade é que ela reflita, da melhor forma possível, as características de cada empresa. Ela deve ser plausível e deve ser aplicável, ou seja, a política deve definir as diretrizes a serem seguidas por todos, e deve definir controles de segurança que deverão ser efetivamente implementados. A Figura 2.14 apresenta as principais características da política de segurança e privacidade que fazem com que ela tenha sucesso na sua implantação. Elas serão discutidas a seguir.

Figura 2.14 | Política de segurança e privacidade: fazendo acontecer

Política de Segurança e Privacidade deve

Refletir as características da empresa

Ser plausível e aplicável

Estar organizada em uma série de documentos

Ser abrangente, principalmente com agentes externos

Ser organizada de acordo com o seu público-alvo

Estar acessível

Estar sempre atualizada

Ser comunicada regularmente

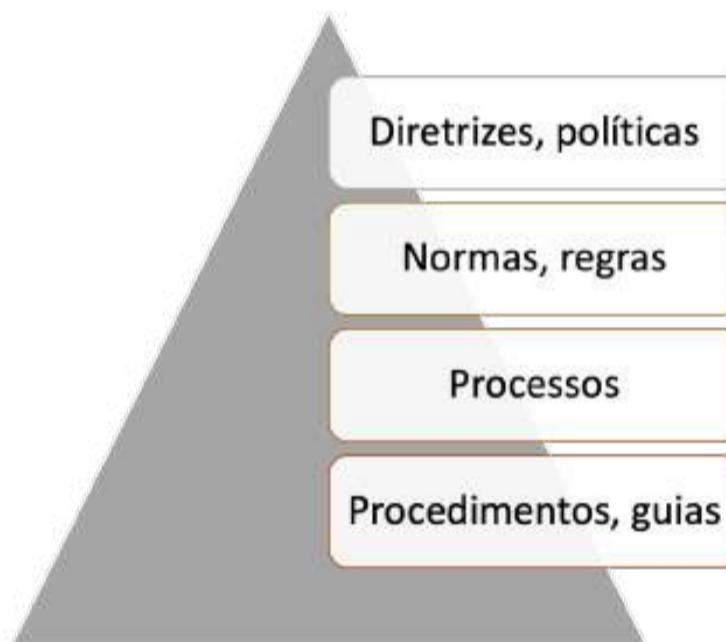
Fonte: elaborada pelo autor.

o

Lembre-se que políticas de segurança são compostas por documentos que incluem normas, diretrizes, processos, procedimentos, termos e guias, por exemplo (Figura 2.15). Assim, um fator crítico de sucesso da política de segurança da informação é a organização de todo o seu conteúdo, facilitando o seu acesso e sendo direcionada ao seu público-alvo.

Ver anotações

Figura 2.15 | Estrutura de documentos que formam a política de segurança da informação



Fonte: elaborada pelo autor.

O direcionamento da política de segurança e privacidade ao seu público-alvo está relacionado à organização do conteúdo e envolve ainda a forma como ela trata os funcionários diretos, prestadores de serviços e os fornecedores. Essa abrangência é essencial para minimizar as chances de ocorrência de incidentes de segurança, considerando, além dos usuários internos, também os agentes externos. Eles, muitas vezes, estão dentro da empresa, tanto física quanto digitalmente, e precisam também seguir a política de segurança e privacidade.

O tratamento da segurança e privacidade por agentes externos é um desafio, pois o nível de comprometimento é diferente, bem como o nível de cultura de segurança e privacidade de cada um. A pergunta que temos que fazer é se estes agentes externos também têm que ter ciência da política de segurança e privacidade da empresa, e em qual nível, comparado com os usuários internos. O que é reforçado na resposta a esta questão é que a organização da política de segurança e privacidade é, de fato, importante, e deve ser feita de modo a fazer com que os agentes externos tomem conhecimento da postura de segurança da empresa e se comprometam a seguir as diretrizes e as regras específicas. Para tanto, pode-se utilizar controles como termos e contratos, que fazem parte do próprio conjunto de documentos que formam a própria política de segurança.

Com o termo de ciência, os agentes externos, sejam eles prestadores de serviços ou fornecedores, que terão acesso à empresa, seja fisicamente ou logicamente, tomam conhecimento das regras de segurança e privacidade da empresa, que devem ser seguidas. A política de segurança e privacidade da empresa pode ser referenciada, mas somente os pontos relevantes para os agentes externos devem estar no termo de ciência, que deve ter pelo menos estes elementos:

- **Objetivo do termo de ciência**, com referência à política de segurança e privacidade da empresa.
- **Regras de segurança e privacidade**, com aspectos específicos da política que devem ser entendidos e seguidos pelos agentes externos. Um exemplo é a proibição de fotografias ou o acesso físico a dispositivos da empresa.
- **Papéis e responsabilidades**, com a inclusão de algum funcionário da empresa que será responsável pelo agente externo, devendo zelar pelo cumprimento da política de segurança e privacidade.

O cumprimento do termo de ciência e a sua conformidade pode e deve ser reforçado por controles de segurança. Um exemplo é o controle de acesso, seja físico ou lógico, que deve ser planejado adequadamente, com identificação que possibilite, de uma forma geral e o que é mais comum na maioria das empresas, a distinção entre funcionários e agentes externos, por conta de requisitos de segurança diferentes.

o

Ver anotações

ATENÇÃO

A assinatura do termo de ciência e responsabilidade por todos deve ser obrigatória e faz com que ninguém possa alegar que foi o pivô de um incidente de segurança ou privacidade por engano, ou porque não sabia que não poderia ter realizado determinadas ações que eram explicitamente contrárias à política de segurança e privacidade da empresa.

Além de ter que tratar de profissionais de naturezas diferentes que fazem parte da empresa, incluindo formas de contratação diferentes que envolvem riscos variados, outro ponto importante é a forma como os administradores de sistemas ou aqueles que possuem acesso privilegiado a variados recursos são tratados na política de segurança e privacidade. Isto reflete principalmente na organização da documentação. As regras de segurança para usuários e as regras para administradores de sistemas podem estar em um mesmo documento, porém cada empresa deve avaliar a sua efetividade. Por exemplo, regras de senhas para o acesso a sistemas, utilizados por usuários, podem definir a sua troca a cada 12 meses, e devem ter no mínimo 8 caracteres. Porém, para o acesso privilegiado de administração de sistemas, regras mais rígidas devem ser adotadas, como a troca de senhas a cada 6 meses e o mínimo de 12 caracteres, por exemplo. Deste modo, uma melhor organização pode ser um documento específico com a norma de senhas para usuários em um documento, e a norma de

senhas para administração de sistemas em um outro documento, de modo que cada documento que compõe a política de segurança e privacidade tenha o seu público-alvo (NAKAMURA & GEUS, 2007).

A política de segurança e privacidade deve existir, mas, principalmente, deve estar disponível e ser constantemente atualizada e comunicada para todos os envolvidos. O fortalecimento de uma cultura de segurança passa pela percepção que os envolvidos têm da própria empresa quanto à forma como a segurança da informação e a privacidade são tratadas. A existência da política de segurança e privacidade indica que há uma preocupação da empresa. Porém, a falta de comunicação e de atualização, que devem ser feitas segundo o processo de melhoria contínua definido no Sistema de Gestão de Segurança da Informação (SGSI), faz com que a percepção seja de que a segurança e privacidade não são tão importantes para a empresa. O reflexo desta percepção é direto e negativo, fazendo com que todos relaxem quanto às suas próprias atitudes, já que percebem que a própria empresa não cuida da segurança e privacidade como deveria.

TERMO OU CONTRATO DE CONFIDENCIALIDADE

A política de segurança e privacidade deve ser conhecida por todos e todos devem ter a percepção de que o que está lá definido é sempre atualizado de acordo com as circunstâncias de negócios. Um papel importante nisto é o da alta administração, que deve zelar pela proteção dos objetivos de negócio da empresa, que envolve cada vez mais a segurança e a privacidade.

Além destes aspectos da política de segurança, um outro instrumento é importante para o dia a dia das empresas: o termo ou contrato de confidencialidade, que é essencial principalmente nas relações de negócios que existem entre diferentes organizações.

O termo ou contrato de confidencialidade geralmente é utilizado quando há troca de informações, como em prestação de serviços, discussões em que há a necessidade de detalhes da empresa, ou em consultorias. O termo ou contrato de confidencialidade garante que há o acesso a informações importantes para a realização da atividade, porém todo o conteúdo deve ser preservado e ser restrito somente à execução das atividades, não podendo ser utilizado posteriormente, e nem divulgado para terceiros. Assim, este documento é essencial para as relações entre empresas. Você deve ter a responsabilidade com as informações quando tem acesso a informações sensíveis, e você deve exigir o mesmo quando disponibiliza informações críticas de sua empresa para terceiros.

É importante destacar que os termos e contratos, como os de ciência ou de confidencialidade, são importantes para deixar explícito os objetivos e as preocupações com a segurança e privacidade, constituindo instrumentos importantes para as operações de segurança da informação. Eles têm valor legal, sendo essencial principalmente após um incidente de segurança como um vazamento de informações, que pode estar infringindo um contrato de confidencialidade.

REFLITA

Um outro instrumento importante para as organizações é o **código de ética**, que vai além de aspectos de segurança e privacidade, o qual tem o intuito de moldar o caráter e os costumes individuais dos colaboradores da empresa.

Geralmente este instrumento é de responsabilidade da área de conformidade ou recursos humanos. A ética significa moral, sendo composta pelo caráter, disposição e hábito.

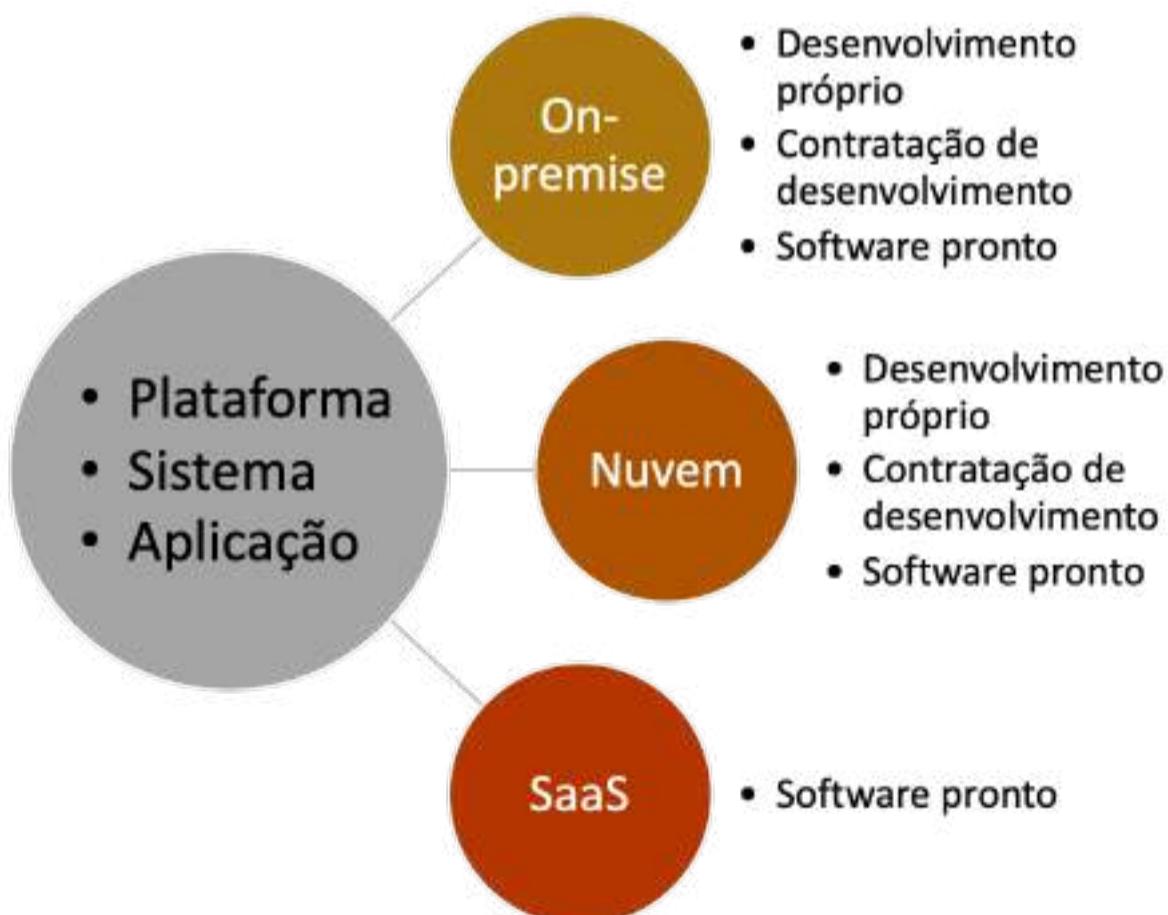
Você considera que a ética é suficiente em segurança e privacidade? Ou são necessários outros instrumentos com valores legais, como os termos e contratos?

SEGURANÇA DA INFORMAÇÃO NA AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS

Um dos papéis mais importantes do profissional de segurança da informação é fazer com que os sistemas, plataformas ou aplicações de *software* sejam adotados pela empresa de uma forma segura (ISO 27002, 2013). Há diferentes alternativas de software para as empresas, como pode ser visto na Figura 2.16. Ele pode ser adquirido, pode ser implementado internamente com uma equipe própria, ou pode ter o seu desenvolvimento adquirido. Além disso, o software pode funcionar no próprio ambiente da empresa (*on premises*) ou na nuvem privada (*cloud*). Além disso, o software pode estar sendo utilizado como serviço, no modelo em que o ambiente é de total responsabilidade do fornecedor (*Software-as-a-Service, SaaS*). Essas alternativas refletem diretamente em como a segurança e privacidade devem ser tratadas por sua empresa, principalmente quanto às responsabilidades (BROOK, 2020).

Ver anotações

Figura 2.16 | Alternativas de softwares na empresa



Fonte: elaborada pelo autor.

Independente do modelo de adoção de *softwares* da empresa, é preciso a adoção do ciclo de desenvolvimento seguro, que define como a empresa adquire ou desenvolve *softwares* de uma forma segura.

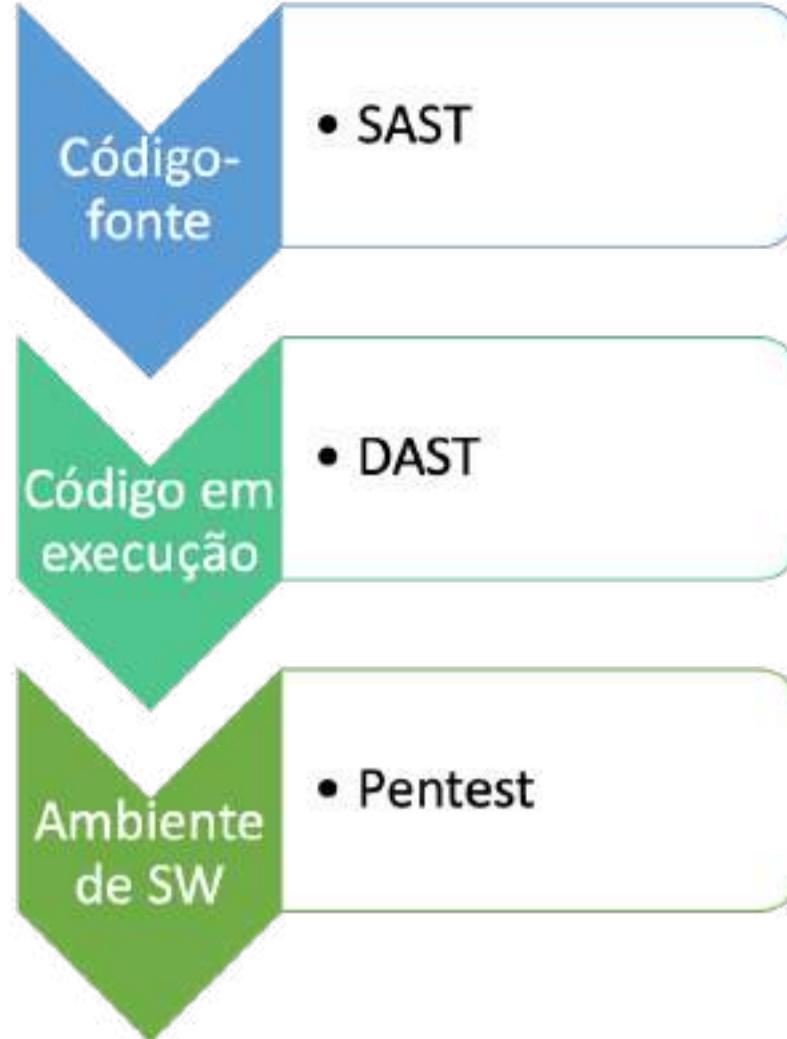
No caso de desenvolvimento próprio e contratação de desenvolvimento, as ações necessárias serão discutidas mais à frente. A diferença entre as duas abordagens é que, no caso da contratação de desenvolvimento, deve-se negociar com a empresa que irá desenvolver o sistema as responsabilidades em cada etapa do desenvolvimento, deixando tudo claro em contrato.

As análises de segurança são fundamentais, em diferentes níveis, como pode ser visto na Figura 2.17: no código-fonte, que deve ser analisado em análise estática ou *Static Analysis Security Testing* (SAST); no software em execução, que deve ser analisado em análise dinâmica ou *Dynamic Analysis Security Testing* (DAST) (KOUSSA, 2018); ou no ambiente de *software*, em que todos os componentes, incluindo as redes, devem ser analisadas com testes de penetração (*penetration testing, pentest*). Estes testes de segurança são importantes também para a auditoria de sistemas, e iremos discutir estes testes em mais detalhes nas próximas unidades da disciplina.

ASSIMILE

SAST deve ser aplicado no código-fonte, e é importante para remover as vulnerabilidades do código antes de o *software* entrar em produção. O DAST também deve ser realizado antes de o *software* entrar em produção, e o teste é com o *software* funcionando, testando-se as interfaces existentes. Há ainda um teste de segurança conhecido como IAST (*Interactive Application Security Testing*), que faz os testes de segurança de uma forma interativa, combinando os testes estáticos e dinâmicos (SAST e DAST).

Figura 2.17 | Análises de segurança em diferentes níveis



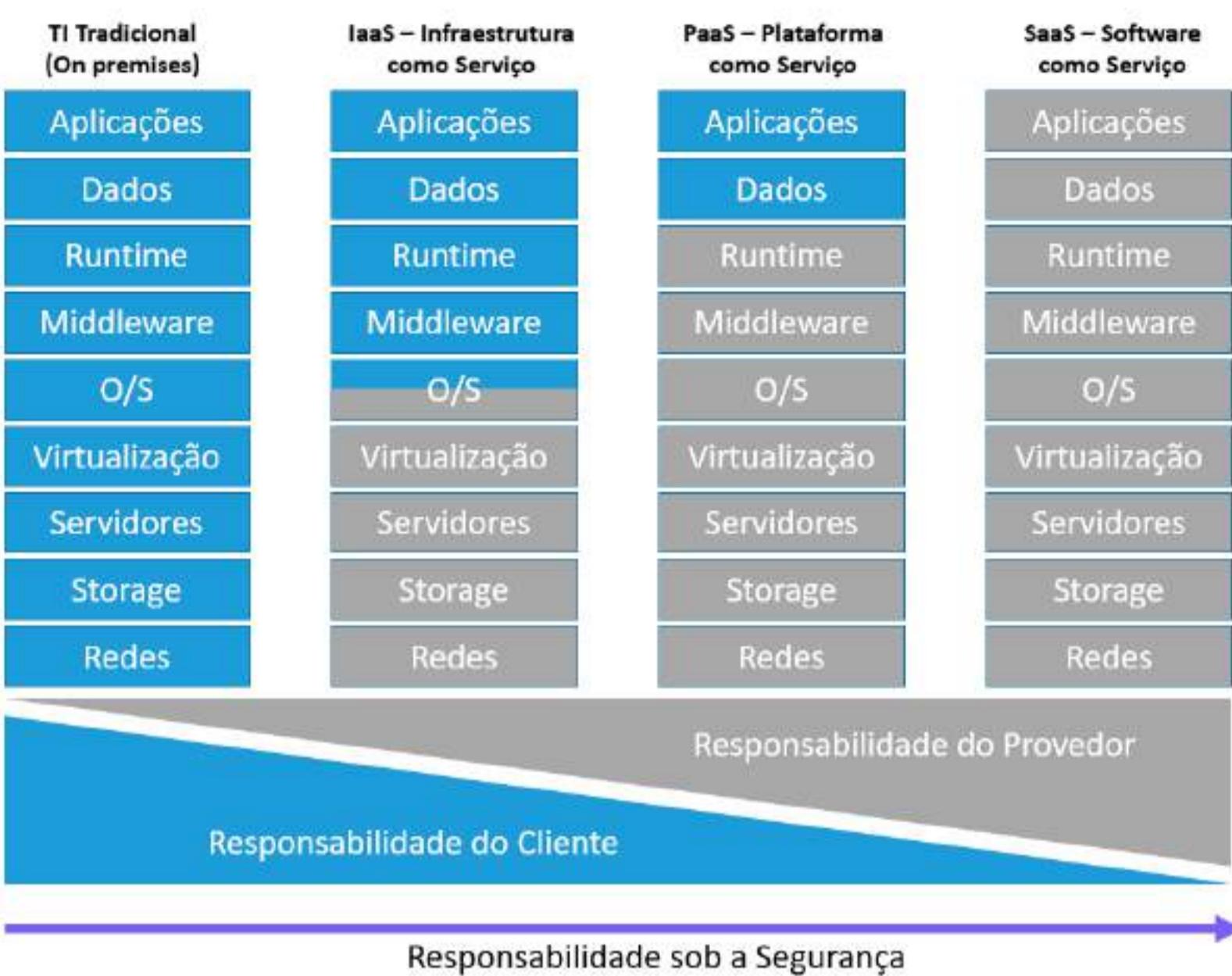
Fonte: elaborada pelo autor.

Quanto às responsabilidades da empresa em cada modelo adotado para as plataformas, a Figura 2.18 apresenta um resumo dos elementos que estão sob responsabilidade do provedor de serviços e quais são de responsabilidade da empresa. No modelo *on premises*, a responsabilidade de todos os elementos é da própria empresa: aplicações, dados, execução (*runtime*), *middleware*, sistema operacional (O/S), virtualização, servidores, armazenamento (*storage*) e redes. Do lado oposto, no SaaS, o fornecedor ou provedor do software como serviço é o responsável por toda a segurança daquele *software*.

No modelo PaaS, o que o fornecedor ou provedor oferece é a plataforma de computação, com a aplicação e os dados sendo de responsabilidade da empresa. Neste caso, os sistemas operacionais e o *middleware* são de responsabilidade do provedor.

Já no modelo IaaS, a empresa contrata a infraestrutura como serviço, o que inclui as redes, armazenamento, virtualização e parte do sistema operacional. A empresa deve, neste caso, cuidar da segurança do sistema operacional, *middleware*, ambiente de execução, dados e aplicações.

Figura 2.18 | Responsabilidades de segurança em diferentes ambientes



Fonte: Jornada (2020).

Ver anotações

AMBIENTE DE DESENVOLVIMENTO SEGURO

Para o desenvolvimento de *software*, deve-se levar em consideração alguns aspectos importantes. Um deles é o uso de dados para testes de software, incluindo o desenvolvimento de tecnologias de inteligência artificial. A segurança dos dados utilizados para homologação de sistemas sempre foi uma preocupação, de modo que em muitos casos dados reais são compilados ou uma base de dados de testes é desenvolvida especialmente para o desenvolvimento de *software*. Isto é normalmente feito porque há a preocupação do compartilhamento de dados sensíveis para toda a equipe de desenvolvimento, e também a possibilidade de vazamento destes dados a partir do ambiente de desenvolvimento, testes e homologação.

Outro fator importante é o uso de dados pessoais, que devem ser protegidos de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD), o que influencia primeiramente no seu uso durante o desenvolvimento, e também impacta fortemente para a segurança, já

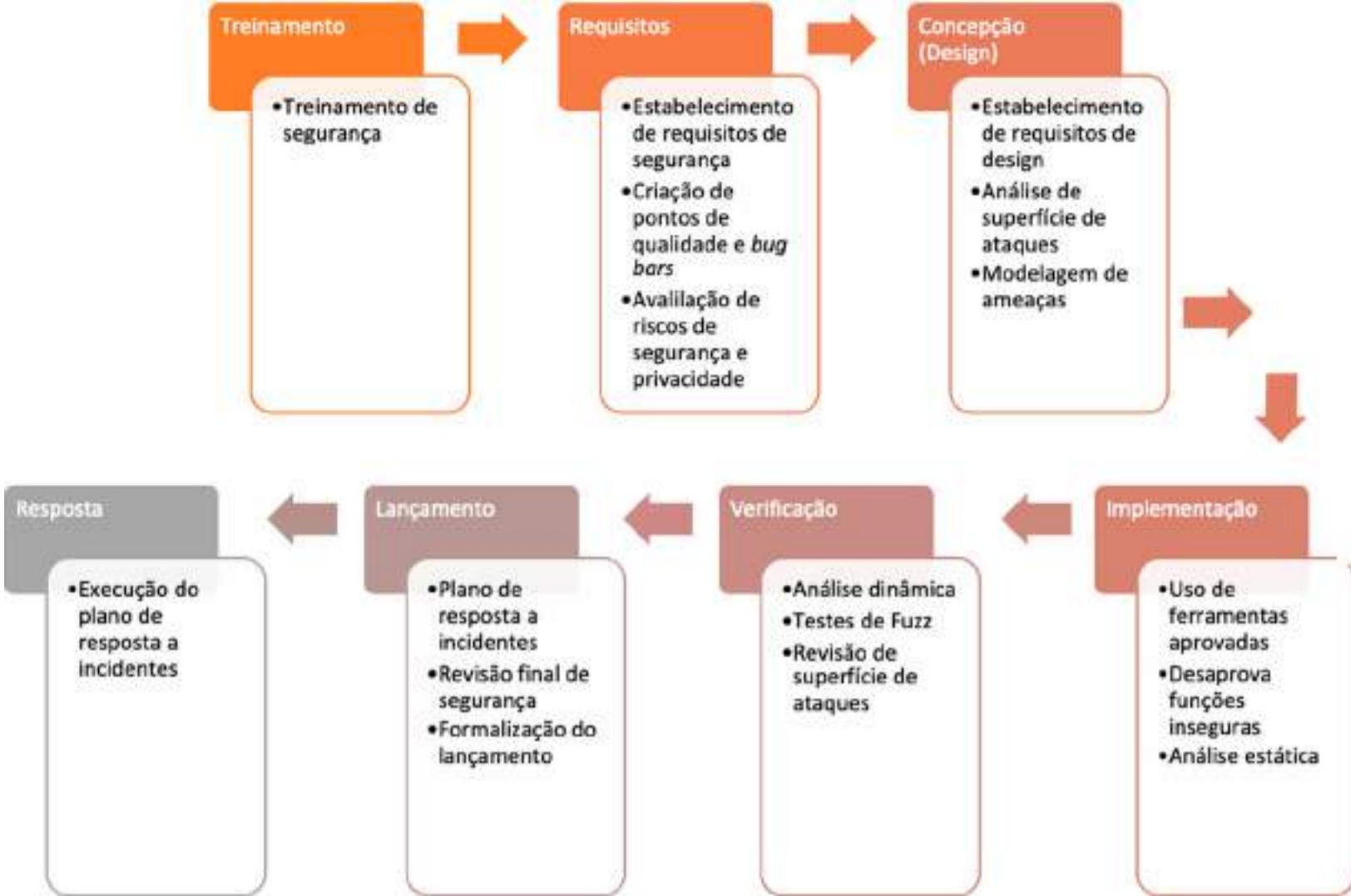
que em caso de vazamento decorrente de um incidente de segurança, há sanções previstas na lei. Assim, as empresas devem desenvolver softwares que não sejam a fonte de vazamento de dados pessoais, seja na própria empresa ou nos clientes que utilizam o *software* da empresa. Em caso de incidente de segurança, há a responsabilização legal e também a corresponsabilidade caso um vazamento ocorra em uma empresa e o seu *software* seja a fonte do incidente.

•
Ver anotações

O desenvolvimento seguro é, assim, fundamental. O objetivo é minimizar as vulnerabilidades e as brechas que podem ser exploradas nos softwares (NAKAMURA, 2016). Quanto antes as falhas forem identificadas, menores os custos de reparação.

O ciclo de vida de desenvolvimento seguro envolve elementos de segurança desde o princípio do desenvolvimento, incluindo o treinamento de segurança e o estabelecimento de requisitos de segurança, criação de pontos de qualidade e avaliação de riscos de segurança e privacidade. Como mostra a Figura 2.19, o desenvolvimento seguro ainda considera a segurança na concepção do *software*, que deve considerar a superfície de ataques e modelagem de ameaças. Um ponto importante é que a segurança não é apenas para evitar vulnerabilidades, mas também para incluir funções de segurança e para minimizar pontos de ataques que podem estar relacionados com a forma como o software iria funcionar. A implementação do *software* envolve o uso de ferramentas aprovadas, cuidados com funções inseguras e a análise de código. O software passa então pela verificação, com análise dinâmica, até chegar ao lançamento, que deve considerar o plano de resposta a incidentes. Este plano é fundamental para ser acionado em caso de incidente de segurança, tornando a resposta ágil e efetiva em situações de crise.

Figura 2.19 | Ciclo de vida de desenvolvimento seguro



Fonte: adaptado de Lipner (2010).

Uma das principais fontes de informações de segurança em aplicações é a *Open Web Application Security Project*, OWASP (OWASP, 2020). Há diferentes informações e projetos, como um *framework* de segurança, ferramenta de testes de segurança e modelo de maturidade de software. É recomendado que desenvolvedores e profissionais de segurança da informação sigam o OWASP Top 10, que indica os riscos mais comuns que devem ser evitados. Elas estão relacionadas na Figura 2.20.

Figura 2.20 | OWASP Top 10, com as principais vulnerabilidades que devem ser evitadas



Fonte: adaptado de OWASP (2020).

Cada um dos tópicos é descrito a seguir:

- **Falhas de injeção**, como no SQL, NoSQL, sistema operacional e LDAP. Dados não confiáveis são enviados como parte de um comando ou consulta;
- **Autenticação quebrada**, incluindo o gerenciamento das sessões, que possibilita o acesso a senhas, credenciais de acesso ou sessões;
- **Exposição de dados sensíveis**, que podem vaziar durante a transmissão e armazenamento;
- ***XML External Entities (XXE)***, em que há o acesso a entidades externas por documentos XML mal configurados, o que abre um leque de possibilidades de ataques;
- **Controle de acesso quebrado**, com falha nas restrições de privilégios e possibilitam acessos desnecessários;
- **Má configuração de segurança**, que fornece informações que podem ser utilizadas em ataques, e abrem acessos a informações e

funções que não deveriam;

- **Cross-Site Scripting XSS**, que possibilita a execução de códigos diretamente no navegador da vítima, devido à falta de validações dos dados processados;
- **Desserialização insegura**, que pode resultar em ataques que incluem ataques replay, ataques de injeção, escalada de privilégios e execução de código remoto;
- **Uso de componentes com vulnerabilidades conhecidas**, incluindo bibliotecas, *frameworks* e outros módulos de *software* que têm os mesmos privilégios da aplicação;
- **Registro e monitoramento insuficiente**, que dificulta a detecção e resposta a incidentes de segurança.

SAIBA MAIS

Um conceito importante no desenvolvimento de sistemas é o DevSecOps. No modelo *shift-left* da esteira de desenvolvimento, considerando os custos de correção de *softwares*, o objetivo é fazer os testes e as validações de segurança desde o início do desenvolvimento. No DevSecOps, há o empoderamento dos desenvolvedores, que passam a fazer, junto com a equipe de segurança e utilizando ferramentas de segurança, os testes e validações de segurança em todas as etapas do desenvolvimento. O DevSecOps é importante no modelo de desenvolvimento atual, que adota metodologia ágeis e necessita seguir as práticas de segurança que vai do treinamento ao processo de resposta a incidentes.

| TENDÊNCIAS E FUTURO

Segurança da informação é uma das áreas mais dinâmicas, com uma evolução que acompanha a forma como o mundo é moldado. A informação sempre precisou ser protegida. E, com a digitalização, o

desafio aumentou.

É necessário estar atento para entender os avanços que são introduzidos na sociedade e que tratam fundamentalmente da informação, o que por sua vez leva à necessidade de segurança e privacidade. Algumas destas tendências em andamento e que estão moldando o futuro são apresentadas a seguir:

- **Transformação digital** (MARTINS, 2019), em que há a convergência entre pessoas, tecnologias, coisas e cidades, em busca de eficiência operacional, novos modelos de negócios, melhor experiência do usuário e segurança operacional. Com isso, atividades, processos, negócios e operações ampliam as conexões e o uso de tecnologias, que refletem na maior complexidade de proteção, já que há ampliação do espectro de impacto, com um incidente de segurança tornando-se cada vez mais crítico.
- **Fusão físico-humano-digital** (LIMA, 2020), em que há o aumento gradual da integração entre esses elementos, com impactos cada vez mais interligados. Um incidente de segurança em um dispositivo da Internet das Coisas (*Internet of Things*, IoT) pode afetar as operações de uma fábrica, causar o caos em cidades, afetar infraestruturas críticas como a de energia ou telecomunicações, e até mesmo levar à perda de vidas humanas, resultantes da dependência incremental de equipamentos médicos conectados. Pode ser até mesmo que em um futuro próximo os humanos estarão conectados diretamente, de uma forma intrínseca, e os aspectos de segurança e privacidade são fundamentais para que isso se torne realidade.
- **Novas tecnologias emergentes** (GARTNER, 2020), que só se tornarão viáveis se forem também seguros. Alguns exemplos de tendências tecnológicas são (i) o eu digital (digital me) com a representação digital das pessoas, (ii) a arquitetura composta que possibilita respostas rápidas para as mudanças constantes dos

negócios construídos com o uso de uma malha de dados flexível, (iii) a inteligência artificial formativa que possibilita mudanças dinâmicas para responder às variações situacionais, (iv) a confiança algorítmica para garantir a privacidade e a segurança dos dados, fonte de ativos e identidade de indivíduos e coisas, e (v) o uso de novos materiais como computação em DNA, sensores biodegradáveis e transistores baseados em carbono.

Assim como há a evolução observada com a transformação digital, fusão físico-humano-digital e as novas tecnologias emergentes, a área de segurança da informação e privacidade também continua a avançar a passos largos. Algumas tendências nessa área são (Figura 2.21):

- **Segurança em nuvem** (GARTNER, 2020), incluindo segurança de conexões e acesso remoto ou *Secure Access Service Edge* (SASE), que considera a distribuição e a necessidade de tratar os dispositivos como de confiança zero (*zero trust network access*) e o uso de mecanismos de virtualização de redes. Há ainda a necessidade de controle de acesso mais adequado ao ambiente de múltiplos provedores de nuvem e da necessidade de proteção de dados, e um dos caminhos é o uso de *security brokers*.
- **Confiança algorítmica** (GARTNER, 2020), que visa tratar de uma forma mais eficiente a segurança e privacidade necessária decorrente do aumento da exposição de dados, de notícias e vídeos falsos e do uso tendencioso da inteligência artificial. Fazem parte desta tendência a proteção dos dados, a garantia de procedência de ativos com o uso de *blockchain* e a identidade e autenticação de pessoas e coisas.
- **Segurança cognitiva** (MELORE, 2018), com a integração da inteligência artificial para a prevenção, detecção e resposta de incidentes de segurança. O aumento da complexidade dos ambientes e também da quantidade de dados para análise faz com que o aprendizado contínuo com algoritmos de inteligência artificial

possibilite não somente a detecção mais assertiva de ataques, como também possibilita uma resposta mais rápida que limita ataques em andamento.

Figura 2.21 | Grandes tendências que estão moldando o futuro



Fonte: elaborada pelo autor.

O futuro também nos mostra as ameaças emergentes (Figura 2.22), que deverão ser tratadas. Uma evolução natural das ameaças é o uso de ataques cibernéticos para fins políticos e militares, como um instrumento de instabilidade. Já citamos aspectos relacionados a impactos em fábricas e cidades decorrente da fusão físico-humano-digital, que leva também a problemas que impactam diretamente os seres humanos. Assim, se antes os incidentes de segurança afetavam as pessoas e as empresas, já há algum tempo os alvos são cidades, países, infraestruturas críticas, fábricas e pessoas. Os impactos estão cada vez mais críticos.

Além disso, os *malwares* estão cada vez mais avançados, como os *ransomwares* (BLACKFOG, 2020), que continuam a fazer cada vez mais vítimas, e deixaram de apenas cifrar os dados, realizando também o vazamento, o que amplia muito os impactos envolvidos, deixando de ser somente a disponibilidade, envolvendo agora também a confidencialidade.

Os avanços tecnológicos também são utilizados pelos criminosos, e o uso da inteligência artificial para os ataques cibernéticos, por exemplo, estão em curso. Isto, por um lado, possibilita uma automatização dos ataques, e do outro lado, reforça a assertividade dos ataques direcionados.

E um outro ponto de atenção é o abuso das identidades digitais, que tende a crescer ainda mais com os avanços da vida digital de pessoas e empresas.

Figura 2.22 | Ameaças emergentes



Fonte: elaborado pelo autor.

PESQUESE MAIS

Para o desenvolvimento de aplicações em nuvem, há um conjunto de recomendações de segurança, que podem ser vistos no Capítulo 6 do livro Aplicativos em nuvem (PETCOV, 2017). Há requisitos de segurança do *The Open Group*, do *Cloud Standards Consumer Council* (CSCC), *Cloud Security Alliance* (CSA) e ISACA. Dentre as boas práticas de segurança

no desenvolvimento de aplicações, são citadas o ambiente de desenvolvimento seguro, uso de métodos seguros no desenvolvimento, revisão de códigos em busca de brechas, e uso do ciclo de desenvolvimento seguro (*Security Development Lifecycle, SDL*).

PETCOV, R. **Aplicativos em nuvem.** São Paulo: Senac São Paulo, 2017.

Assim, chegamos ao final desta seção, em que vimos que o fortalecimento da cultura de segurança e privacidade passa por elementos que incluem a política de segurança e privacidade, o treinamento, a conscientização e a participação ativa da alta administração. Vimos também que o ambiente de desenvolvimento seguro é importante, e há vários aspectos a serem considerados. Por fim, é importante reforçar que o mundo evolui, o que inclui também a segurança e privacidade. Apesar do constante surgimento de novas tecnologias de segurança, ainda há muitas ameaças que precisam ser tratadas. É um vasto mundo de oportunidades, que nós construiremos.

Até a próxima aula!

FAÇA VALER A PENA

Questão 1

A cultura de segurança e privacidade de uma empresa depende de todos e só pode ser fortalecida se todos fizerem a sua parte e cumprirem o seu papel, com diligência e uma postura que visa a proteção.

Assinale a alternativa que contém o elemento considerado um fator para fortalecer a cultura de segurança e privacidade da empresa.

a. Usar o melhor *firewall* de mercado.

b. Utilizar criptografia.

c. Manter em segredo a política de segurança e privacidade.

d. Usar esteganografia.

e. Disseminar a política de segurança e privacidade.

Questão 2

Considere a política de segurança e privacidade, que deve ser disseminada e seguida por todos os usuários. Ela é parte importante do fortalecimento da cultura de segurança e privacidade das empresas.

Dentre os seguintes elementos:

- I. Ser plausível e aplicável.
- II. Ser abrangente, principalmente com agentes externos.
- III. Estar sempre atualizada.
- IV. Ser comunicada regularmente.

Sobre os elementos que melhoram a política de segurança e privacidade e reforçam a percepção de que a empresa está vigilante, é correto o que se afirma em:

a. I e II, apenas.

b. II e III, apenas.

c. II e IV, apenas.

d. I, II e III, apenas.

e. I, II, III e IV.

Questão 3

Os ataques cibernéticos são executados com a exploração de vulnerabilidades. As aplicações são grandes fontes de vulnerabilidades, e um ciclo de vida de desenvolvimento seguro é essencial para que as vulnerabilidades possam ser tratadas adequadamente.

Assinale a alternativa em que os todos os elementos citados fazem parte do ciclo de vida de desenvolvimento seguro.

a. Análise estática, análise dinâmica e firewall.

b. Modelagem de ameaças, uso de ferramentas aprovadas e firewall.

c. Pentes, resposta a incidentes e *firewall*.

d. Análise estática, análise dinâmica e *pentest*.

e. Modelagem de ameaças, *pentest* e conscientização e usuário

REFERÊNCIAS

ABNT. **ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.**

AGUILERA-FERNANDES, E. **Padrões, Normas e Política de Segurança da Informação.** São Paulo: Editora Senac São Paulo, 2017. Disponível em: <https://bit.ly/2MlbGtB>. Acesso em: 9 dez. 2020.

BLACKFOG. **The State of Ransomware in 2020.** Disponível em: <https://bit.ly/308spcy>. Acesso em: 8 nov. 2020.

BROOK, C. Differences Among InfoSec Cloud Delivery Models (IaaS, SaaS, and PaaS) – and How to Choose. **Data Insider**, 11 ago. 2020. Disponível em:

<https://bit.ly/386EhAp>. Acesso em: 9 dez. 2020.

COACHMAN, E. **Segurança da Informação.** São Paulo: Pearson Education. 2010. Disponível em: <https://bit.ly/3uTE656>. Acesso em: 9 dez. 2020.

GARTNER Inc. **Gartner Identifies Five Emerging Trends That Will Drive Technology Innovation for the Next Decade.** 18 ago. 2020. Disponível em: <https://gtnr.it/3sNrbjy>. Acesso em: 8 nov. 2020.

GARTNER Inc. **Top Actions From Gartner Hype Cycle for Cloud Security, 2020**, 27 ago. 2020. Disponível em: <https://gtnr.it/3rhclvH>. Acesso em: 8 nov. 2020.

HICKEN, A. Parasoft, 15 set. 2016. Disponível em: <https://bit.ly/3qdB9Jd>. Acesso em: 2 nov. 2020.

JORNADA para Nuvem. **Os 6 pilares fundamentais para sua longa e única Jornada para Nuvem.** Disponível em: <https://bit.ly/30bgqLq>.

Acesso em: 7 nov. 2020.

KASPERSKY. **Um breve histórico dos vírus de computador e qual será seu futuro.** Disponível em: <https://bit.ly/3uUmNRk>. Acesso em: 8 nov. 2020.

KOUSSA, S. **What Do Sast, Dast, last And Rasp Mean To Developers?** 2 nov. 2018. Disponível em: <https://bit.ly/3kJLIYA>. Acesso em: 9 dez. 2020.

LIMA, A. R. 4^a revolução industrial e as mudanças no mercado de trabalho. **DMT**, 16 mar. 2020. Disponível em: <https://bit.ly/387yytU>. Acesso em: 8 nov. 2020.

LIPNER, S. The Security Development Lifecycle. Microsoft Corporation. **The OWASP Foundation**, 24 jun. 2010. Disponível em: <https://bit.ly/3uRFJAo>. Acesso em: 2 nov. 2020.

MARTINS, H.; DIAS, Y. B.; CASTILHO, P.; LEITE, D. Transformações digitais no Brasil: insights sobre o nível de maturidade digital das empresas no país. **McKinsey & Company**. Disponível em: <https://mck.co/3rgBfku>. Acesso em: 8 nov. 2020.

MELORE, M. The Future of Cognitive Security Is Now. **Security Intelligence**. Disponível em: <https://ibm.co/387cxLP>. Acesso em: 8 nov. 2020.

MICROSOFT Corporation. **What are the Microsoft SDL practices?** Disponível em: <https://bit.ly/3bXGWxx>. Acesso em: 2 nov. 2020.

NAKAMURA, E. T., GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

NAKAMURA, E. T. **Segurança da Informação e de Redes**. Belo Horizonte: Editora e Distribuidora Educacional S.A., 2016.

Disponível em: <https://bit.ly/3q7BLjy>. Acesso em: 8 nov. 2020.

PEREKALIN, A. Dispositivos USB usados como vetor de ataque.

Kaspersky Daily, 24 abr. 2019. Disponível

em: <https://bit.ly/2Ooh31q>. Acesso em: 3 nov. 2020.

STREICHSBIER, S. The State of DevSecOps. **DevOpsDays Jakarta**, 2019.

Disponível em: <https://bit.ly/3re5FUt>. Acesso em: 2 nov. 2020.

FOCO NO MERCADO DE TRABALHO

CULTURA DE SEGURANÇA

Emilio Tissato Nakamura

Ver anotações

FORTALECIMENTO DA CULTURA DE SEGURANÇA E PRIVACIDADE

Os elementos fundamentais para o fortalecimento da cultura de segurança e privacidade são as definições da política de segurança, os treinamentos, a conscientização dos usuários e a participação ativa da alta administração.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Você é o gerente de processos de segurança da empresa e deverá obter informações com seus pares, os gerentes de governança de segurança e de tecnologias de segurança. O seu papel é chave, pois a empresa depende da definição e implementação de controles de segurança que integram os aspectos de pessoas, processos e tecnologias.

Na apresentação, o primeiro ponto tratado, sobre a cultura de segurança e privacidade da empresa, explice que, para que ela seja forte, todos devem fazer a sua parte.

Mostre que vocês estão com um plano de treinamento e conscientização e que a política de segurança e privacidade está quase finalizada. Reforce que há o apoio, mas que o diretor de segurança da informação deve buscar a participação ativa da alta administração, que está planejada nas ações de treinamento e conscientização.

Sobre a política de segurança e privacidade, mostre que há a definição de como a empresa deve tratar os agentes externos, que consta em uma norma específica. As definições envolvem as regras para o acesso físico e lógico de fornecedores e prestadores de serviço. Um ponto importante é o uso de termos e contratos de ciência e de confidencialidade. Reforce que os trabalhos só podem ser iniciados pelos agentes externos após a assinatura dos documentos. Indique que este é um dos pontos importantes do treinamento e conscientização, já que todos os funcionários de todos os locais devem conhecer e cumprir o que está definido na política de segurança e privacidade. Você pode aplicar um questionário para validar se o treinamento em segurança foi proveitoso para os colaboradores. Para avaliar a eficácia do processo, podem ser utilizadas métricas de treinamento, como o número de colaboradores treinados e a média obtida nos questionários. Mostre otimismo com o andamento deste assunto, pois isso contribuirá efetivamente para o fortalecimento da cultura de segurança e privacidade da empresa.

Já sobre como as definições de segurança para os usuários e os administradores de sistemas, mostre uma visão de riscos que deixa claro as diferenças entre os dois acessos. No caso de senhas, por exemplo, o roubo de identidade de um usuário é crítico, porém no caso das credenciais do administrador de sistemas, os impactos são muito maiores, o que exige controles de segurança diferenciados. Cite a política de senhas definidas para os usuários e para os administradores de sistemas.

Na sua apresentação, faça um relato sobre a organização da política de segurança e privacidade. Mostre que as diretrizes gerais, como a definição das responsabilidades gerais em proteger a confidencialidade, integridade e disponibilidade das informações, estão definidas na política, enquanto os assuntos são tratados em normas específicas, como é o caso da norma de senhas. Relate que, além desta organização,

o público-alvo também foi considerado, ou seja, agentes externos têm uma documentação própria e direcionada, e os usuários internos não precisam ler detalhes destinados aos agentes externos.

Sobre a segurança no desenvolvimento de sistemas, considere que a empresa segue o modelo SaaS, com a contratação de serviços. Reforce, no entanto, que análises de segurança são feitas para a definição e homologação dos fornecedores e provedores dos serviços.

Para finalizar, faça uma comparação entre os modelos de desenvolvimento de sistemas em que a equipe de desenvolvimento é da empresa e disponibilizado *on premises*, em provedor de nuvem IaaS e em provedor de nuvem PaaS.

AVANÇANDO NA PRÁTICA

EQUIPE DE DESENVOLVIMENTO PRÓPRIO E CONTRATAÇÃO DE PROVEDOR DE NUVEM

Sua empresa tem uma equipe dedicada que está desenvolvendo um sistema crítico. Ultimamente, a diretoria executiva está preocupada, pois vários ataques cibernéticos estão ocorrendo em empresas do setor, e eles solicitaram uma avaliação sobre como a segurança está sendo tratada neste desenvolvimento. A diretoria executiva também quer saber qual o modelo de contratação de nuvem foi feito, e as implicações de segurança, entre o modelo de infraestrutura como serviço (IaaS) e plataforma como serviço (PaaS).

Ver anotações

RESOLUÇÃO



Prepare um relatório indicando o ciclo de vida de desenvolvimento seguro de *software* adotado pela empresa, incluindo elementos como os requisitos de segurança desde a concepção, e testes de segurança de análise estática (SAST) e de análise dinâmica (DAST). Além disso, apresente a modelagem da superfície de ataques e de ameaças que foi considerado, justificando as medidas de segurança que estão sendo implementadas. Mostre que, antes de o sistema ir para o ambiente de produção, estão previstos *pentests*.

Sobre o modelo de contratação de nuvem, mostre as responsabilidades de segurança envolvidos no IaaS e no PaaS.

Apresente as responsabilidades de sua equipe de segurança. Por fim, faça uma matriz de responsabilidades de sua equipe e dos provedores de nuvem, justificando as razões pela escolha pelo IaaS, contando com a sua equipe capacitada a executar as atividades necessárias de segurança.

NÃO PODE FALTAR

ARMAZENAMENTO DE DADOS

Emilio Tissato Nakamura

Ver anotações 0

O VALOR DA INFORMAÇÃO E SUA PROTEÇÃO

Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos (ISO 27002, 2013).



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

PRATICAR PARA APRENDER

Olá, aluno, nesta seção você irá se aprofundar na proteção de dados, partindo do entendimento entre o dado e a informação. Entender os dados é importante porque eles são armazenados em ativos de TI, e são a base para a informação, que por sua vez é a base para o conhecimento. Como têm valor, devem ser protegidos. E a proteção não é simples, já que os dados e a informação existem em meios físicos, como no papel, em meios digitais, como em banco de dados e, ainda, na cabeça das pessoas. Para tornar a vida do profissional de segurança e privacidade mais complexa ainda, os dados e a informação existem em estados diferentes: em transmissão, em processamento ou em armazenamento.

Com a Lei Geral de Proteção de Dados Pessoais, a LGPD, o entendimento sobre estes aspectos ganha ainda mais importância. O foco da LGPD é nos dados pessoais, mas o que você irá ver aqui se aplica também a outros tipos de dados, como os confidenciais e secretos.

E a proteção dos dados vai além do uso da criptografia, a qual apresenta vários desafios de aplicação, principalmente com relação à gestão de chaves criptográficas, que podem estar com o usuário, com a aplicação ou com o banco de dados. Além da criptografia, há mecanismos como a anonimização, pseudonimização e mascaramento de dados. E o ciclo de vida dos dados e da informação é um aliado importante para que você possa proteger da melhor forma possível a sua empresa.

Outro aspecto importante é que cada vez mais os dados estão distribuídos, e os provedores de serviços de nuvem têm um papel importante neste contexto. Já vimos que as responsabilidades de segurança mudam de acordo com o tipo de serviço contratado dos provedores de nuvem. E isto precisa ser reforçado.

Uma empresa com foco em energias renováveis é composta por uma matriz em Natal, no Rio Grande do Norte, e filial em Belo Horizonte, em Minas Gerais. O desenvolvimento de novas tecnologias é feito por uma

equipe que fica em Santiago, no Chile. Há laboratórios conectados em Belo Horizonte e Santiago. A empresa tem projetos com militares argentinos, o que exige um alto nível de segurança, já que envolve aspectos de segurança nacional.

A empresa tem um diretor de segurança da informação, que é o responsável por uma estrutura que inclui uma gerência de governança de segurança, uma gerência de tecnologias de segurança e outra gerência de processos de segurança.

Você é o gerente de processos de segurança, e deve trabalhar em sinergia com os outros dois gerentes para alinhar os planos e atividades de segurança da informação da empresa.

O diretor de segurança da informação da empresa solicitou um status de alguns aspectos de armazenamento de dados da empresa, principalmente aqueles relacionados com a Lei Geral de Proteção de Dados Pessoais (LGPD). Você deve preparar uma apresentação, então, com as informações solicitadas.

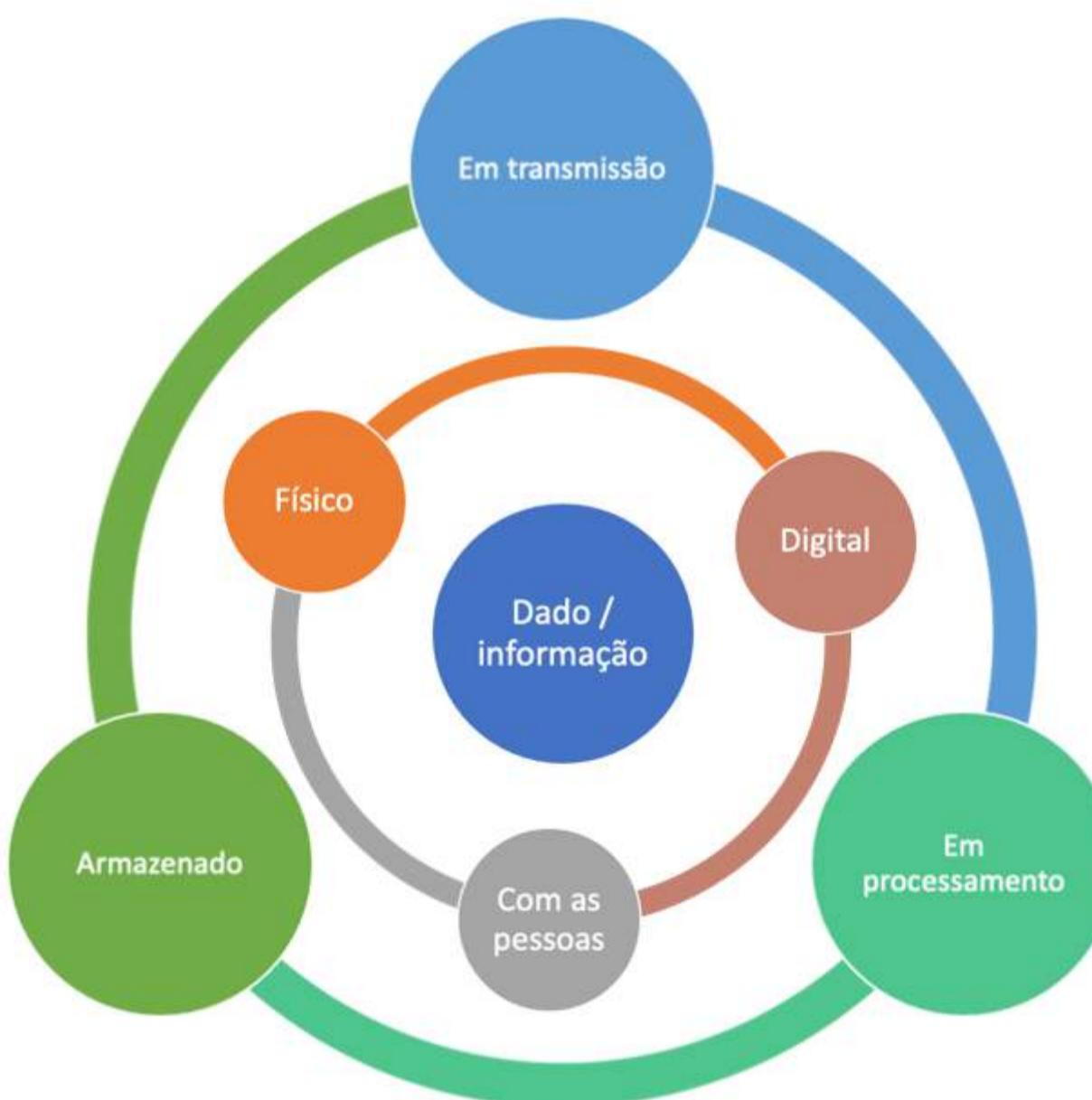
Estruture sua apresentação com os seguintes tópicos:

1. Tratamento de dados pessoais.
2. Controles de segurança para proteção dos dados pessoais.
3. Uso de provedores de nuvem.

A proteção de dados é cada vez mais importante para você. Com os dados pessoais, você, como cidadão, precisa ter a sua privacidade preservada e a LGPD cumprida pelas empresas com as quais você se relaciona. Você deve exigir isto das empresas. E para você como profissional, porque as empresas precisam adequar seus sistemas e processos para proteger os dados e as informações, incluindo as confidenciais e sigilosas, sem deixar de lado as pessoas, já que a segurança e privacidade são de responsabilidade de todos. Vamos estudar os elementos importantes neste contexto.

Caro aluno, nesta seção, você conhecerá diferentes aspectos da segurança de dados, principalmente daqueles que estão armazenados. Pode-se considerar que a segurança da informação se aplica na segurança de dados, e a diferença está na especificidade do que está sendo protegido. O que você deve conhecer é que os dados e a informação estão em fluxo constante e existem em diferentes estados: a transmissão, o processamento, o armazenamento. Estão em meio físico, em meio digital e, ainda, na cabeça das pessoas. A Figura 2.23 resume os dados e informações que fluem o tempo todo. E os dados e as informações precisam de segurança em todo este fluxo que envolve seus diferentes estados e meios em que existem, conforme o momento.

Figura 2.23 | Dados e informação fluem



Fonte: elaborada pelo autor.

| DADOS, INFORMAÇÃO, CONHECIMENTO

Segundo Zeferino (2018), os dados são registros que servem como matéria-prima para a construção da informação e do conhecimento, por meio da análise, manipulação e processamento de dados. A informação

é a estruturação e organização de dados, ou seja, ela é o resultado da aplicação de contexto aos dados, necessário para compreender determinado assunto em específico. O objetivo da informação é de esclarecer e reduzir incertezas, a fim de levar ao conhecimento e sabedoria. Já o conhecimento é a informação processada e transformada. Também é resultado de aprendizagem que ocorre quando somos expostos a diversas informações novas, que alteram nosso comportamento e relacionamento com o que está a nossa volta. Em outras palavras, a informação são os dados processados sobre algo ou alguém, e o conhecimento é um conjunto de informações úteis que foram adquiridas por meio de aprendizados e experiência (ZEFERINO, 2018).

A norma ABNT NBR ISO/IEC 27002 coloca o contexto de que as organizações de todos os tipos e tamanhos (incluindo o setor privado e público, organizações comerciais e sem fins lucrativos), coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal (por exemplo, conversões e apresentações) (ISO 27002, 2013).

Além disso, segundo a norma, o valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos (ISO 27002, 2013).

DADOS PESSOAIS, DADOS PESSOAIS SENSÍVEIS, DADOS CONFIDENCIAIS

A Lei nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), visa proteger os dados pessoais. Segundo a LGPD, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável

(BRASIL, 2020). Um outro tipo de dado importante definido na LGPD e que requer um nível de proteção maior é o dado pessoal sensível, que é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2020). Ou seja, o dado sensível é aquele que discrimina uma pessoa ou indivíduo e pode ser utilizado contra ele ou contra a sua reputação.

É importante você diferenciar dados pessoais, que dizem respeito ao indivíduo, de dados confidenciais, que envolvem também dados de empresas. Os dados e informações confidenciais são definidos com a classificação da informação, que iremos discutir ainda nesta seção. Uma informação confidencial é aquela que, se divulgada tem um impacto significativo nas operações ou nos objetivos táticos da empresa e, portanto, pode ser acessado somente por um grupo de pessoas.

| ESTADO DOS DADOS EM MEIOS DIGITAIS: DIU, DAR, DIM

Os dados em meios digitais existem em três estados (Figura 2.24).

Figura 2.24 | Estados dos dados



Fonte: elaborada pelo autor.

Dados transmitidos, seja em redes sem fio ou em qualquer tipo de conexão, incluindo a internet, são conhecidos com *Data-In-Motion* (DIM). Estes dados podem ser comprometidos durante a transmissão, o que pode comprometer a sua confidencialidade, integridade ou disponibilidade.

EXEMPLIFICANDO

Um usuário pode acessar um serviço pela internet, via navegador. O caminho dos dados inseridos pelo usuário em seu dispositivo, até chegar ao servidor que executa o serviço, na nuvem ou no datacenter da empresa, é composto por uma série de pontos que podem levar ao ataque cibernético. Há riscos envolvidos com uma rede Wi-Fi, o provedor *internet* do usuário e o link *internet* da empresa. Equipamentos de rede vulneráveis podem ser explorados nestes ataques, ou caso os dados sejam transmitidos em claro, podem ser acessados indevidamente ou mesmo modificados. O controle de segurança mais comum que deve ser utilizado pelo provedor de serviço é o uso de um canal seguro *Hyper Text*

Transfer Protocol Secure (HTTPS), que protege as conexões *Hyper Text Transfer Protocol (HTTP)* com o *Transport Layer Security (TLS)*.

Já os **dados em processamento** são conhecidos como *Data-In-Use* (DIU), que realizam as transformações dos dados necessários para as operações e possibilitam as interações necessárias entre o usuário e o serviço. Há um espaço limitado de oportunidade para que ataques cibernéticos aconteçam com o DIU, já que as aplicações realizam as operações necessárias e os dados continuam o seu fluxo, normalmente para o armazenamento.

EXEMPLIFICANDO

Dados em processamento existem nas aplicações e em outros ativos como sistema operacional e protocolos. Há uma intensa interação entre esses elementos computacionais quando um dado está em processamento, envolvendo ainda ativos físicos como a memória RAM e a memória virtual, que podem conter dados relevantes e são alvos naturais de ataques cibernéticos. Um dos principais controles de segurança para evitar incidentes envolvendo DIU é o desenvolvimento seguro, que vimos na seção anterior. Porém, na prática, o que protege o DIU é o conjunto de controles de segurança, envolvendo gestão de vulnerabilidades, gestão de identidades e controle de acesso, por exemplo.

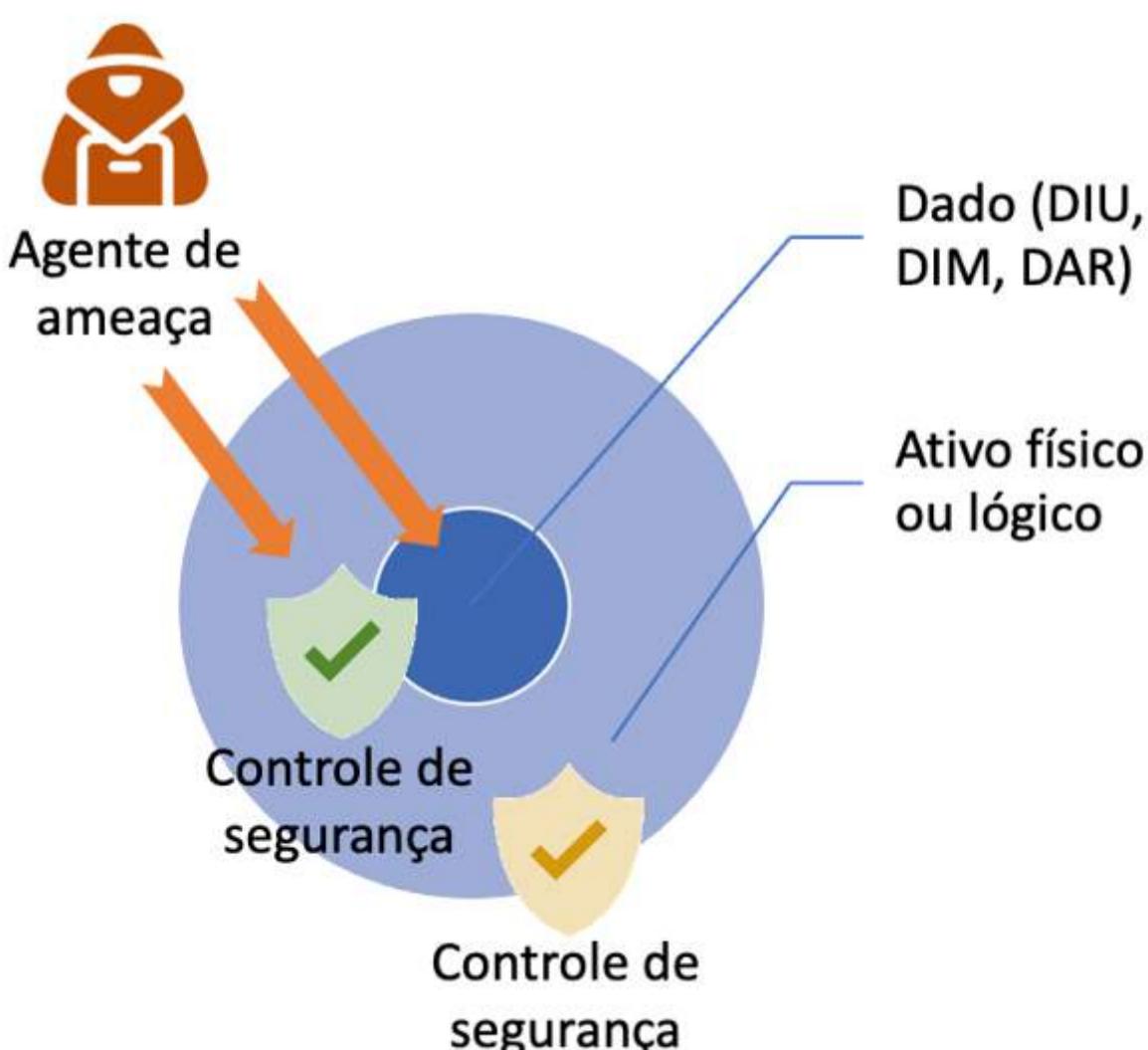
Os **dados armazenados**, conhecidos como *Data-At-Rest* (DAR), têm uma grande exposição aos agentes de ameaça, e recebem grande parte da atenção de segurança. Porém, é preciso entender que para que um atacante chegue aos dados armazenados, é preciso passar pelos ativos que estão custodiando os dados.

Os dados podem estar armazenados em ativos lógicos como em um banco de dados ou servidor de arquivos e em meios físicos, como em papéis, *pendrives* e mídias de *backup*. Um dos principais controles de segurança aplicado diretamente aos dados armazenados é a criptografia. Para que o agente de ameaça tenha acesso aos dados, deve passar pelos ativos, que possuem seus próprios controles de segurança, como a gestão de identidades e acessos.

| DEVEMOS PROTEGER OS DADOS EM TODOS OS SEUS ESTADOS

Os dados existem em diferentes estados (DIU, DIM e DAR), em ativos físicos ou lógicos, como mostra a Figura 2.25. Quando um dado está em processamento, há uma aplicação, por exemplo, realizando as operações nos dados. Já quando um dado está em transmissão, há a rede envolvida, bem como os equipamentos de rede. E quando um dado está armazenado, há um banco de dados, por exemplo, ou um servidor de arquivos. Em backups, os dados estão em mídias físicas como discos rígidos ou mídias de backup.

Figura 2.25 | Estados dos dados



Você deve conhecer estas possibilidades de existência dos dados, em seus diferentes estados, definir e implementar os controles de segurança mais adequados, de acordo com uma visão de riscos. Considere que um agente de ameaça sempre chega aos dados, que estão em um ativo físico ou lógico. E os controles de segurança podem ser aplicados nos dados, ou nos ativos físicos ou lógicos. O objetivo é fazer com que o agente de ameaça tenha o mínimo de acesso possível aos dados, o que significa o mínimo de acesso possível aos ativos físicos ou lógicos (NAKAMURA, 2016).

Os acessos aos ativos podem ser controlados com mecanismos de controle de acesso, que envolvem a identificação, autenticação e autorização. Um banco de dados é um exemplo de ativo que gerencia os dados. O controle de acesso faz com que os dados sejam acessados somente por usuários legítimos. Porém, em caso de vulnerabilidades em banco de dados, ou de qualquer outro componente que faz parte do sistema, como no sistema operacional, o agente de ameaça pode acessar indevidamente os dados. Neste caso, é importante o uso de controles de segurança como a criptografia, que protege a confidencialidade dos dados.

ASSIMILE

Controles de segurança podem ser aplicados nos dados, como a criptografia, ou nos ativos que gerenciam os dados, como o controle de acesso do banco de dados. O uso de múltiplos controles de segurança é importante porque constituem uma segurança em camadas. Neste exemplo, caso o controle de acesso do banco de dados ou do servidor de arquivos seja comprometido, a criptografia pode fazer com que o conteúdo dos dados não seja acessado, devido à

criptografia. Além disso, outro controle de segurança importante são os logs ou registros de quem acessa os dados, principalmente aqueles mais sensíveis.

MASCARAMENTO, ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Além da criptografia, há outros controles de segurança que devem ser conhecidos e considerados para serem utilizados para a proteção de dados. Um dos controles que protegem os dados, limitando a exposição, é o **mascaramento de dados**. Com esta técnica, os dados não são expostos em toda a sua totalidade, com apenas trechos que sejam suficientes para as operações. No contexto do *Payment Card Industry Data Security Standard* (PCI DSS), o mascaramento é um método para ocultar um segmento de dados ao ser exibido ou impresso (PCI, 2014). Já o truncamento é um método que remove permanentemente um segmento dos dados no armazenamento (PCI, 2014). Um exemplo é ilustrado na Figura 2.26, com o mascaramento sendo aplicado na exibição. Caso haja o armazenamento, há o truncamento ao invés do mascaramento, que é utilizado apenas na sua exibição ou impressão. Como no caso do truncamento utilizado no armazenamento a remoção é permanente, as substituições podem ser feitas de uma forma mais geral, sem indicar o número de algarismos substituídos.

Figura 2.26 | Mascaramento de dados quando exibido e truncamento quando armazenado

Número de cartão de crédito original:	1234 1234 1234 1234
Número de cartão de crédito com mascaramento:	1234 12XX XXXX XX34
Número de cartão de crédito com truncamento:	1234 12 - 34

Fonte: elaborada pelo autor.

Há casos muito específicos em que números de cartões de créditos precisam ser armazenados, como em pré-autorizações ou em bancos emissores. Para os demais casos, que são a grande maioria, os dados completos do cartão não podem ser armazenados, de acordo com o PCI DSS. No atendimento aos clientes dos bancos emissores, em que há o acesso dos atendentes aos dados, os riscos envolvidos podem ser reduzidos com o uso de mascaramento. O atendente pode realizar as operações utilizando os dados com mascaramento, o que limita a possibilidade de vazamentos e posterior uso indevido dos cartões.

Outra técnica de proteção de dados é o uso da **anonimização**. Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), a anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (BRASIL, 2020).

Já a **pseudonimização** é tratada pela lei como o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (BRASIL, 2020).

O Quadro 2.5 mostra a diferença entre a anonimização e a pseudonimização. Uma forma simples é que no primeiro caso o processo inverso, ou seja, o retorno ao dado original não é possível, enquanto no segundo caso (pseudonimização) é possível retornar ao dado original com o uso de uma informação adicional. No exemplo, José, Paulo, Maria e Rita podem ser anonimizados, sendo representado por "xxxx". Já no caso de serem pseudonimizados, eles são identificados como sendo, respectivamente, "N1", "N2", "N3" e "N4". O armazenamento, assim, deve ser feito utilizando-se uma das duas técnicas.

No caso do uso da anonimização, são armazenados os dados referentes ao nome anonimizado, cidade e faixa etária. Qualquer necessidade de uso destes dados não possibilita o processo reverso de identificar o titular dos dados. A empresa que adota esta técnica, assim, não pode trabalhar com dados individualizados.

Já no caso do uso da pseudonimização, são armazenados os dados referentes ao nome pseudonimizado, cidade e faixa etária. Além disso, há uma outra base, com informações de nome e nome pseudonimizado, que permite a reversão e a identificação do indivíduo. Como definido na LGPD, essa base adicional deve ser mantida separadamente pela empresa em ambiente controlado e seguro.

Quadro 2.5 | Anonimização e pseudonimização

	Nome Nome anonimizado	Nome pseudonimizado	Cidade	Faixa Etária
José	xxxx	N1	Manaus	18-20
Paulo	xxxx	N2	Recife	21-23
Maria	xxxx	N3	Manaus	24-26
Rita	xxxx	N4	Recife	18-20

Fonte: elaborado pelo autor.

REFLITA

Com o uso da pseudonimização, há duas bases. Uma com os dados, que são ligados a um indivíduo pseudonimizado ou codificado, e outra, com a relação entre o indivíduo e o pseudônimo ou código. Essas duas bases devem ser mantidas isoladas. No caso de um incidente de segurança envolvendo somente a base com dados pseudonimizados, não se sabe a quem pertence aqueles dados. Já no caso de um outro incidente de segurança envolvendo somente a base

de ligação entre o indivíduo e o pseudônimo, não há dados envolvidos. No caso de um incidente de segurança envolvendo as duas bases, o agente de ameaça passa a ter acesso a todos os dados. Você deve também considerar que, dependendo da base de dados pseudonimizado, há a possibilidade de inferências ou uso de outras informações para se chegar ao indivíduo, principalmente quando há dados mais detalhados envolvidos. Por exemplo, um indivíduo “N1” que mora em Manaus e possui entre 18 e 20 anos dá poucas informações para se chegar ao indivíduo “N1”. Porém, caso esta base de dados possua um dado a mais, como o endereço residencial, “N1” pode ser facilmente descoberto. Neste caso, uma técnica é o uso de bancos de dados mais segmentados.

ASSIMILE

Um ponto importante da LGPD é aquela que determina que os dados anonimizados não serão considerados dados pessoais para os fins desta lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Segundo a lei, a determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios (BRASIL, 2020). Assim, em alguns casos, não é necessário identificar o titular dos dados pessoais, e sempre que possível, a anonimização simplifica a adequação à LGPD.

A norma ABNT NBR ISO 27002, que define os objetivos de controle e os controles de segurança da informação, define que convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada (ISO 27002, 2013).

REFLITA

A informação deve ser classificada. E quanto aos ativos que armazenam, processam, manuseiam ou protegem a informação? A norma ABNT NBR ISO 27002 estabelece que convém que estes ativos também sejam classificados, de acordo com as informações relacionadas (ISO 27002, 2013).

Um exemplo de esquema de classificação de confidencialidade da informação define quatro níveis:

- **Pública:** quando sua divulgação não causa nenhum dano.
- **Interna:** quando a divulgação causa constrangimento menor ou inconveniência operacional menor.
- **Confidencial:** quando a divulgação tem um impacto significativo nas operações ou objetivos táticos.
- **Sigilosa:** quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

Como um dos objetivos da classificação da informação é evitar a divulgação não autorizada, é importante que haja um alinhamento com a política de controle de acesso.

O controle de acesso considera a classificação da informação, como no exemplo:

- **Pública:** pode ser disponibilizado para o público em geral, e acessado por todos.

- **Interna:** pode ser acessado somente por colaboradores.
- **Confidencial:** pode ser acessado por um grupo de pessoas.
- **Sigilosa:** pode ser acessado somente por algumas pessoas específicas.

Os resultados da classificação devem ser atualizados de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida. A informação pode deixar de ser sensível ou crítica após certo período, por exemplo, quando a informação se torna pública. Segundo a norma ABNT NBR ISO/IEC 27002, convém que estes aspectos sejam levados em consideração, pois uma classificação superestimada pode levar à implementação de controles desnecessários, resultando em despesas adicionais ou, pelo contrário, classificações subestimadas podem pôr em perigo o alcance dos objetivos de negócio (ISO 27002, 2013). Um exemplo é o balanço de uma empresa listada na Bolsa de Valores, que é sigiloso antes da publicação no jornal e divulgação pela CVM, pois pode impactar diretamente no preço das ações e causar fraudes na compra ou venda dos papéis. Porém, depois de publicada, essa informação sigilosa passa para pública, apesar de poder interferir no preço dos papéis.

REFLITA

Quem deve classificar a informação? Segundo a norma ABNT NBR ISO/IEC 27002, os proprietários de ativos de informação sejam os responsáveis por sua classificação.

A classificação da informação por seus proprietários é feita a partir de um esquema de classificação que seja consistente e faça parte dos processos da organização. A classificação envolve também o uso de rótulos, considerando informações em formato físico ou digital. E o tratamento das informações envolve o entendimento comum dos

requisitos de proteção para que os controles possam ser aplicados adequadamente. A Figura 2.27 ilustra o fluxo envolvido com a classificação da informação.



Fonte: elaborada pelo autor.

A rotulagem da informação é um requisito-chave para acordos de compartilhamento de informações e deve ser conhecido por todos os colaboradores. Há casos em que o procedimento pode dispensar a rotulagem, como de informações públicas. Um ponto a ser considerado também é que ativos rotulados são mais fáceis de identificar e selecionar para roubos, por exemplo, já que ativos sigilosos possuem mais valor.

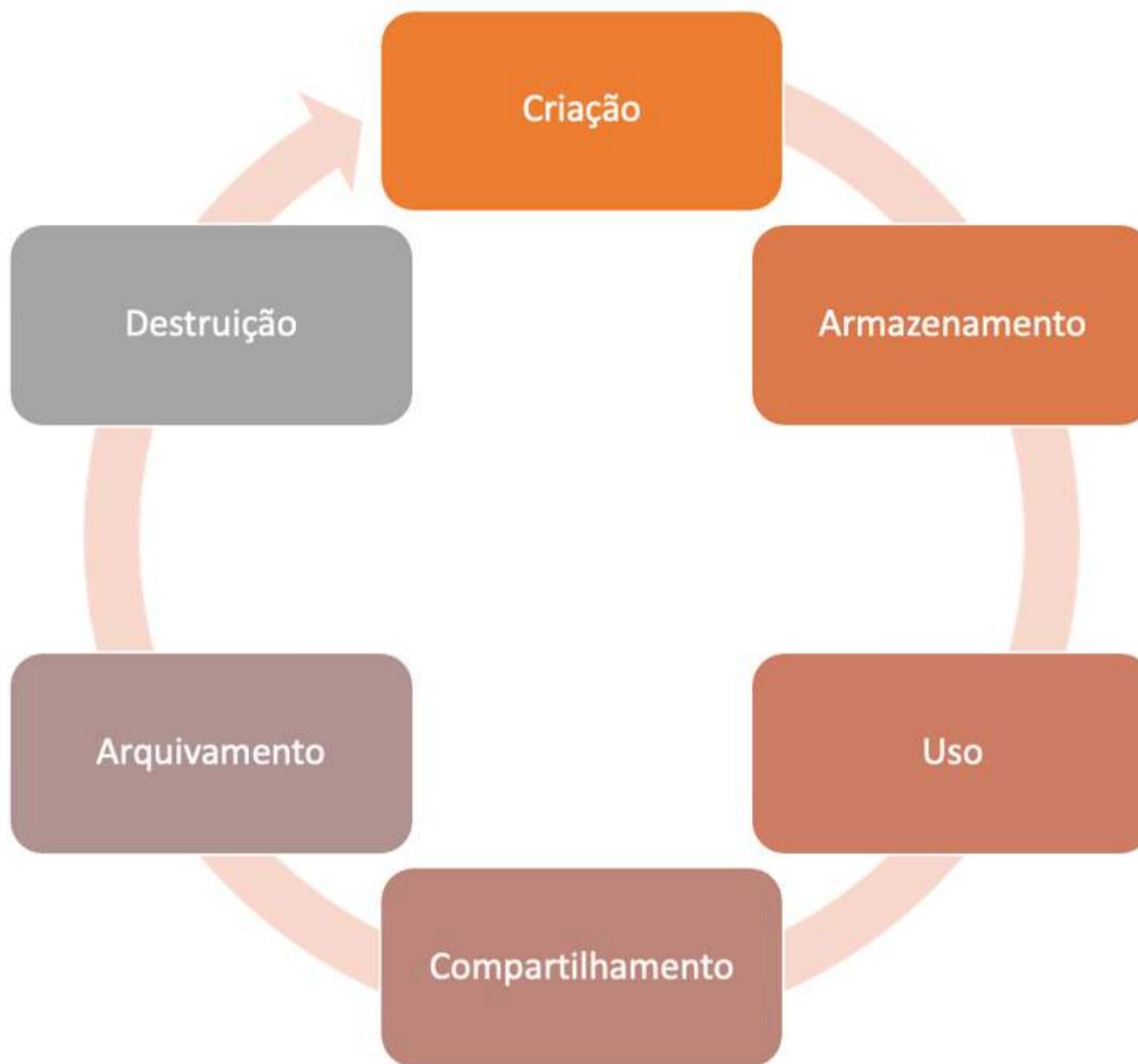
| CICLO DE VIDA E TRATAMENTO DOS DADOS/INFORMAÇÃO

Um dado possui um ciclo de vida da criação à destruição (ROTHMAN, 2020), que pode ser visto na Figura 2.28:

- **Criação:** é a geração de um novo conteúdo ou a alteração/atualização de um conteúdo existente, dentro ou fora da nuvem, por um humano ou por uma máquina ou algoritmo.
- **Armazenamento:** é o ato de colocar o dado em um repositório de armazenamento e, tipicamente, ocorre quase simultaneamente à criação.
- **Uso:** dados são vistos, processados ou utilizados em outras atividades, por humanos, por algoritmos e por máquinas.
- **Compartilhamento:** troca de dados entre usuários, consumidores ou parceiros.

- **Arquivamento:** dados deixam de ser utilizados ativamente e vão para o armazenamento de longo prazo, mesmo offline.
- **Destrução:** destruição permanente dos dados utilizando meios físicos ou digitais.

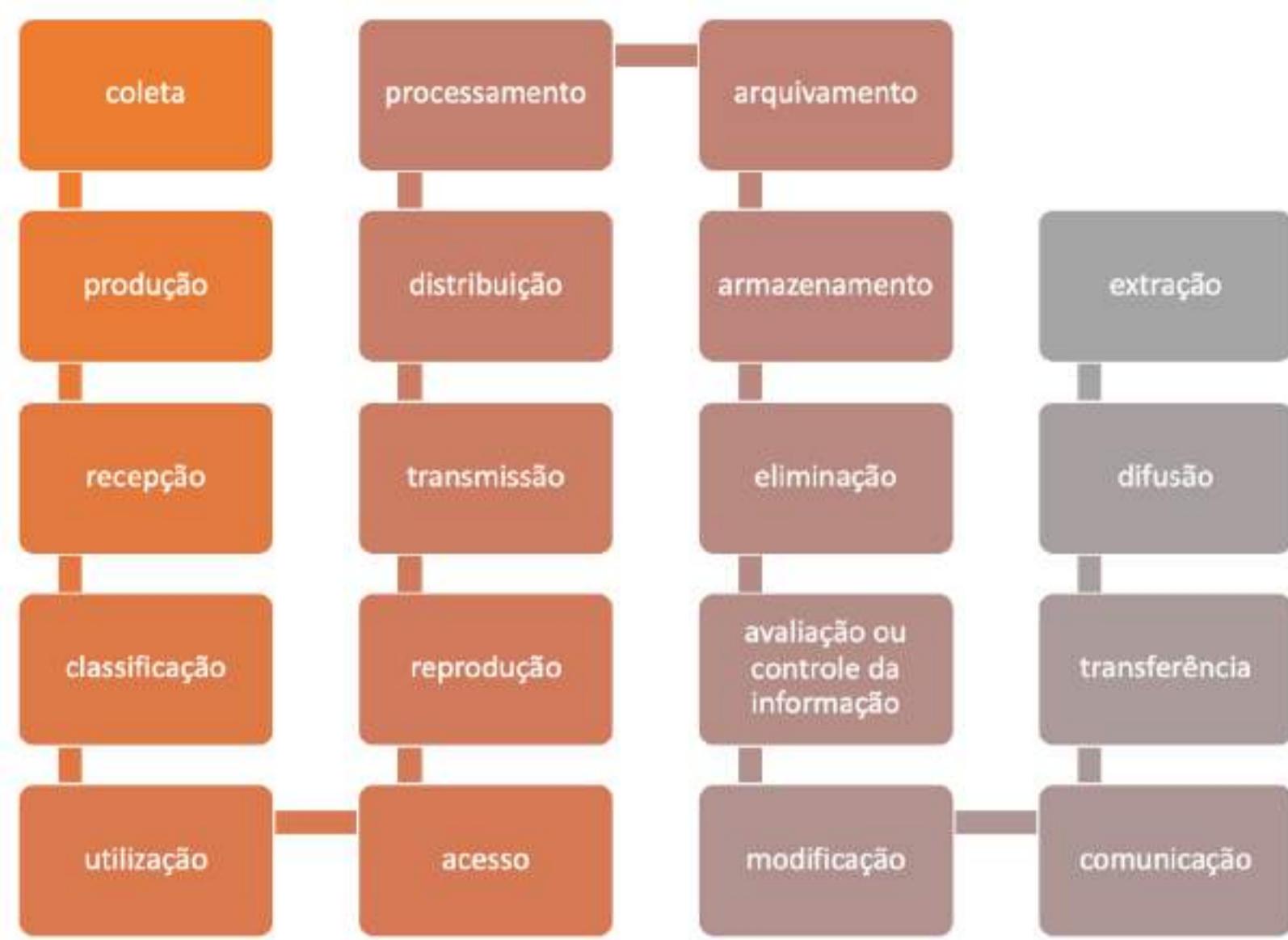
Figura 2.28 | Ciclo de vida da informação



Fonte: adaptado de Rothman (2020).

A LGPD define o tratamento de dados como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2020), na Figura 2.29.

Figura 2.29 | Tratamento de dados pessoais, segundo a LGPD



Fonte: adaptado de Brasil (2020).

Como há as responsabilidades pelo tratamento de dados, reforçado por leis como a LGPD, é importante considerar o ciclo de vida dos dados para a eliminação ou destruição assim que a finalidade seja alcançada. A LGPD determina as hipóteses em que ocorre o término do tratamento de dados (BRASIL, 2020):

- Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.
- Fim do período de tratamento.
- Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público.
- Ou, determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Sobre a retenção de dados, há aspectos legais e regulatórios que determinam um período de conservação de dados. No caso da LGPD, os dados pessoais podem ser conservados para as seguintes finalidades:

- Cumprimento de obrigação legal ou regulatória pelo controlador.
- Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
- Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei.
- Ou, uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

EXEMPLIFICANDO

O cumprimento da obrigação legal é a necessidade de utilizar o dado para a adequação de alguma lei que peça o seu arquivamento. Por exemplo, a legislação trabalhista e fiscal, que é uma das mais complexas, pede a guarda dos dados dos colaboradores em média por até 5 anos após a sua demissão. Mas, para fins previdenciários, as informações do contrato de trabalho devem ser mantidas indefinidamente e as informações fiscais por até 10 anos. Assim, mesmo que o colaborador peça a remoção dos seus dados, não são todas as informações que a empresa pode descartar.

| SEGURANÇA DE DADOS NA NUVEM

Já no contexto de provedores de nuvem, é preciso atentar para os dados tratados pelo provedor de nuvem, considerando ainda o término do contrato. De uma forma geral, o uso de um provedor de nuvem envolve o provisionamento, a migração e o desprovisionamento. Os dados não podem ser acessados indevidamente em nenhum momento pelo provedor de nuvem.

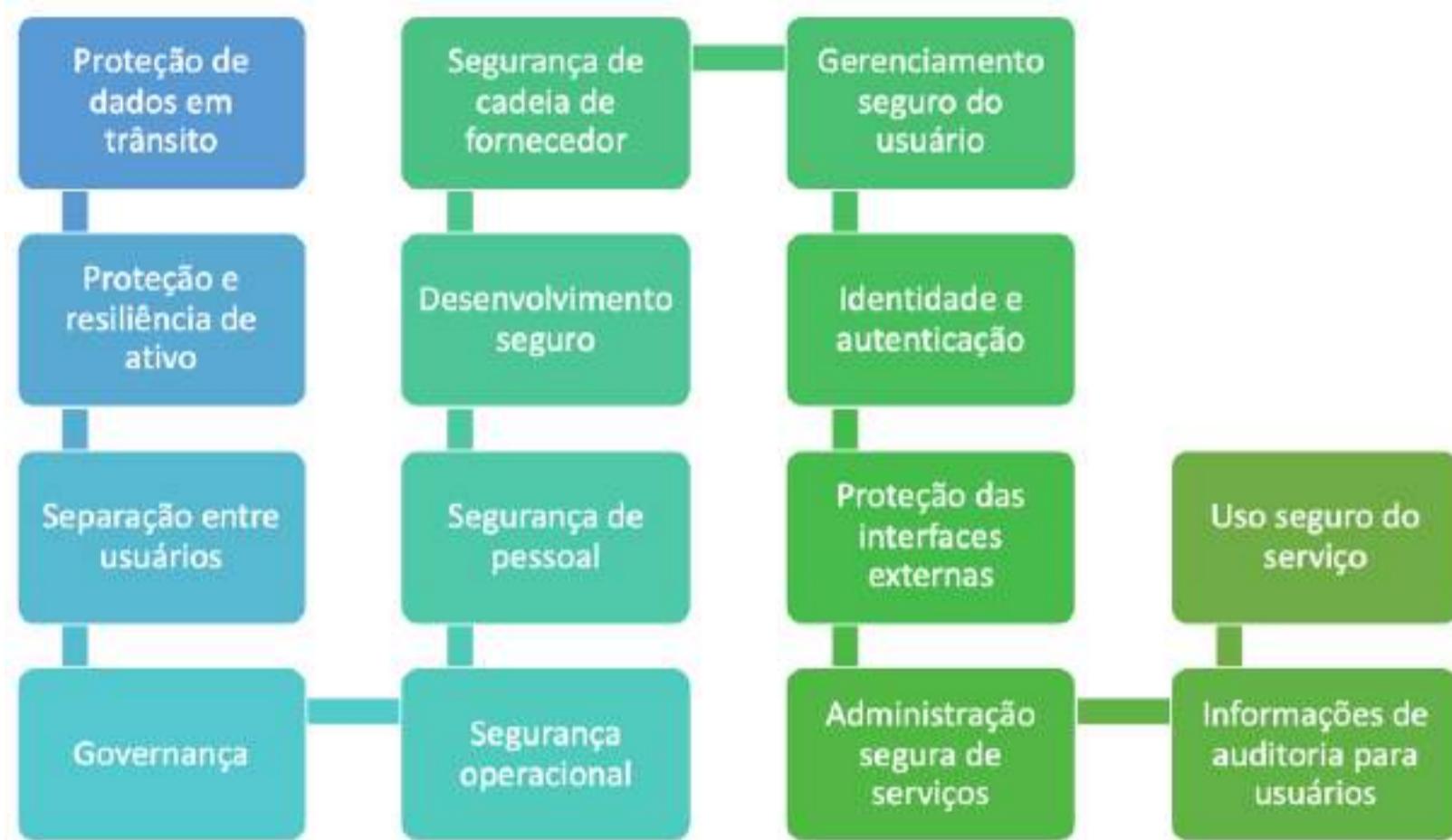
Segundo a *National Cyber Security Centre* (NCSC), do Reino Unido, os princípios da segurança em nuvem envolvem a proteção dos dados (NCSC, 2020) e estão resumidos na Figura 2.30:

1. Proteção de dados em trânsito, principalmente contra alteração e espionagem na rede.
2. Proteção e resiliência de ativo, incluindo dados e ativos que armazenam ou processam os dados, contra adulteração física, perda, dano ou captura.
3. Separação entre usuários, de modo que um usuário comprometido não afete o outro.
4. Governança, para coordenar e direcionar o gerenciamento do serviço e das informações relacionadas.
5. Segurança operacional, que gerencia o serviço para impedir, detectar ou prevenir ataques.
6. Segurança de pessoal, incluindo treinamento e triagem para reduzir as chances de incidentes accidentais ou maliciosos do pessoal do provedor de serviços.
7. Desenvolvimento seguro, com identificação de ameaças e mitigação de riscos que podem comprometer os dados, causar problemas no serviço ou permitir outras atividades maliciosas.
8. Segurança de cadeia de fornecedor, assegurando que todos cumpram a implementação da segurança.
9. Gerenciamento seguro do usuário, com ferramentas para o gerenciamento seguro do serviço, prevenindo acessos não autorizados e alteração de recursos, aplicações e dados.
10. Identidade e autenticação em todos os acessos aos serviços.
11. Proteção das interfaces externas, que devem ser identificadas e protegidas adequadamente.
12. Administração segura de serviços, que possuem acessos privilegiados que resultam em grandes impactos em caso de comprometimento.

13. Informações de auditoria para usuários, monitorando os acessos aos serviços e aos dados relacionados.

14. Uso seguro do serviço, com responsabilidade.

Figura 2.30 | Princípios da segurança em nuvem



Fonte: adaptado de NCSC (2020).

E a proteção dos dados nos provedores de nuvem?

Você deve exigir, como cliente, que os provedores façam a proteção dos dados armazenados (DAR) em diferentes níveis. Os dados estão sob responsabilidade do provedor, existem no centro de dados e também em mídias. Há o acesso físico aos servidores e às mídias, como de backups. E um incidente de segurança pode ser decorrente de acidente ou de atividade maliciosa. Assim, os controles de segurança básicos dos provedores de nuvem são o controle de acesso físico, uso de técnicas como a ofuscação para tornar a identificação de dados mais difícil e o uso de criptografia diretamente na mídia física.

REFLITA

Como foi visto na unidade anterior da disciplina, a criptografia é tão forte quanto a sua chave. E o gerenciamento de chaves criptográficas é um grande desafio

de quem utiliza a criptografia. Quem tem o acesso às chaves, onde elas são guardadas?

Outro ponto importante envolvido com o uso de provedores de nuvem é quanto à eliminação e destruição dos dados. Quando uma empresa utiliza um provedor de nuvem, a sanitização de dados deve ser exigida.

EXEMPLIFICANDO

A sanitização, destruição ou eliminação de dados do provedor de nuvem deve garantir que, após a finalização do contrato e o desprovisionamento, os dados não permaneçam com o provedor. Um ponto importante é que os dados não possam ser acessados de alguma forma quando os recursos são reutilizados por um outro cliente do provedor de nuvem. Além disso, os dados em mídias físicas também devem se descartados adequadamente, pois podem resultar em acesso indevido aos dados. Há o exemplo da destruição da mídia física (HD) em casos mais críticos, em que o hardware passa por um processo de desmagnetização ou mesmo a destruição física.

| NAVIGAÇÃO EM DADOS COM CRIPTOGRAFIA

O uso de criptografia para proteger os dados é importante (STALLINGS, 2015). Porém, é preciso considerar uma série de elementos que fazem com que o nível de segurança seja corretamente avaliado. Os dois principais elementos são a chave criptográfica utilizada para decifrar os dados e a possibilidade de vulnerabilidades em ativos relacionados que dão acesso a estas chaves.

Os dados em trânsito (DIM) são tradicionalmente protegidos com o HTTPS, que é baseado em criptografia. No HTTPS, as chaves criptográficas são geradas dinamicamente, para cada sessão. Em aplicativos como os de mensagens, a criptografia é fim a fim, com um protocolo fazendo a troca de chaves para proteger a comunicação.

Já no caso dos dados armazenados (DAR), há diferentes possibilidades de uso da criptografia. Os dados armazenados em um banco de dados passam do usuário para uma aplicação, que se conecta ao banco de dados. Há, neste exemplo, três pontos que podem gerenciar a criptografia e as suas chaves criptográficas: usuário, aplicação e banco de dados. Você pode desenvolver uma aplicação em que a criptografia é feita, e a chave criptográfica é definida pelo próprio usuário. Assim, no caso de o usuário esquecer ou perder esta chave, os dados também são perdidos. E os dados só podem ser acessados pelo próprio usuário, de modo que nem a empresa, nem o provedor de nuvem possuem o acesso aos dados em claro (NAKAMURA & GEUS, 2007).

Já no caso de DAR protegido pela aplicação, os dados são cifrados pela aplicação antes de serem armazenados em um banco de dados. O desafio é o gerenciamento de chaves, e o que se deve evitar é armazenar a chave criptográfica na própria aplicação, o que representa uma vulnerabilidade que facilita o acesso indevido aos dados.

Outra possibilidade é o uso de criptografia do banco de dados, de modo que todos os dados são gerenciados e cifrados pelo sistema de banco de dados.

É preciso avaliar cada caso, a arquitetura do sistema e as operações da empresa para definir a melhor forma de proteger os dados armazenados (DAR).

REFLITA

Hardware Security Module (HSM) é um dispositivo de criptografia baseado em hardware que fornece funções criptográficas para geração e armazenamento de chaves criptográficas simétricas e assimétricas, fisicamente seguro e resistente à violação (HOSTONE, 2019).

Para alguns sistemas mais críticos, as chaves criptográficas podem ser geradas e gerenciadas por HSM, de modo que os sistemas se tornam mais seguros, eliminando a possibilidade

de inserção de vulnerabilidades como chaves *hardcoded* ou inseridas no próprio código, o que é fatal.

Um outro tipo de criptografia, a **homomórfica**, pode tratar, ao mesmo tempo, de proteção de DIU, DIM e DAR. Por meio de operações matemáticas diretas nos dados cifrados, a criptografia homomórfica faz com que os dados permaneçam cifrados mesmo enquanto são manipulados. Assim, ela permite ao usuário realizar uma pesquisa em um banco de dados sem que mesmo o administrador do sistema saiba sobre os termos pesquisados pelo usuário e os resultados mostrados. Ambas as partes podem descobrir intersecções dos conjuntos de dados, mas sem revelar o real conteúdo vasculhado (ROLFINI, 2020).

• Ver anotações

SAIBA MAIS

A criptografia de dados é um dos principais controles de segurança que podem ser utilizados pelas empresas. A criptografia funciona com as chaves criptográficas. Você pode proteger os dados utilizando a criptografia, mas tem que pensar como será o gerenciamento das chaves, e precisa saber dos aspectos envolvidos, que estão em forma de perguntas:

- Cada usuário terá sua própria chave criptográfica para proteger seus dados? E se ele esquecer ou perder a chave, como sua empresa atuará?
- Você usará chave criptográfica na sua aplicação, que fará a criptografia dos dados antes de serem armazenados no banco de dados? E onde estará esta chave, na própria aplicação? E no caso de um comprometimento desta chave, como você fará a atualização?
- Ou você utilizará a criptografia do banco de dados? Quem terá acesso a esta chave? E o provedor de nuvem? O que você fará em caso de comprometimento desta chave?

Uma discussão interessante sobre a segurança da informação, proteção da privacidade e dos dados pessoais é feita em Vaz (2007). Leia o artigo, principalmente nas seções sobre proteção da privacidade e dos dados pessoais, que indica os caminhos trilhados por Portugal.

VAZ, A. Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais, **Nação e Defesa**, Verão 2007, n. 117, 3^a série, p. 35-63.

Chegamos ao fim desta seção, que foca da proteção dos dados, que é cada vez mais importante para você, como cidadão, porque precisa ter a sua privacidade preservada e a LGPD cumprida pelas empresas com as quais você se relaciona. E para você como profissional, porque as empresas precisam adequar seus sistemas e processos para proteger os dados e as informações, incluindo as confidenciais e sigilosas, sem deixar de lado as pessoas, já que a segurança e privacidade é de responsabilidade de todos.

Até a próxima aula!

FAÇA VALER A PENA

Questão 1

As empresas precisam preservar a confidencialidade, integridade e disponibilidade das informações. Os dados e as informações existem em meios físicos, meios digitais e na cabeça das pessoas. E uma das necessidades é proteger o armazenamento de dados.

Assinale a alternativa que apresenta o tipo de controle de segurança relacionado diretamente com a proteção dos dados armazenados.

a. Criptografia.

b. IPS.

c. Malware.

d. Firewall.

e. Conscientização.

Questão 2

Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento de dados pessoais exige que eles sejam protegidos, com a implementação de controles de segurança em todo o fluxo dos dados para preservar a privacidade dos brasileiros.

O mecanismo de segurança que faz com que os dados não sejam considerados dados pessoais é?

a. Criptografia.

b. Pseudonimização.

c. Anonimização.

d. Firewall.

e. Conscientização.

Questão 3

Dados e informações devem ser protegidos com a implementação de controles de segurança. Há diferentes tipos de dados e informações, os quais devem ser classificados. Há dados e informações pessoais, públicos, internos, secretos, confidenciais, entre outros.

Análise as afirmativas a seguir.

- I. Dados e informações devem ser protegidos, independentemente de sua classificação.
- II. Dados e informações devem ser descartados no fim de seu ciclo de vida.
- III. Dados e informações devem ser armazenados em um provedor de nuvem.

Assinale V para as afirmações verdadeiras, e F para as afirmações falsas, e indique a alternativa correta para as respectivas três afirmações.

a. F – F – F.

b. F – V – V.

c. F – V – F.

d. V – V – F.

e. F – V – V.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.** Rio de Janeiro. 2013.

BRASIL. **Lei Geral de Proteção de Dados Pessoais.** Presidência da República – Secretaria-Geral – Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://bit.ly/3qbyuzO>. Acesso em: 25 out. 2020.

HOSTONE. **Descubra o que é HSM e quais são seus benefícios,** 24 dez. 2019. Disponível em: <https://bit.ly/389xoOR>. Acesso em: 14 nov. 2020.

JORNADA para Nuvem. **Os 6 pilares fundamentais para sua longa e única Jornada para Nuvem.** Disponível em: <https://bit.ly/3benzRz>. Acesso em: 7 nov. 2020.

NAKAMURA, E. T., GEUS, P. L. **Segurança de redes em ambientes cooperativos.** São Paulo: Editora Novatec, 2007.

NAKAMURA, E. T. **Segurança da Informação e de Redes.** São Paulo: Editora e Distribuidora Educacional S.A., 2016.

NATIONAL Cyber Security Centre. **Implementing the Cloud Security Principles.** Disponível em: <https://bit.ly/3kFRi9b>. Acesso em: 11 nov. 2020.

Environments. Disponível em: <https://bit.ly/2OI3Ne0>. Acesso em: 11 nov. 2020.

ROLFINI, F. Testes apontam eficácia de criptografia totalmente homomórfica. **Olhar Digital**, 8 ago. 2020. Disponível em: <https://bit.ly/3e6O9xG>. Acesso em: 14 nov. 2020.

ROTHMAN, M. Data Security in the SaaS Age: Focus on What You Control. **Securosis**, 15 jun. 2020. Disponível em: <https://bit.ly/3kl6ulZ>. Acesso em: 12 nov. 2020.

PCI Security Standards Council. **Indústria de cartões de pagamento (PCI) Padrão de segurança de dados (DSS) e Padrão de segurança de dados de aplicativos de pagamento (PA-DSS)**, janeiro de 2014. Disponível em: <https://bit.ly/3kGnU2q>. Acesso em: 14 nov. 2020.

STALLINGS, W. **Criptografia e segurança de redes**. 6 ed. São Paulo: Pearson, 2015. Disponível em: <https://bit.ly/3klrr0d>. Acesso em: 9 dez. 2020.

ZEFERINO, D. **Dados, informação e conhecimento**: qual a diferença dos conceitos?, 12 de agosto de 2018. Disponível em: <https://bit.ly/3e5vqTf>. Acesso em: 14 nov. 2020.

FOCO NO MERCADO DE TRABALHO

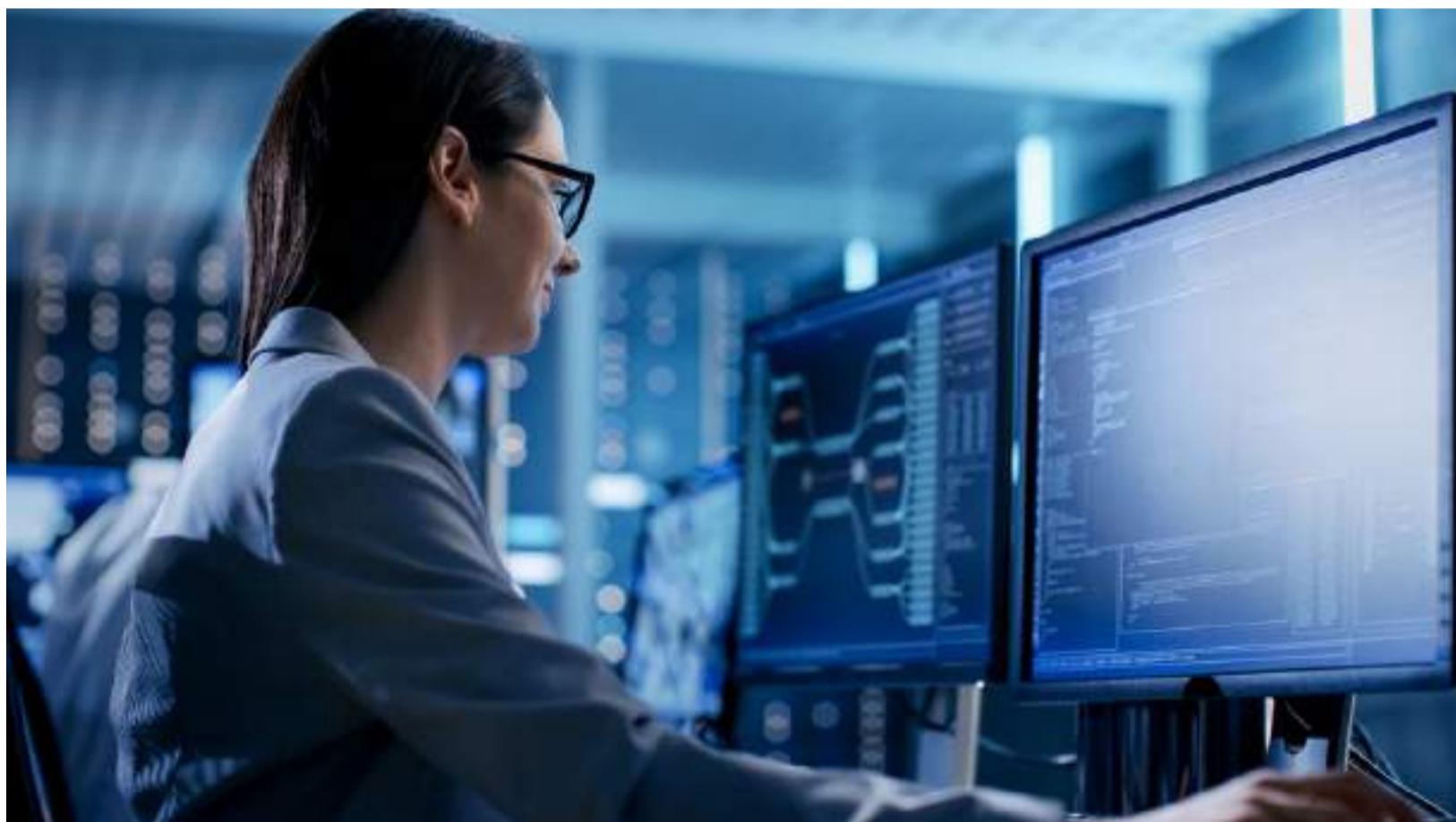
ARMAZENAMENTO DE DADOS

Emilio Tissato Nakamura

Ver anotações

MECANISMOS PARA PROTEÇÃO DOS DADOS

Além da criptografia, há mecanismos como a anonimização, pseudonimização e mascaramento de dados.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você, como gerente de processos de segurança, deve alinhar as informações e as ações com os gerentes de tecnologias de segurança e a de governança de segurança.

Estruture a sua apresentação com um contexto sobre a empresa, que é composta por uma matriz em Natal, no Rio Grande do Norte, e filial em Belo Horizonte, em Minas Gerais. O desenvolvimento de novas tecnologias é feito por uma equipe que fica em Santiago, no Chile. Há laboratórios conectados em Belo Horizonte e Santiago. A empresa tem projetos com militares argentinos, o que exige um alto nível de segurança, já que envolve aspectos de segurança nacional.

Um ponto importante para ser colocado na apresentação é que a empresa trata de diversos dados e informações confidenciais e sigilosos, e este não é o foco desta apresentação, que foca nos dados pessoais. Reforce que LGPD trata de proteção de dados pessoais, mas dados confidenciais e sigilosos são tratados em um outro contexto, de uma forma integrada e sinérgica.

Mostre na apresentação que você conduziu a criação do mapeamento de dados pessoais, com todo o fluxo nos sistemas da empresa. Um dos dados pessoais identificados na empresa são os de colaboradores, incluindo funcionários diretos, terceiros e prestadores de serviços. Estes dados pessoais são utilizados para os processos internos da empresa, principalmente os relacionados a recursos humanos e financeiro. Como há uma interação grande entre os diferentes locais da empresa (Natal, Belo Horizonte e Santiago), os dados pessoais também são muito utilizados em viagens, que envolve o envio destes dados para agências de turismo e companhias aéreas. Outro dado pessoal identificado foi de clientes, incluindo os militares argentinos. Neste caso, como a empresa realiza negócios B2B, e não B2C, os dados pessoais são mais corporativos, mas há dados pessoais de contatos dos clientes. Você pode continuar citando dados pessoais da empresa, e uma boa forma

de identificar estes dados é analisando os processos da empresa, que indicará a finalidade e quais dados pessoais são necessários para cada atividade.

Mostre para o diretor de segurança da informação da empresa que toda a parte jurídica está equacionada, com os ajustes de termos de ciência, termos de responsabilidade, termos de uso e contratos com fornecedores e prestadores de serviços contendo cláusulas relacionados à privacidade e proteção de dados pessoais.

Para a proteção destes dados pessoais, mostre que a empresa está utilizando a pseudonimização para limitar os riscos em caso de vazamento. Mostre também que a anonimização está sendo utilizada para a criação de indicadores corporativos. Reforce que todas as bases com a pseudonimização e a anonimização estão segmentadas e utilizam controles de segurança que envolvem a gestão de identidades e de acesso. Além disso, relembrre que os controles de segurança utilizados para proteger as informações, principalmente as confidenciais e secretas, fazem parte da proteção dos dados pessoais também.

Sobre a criptografia, mostre que ela está sendo utilizada no nível de aplicação, com uso de HSM. Mostre os benefícios do uso do HSM, partindo dos riscos envolvidos com o uso de chaves criptográficas por aplicações.

Para finalizar, mostre que a empresa está adotando práticas de segurança de acordo com as responsabilidades compartilhadas com os provedores de nuvem. A empresa está utilizando dois provedores de nuvem, na modalidade de plataforma como serviço (PaaS). Reforce que, neste modelo, a empresa é responsável pela segurança dos dados e das aplicações.

AVANÇANDO NA PRÁTICA

DEFININDO A ESTRATÉGIA DE ARMAZENAMENTO DE DADOS PESSOAIS DA EMPRESA

Com a necessidade de conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), você deve definir uma estratégia de proteção de dados pessoais da sua própria empresa, que está sendo constituída. A sua empresa é uma loja virtual que precisa coletar os seguintes dados: nome completo, CPF, endereço e referência comercial. Defina sua estratégia de proteção de dados pessoais, considerando o seu armazenamento e o uso de um provedor de nuvem.

Ver anotações

RESOLUÇÃO



Sua empresa deverá coletar dados pessoais, incluindo o nome completo, CPF, endereço e referência comercial. O termo de privacidade deve citar quais são os dados que estão sendo coletados, descrevendo claramente a finalidade, e como eles estarão protegidos, citando ainda os provedores de serviços, se estiverem sendo utilizados. Você deve definir também se estes dados serão compartilhados com algum terceiro e, em caso afirmativo, deve obter um consentimento de cada usuário.

Para o armazenamento dos dados coletados, você deve pensar nos mecanismos de proteção. Além dos controles de segurança para proteger os ativos físicos e lógicos, os dados podem ser pseudonimizados. Assim, você pode utilizar um código como “Cliente0001” para o João, “Cliente0002” para Maria, e assim por diante. No banco de dados, você pode armazenar este código do cliente como identificador, juntamente com os dados de CPF, endereço e referência comercial. Este relacionamento entre o código do cliente e o nome real também deve ser armazenado, de uma forma segura e em local distinto da base de dados dos clientes.

Para aumentar a segurança, você pode dividir ainda mais o banco de dados, com o CPF em um, e o endereço e referência comercial em outro, usando o código do cliente como identificador.

A anonimização não pode ser aplicada no seu caso, pois você precisa identificar o cliente. Ela pode, no entanto, ser utilizada para criar uma base distinta para inteligência de negócios, por exemplo.

Outro ponto que você deve definir é como a criptografia irá funcionar, se na aplicação ou no banco de dados.

Além disso, devem ser consideradas as responsabilidades de segurança, de acordo com o tipo de serviço contratado do provedor de nuvem. Há as modalidades de contratação de infraestrutura, plataforma ou o serviço.

NÃO PODE FALTAR

SEGURANÇA NA INTERNET

Emilio Tissato Nakamura

Ver anotações 0

O QUE SÃO TRANSAÇÕES WEB?

Uma transação web pode ser uma compra online, uma transação bancária, a realização de algum serviço governamental ou até mesmo uma postagem em uma rede social, a qual envolve diferentes tipos de dados ou informações, dados pessoais, financeiros e confidenciais.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

CONVITE AO ESTUDO

Olá, nesta unidade, abordaremos tópicos do nosso cotidiano, em que há o uso cada vez mais intenso da internet para as atividades que vão desde a comunicação pessoal e profissional, passando por transações financeiras, compras virtuais e acesso a conteúdos especializados, chegando até ao cumprimento de obrigações como cidadãos brasileiros.

E é justamente nossa maior dependência da internet que faz com que a importância da segurança e privacidade aumente. Como usuários, devemos exigir e utilizar serviços e plataformas que não comprometam nossa segurança e protejam nossa privacidade. Como profissionais de segurança e privacidade, devemos trabalhar para que os serviços, plataformas, aplicações, aplicativos e sistemas sejam construídos de forma a não potencializar as ameaças existentes na internet, as quais podem resultar em prejuízos que vão além do aborrecimento, indo para comprometimento de reputação, perdas financeiras e que podem chegar até mesmo ao comprometimento da saúde e vida, nos casos que envolvem a internet das coisas ou *Internet of Things, IoT*.

A segurança na internet é um dos assuntos abordados nesta unidade, com o entendimento dos aspectos envolvidos nas transações *web*, que devem ser protegidos, principalmente dos dados que trafegam pela internet. Uma vez que seus dados chegam ao destinatário, eles devem ser protegidos para que não vazem ou sejam utilizados de forma ilícita. Os dados dos usuários são cada vez mais valiosos, já que podem ser utilizados para que identidades digitais das vítimas sejam criadas de uma forma ilegítima ou usados diretamente para transações ilegais, no caso de dados bancários, por exemplo. E há diversos tipos de golpes na internet que podem levar ao acesso ilegal a dados dos usuários. Alguns desses principais golpes serão discutidos, bem como o uso seguro de internet, e as questões para a privacidade na *Web*.

O acesso à internet é feito com o uso de dispositivos e um dos principais é o dispositivo móvel, com os smartphones, representando grande parte dos acessos à rede. Iremos discutir o que isso representa, sob o

ponto de vista de segurança e privacidade, analisando principais ameaças, ataques e mecanismos de defesa em dispositivos móveis, incluindo a camada de aplicação e o uso de antivírus para a proteção.

Outro ponto importante é a proteção dos usuários dos dispositivos móveis, que estão sujeitos a ataques de engenharia social, que podem resultar no acesso às informações pessoais.

O acesso à internet é feito com o uso de dispositivos e um dos principais é o dispositivo móvel, com os *smartphones*, representando grande parte dos acessos à rede. Iremos discutir o que isso representa, sob o ponto de vista de segurança e privacidade, analisando principais ameaças, ataques e mecanismos de defesa em dispositivos móveis, incluindo a camada de aplicação e o uso de antivírus para a proteção.

Outro ponto importante é a proteção dos usuários dos dispositivos móveis, que estão sujeitos a ataques de engenharia social, que podem resultar no acesso às informações pessoais.

Após o entendimento dos principais ataques na internet e as particularidades da segurança em dispositivos móveis, abordaremos uma das principais atividades de profissionais de segurança da informação, que leva ao entendimento do ambiente, dos componentes ou ativos deste ambiente e das vulnerabilidades que podem ser exploradas em ataques. Já vimos que um incidente de segurança é resultado da exploração de vulnerabilidades de ativos por agentes de ameaça, fazendo com que uma ameaça se concretize. Uma das principais formas de se evitar incidentes de segurança é, assim, identificar e tratar as vulnerabilidades dos diferentes ativos do ambiente. Há uma série de métodos e formas de se trabalhar com as vulnerabilidades, incluindo testes de intrusão ou pentests e análises de vulnerabilidades. E, dependendo da informação disponível para realizar os testes ou análises, o trabalho pode ser definido como *blackbox* ou *whitebox*. Teremos uma sessão inteira para aprofundar este tema.

Vamos iniciar os estudos pela segurança na internet.

PRATICAR PARA APRENDER

Olá, nesta seção, discutiremos aspectos importantes de segurança e privacidade na internet, focando nas transações *web*. Neste contexto, há três ambientes que podem ser explorados pelos agentes de ameaça e que, portanto, precisam ser protegidos: o ambiente do usuário, o ambiente do provedor de internet e o ambiente do provedor de serviços. Os dados e as informações podem ser modificados, furtados ou destruídos nestes três ambientes.

Os controles de segurança, que são técnicos, físicos ou processuais, podem ser implementados na sua empresa. Porém, as transações *web* podem chegar à empresa já sem a autenticidade ou integridade, como no caso das transações fraudulentas com uso de identidades furtadas ou uso de cartões de créditos de terceiros.

Desta forma, além de proteger o perímetro de sua empresa, é preciso atuar também com os seus clientes, que podem ser vítimas de ataques como o *phishing*, que leva à instalação de *malwares* que furtam, modificam informações ou levam a sites falsos, onde as vítimas inserem seus dados e informações, os quais são furtados e utilizados em atividades criminosas.

Discutiremos também como os usuários podem ser atingidos por golpes na internet e como eles podem fazer o uso seguro dessa ferramenta, cuidando de sua privacidade.

Você foi contratado como analista de segurança e privacidade de um inovador site de comércio online em que pequenos negócios são conectados com os consumidores em uma plataforma digital baseada no uso de inteligência artificial. A sua função é essencial para a empresa, e você participa de todas as decisões sobre a evolução da plataforma. Há as questões envolvidas com o desenvolvimento seguro, para que vulnerabilidades não sejam inseridas. Há ainda as questões de segurança e privacidade envolvidas com o uso de provedor de nuvem. E, como a empresa trabalha com inteligência artificial, há necessidade de fazer o desenvolvimento utilizando bases de dados que não interfiram na privacidade dos clientes.

Além da segurança da informação da plataforma da empresa, que está hospedada em um provedor em nuvem na Europa, você tem três preocupações principais:

1. Como diminuir as possíveis fraudes cometidas por usuários falsos que se passam por clientes, com uso de identidades falsas ou uso de recursos financeiros ilícitos;.
2. Como diminuir as possíveis fraudes cometidas por pequenos negócios falsos, que podem não cumprir os compromissos comerciais estabelecidos com os clientes que utilizam a plataforma digital;.
3. Como proteger os dados pessoais dos clientes principalmente contra vazamentos, que pode levar a sanções previstas na LGPD.

Você deverá fazer um planejamento e preparar um relatório com uma lista de aspectos que devem ser considerados pela empresa para a definição de uma estratégia de segurança e privacidade. O foco deste planejamento deve ser a segurança na internet, com o seu direcionamento quanto à segurança em transações web, considerando

o ambiente de negócios da empresa e as três preocupações principais que você tem: fraudes cometidas por usuários falsos, fraudes cometidas por pequenos negócios falsos e como proteger os dados pessoais dos clientes.

O conteúdo desta seção é importante e útil para todos, desde o ponto de vista de usuário, empresa, clientes e fornecedores. E você, como profissional de segurança e privacidade, deve adotar estes conceitos para trabalhar o treinamento e a conscientização de todos, fazendo com que a empresa tenha o nível de segurança e privacidade elevado.

o

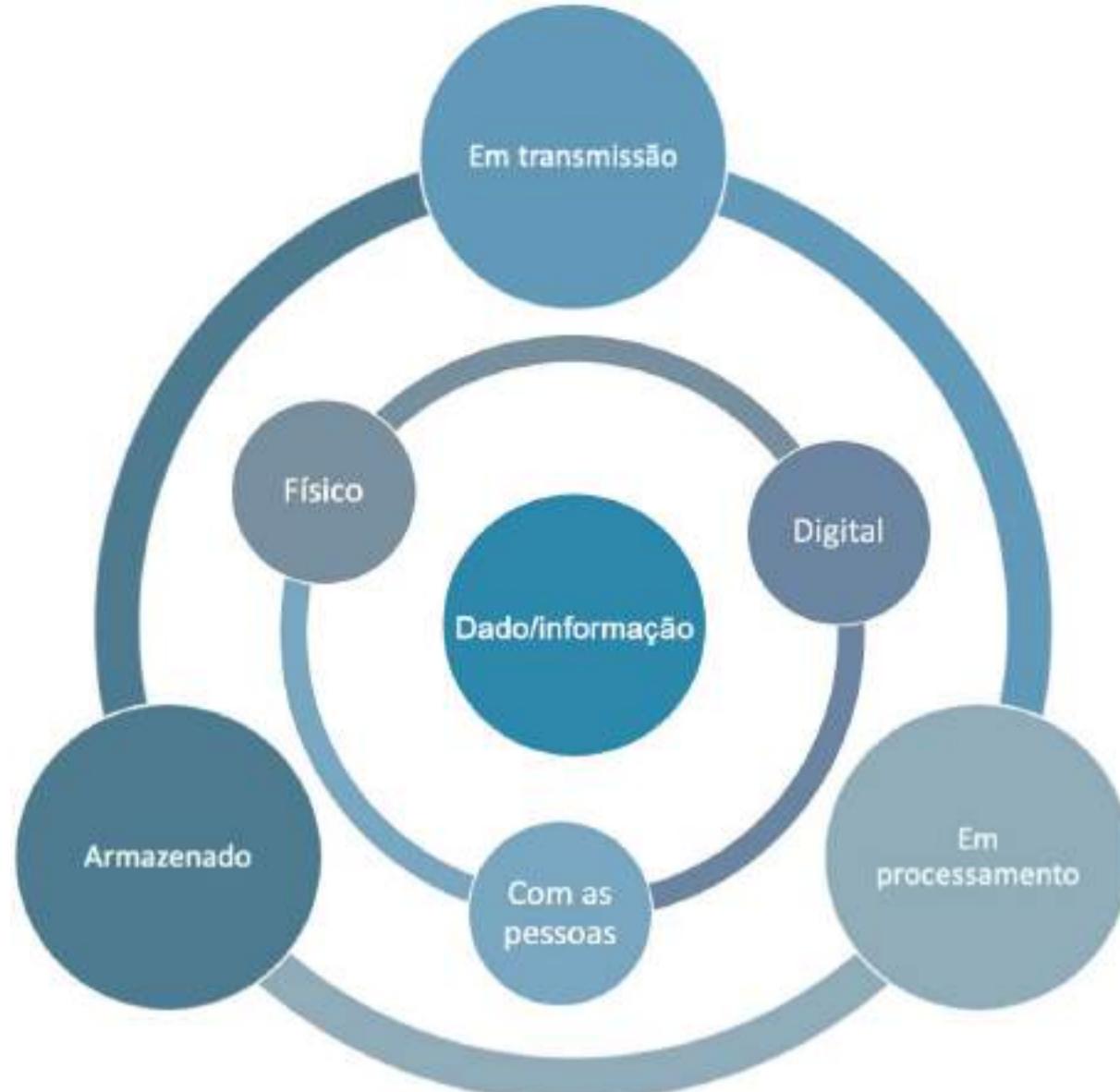
Ver anotações

Uma cultura forte em segurança e privacidade é essencial para todos os profissionais da área.

CONCEITO-CHAVE

A segurança e privacidade na internet passam pelo entendimento de diferentes elementos que envolvem o que deve ser protegido e os componentes ou ativos de um ambiente que podem ser explorados em ataques. Vamos relembrar estes elementos para seguirmos adiante. A Figura 3.1 ilustra que o dado ou a informação existe na forma digital como nos servidores de banco de dados, na forma física como em papel ou na cabeça das pessoas. Além disso, os dados digitais estão em diferentes estados: em transmissão, em processamento ou armazenados. O escopo da segurança da informação abrange diferentes formas e estados dos dados e das informações. E a proteção é para que sejam preservadas a tríade CID, que corresponde à confidencialidade, integridade e disponibilidade (Figura 3.2) dos dados e informações, em todas as suas formas e todos os estados.

Figura 3.1 | Formas e estados do dado e informação



Fonte: elaborada pelo autor.

Figura 3.2 | Tríade CID: confidencialidade, integridade e disponibilidade



Fonte: elaborada pelo autor.

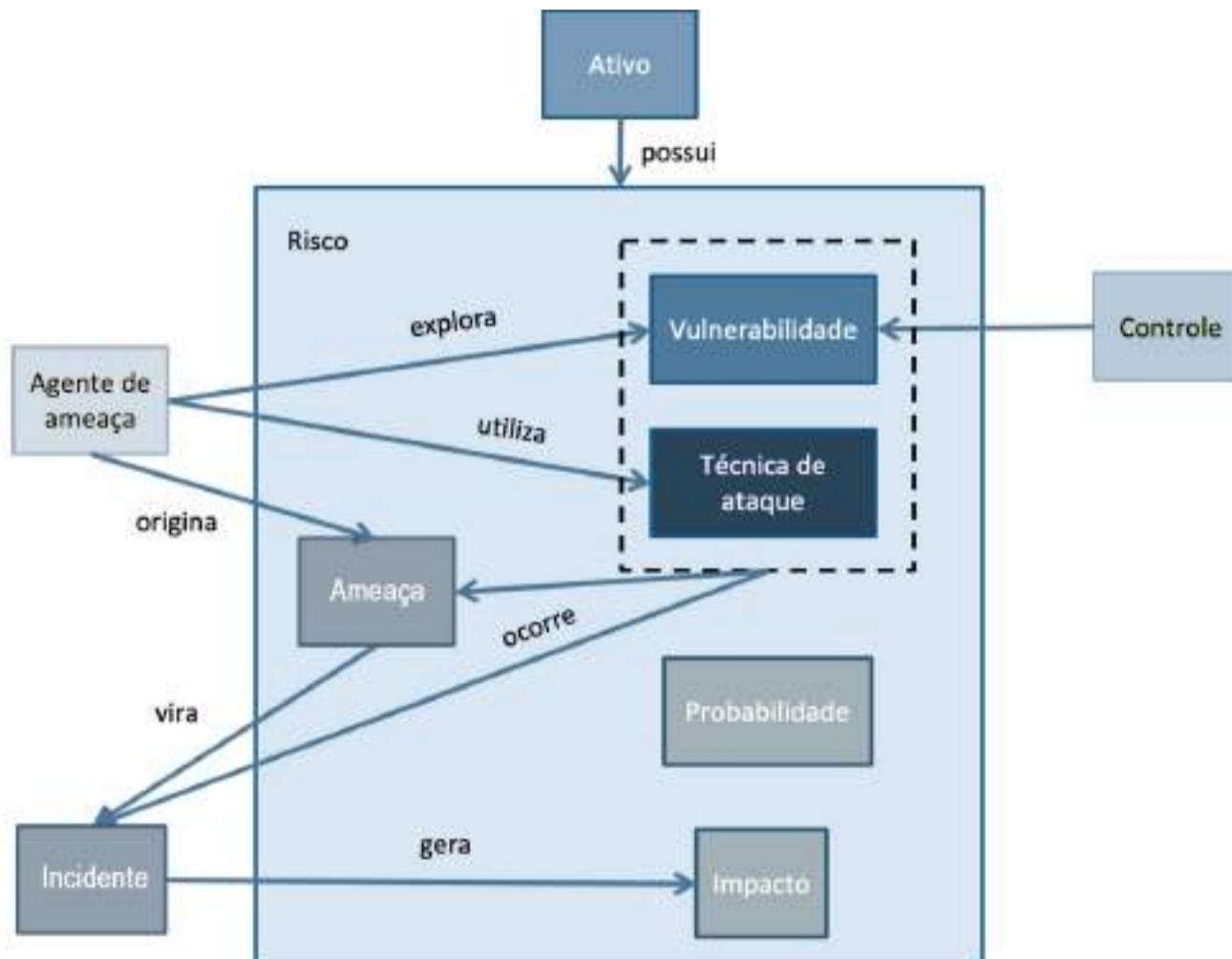
Outros elementos importantes são aqueles do risco, que podem ser vistos na Figura 3.3. Um risco é a probabilidade de um agente de ameaça explorar vulnerabilidade de um ativo utilizando uma técnica de

ataque, o que faz com que uma ameaça se torne um incidente de segurança, o que resulta em impactos para a organização. Os controles de segurança são implementados para tratar as vulnerabilidades específicas daquele ativo.

o

Ver anotações

Figura 3.3 | Elementos do risco



Fonte: elaborada pelo autor.

Todos esses elementos fazem parte do entendimento da segurança na internet. As transações web, que partem dos usuários que utilizam seus dispositivos a partir de algum local em que há uma conexão com a internet, passam por variados componentes até chegar à loja virtual, ao serviço do governo ou ao banco. Neste caminho, os agentes de ameaça estão à espreita em busca de oportunidades para roubar os dados pessoais, dados das transações web e as identidades digitais. Além da exploração de vulnerabilidades, estes agentes de ameaça buscam os golpes na internet para o mesmo fim, isto é, ter acesso a informações valiosas (OLIVEIRA, 2017).

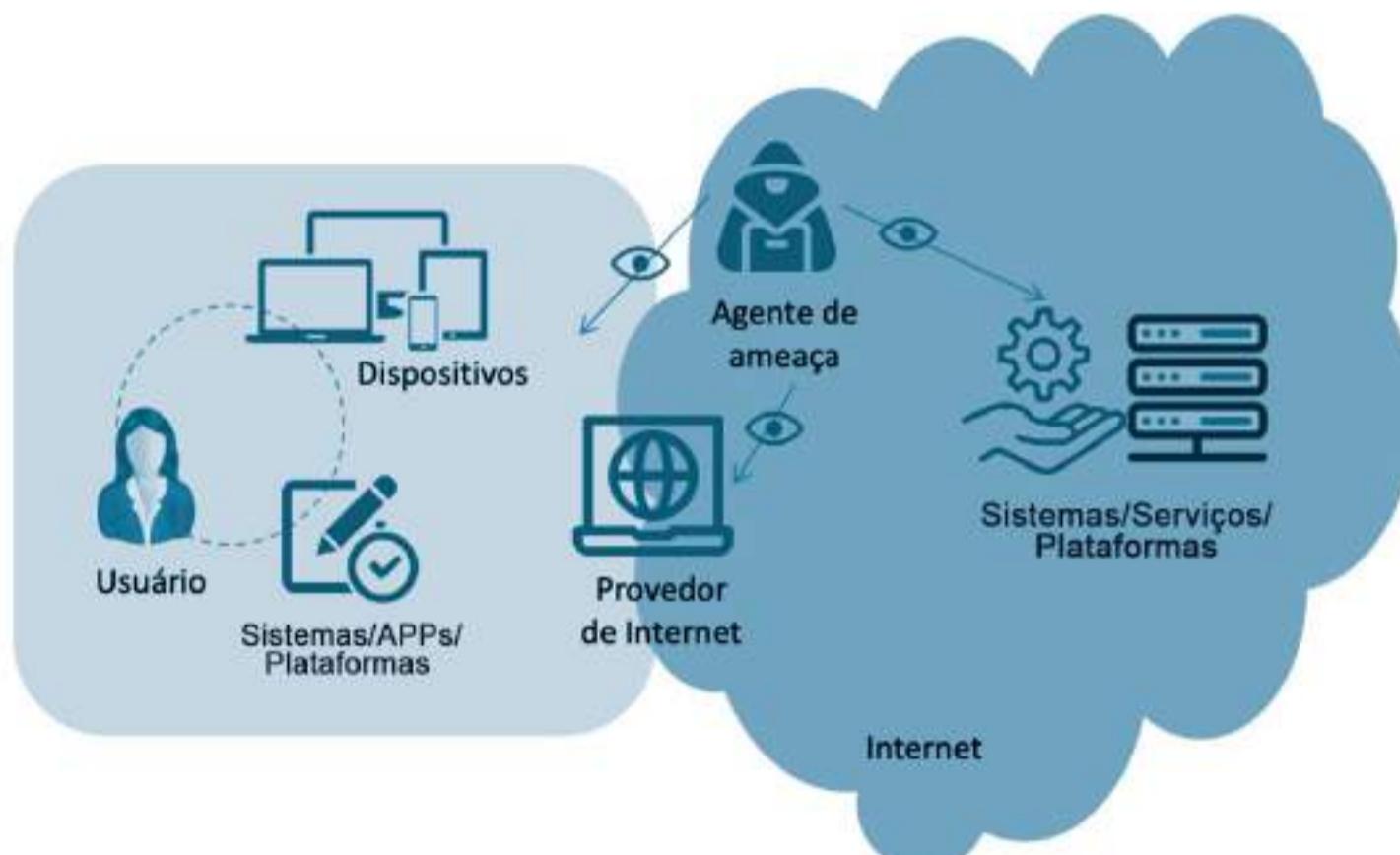
A Figura 3.4 ilustra esta dinâmica da segurança na internet, com o agente de ameaça buscando oportunidades em três ambientes:

- No ambiente do usuário.

- No ambiente de Internet que inclui o provedor de internet.
- No ambiente dos provedores de serviços, sistemas e plataformas.

Há a necessidade de segurança pelo usuário, que deve proteger o seu ambiente composto por ele próprio, os dispositivos e os sistemas, aplicativos e plataformas que ele instala em seus dispositivos. Há ainda a necessidade de segurança pelo provedor de internet, que além do canal de comunicação que dá o acesso à internet provê o acesso a serviços fundamentais como o *Domain Name Service (DNS)*, o qual em caso de comprometimento pode levar os usuários a sites falsos. E há a necessidade de segurança pelos provedores de sistemas, serviços e plataformas, compostos pelas empresas que incluem bancos, comércio eletrônico, serviços de governo, serviços de saúde, comunicação, entre outros.

Figura 3.4 | Segurança na internet



Fonte: elaborada pelo autor.

SEGURANÇA EM TRANSAÇÕES WEB

As transações *web*, realizadas pela internet, envolvem uma série de questões de segurança que partem do usuário e chegam ao provedor de serviços, como um banco, passando pelo provedor de internet.

Uma transação *web* pode ser uma compra online, uma transação bancária, a realização de algum serviço governamental ou até mesmo uma postagem em uma rede social.

E as transações podem envolver diferentes tipos de dados ou informações: dados pessoais, dados financeiros ou dados confidenciais, que podem sofrer modificações, vazamentos ou destruições, afetando, respectivamente, a integridade, confidencialidade e disponibilidade.

REFLITA

Uma transação possui diferentes significados, dependendo do contexto. No seu conceito mais amplo, uma transação significa a troca de bens. Já no contexto da tecnologia, no caso de banco de dados, uma transação significa uma operação ou uma unidade de trabalho executado de uma forma coerente e confiável, independente de outras transações (CONCEITOS, 2020). E, com os ataques cibernéticos, as transações podem ser manipuladas, vazadas ou removidas antes, durante ou após chegarem ao seu destino.

A segurança em transações web passa pela proteção dos três ambientes, como pode ser visto na Figura 3.5:

- Ambiente do usuário, composto pelo próprio usuário, seus dispositivos e os sistemas, aplicativos e plataformas instaladas.
- Ambiente de internet, composto pela comunicação e o provedor de internet.
- Ambiente do serviço, sistema, plataforma ou aplicação, composto pela empresa que presta o serviço que está sendo acessado pelo usuário.



Fonte: elaborada pelo autor.

Os dados e as informações existem em seus três estados (em processamento, em transmissão e em armazenamento) e podem sofrer ataques em qualquer ponto de um dos três ambientes. Estes pontos de ataques são representados por ativos humanos, físicos ou tecnológicos. Por exemplo: um agente de ameaça pode atacar o próprio usuário buscando a engenharia social para a instalação de um *malware*. Ou o agente de ameaça pode monitorar o tráfego de um provedor de internet em busca de dados e informações. Além dessas possibilidades, o agente de ameaça pode explorar vulnerabilidades da aplicação do provedor de serviços para o acesso não autorizado aos dados das transações.

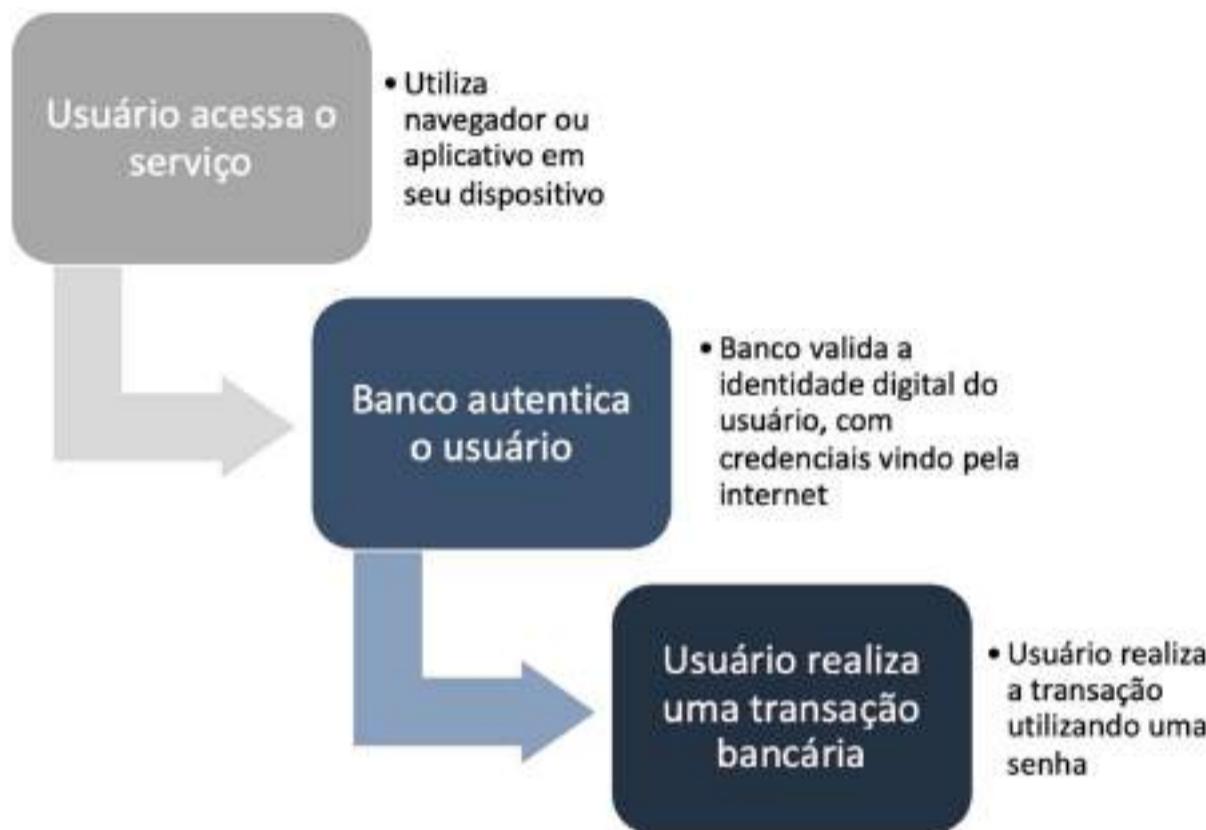
Em um exemplo de transação bancária, o fluxo simplificado pode ser visto na Figura 3.6. O usuário utiliza seu dispositivo e acessa a instituição financeira, o banco, por seu navegador ou pelo uso de uma aplicação instalada em seu dispositivo. O usuário então se identifica utilizando uma identidade digital como o seu CPF, número de agência e conta ou nome de usuário. A validação da identidade, ou autenticação do usuário, é feita pelo uso de uma senha. Uma vez dentro do serviço do

banco após a autenticação, o usuário pode fazer uma transação bancária, como uma transferência ou um pagamento de conta. Essa transação exige uma autenticação adicional, como o uso da senha do cartão bancário. E toda essa comunicação entre o usuário, a partir do navegador ou aplicativo, chega ao servidor do banco, passando pela internet.

o

Ver anotações

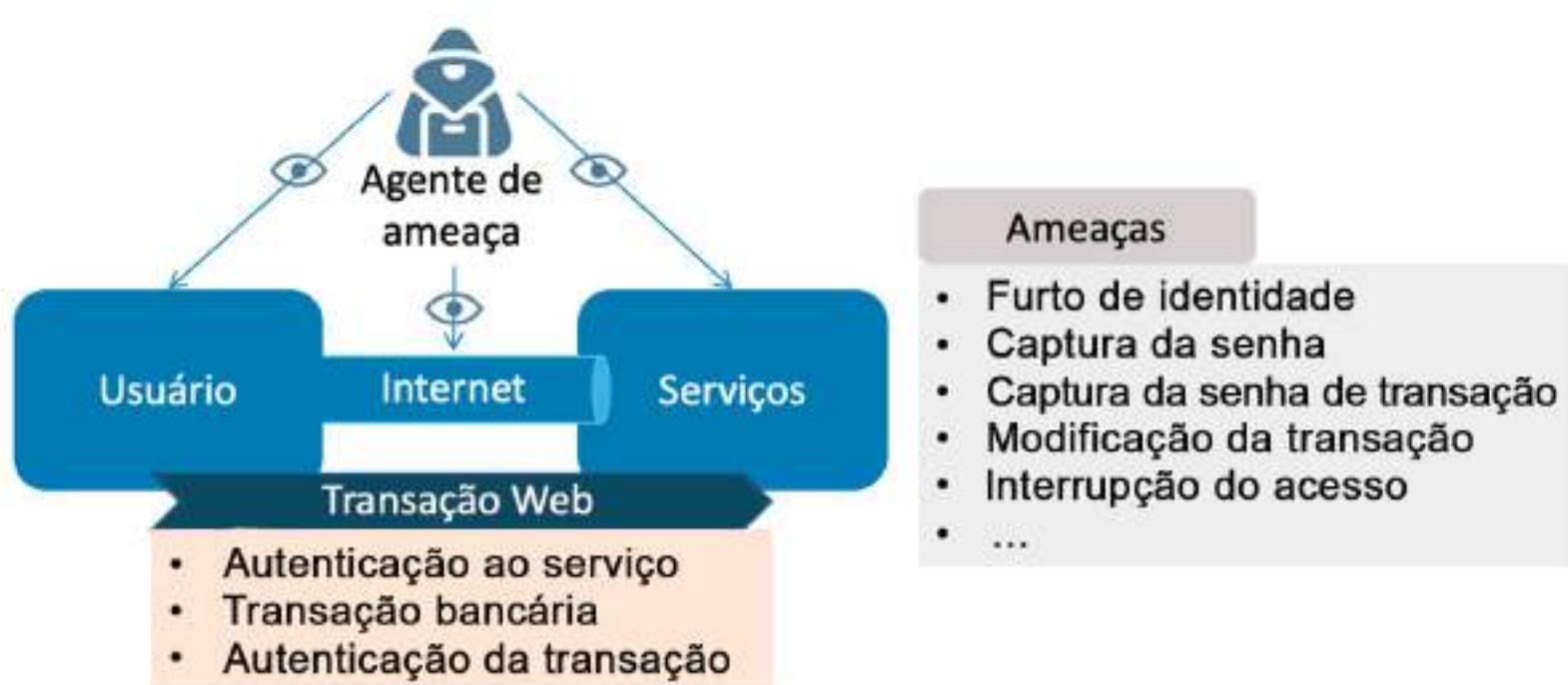
Figura 3.6 | Exemplo de transação *web* em bancos



Fonte: elaborada pelo autor.

As ameaças, neste exemplo, são o furto de identidade, a captura da senha, a captura da senha de transação, a modificação da transação e a interrupção do acesso, que podem afetar a autenticação ao serviço, a transação bancária e a autenticação da transação (Figura 3.7). Elas podem ocorrer em qualquer um dos três ambientes, porém de uma forma diferente, o que leva à necessidade de controles de segurança diferentes, que afetam também as responsabilidades.

Figura 3.7 | Ameaças no exemplo de transação *web* em bancos



Fonte: elaborada pelo autor.

Os três ambientes precisam ser protegidos. Os dados de autenticação ao serviço, da transação bancária e da autenticação da transação podem ser capturados, modificados ou removidos de diferentes formas.

No **ambiente do usuário**, as transações *web* exigem segurança porque malwares podem capturar e modificar dados a partir da origem no próprio usuário. Neste caso, a transação chega ao provedor de serviços, como o banco, já de uma forma ilegítima, seja pela modificação da transação ou pelo furto de identidade. O provedor de serviços, assim, além de ter de proteger o seu próprio ambiente, tem o desafio de receber uma transação vindo de um criminoso, que furtou a identidade do usuário verdadeiro.

EXEMPLIFICANDO

Os bancos têm investido muito em comunicação e campanhas para os seus clientes, para que não sejam vítimas de fraudes que levam ao furto de identidades. Além disso, utilizam mecanismos de segurança como autenticação de duplo fator e sistemas antifraude (CARVALHO, 2018). Com a autenticação de duplo fator, é necessário, além da senha, um código único que é enviado para o dispositivo móvel do usuário, de uma forma que, no caso de furto de credencial do usuário, ainda é necessário o código enviado para o dispositivo móvel para o acesso ou a transação bancária.

Outro fator de autenticação, utilizado normalmente para confirmar as transações, é a biometria. Já o sistema antifraude analisa diferentes parâmetros das transações com base em perfil de usuário para tentar identificar se é realmente o usuário legítimo que está fazendo a transação.

No **ambiente de internet**, em que o agente de ameaça pode capturar ou modificar as transações web, é importante que elas sejam realizadas com o uso de um canal seguro, que deve ser provido pelo provedor de serviços, como o banco. As conexões web podem ser protegidas com o uso de protocolos de segurança como o *Hyper Text Transfer Protocol Secure* (HTTPS), que foi visto na Unidade 1 da disciplina. O HTTPS possibilita o uso do HTTP sobre uma sessão *Secured Socket Layer* (SSL) ou *Transport Layer Security* (TLS), com a criação de um túnel seguro por onde trafegam as informações. Além de garantir a confidencialidade (dados cifrados com chave simétrica de sessão), eles podem visar também a integridade dos dados (uso de *Message Authentication Code*, MAC) e a autenticidade das partes (as entidades podem ser autenticadas com o uso de criptografia de chave pública).

Já no **ambiente do provedor de serviços**, como no caso de bancos, o ambiente pode ser atacado em qualquer um dos componentes, incluindo as aplicações, os servidores de aplicação, os sistemas operacionais, as máquinas virtuais, os bancos de dados. Toda a estratégia de segurança da informação corporativa deve ser seguida pelos provedores de serviços, incluindo as ações de segurança e privacidade com os processos e as pessoas. É importante que o profissional de segurança e privacidade considere que os ataques podem ter origem externa, mas também interna.

ASSIMILE

A segurança em transações web envolve o entendimento das ameaças que existem em três ambientes: do usuário, da internet e do provedor de serviços. Uma transação web tem a

origem no usuário, que utiliza dispositivos e aplicações, que chegam até os servidores do provedor de serviços, como os bancos, pela internet. Há ameaças neste caminho também quando as transações chegam ao provedor de serviços. Os dados e as informações passam por diferentes estados neste fluxo das transações web, sendo processados, transmitidos e armazenados.

I GOLPES NA INTERNET

As ameaças existentes nas transações web envolvem os usuários, os provedores de internet e os provedores de serviços. Um dos grandes desafios dos profissionais de segurança e privacidade é fazer com que o equilíbrio da segurança possa ser estabelecido, o que é difícil para os provedores de serviços, que vêm implementando um conjunto de controles de segurança para minimizar os efeitos negativos de um ambiente de usuário contaminado. Esta contaminação faz com que uma transação já chegue de uma forma insegura, como no caso de um criminoso se passando pelo usuário legítimo.

E a contaminação do usuário é um ponto essencial para ser tratado, já que leva ao furto de identidades e a transações fraudulentas, como pagamento de boletos falsos, levando a prejuízos tanto para o usuário quanto para as empresas.

EXEMPLIFICANDO

Bolware é um tipo de ataque em que os usuários são vítimas de um vírus que altera os boletos. Quando uma operação de pagamento está sendo realizada, o *malware* intercepta a transmissão e troca os dados do boleto legítimo. O sistema do banco acaba então recebendo e processando as informações do boleto falso (ALECRIM, 2014).

Os golpes na internet, assim, visam explorar os usuários, com uso de técnicas de engenharia social que levam à instalação de *malwares*, ao direcionamento para *sites falsos* e ao envio de dados sensíveis para criminosos. O resultado é um conjunto de atividades maliciosas que incluem o furto de identidades para criação de contas fraudulentas em serviços *online* e bancos, a realização de transações ilícitas, o envio de mensagens falsas, o acesso a serviços variados por terceiros, entre outras atividades possíveis a partir das credenciais das vítimas ou dados sensíveis.

O CERT.br (2020) lista alguns dos principais golpes aplicados na internet (Figura 3.8):

- **Furto de identidade**, com o criminoso tentando a se passar pelo usuário real, podendo criar contas em seu nome, realizando transações indevidas ou enviando mensagens ou postagens em seu nome.
- **Fraude de antecipação de recursos**, em que o golpista procura induzir a vítima a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício. Exemplos são o golpe da Nigéria, e outros que envolvem loteria internacional, crédito fácil, doação de animais, oferta de emprego e noiva russa. Outro golpe é o do WhatsApp, em que o golpista obtém o acesso à conta da vítima se passando por um funcionário de uma empresa que solicita um código de reinicialização (que na realidade é do WhatsApp) e a partir dessa transferência das credenciais para o golpista, os contatos da vítima passam a receber solicitações de depósitos para pagamento de uma dívida, que são feitas na conta do golpista.
- **Phishing ou scam**, em que o golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. Este golpe explora a atenção, curiosidade, caridade, medo ou possibilidade de obtenção de

vantagem financeira, com o criminoso se passando por uma instituição como banco, empresa ou *site* popular. Envolve a possibilidade de inscrição em serviços de proteção de crédito, ou o cancelamento de cadastro, conta bancária ou cartão de crédito, e leva a vítima a páginas falsas em que entregam suas credenciais, senhas ou informações sensíveis, além da instalação de códigos maliciosos.

o

- **Pharming**, em que a vítima tem a sua navegação redirecionada por meio de alterações no serviço de *Domain Name System* (DNS), que ao invés do site correto, leva a um site falso. Essa alteração pode ser feita no dispositivo do usuário, ou no provedor de internet;
- **Golpes de comércio eletrônico**, em que são exploradas as relações de confiança existentes entre partes envolvidas em uma transação comercial. Envolvem a criação de site de comércio eletrônico fraudulento e o uso *sites* de compras coletivas ou de leilão, em que obtém os recursos, porém não cumprem os acordos comerciais, como uma venda em que o dinheiro é obtido sem a entrega dos produtos.
- **Boato ou hoax**, em que conteúdos alarmantes ou falsos levam a tentativas de golpes, como correntes e pirâmides, além de poder conter códigos maliciosos, espalhar desinformação pela internet e comprometer a credibilidade e reputação de pessoas e empresas.

Ver anotações

Figura 3.8 | Principais golpes na internet



Fonte: elaborada pelo autor.

DICA

Uma fonte de informações sobre fraudes, golpes, burlas, lavagem de dinheiro, corrupção e outros perigos que existem na vida privada, na internet, no setor público e no mundo financeiro e dos negócios é o Monitor das Fraudes (MONITOR, 2020). Outra fonte é o Catálogo de Fraudes da RNP (RNP, 2020), que alerta a comunidade sobre os principais golpes em circulação na internet.

As principais ações para a proteção contra os golpes aplicados na internet são a notificação para a organização envolvida a fim de se tomar as medidas cabíveis e a busca constante de informação sobre o assunto. Em alguns casos, ataques de negação de serviço coordenados (*Distributed Denial of Service*, DDoS) são utilizados em conjunto, o que tornam serviços como o comércio eletrônico das empresas indisponíveis e tornam as fraudes mais plausíveis.

O uso seguro de internet pelos usuários é parte fundamental da segurança das empresas. No caso dos bancos, por exemplo, uma transação pode chegar à instituição já de uma forma fraudulenta, seja pelo furto de identidade de um cliente legítimo, seja pela alteração de transações, como no caso de boletos bancários.

Assim, um papel importante do profissional de segurança é considerar os usuários e clientes como um dos principais ativos a serem protegidos, com o uso constante de treinamento e conscientização.

O uso seguro de internet pelos usuários envolve, principalmente, dois pontos principais:

- Como saber se um *site* é seguro?
 - A empresa deve configurar o HTTPS/TLS/SSL e o usuário deve verificar as informações do certificado digital utilizado para validar a empresa e o site, se possuem as informações correspondentes.
- Como saber se um *site* é falso?
 - A empresa deve configurar o HTTPS/TLS/SSL e o usuário deve verificar o endereço ou URL que está sendo acessado, com atenção, já que *sites* falsos costumam inserir caracteres especiais ou modificações sutis do endereço real. Endereços falsos são enviados a vítimas em *e-mails*, ou SMS, de modo que os endereços de sites devem ser digitados diretamente no navegador.

Algumas das principais recomendações para usuários, que devem ser incluídas em treinamentos e campanhas de conscientização, são (CARVALHO, 2018):

1. Não acesse *sites* a partir de computadores compartilhados, que podem conter *malwares* que capturam os dados inseridos, como dados sensíveis ou credenciais de acessos.

2. Não acesse *sites* a partir de redes *wi-fi* públicas, que podem direcionar a *sites* falsos ou fazem a conexão com sites, com a captura dos dados trafegados.
3. Mantenha o antivírus do dispositivo sempre atualizado, para que seus dispositivos não sejam contaminados com *malwares*.
4. Digite o endereço do site no navegador, para evitar sites falsos a partir de *links* recebidos por *e-mails* ou SMS.
5. Habilite a verificação em duas etapas ou o duplo fator de autenticação, para evitar acessos indevidos às contas em caso de furto de identidade ou credenciais de acesso.
6. Não clique em *links* recebidos por *e-mail* ou SMS, para evitar ser direcionado a *sites* falsos que buscam obter seus dados sensíveis e credenciais de acesso.
7. Cuidado ao usar extensões no navegador, que podem instalar *malwares* em seus dispositivos.

PRIVACIDADE NA WEB

A privacidade na *web* possui visões a serem consideradas. De um lado, há o rastreamento do que as pessoas fazem na *web*, como os *cookies*. Do outro, há a divulgação espontânea de informações pessoais em redes sociais, que podem resultar em crimes que transcendem o digital e podem afetar diretamente as pessoas com fraudes e crimes diversos. E, com a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2020), todos devem preservar a privacidade e a proteção de dados pessoais.

REFLITA

A privacidade é um direito fundamental da pessoa natural, e diz respeito à proteção de dados pessoais, que, segundo a LGPD, é a informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2020). Dados e informações corporativos podem ser considerados sigilosos e

confidenciais, dependendo dos níveis de classificação da informação, e não possuem relação direta com a privacidade. Alguns dados pessoais, no entanto, podem existir em documentos sigilosos ou confidenciais.

O rastreamento do que as pessoas fazem na *web* corresponde a dados que identificam uma pessoa e do mesmo modo devem ser protegidos segundo a LGPD. A privacidade na *web*, neste contexto, faz com que os dados pessoais devam ser tratados pelas empresas com toda a segurança necessária. Os usuários, que são os donos ou titulares dos seus dados, devem ter o total conhecimento sobre o que está sendo tratado e como estão sendo protegidos pelas organizações. A privacidade na *web*, assim, não significa que as organizações não podem tratar os dados pessoais, mas sim que os usuários têm direitos sobre estes dados e eles devem ser protegidos com a segurança da informação. Um dos mecanismos para que a privacidade funcione é o consentimento, que pode ser de acordo com uma base legal (BARROS, 2020).

De uma forma geral, o usuário, ao acessar um *site*, deve saber que um *cookie* está ativo, se for o caso, e deve aceitar o seu uso. Já no momento de inserir dados pessoais, o usuário deve ter acesso a um aviso de privacidade, que diz quais dados e a finalidade da coleta, o compartilhamento com outras entidades e a forma como eles serão protegidos. Após o aceite do usuário, a empresa deve proteger os dados coletados para evitar vazamentos. Em caso de vazamento ou a falta de aviso de privacidade, a empresa está sujeita às sanções da LGPD, que podem chegar à multa e à paralização das operações. O usuário tem uma série de direitos, como o de consulta sobre quais dados estão de posse da empresa, e de solicitação de remoção, que deve ser feito em caso de não haver uma exigência legal para que eles sejam preservados.

Assim, a privacidade na web tem elementos que exigem uma série de atividades do profissional de segurança e privacidade. A LGDP reforça a necessidade dos controles de segurança, já que um vazamento pode resultar em sanções previstas na lei. As questões de privacidade e proteção de dados pessoais devem fazer parte das atividades dos profissionais de segurança da informação.

o

Ver anotações

SAIBA MAIS

O CERT.br (2020) faz uma série de recomendações importantes para a privacidade. Para a proteção da sua vida profissional, algumas recomendações são:

- Cuide da sua imagem profissional. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode atrapalhar um processo seletivo que você venha a participar (muitas empresas consultam as redes sociais à procura de informações sobre os candidatos, antes de contratá-los);
- Verifique se sua empresa tem um código de conduta e procure estar ciente dele. Observe principalmente as regras relacionadas ao uso de recursos e divulgação de informações;
- Evite divulgar detalhes sobre o seu trabalho, pois isto pode beneficiar empresas concorrentes e colocar em risco o seu emprego;
- Preserve a imagem da sua empresa. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode prejudicar a imagem e os negócios da empresa e, indiretamente, você mesmo;
- Proteja seu emprego. Sua rede de contatos pode conter pessoas do círculo profissional que podem não gostar de saber que, por exemplo, a causa do seu cansaço ou da

sua ausência é aquela festa que você foi e sobre a qual publicou diversas fotos;

- Use redes sociais ou círculos distintos para fins específicos. Você pode usar, por exemplo, uma rede social para amigos e outra para assuntos profissionais ou separar seus contatos em diferentes grupos, de forma a tentar restringir as informações de acordo com os diferentes tipos de pessoas com os quais você se relaciona.

PESQUISE MAIS

Atacantes podem ser internos e externos e têm motivações diferentes. Eles executam uma série de ataques, os quais exigem que as organizações implementem seus controles de segurança. O livro *Tópicos de segurança da informação*, de OLIVEIRA (2017), no capítulo 6, sobre “Principais Ataques Virtuais e suas Contramedidas”, cita os perfis de atacantes, e os principais ataques e contramedidas. (OLIVEIRA, 2017).

OLIVEIRA, R. C. Q. **Tópicos de segurança da informação**. São Paulo: Editora Senac São Paulo, 2017.

Chegamos ao final desta seção, que tratou de aspectos da segurança na internet, que envolve usuários, provedores de internet e provedores de serviços. As transações *web* precisam de segurança e, muitas vezes as empresas dependem da segurança do ambiente dos usuários, que podem ter suas identidades furtadas ou serem fonte de transações fraudulentas. O treinamento e a conscientização dos usuários são essenciais, para que recebam recomendações para não cair em golpes na internet e para que façam uso seguro da internet. A privacidade na web ganhou ainda mais importância com a LGPD, que estabelece direitos para os usuários, os quais têm o direito fundamental à privacidade. Os dados pessoais devem ser protegidos e os direitos dos usuários, incluindo a transparência relacionada ao tratamento dos dados, devem ser cumpridos.

FAÇA VALER A PENA

Questão 1

Um dos principais ataques contra usuários explora atenção, curiosidade, caridade, medo ou possibilidade de obtenção de vantagem financeira, com o criminoso se passando por uma instituição como banco, empresa ou site popular. Envolve a possibilidade de inscrição em serviços de proteção de crédito ou o cancelamento de cadastro, conta bancária ou cartão de crédito, e leva a vítima a páginas falsas onde entregam suas credenciais, senhas ou informações sensíveis, e podem instalar no dispositivo do usuário códigos maliciosos.

Assinale a alternativa que apresenta o tipo de ataque que explora diretamente os usuários.

a. Phishing.

b. Pharming.

c. Malware

d. DDoS.

e. Firewall.

Questão 2

Em ataques de *phishing*, o golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. Uma das principais técnicas é o envio de uma mensagem de e-mail ou um SMS com um *link* para um assunto de interesse da vítima.

Assinale a alternativa que contém uma forma em que o usuário pode se proteger contra ataques de *phishing*.

a. Não há proteção contra este ataque.

b. Instalando um *firewall*.

c. Instalando um antimalware.

d. Não clicando em links recebidos.

e. Atacando o remetente.

Questão 3

Você trabalha em uma empresa que comercializa materiais de construção pela internet. Ultimamente a empresa tem recebido muitos pedidos fraudulentos, os quais têm gerado um grande prejuízo. Estes pedidos são feitos por clientes antigos, que depois negam os pedidos, já que nem receberam os produtos. Já outros clientes entram em contato porque estranham transações em seus cartões de crédito na loja, sem que tenham feito pedidos.

Você acredita que um ataque cibernético está levando a essas fraudes. O acesso ao serviço é feito pelos clientes usando HTTPS. E, além do IPS não ter emitido nenhum alerta, você já analisou os logs dos servidores, não detectando nenhum acesso suspeito, principalmente no banco de dados. O fato pode estar ocorrendo pois:

a. sua empresa foi *hackeada* e os rastros foram apagados.

b. os usuários estão sendo contaminados com uma nova campanha de *phishing*.

c. os hackers estão invadindo bancos e roubando números de cartões de crédito.

REFERÊNCIAS

ALECRIM, E. RSA: malware que altera boletos bancários pode ter causado prejuízo de R\$ 8,5 bilhões. **Tecnoblog**, Antivírus e Segurança, 2 jul. 2014. Disponível em: <https://bit.ly/2PjVEal>. Acesso em: 20 dez. 2020.

BARROS, M. 10 Bases Legais da LGPD: Quais são? [Guia Completo]. **Legalcloud**, Análise de leis, LGPD, 4 nov. 2020. Disponível em: <https://bit.ly/3siaVqV>. Acesso em: 20 dez. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Presidência da República – Secretaria-Geral - Subchefia para Assuntos Jurídicos. Disponível em: <https://bit.ly/2QBxU28>. Acesso em: 25 out. 2020.

CARVALHO, T. *Sites de bancos: perguntas e respostas sobre segurança*. **TechTudo**, 8 out. 2018. Disponível em: <https://glo.bo/2Qv5uGR>. Acesso em: 20 dez. 2020.

CERT.br. Golpes na internet. **Cartilha de segurança para internet**. Disponível em: <https://bit.ly/39aYpSh>. Acesso em: 19 dez. 2020.

CONCEITOS. **Transação – Conceito, o que é, significado**. Disponível em: <https://bit.ly/3IKBEK0>. Acesso em: 19 dez. 2020.

MONITOR. **Monitor das fraudes**. Disponível em: <http://www.fraudes.org>. Acesso em: 20 dez. 2020.

OLIVEIRA, R. C. Q. **Tópicos de segurança da informação**. São Paulo: Editora Senac São Paulo, 2017.

REDE Nacional de Ensino e Pesquisa. **Catálogo de fraudes**. Disponível em: <https://bit.ly/31bRUKz>. Acesso em: 20 dez. 2020.

FOCO NO MERCADO DE TRABALHO

SEGURANÇA NA INTERNET

Emilio Tissato Nakamura

Ver anotações 0

QUAIS SÃO OS PRINCIPAIS GOLPES DE INTERNET?

Os principais golpes de internet são: furto de identidade, fraude na antecipação de recursos, *phishing* ou *scam*, *pharming*, golpes de comércio eletrônico, boato ou *hoax*.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Você, como especialista em segurança e privacidade de uma plataforma digital, tem grandes responsabilidades. O planejamento dos principais aspectos que a empresa deve considerar para a segurança e privacidade é importante para direcionar a estratégia da empresa. O foco deste planejamento está na segurança em transações *web*, que complementa a segurança da informação da plataforma digital em si. Como a plataforma digital está em um provedor de nuvem, há vários aspectos como a arquitetura segura, desenvolvimento seguro, gestão de vulnerabilidades e gestão de continuidade de negócios, por exemplo.

Para a segurança em transações *web*, você pode começar o seu planejamento considerando os seguintes aspectos, os quais devem ser detalhados e desenvolvidos:

- Transação parte do usuário, que utiliza dispositivos e possui instalados aplicativos ou aplicações.
- Transação trafega pela internet, passando pelo provedor de internet.
- Transação chega à empresa e os dados são processados e armazenados.
- Há ameaças no ambiente do usuário, do provedor de internet e da empresa.
- Se o usuário for comprometido, a empresa também pode ser.
- O que pode ser feito para que o usuário não seja comprometido.
- O que deve ser feito pela empresa após receber os dados pessoais e transacionais.

O ponto central a ser planejado é que, além dos controles de segurança para proteger a transmissão dos dados dos clientes para a sua empresa, usando HTTPS/TLS/SSL, os clientes são parte central da segurança e privacidade, pois transações fraudulentas podem chegar à empresa a partir deles.

Mostre que pode haver o furto de identidade, a captura da senha, a captura da senha de transação, a modificação da transação e a interrupção do acesso. Essas ameaças existem no ambiente do cliente, no ambiente de internet e no próprio ambiente da empresa, que utiliza um provedor de nuvem.

Mostre que, no ambiente do cliente, os golpes na internet potencializam as ameaças, aumentando o nível de risco. E, como é o ambiente com menor controle, o desafio é maior nos clientes. Apresente os principais golpes na internet que podem comprometer a empresa, com destaque para o *phishing* e o *pharming*.

Defina a partir deste mapeamento um plano de conscientização para os clientes, minimizando as probabilidades deles caírem em fraudes na *internet*, e também de serem vítimas de *malwares*. Dentre as dicas, podem ser inclusos pontos como não clicar em *links* recebidos por e-mails e SMS, além de verificar sempre se uma conexão segura está estabelecida com a empresa, verificando os dados do certificado digital.

Um outro ponto importante para aumentar o nível de segurança é o uso de autenticação de duplo fator. Com este controle de segurança, em caso de furto de identidade, ainda é necessário o dispositivo móvel para o acesso aos serviços da empresa, o que torna o acesso indevido mais difícil.

Com relação à privacidade e proteção de dados pessoais, o planejamento deve incluir os avisos de privacidade na coleta das informações dos clientes. Além disso, a proteção destes dados pela empresa é parte da estratégia de segurança e privacidade, com o reforço de que há sanções previstas na LGPD.

Outro ponto importante a ser planejado são os processos e mecanismos para o atendimento às solicitações dos clientes, que podem consultar e solicitar a remoção dos seus dados pessoais.

Assim, com o tratamento destes principais aspectos, a empresa poderá operar com a necessária segurança e privacidade, minimizando os problemas de acessos a partir de clientes falsos, resultando em melhores resultados.

0

Ver anotações

AVANÇANDO NA PRÁTICA

AUMENTANDO A SEGURANÇA NO ACESSO PELO NAVEGADOR

Os clientes de sua empresa virtual fazem o acesso pelo navegador, digitando o *link*. Você já implementou a segurança do servidor e envia constantemente mensagens para seus clientes para que eles aumentem o nível de conscientização e não caiam em golpes que podem levar ao furto de identidade, que no final resulta em prejuízos para a sua empresa. Cite os pontos que podem levar à contaminação do ambiente do cliente e por que evitar o furto de identidade é crucial para a sua empresa. Além disso, cite algumas possibilidades para você aumentar a segurança no acesso do cliente pelo navegador.

RESOLUÇÃO



A empresa deve evitar as transações maliciosas, que podem chegar de duas formas principais: a partir de um criminoso que furtou a identidade do cliente e faz as transações como se fosse ele, utilizando recursos financeiros também de terceiros; e a partir de transações modificadas que partem do cliente legítimo, mas com os dados alterados para beneficiar o criminoso. A identidade pode ser furtada com a instalação de *malwares* que capturam os dados, os quais podem contaminar os clientes com o uso de *phishing* ou *pharming* como principal vetor, além de poder ser pela exploração de vulnerabilidades em diferentes componentes do dispositivo do cliente. Com o *phishing*, o cliente pode clicar em um *link* que leva para um site falso que coleta os dados de acesso e dados pessoais, incluindo o nome de usuário e senha. O *phishing* também pode fazer com que *malwares* sejam instalados quando executados pelos clientes. Os *malwares* podem também modificar os dados das transações na saída do ambiente do cliente e a empresa recebe essas transações adulteradas.

Uma vez com as credenciais do cliente, o agente de ameaça pode fazer as transações como se fosse ele, porém em benefício próprio.

Um mecanismo tradicional de se utilizar para evitar o uso de identidades furtadas é o uso de autenticação de dois passos ou de duplo fator. Em autenticação, os fatores são algo que o usuário sabe (como senhas), algo que o usuário possui (como tokens ou dispositivos móveis) ou algo que o usuário é (como a biometria).

Com o uso de autenticação de duplo fator, é necessário, além da senha, um outro elemento, como um código único temporário enviado ao dispositivo móvel do usuário via SMS.

Há ainda a possibilidade de utilizar mecanismos de segurança que fazem uma proteção contra *malwares* para evitar a contaminação pelos usuários. Estes mecanismos devem ser instalados e fazem a proteção contra *malwares*, mas apresentam pontos negativos, como o uso de recursos computacionais dos dispositivos dos usuários, bem como a interferência na usabilidade.

Assim, como profissional de segurança, você deve adotar a abordagem em camadas, podendo utilizar ainda controles de segurança como processos de validação de transações ou uso de plataformas antifraude. Uma visão de riscos é fundamental, já que os controles de segurança podem afetar tanto a usabilidade dos clientes quanto a própria operação, que pode ficar mais complexa com as validações. Uma forma de flexibilizar as validações é a adoção de níveis, com base, por exemplo, em valores das transações. Deste modo, transações maiores teriam validações mais estruturadas, enquanto as menores teriam validações mais automatizadas, por exemplo. Isto deve ser definido com uma visão de riscos, e deve ser dinâmica, com atualizações constantes.

NÃO PODE FALTAR

PROTEÇÃO PARA DISPOSITIVOS MÓVEIS

Emilio Tissato Nakamura

Ver anotações 0

QUAIS SÃO OS RISCOS NO USO DE DISPOSITIVOS MÓVEIS NO MUNDO CORPORATIVO?

Além dos riscos já comuns em outros ambientes, há também os riscos pelas próprias características dos dispositivos móveis, que passam a ser mais distribuídos, os dados corporativos passam a existir fora dos servidores da empresa e há a mistura com os dados pessoais que podem comprometer a privacidade dos usuários.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Olá, nesta aula discutiremos um dos assuntos mais importantes para a estratégia de segurança e privacidade das empresas: o uso de dispositivos móveis. Eles são um dos principais vetores de ataques, por meio dos quais os criminosos virtuais buscam maximizar seus resultados visando o canal em que há maior número de alvos e possibilidades de sucesso.

Os dispositivos móveis representam um grande desafio para as empresas, já que, além dos dados corporativos, há os dados pessoais de seus usuários. E isso implica no aumento da complexidade de proteção, além do intrínseco aumento de riscos. Um exemplo desse desafio é quando um colaborador instala jogos em seu dispositivo móvel, mas a partir de fontes não confiáveis. O resultado pode ser a introdução no dispositivo de malwares que comprometem a privacidade do colaborador, assim como dos dados confidenciais corporativos que podem estar no dispositivo ou serem acessados a partir dele.

Nesta aula entenderemos também as ameaças e os ataques voltados para o mundo móvel, para então provermos a defesa necessária. E os elementos de segurança são diferentes do tradicional, já que os dispositivos móveis têm características próprias que precisam ser consideradas. Uma delas é o seu formato, que é portátil e, portanto, pode levar ao acesso físico ao dispositivo que contém dados. Outra característica para as empresas é que os dispositivos móveis expandem o perímetro da empresa, com os dados sendo distribuídos de uma forma ampla e sem limites físicos.

Há modelos de implantação de dispositivos móveis nas empresas, que levam em consideração a propriedade dos dispositivos, e a permissão para uso particular. E as políticas e configurações desses dispositivos devem ser gerenciados de uma forma apropriada.

Para os desenvolvedores de aplicativos móveis há uma série de cuidados de segurança e privacidade que precisam ser tomados para que vulnerabilidades não sejam introduzidas nesses aparelhos.

Você verá que os dispositivos móveis seguem um ciclo de vida que vai do planejamento da implantação até as operações e descarte, que deve ser feito de modo a não comprometer os dados pessoais e os dados confidenciais da empresa.

Você é o especialista em segurança e privacidade de um inovador site de comércio online em que pequenos negócios são conectados com os consumidores em uma plataforma digital baseada no uso de inteligência artificial. A sua função é essencial para a empresa, e você participa de todas as decisões sobre a evolução da plataforma. Há as questões envolvidas com o desenvolvimento seguro, para que vulnerabilidades não sejam inseridas indevidamente no sistema. Há ainda as questões de segurança e privacidade envolvidas com o uso de provedor de nuvem. E, como a empresa trabalha com inteligência artificial, há necessidade de fazer o desenvolvimento utilizando bases de dados que não interfiram na privacidade dos clientes.

Além da segurança da informação da plataforma da empresa, que está hospedada em um provedor em nuvem na Europa, você tem três preocupações principais:

1. Como diminuir as possíveis fraudes cometidas por usuários falsos que se passam por clientes, com uso de identidades falsas ou uso de recursos financeiros ilícitos.
2. Como diminuir as possíveis fraudes cometidas por pequenos negócios falsos, que podem não cumprir os compromissos comerciais estabelecidos com os clientes que utilizam a plataforma digital.
3. Como proteger os dados pessoais dos clientes principalmente contra vazamentos, que pode levar a sanções previstas na LGPD.

Após já ter mostrado um planejamento sobre os aspectos que devem ser considerados pela empresa para a definição de uma estratégia de segurança e privacidade, com o seu direcionamento quanto à segurança em transações *web*, vamos para o próximo passo. O que deve ser planejado agora é a expansão para a nova versão da plataforma, baseada em aplicativos para dispositivos móveis. Apresente o seu planejamento, pensando que neste novo cenário você terá colaboradores que também utilizarão dispositivos móveis para expandir a rede de pequenos negócios parceiros. Esses colaboradores farão os contatos com os pequenos negócios assim como o acesso junto com eles na plataforma digital, utilizando dispositivos móveis.

Os desafios de segurança e privacidade relacionados aos dispositivos móveis são grandes e oferecem grandes oportunidades. Seja para desenvolver aplicativos móveis com mais segurança ou para implantar o uso de dispositivos móveis de uma forma segura, esses tópicos são importantes e fazem parte de nossas vidas.

o

Ver anotações

CONCEITO-CHAVE

DISPOSITIVOS MÓVEIS

Um dispositivo móvel é, segundo o *National Institute of Standards and Technology*, NIST (NIST, 2020), um dispositivo computacional portátil que possui um formato pequeno e que pode ser carregado por um indivíduo, sendo construído para operar sem uma conexão física, com armazenamento de dados local não removível e que funciona por um período de tempo com uma fonte de energia própria. Pode incluir capacidades de comunicação por voz e sensores que possibilitam a captura de informação e tem a capacidade de sincronização com locais remotos.

As principais características de dispositivos móveis são, assim, portabilidade, comunicação sem fio, armazenamento local e funcionamento por bateria. Essas características influenciam diretamente nos aspectos de segurança e privacidade, por mudarem, principalmente, os perímetros das empresas, que se expandem com os dispositivos móveis.

Além delas, a conexão em redes celulares sempre ativas também é uma característica relevante para os aspectos de segurança, mas não é uma realidade em todos os dispositivos móveis, como nos tablets.

REFLITA

Com a chegada da rede 5G, o que acontece com a segurança e a privacidade? A tecnologia 5G possibilita conexões com maior velocidade e menor latência, além de conexões

permanentes de qualquer coisa ou dispositivo, tornando a internet das coisas (IoT) onipresente, com tudo conectado, desde drones até cafeteiras, incluindo carros (HIGA, 2016).

Os principais componentes dos dispositivos móveis podem ser vistos na Figura 3.9, com a divisão entre *hardware*, *firmware*, sistema operacional e aplicação. Cada um destes componentes representa pontos que podem ser atacados (FRANKLIN *et al.*, 2020).

Figura 3.9 | Componentes de dispositivos móveis



Fonte: adaptada de Franklin *et al.* (2020).

O uso de dispositivos móveis traz uma série de vantagens para as empresas, principalmente com o aumento da eficiência e produtividade decorrente do acesso aos recursos da empresa a qualquer momento, de qualquer localidade. E isto resulta em necessidades de segurança (NCCoE, 2020), devido aos riscos existentes neste ambiente.

AMEAÇAS E SEGURANÇA EM DISPOSITIVOS MÓVEIS

Os principais riscos envolvidos com o uso de dispositivos móveis no mundo corporativo podem ser vistos na Figura 3.10, e são (HOWELL *et al.*, 2020):

- Comprometimento da privacidade do usuário ou dos dados sensíveis da empresa a partir na inexistência de separação entre contextos de uso pessoal e profissional, de modo que problemas de segurança em um contexto afetam o outro.

- Instalação de aplicativos vulneráveis a partir de fontes não oficiais, o que aumenta a chance de inserção de vulnerabilidades no ambiente.
- Instalação de *malwares* a partir de fontes não oficiais, que podem vir junto de aplicativos falsificados ou cavalos de Troia.
- Interceptação de tráfego a partir de conexões não confiáveis, que pode resultar em vazamento de dados e furto de identidades.
- Conexões não confiáveis aceitas pela empresa, que precisa abrir o *firewall* para as conexões de quaisquer dispositivos.

Figura 3.10 | Riscos no uso de dispositivos móveis no mundo corporativo



Fonte: adaptado de Howell *et al.* (2020).

ASSIMILE

As ameaças existentes no mundo móvel são muito similares às de outros ambientes, apesar de algumas especificidades. Os níveis de risco das empresas mudam, pelas próprias características dos dispositivos móveis, que aumentam a superfície de ataque ao ampliar os parâmetros da empresa, que passam a ser mais distribuídos. Os dados corporativos passam a existir fora dos servidores da empresa e há a mistura com os dados pessoais que podem comprometer a privacidade dos usuários.

As ameaças para dispositivos móveis precisam ser entendidas para que a melhor estratégia de segurança possa ser definida pela empresa, incluindo a aplicação de melhores práticas de segurança e o uso de soluções de segurança para a proteção de todo o ambiente (BROWN *et al.*, 2016) (NIST, 2020).

As principais ameaças relacionadas aos dispositivos móveis são descritas a seguir e detalham os principais riscos vistos na figura 3.10 (HOWELL *et al.*, 2020) (NCCoE, 2020) (FRANKLIN *et al.*, 2020):

- **Acesso não autorizado às informações sensíveis via aplicação maliciosa ou intrusiva para a privacidade:** uma aplicação móvel, mesmo legítima, pode tentar coletar e enviar qualquer informação a que ela tem acesso. Alguns exemplos de informações que podem ser acessadas de acordo com os níveis de permissão da aplicação são os contatos, calendários, histórico de ligações ou as fotos, e ainda as informações gerais do dispositivo, como o *Mobile Equipment Identity* (MEI), fabricante, modelo e número de série. Além disso, uma aplicação maliciosa pode explorar vulnerabilidades de outras aplicações, do sistema operacional ou do *firmware* para escalar privilégios, visando obter o acesso não autorizado aos dados armazenados no dispositivo.
- **Furto de identidade por campanhas de *phishing* por *Short Message Service (SMS)* ou *e-mail*:** uso de técnicas de engenharia social e uso de senso de urgência para obter a atenção e promover o direcionamento das vítimas a *sites* fraudulentos, onde eles entregam suas credenciais de acesso e outras informações sensíveis.
- **Aplicações maliciosas instaladas via URLs em mensagens SMS ou *e-mail*:** uso de técnicas de engenharia social e uso de senso urgência para instigar a vítima a clicar em um *link* que contém *malware*, que é então instalado no dispositivo móvel.
- **Perda de confidencialidade e de integridade com a exploração de vulnerabilidades conhecidas em sistema operacional e**

firmware: a exploração de vulnerabilidades pode levar à execução de códigos arbitrários e à instalação de *malware*, como um *backdoor*.

- **Violação da privacidade por mal-uso de sensores do dispositivo:** sensores como microfone, câmera, giroscópio e *Global Positioning System* (GPS) podem ser explorados para obter informações sensíveis ou comprometer a privacidade dos usuários.
- **Comprometimento da integridade do dispositivo ou da comunicação de rede pela instalação de *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM), perfis de rede, *Virtual Private Network* (VPN) ou certificados digitais maliciosos:** com a instalação de EMM/MDM malicioso, o agente de ameaça pode ter acesso à plataforma de gerenciamento dos dispositivos móveis, tendo o controle do dispositivo e das comunicações, podendo assim instalar aplicações maliciosas, localizar remotamente um usuário, ou apagar remotamente os dados. Já a manipulação da rede e da VPN possibilita o direcionamento das conexões para redes não confiáveis, de onde os dados são furtados. A manipulação de certificados digitais estabelece uma relação de confiança falsa que possibilita a conexão a servidores e redes contaminados e a instalação de aplicativos maliciosos.
- **Perda de confidencialidade por monitoramento de comunicações expostas:** redes sem fio públicas abertas são alvos de monitoramento e ainda podem levar a ataques como o *watering hole* ou o *Man-In-The-Middle* (MITM). Além disso, podem levar os usuários a se conectarem a sites falsos.
- **Comprometimento da integridade do dispositivo móvel pela observação, inferência ou força-bruta do código de desbloqueio do dispositivo:** além do acesso aos dados do dispositivo, a obtenção do código de desbloqueio pode levar ao acesso a outras aplicações.

caso o código de desbloqueio seja utilizado como credencial de acesso para outros sistemas.

- **Acesso não autorizado a serviços de *backend* pela autenticação ou falhas no armazenamento de credenciais em aplicações desenvolvidas internamente:** aplicações próprias devem ser desenvolvidas com cuidados na implementação de mecanismos de autenticação e armazenamento de credenciais, além de não inserir vulnerabilidades que podem dar o acesso a essas informações essenciais para um ataque.
- **Acesso não autorizado a recursos da empresa a partir de dispositivos comprometidos ou não gerenciados:** dispositivos não gerenciados não utilizam os mecanismos de segurança definidos pela empresa.
- **Perda de dados da empresa devido à perda ou furto do dispositivo:** a probabilidade aumenta pela natureza dos dispositivos, que é portátil, e o agente de ameaça pode ter acesso não autorizado dos dados sensíveis ou recursos disponíveis no dispositivo.
- **Perda de confidencialidade dos dados da empresa devido ao armazenamento não autorizado em serviços sem homologação:** o uso de serviços não gerenciados pela empresa impossibilita o monitoramento e acompanhamento dos serviços. O resultado pode ser o acesso não autorizado aos dados da empresa a partir destes serviços.

O *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM) é um dos principais controles de segurança para dispositivos móveis das empresas (FRANKLIN *et al.*, 2020). O EMM/MDM é uma solução para prover segurança em dispositivos móveis de usuários que são autorizados a acessar recursos da empresa.

Geralmente o EMM/MDM é composto por dois componentes principais. O primeiro é um serviço *backend* que os administradores utilizam para gerenciar as políticas, configurações e outras ações de segurança que são aplicadas nos dispositivos móveis. O segundo componente é um agente que é instalado no dispositivo que permite a aplicação das ações definidas pela empresa.

Há o provisionamento dos perfis de configuração para os dispositivos, a aplicação das políticas de segurança nos dispositivos e o monitoramento de conformidade com as políticas pelos dispositivos. O agente no dispositivo pode enviar notificações em caso de configurações não conformes com a política da empresa, e pode corrigir automaticamente configurações desta natureza.

O EMM/MDM pode ainda prover informações importantes para a segurança do ambiente. Os dados de conformidade com a política de disponíveis móveis, por exemplo, podem ser utilizados pela empresa para o controle de acesso, como um parâmetro adicional para aceitar as conexões somente de dispositivos que estejam cumprindo um determinado nível de segurança.

ASSIMILE

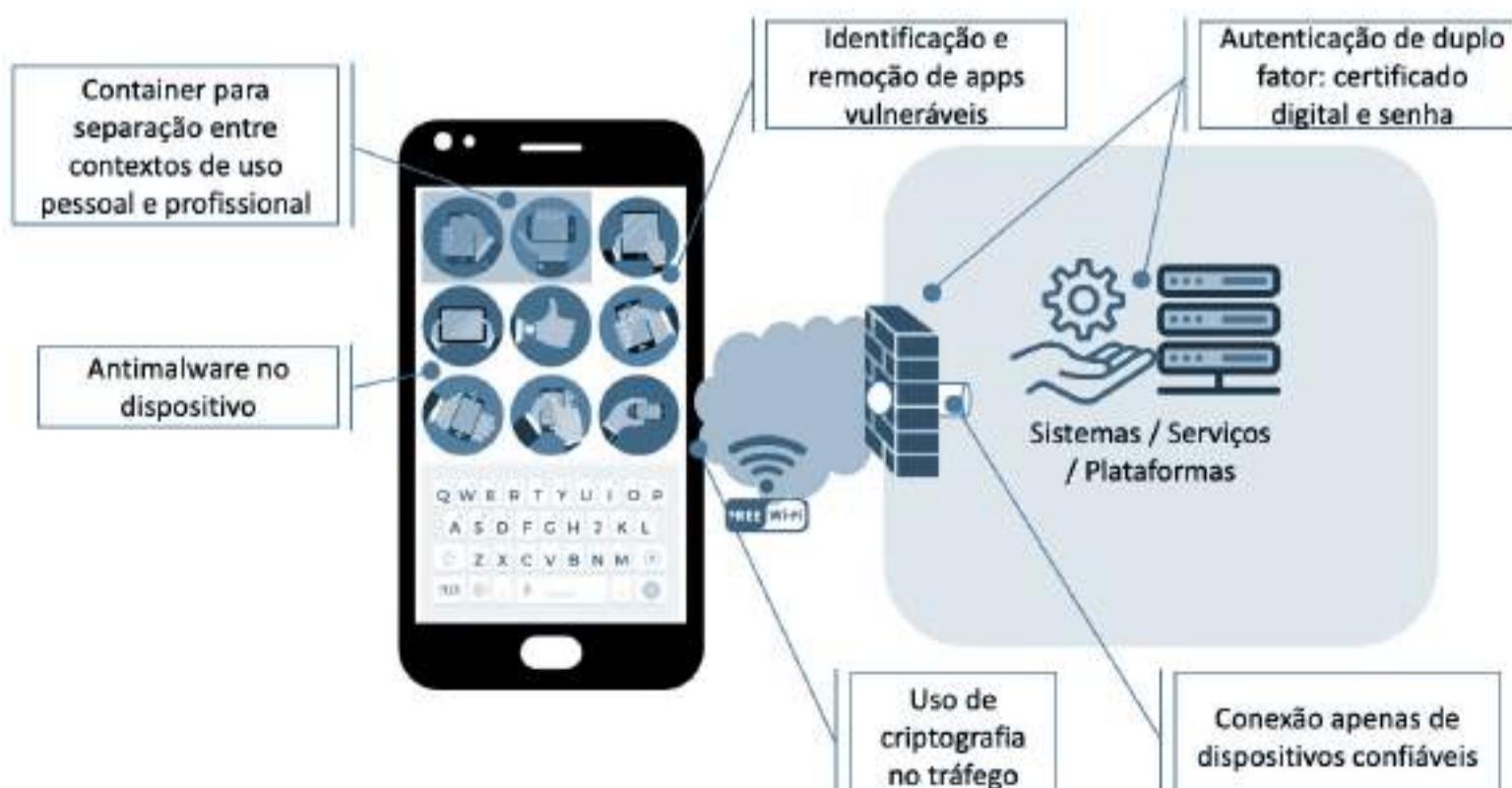
O *watering hole* é um golpe direcionado e personalizado, em que os atacantes comprometem algum *site* que eles sabem que o alvo irá visitar, para que assim o infectem com um código malicioso. Com isso, a taxa do golpe dar certo aumenta consideravelmente. Para este ataque, os atacantes podem utilizar dados expostos de tráfego, em que aprendem o comportamento do alvo.

O ataque *watering hole*, assim, é similar ao *spear phishing*, que é direcionado e personalizado (ROHR, 2016).

Assim, vimos os principais riscos e as principais ameaças que devemos considerar para a segurança em dispositivos móveis. Os objetivos de segurança no uso de dispositivos móveis no mundo corporativo devem ser, no mínimo, os relacionados a seguir. Eles também são apresentados na Figura 3.11 (HOWELL *et al.*, 2020):

- Usar contêiner para isolar o contexto pessoal do contexto profissional, de modo que problemas de segurança em um contexto não afete o outro.
- Identificar e remover aplicativos vulneráveis, bem como definir e aplicar uma política de segurança clara sobre a instalação de aplicativos nos dispositivos.
- Usar *antimalware* nos dispositivos, bem como definir e aplicar uma política de segurança clara sobre a instalação de aplicativos nos dispositivos.
- Usar criptografia nas conexões com a empresa, como uma VPN.
- Aceitar conexões apenas de dispositivos confiáveis, com uso de certificados digitais, que podem fazer parte da autenticação de duplo fator, o que aumenta a segurança em caso de furto de identidade.

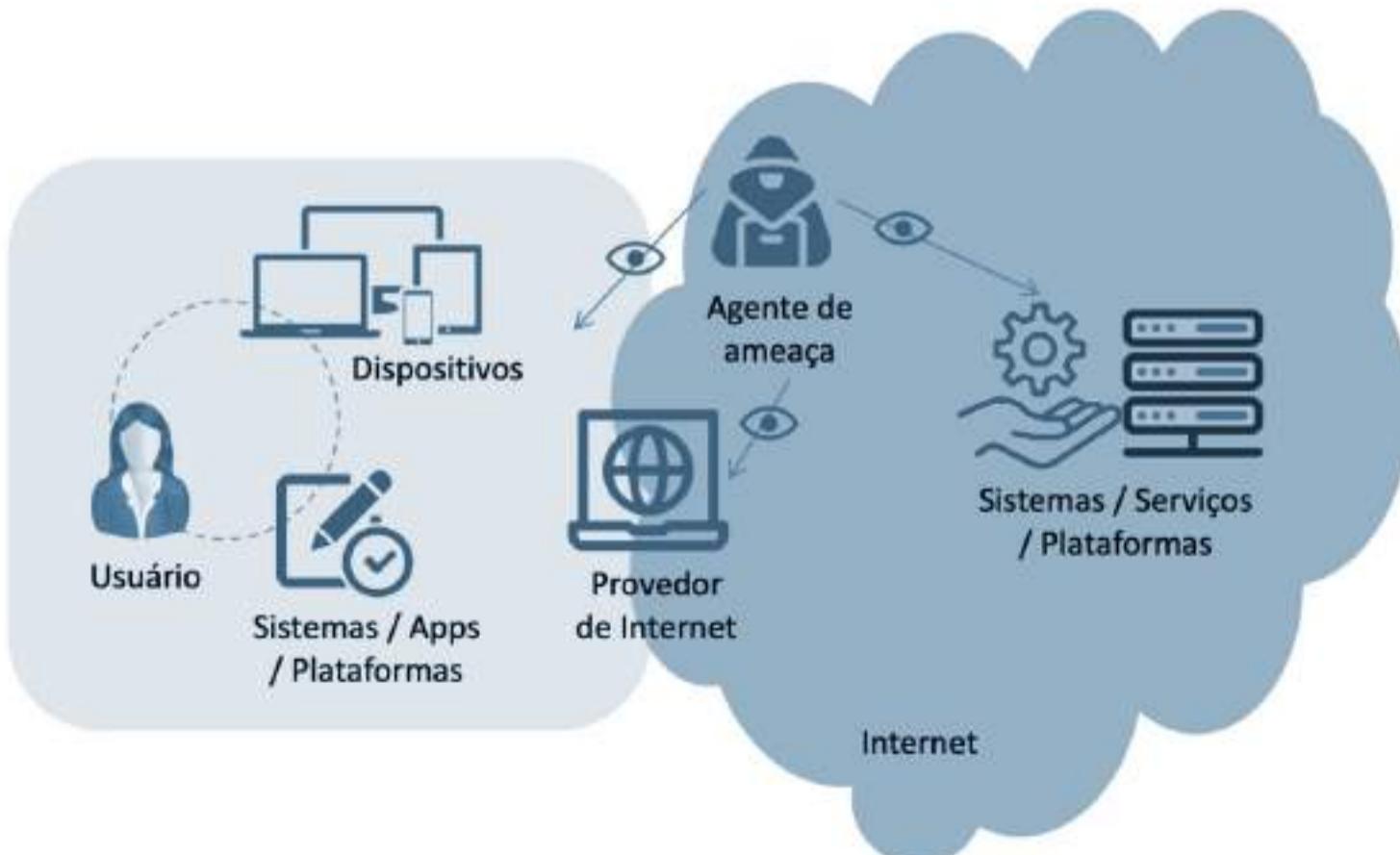
Figura 3.11 | Objetivos de segurança no uso de dispositivos móveis no mundo corporativo



Os ataques relacionados a ambientes móveis envolvem todos os aspectos de segurança da informação. O agente de ameaça pode explorar o lado do usuário, fazendo com que o usuário clique em um *link* com conteúdo malicioso com um *phishing*, explorar o dispositivo móvel ou ainda uma aplicação. Ele pode ainda explorar a comunicação, atacando o provedor de internet, que pode ser uma rede wi-fi pública. E o atacante pode ainda atacar a empresa, explorando vulnerabilidades no ambiente formado por sistemas, serviços e plataformas, adicionalmente aos funcionários e processos da empresa. A Figura 3.12 mostra esses pontos de ataque, que complementa a visão dos principais riscos no uso de dispositivos móveis pelas empresas:

- Dados pessoais e dados corporativos se misturando.
- Instalação de aplicativos vulneráveis.
- Instalação de *malwares* a partir de fontes não oficiais.
- Interceptação de tráfego a partir de conexões não confiáveis.
- Conexões não confiáveis aceitas pela empresa.

Figura 3.12 | Pontos de ataques em um acesso a empresas



Fonte: elaborada pelo autor.

Os ataques em disponíveis móveis têm evoluído, partindo de instalação de *backdoors* e mineração de moeda digital, para códigos maliciosos mais sofisticados, capazes de esconder seus ataques, sendo mais difíceis de serem identificados e removidos (SECURITY, 2020).

Um dos ataques, ocorrido na Coreia do Sul, comprometeu uma empresa de *software* com boa reputação no país, fazendo com que os aplicativos usassem uma biblioteca e *plugin* modificados. O *malware*, conhecido como MalBus, fazia a coleta e o envio de informações confidenciais dos dispositivos das vítimas que utilizavam os aplicativos, que eram de utilidade pública, sobre o trânsito (SECURITY, 2020).

Para as empresas, que precisam proteger as informações sensíveis que estão agora fora do perímetro físico da própria empresa, há desafios como a particularidade dos ataques a dispositivos móveis, que estão sempre conectados na internet e as implicações de privacidade com os colaboradores utilizando os dispositivos também para atividades pessoais (FRANKLIN *et al.*, 2019).

E há os desafios relacionados à forma como os controles de segurança para dispositivos móveis corporativos podem ser implementados (HOWELL *et al.*, 2020):

- **Bloqueio de acesso e remoção dos dados (*wiping*):** o uso do dispositivo para fins profissionais e pessoais é comum. Solução: bloqueio do acesso corporativo até uma nova concessão de acesso, de acordo com a política de segurança; remoção seletiva de dados, e não de todo o dispositivo; política que exige o *backup* dos dados pessoais, que poderão ser removidos.
- **Monitoramento do colaborador:** coleta e análise de dados sobre o dispositivo e suas atividades, que pode ser feito por múltiplos fornecedores. Solução: desenvolver uma política de segurança e utilizar técnicas que limitam a coleta de dados específicos;

desenvolver uma política de segurança e utilizar técnicas para o descarte de informação de identificação pessoal.

- **Compartilhamento de dados:** uso de variados serviços e provedores de nuvens pode levar à confusão sobre quem possui o acesso às informações corporativas e aos dados pessoais. Solução: desenvolver uma política de segurança e utilizar técnicas de pseudonimização de dados; utilizar criptografia; desenvolver uma política de segurança e utilizar técnicas que limitam a coleta de dados específicos; utilizar contratos para limitar o processamento de dados por terceiros.

Além do aspecto humano para que os colaboradores não sejam vítimas de *phishing*, há a necessidade de configuração segura dos dispositivos e o provisionamento das políticas corporativas de gerenciamento dos dispositivos para a defesa. Isto pode ser feito com o *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM).

A defesa de dispositivos móveis pode ser definida de acordo com um conjunto de capacidades de segurança para dispositivos móveis, como pode ser visto na Figura 3.13 (NCCoE, 2020):

- Proteção dos dados armazenados no dispositivo móvel.
- Gerenciamento centralizado para aplicar políticas e configurações aos dispositivos.
- Avaliação da segurança das aplicações móveis.
- Proteção contra o acesso indevido aos dados do dispositivo móvel.
- Configurações de privacidade para proteger os dados dos usuários.
- Proteção contra tentativas de *phishing*.

Figura 3.13 | Capacidades de segurança necessárias



Fonte: adaptada de NCCoE(2020).

ATAQUES DE CAMADAS DE APLICAÇÕES E ANTIVÍRUS PARA DISPOSITIVOS MÓVEIS

A camada de aplicação de um dispositivo móvel é uma das que podem ser atacadas pelos agentes de ameaça. Ataques na camada de aplicação em dispositivos móveis exploram as vulnerabilidades técnicas de aplicativos instalados pelo usuário. Desta forma, os desenvolvedores de aplicativos móveis devem evitar códigos que insiram vulnerabilidades.

Segundo a *Open Web Application Security Project* (OWASP), as 10 maiores vulnerabilidades em aplicativos móveis são (OWASP, 2016):

- 1. Uso impróprio de plataforma:** uso incorreto de característica da plataforma ou falha no uso de controles de segurança da plataforma, como as permissões ou biometria.
- 2. Armazenamento inseguro de dados:** a proteção deve considerar um agente de ameaça que tenha a posse física do dispositivo móvel, ou um *malware* ou outro aplicativo que é executado no dispositivo.
- 3. Comunicação insegura:** dados que trafegam em um modelo cliente-servidor podem ser interceptados em diferentes pontos, tais como uma rede de acesso comprometido, dispositivos do provedor de internet atacados ou por um *malware* no dispositivo móvel.

4. Autenticação insegura: ataques que exploram vulnerabilidades de forma automatizada em busca de acessos usando credenciais falsas ou que podem ser dribladas.

5. Criptografia insuficiente: a proteção deve considerar um agente de ameaça que possui a posse física do dispositivo móvel, ou um *malware* ou outro aplicativo que é executado no dispositivo.

6. Autorização insegura: ataques que exploram vulnerabilidades de forma automatizada em busca de acesso a áreas após a autenticação.

7. Má qualidade de código: a proteção deve considerar agentes de ameaça que podem utilizar entradas não confiáveis para as chamadas do código, que podem levar à execução de códigos arbitrários.

8. Modificação de código: a exploração pode ser pelo uso de fontes de aplicativos de terceiros que hospedam os códigos modificados, ou pela instalação pelo usuário vítima de *phishing*.

9. Engenharia reversa: o atacante analisa o aplicativo com a ajuda de diversas ferramentas para entender e explorar as funções.

10. Funcionalidade exposta: a exposição em aplicativos pode relevar funcionalidades de sistemas de *backend*, que pode então ser explorada diretamente.

Os antivírus para dispositivos móveis devem ser considerados uma camada de proteção, não podendo ser considerado uma solução para os problemas de segurança e privacidade. Muitos antivírus fazem a detecção de *malware* com base em assinaturas, o que significa que somente aqueles conhecidos poderão ser detectados. Os *malwares* novos e o *phishing* são detectados com dificuldades pelos antivírus e outros mecanismos devem ser utilizados pela empresa para complementar a proteção.

■ ENGENHARIA SOCIAL (ACESSO AS INFORMAÇÕES PESSOAIS) DE DISPOSITIVOS MÓVEIS

O *phishing* conta com a engenharia social, que explora a atenção, curiosidade, caridade, medo ou possibilidade de obtenção de vantagem financeira, com o criminoso se passando por uma instituição como banco, empresa ou *site* popular. Envolve a possibilidade de inscrição em serviços de proteção de crédito, ou o cancelamento de cadastro, conta bancária ou cartão de crédito, e leva a vítima a páginas falsas em que entregam suas credenciais, senhas ou informações sensíveis, além de poderem, ainda, instalar códigos maliciosos (CERT, 2020).

O usuário recebe um *phishing* e clica em um *link* que pode levar a um site onde ele entrega informações pessoais ou as suas credenciais de acesso, ou pode levar à instalação de *malware*.

EXEMPLIFICANDO

O *phishing* é explorado também no mundo dos jogos eletrônicos, com os atacantes distribuindo *malwares* via *links* em *chat* de jogos e criando aplicativos falsos que visam ser populares, utilizando inclusive ícones similares para ludibriar as vítimas (SECURITY, 2020).

Um dos *malwares*, distribuído via mídia social, plataforma de jogos ou *chat* de jogos, é o LeifAccess ou o Shopper, que envia mensagens falsas de alertas para que o usuário ative serviços de acessibilidade do dispositivo móvel. O *malware* então utiliza as funções de acessibilidade para criar contas, baixar aplicativos e postar mensagens usando a conta da vítima (SECURITY, 2020).

■ SEGURANÇA EM DISPOSITIVOS MÓVEIS PARA EMPRESAS

Para as empresas é importante adotar uma arquitetura de referência para os dispositivos móveis de forma a prover acesso seguro ao mesmo tempo em que a privacidade dos usuários seja preservada (HOWELL et

al., 2020).

Um dos principais pontos da arquitetura é a definição do modelo a ser adotado, que pode ser a disponibilização de dispositivos móveis somente para o uso corporativo, a permissão para uso pessoal (*Corporate-Owned Personally-Enabled*, COPE) ou o *Bring Your Own Device* (BYOD) ou *Choose Your Own Device* (CYOD). No modelo BYOD ou CYOD, o dono do dispositivo móvel é o próprio usuário, enquanto nos outros a propriedade é da empresa. O modelo COPE provê flexibilidade de uso ao permitir que tanto a empresa quanto o usuário possam instalar aplicativos no dispositivo, que é de propriedade da empresa (NCCoE, 2020).

Neste contexto, algumas recomendações de segurança e privacidade para empresas adotarem no uso de dispositivos móveis são (FRANKLIN *et al.*, 2020):

- Conduzir uma análise de riscos em dispositivos móveis e para as informações acessadas por eles, considerando todos os elementos do risco: componentes, vulnerabilidades, ameaças, probabilidade, impacto, e agentes de ameaça.
- Adotar tecnologias de segurança móvel como *Enterprise Mobility Management* (EMM), plataformas de defesa contra ameaças móveis ou serviço de voto a aplicações móveis, que utiliza uma variedade de técnicas estáticas, dinâmicas e comportamentais para determinar, com o uso de uma pontuação, se uma aplicação ou dispositivo demonstram qualquer comportamento que representa um risco de segurança ou de privacidade. Este serviço de voto pode ser utilizado antes da instalação nos dispositivos móveis.
- Reforçar o ciclo de vida de implantação de dispositivos móveis corporativos, com passos-chave para que os dispositivos cheguem aos colaboradores de uma forma segura, incluindo a análise de riscos, o modelo adotado que pode ou não permitir o uso de dispositivos particulares, inventário, monitoramento e atualizações.

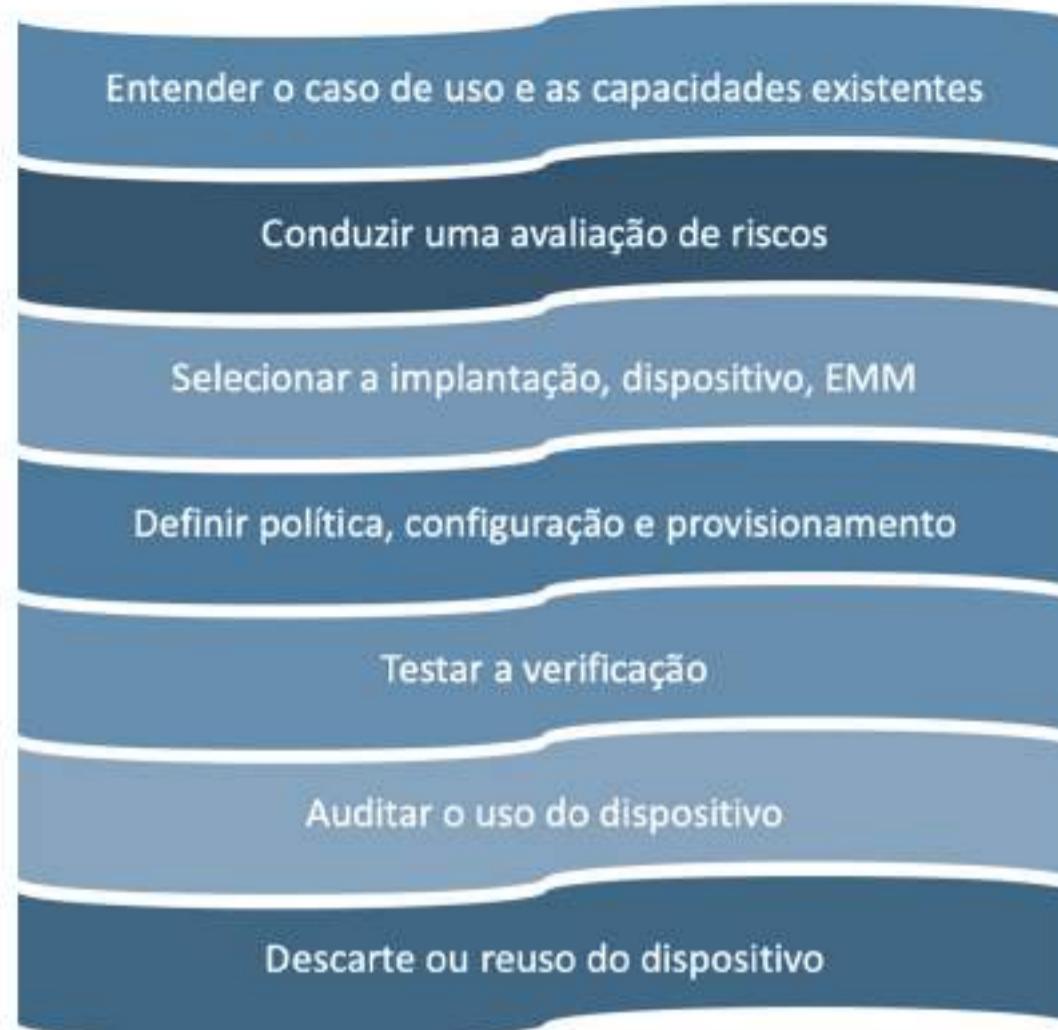
- Implementar e fazer um piloto da solução de dispositivo móvel antes de colocá-la em produção, considerando conectividade, proteção, autenticação, funcionalidades, gerenciamento, registros e desempenho.
- Prover a segurança em cada dispositivo móvel corporativo antes de permitir o acesso a sistemas e informações corporativas, com uso de uma solução de gerenciamento de mobilidade corporativa (EMM/MDM).
- Manter atualizados o sistema operacional e os aplicativos móveis, minimizando as vulnerabilidades.
- Manter regularmente a segurança dos dispositivos móveis, fazendo avaliações periódicas de segurança e de cumprimento da política de segurança.

As recomendações fazem parte do ciclo de vida de implantação de dispositivos móveis corporativos (Figura 3.14), que considera aspectos de planejamento, implantação e operação dos dispositivos móveis na empresa (FRANKLIN *et al.*, 2020):

- **Identificar os requisitos para o uso de dispositivos móveis**, com o entendimento do caso de uso e as capacidades existentes. É importante a visão de TI e de negócios. O caso de uso pode envolver a realização de atividades fora da empresa, bem a interação com profissionais de empresas parceiras. O caso de uso pode incluir elementos comuns como a definição dos usuários, a razão deles precisarem dos dispositivos móveis e quais aplicativos ou características do dispositivo móvel serão necessários para o cumprimento dos objetivos corporativos. As capacidades existentes envolvem os dispositivos móveis atualmente utilizados pelos colaboradores, que influenciam na definição do modelo de implantação corporativo, que pode ser o uso estritamente corporativo, COPE ou BYOD / CYOD.

- **Fazer uma avaliação de riscos**, considerando os dispositivos móveis, aplicações e sistemas utilizados para gerenciar todo o sistema. É importante ter uma visão no nível organizacional, além do tecnológico.
- **Implantar a estratégia corporativa para o sistema móvel**, com o EMM/MDM podendo ser utilizado na empresa (*on-premise*) ou na nuvem. Os serviços de infraestrutura da empresa precisam se integrar ao EMM, como os serviços de autenticação.
- **Definir e implantar a política dos dispositivos**, incluindo o modelo de implantação corporativo, e a possibilidade de uso pessoal dos dispositivos. Após as configurações, os dispositivos móveis devem ser provisionados para os usuários.
- **Testar as configurações e os softwares instalados**, em um processo de gestão de mudanças, avaliando os impactos das implantações dessas mudanças, que devem envolver também as atualizações e instalação de *patches*. A implantação dessas mudanças também deve ser testada e planejada cuidadosamente.
- **Auditar todo o ambiente periodicamente para validar a efetividade dos controles de segurança**, e atualizar os mecanismos de segurança de acordo com os riscos, que são dinâmicos. Além da auditoria da segurança, é importante auditar o uso dos dispositivos pelos usuários, que devem estar de acordo com a política definida.
- **Descartar ou reusar os dispositivos móveis** após um processo de sanitização é importante para preservar as informações corporativas e pessoais existentes nesses aparelhos.

Figura 3.14 | Ciclo de vida de implantação de dispositivos móveis corporativos



Fonte: adaptada de Franklin *et al.* (2020).

EXEMPLIFICANDO

Um exemplo de caso de uso para dispositivos móveis é o desenvolvimento de pesquisas médicas, que antes eram feitas com os voluntários sendo conduzidos para a empresa. Em um novo cenário, os pesquisadores irão visitar os voluntários, coletando dados e fazendo diagnósticos de forma remota. É preciso que os pesquisadores tenham acesso aos dados históricos dos voluntários que estão no servidor da empresa, mas por meio do dispositivo móvel. A empresa precisa prover este acesso remoto ao servidor de uma forma segura.

SAIBA MAIS

Com o avanço no uso de dispositivos móveis, este canal tem se tornado o canal preferido pelos criminosos. O termo *phishing* surgiu no contexto de e-mails. O *phishing* conta com a engenharia social, que explora a atenção, curiosidade, caridade, medo ou possibilidade de obtenção de vantagem financeira, com o criminoso se passando por uma instituição como banco, empresa ou site popular. Envolve a

possibilidade de inscrição em serviços de proteção de crédito, ou o cancelamento de cadastro, conta bancária ou cartão de crédito, e leva a vítima a páginas falsas em que entregam suas credenciais, senhas ou informações sensíveis, além da instalação de códigos maliciosos.

Quando o ataque acontece por mensagens de texto SMS enviados ao dispositivo móvel do alvo, o termo utilizado pode ser *SMiShing*.

PESQUISE MAIS

Para o desenvolvimento de aplicativos móveis seguro, você pode adotar os testes previstos no *Mobile Security Testing Guide* (MSTG), do OWASP (OWASP, 2019). Os testes propostos buscam identificar e tratar as vulnerabilidades, e visam a autenticação, rede, criptografia, qualidade do código, engenharia reversa e a educação do usuário. Há testes específicos para Android e para iOS.

OWASP. **Intermediate update 1.1.3** (OSS Release), 4 ago.

2019. Disponível em: <https://bit.ly/31cu55B>. Acesso em: 26 dez. 2020.

Chegamos ao fim dos aspectos de segurança e privacidade em dispositivos móveis. Atualmente, grande parte dos acessos a variados serviços é feito pelo dispositivo móvel. Como usuário, é importante saber utilizar o dispositivo móvel de uma forma segura. E, como profissional de segurança, vários aspectos devem ser planejados e implementados, começando com a definição do modelo, que pode ou não mesclar dados corporativos com dados pessoais, o que exige o planejamento e a implantação de diferentes controles de segurança. E as ameaças estão presentes em diferentes ambientes e em variados componentes.

Questão 1

Um dos grandes desafios para a segurança em dispositivos móveis é que, além de ampliarem o perímetro da empresa, há dados pessoais junto dos dados corporativos, que precisam ser protegidos. Há alguns modelos que podem ser adotados pelas empresas quanto a este desafio.

O modelo que não permite que o usuário da empresa utilize o dispositivo móvel para fins particulares é o:

- a. Dispositivo cedido para uso exclusivamente corporativo.
- b. Corporate-Owned Personally-Enabled (COPE).
- c. Bring Your Own Device (BYOD).
- d. Choose Your Own Device (CYOD).
- e. Enterprise Mobility Management (EMM).

Questão 2

Considere as seguintes capacidades de segurança:

- I. Proteção dos dados armazenados no dispositivo móvel.
- II. Gerenciamento centralizado para aplicar políticas e configurações aos dispositivos.
- III. Avaliação da segurança das aplicações móveis.
- IV. Proteção contra o acesso indevido aos dados do dispositivo móvel.
- V. Configurações de privacidade para proteger os dados dos usuários.
- VI. Proteção contra tentativas de *phishing*.

Estas capacidades de segurança devem ser aplicadas no contexto de:

- a. Dispositivos móveis.
- b. Gerenciamento de riscos.
- c. Phishing.

d. Auditoria.

e. Criptografia.

Questão 3

O *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM) é um dos principais controles de segurança para dispositivos móveis das empresas. O EMM/MDM é uma solução para prover segurança em dispositivos móveis de usuários que são autorizados a acessar recursos da empresa.

Considere as seguintes afirmativas a seguir:

- I. O EMM/MDM provisiona os perfis de configuração para os dispositivos.
- II. O EMM/MDM aplica as políticas de segurança nos dispositivos.
- III. O EMM/MDM monitora a conformidade dos dispositivos com as políticas.

É correto o que se afirma em:

a. I, II e III.

b. I e III, apenas.

c. III, apenas.

d. I e II, apenas.

e. I, apenas.

REFERÊNCIAS

BROWN, C. et al. **Assessing Threats to Mobile Devices & Infrastructure** – The Mobile Threat Catalogue. Draft NIST 8144.

National Institute of Standards and Technology. U.S. Department of Commerce, set. 2016. Disponível em: <https://bit.ly/39b20jr>. Acesso em: 22 dez. 2020.

CERT.br. Golpes na Internet. **Cartilha de segurança para internet.**

Disponível em: <https://bit.ly/2Qq55FF>. Acesso em: 19 dez. 2020.

FRANKLIN, J. M. et al. Mobile Device Security – Cloud and Hybrid Builds.

NIST Special Publication 1800-4. National Institute of Standards and Technology. U.S. Department of Commerce, fev. 2019. Disponível em: <https://bit.ly/3diWGMj>. Acesso em: 22 dez. 2020.

FRANKLIN, J. M. et al. Guidelines for Managing the Security of Mobile Devices in the Enterprise. **Draft NIST Special Publication 800-124,** Revision 1. NIST, National Institute of Standards and Technology. U.S. Department of Commerce, mar. 2020. Disponível em: <https://bit.ly/3vQqS9X>. Acesso em: 22 dez. 2020.

HIGA, P. **Por que o 5G vai mudar sua vida (mesmo que você não tenha nem 4G).** Tecnoblog, 2016. Disponível em: <https://bit.ly/39cejvE>. Acesso em: 26 dez. 2021.

HOWELL, G. et al. NCCoE, National Cybersecurity Center of Excelence. NIST, National Institute of Standards and Technology. U.S. Department of Commerce. **NIST SPECIAL PUBLICATION 1800-21. Mobile Device Security: Corporate-Owned Personally-Enabled (COPE).** Disponível em: <https://bit.ly/2QCg672>. Acesso em: 22 dez. 2020.

KASPERSKY. **Top 7 Mobile Security Threats in 2020.** Disponível em: <https://bit.ly/3slu5Mi> Acesso em: 26 dez. 2020.

KRISTIINA. **OWASP mobile top 10 security risks explained with real world examples.** The Startup, 17 mar. 2019. Disponível em: <https://bit.ly/3vZnglR>. Acesso em: 27 dez. 2020.

MCAFEE. **McAfee Mobile Threat Report – Mobile Malware Is Playing Hide and Steal,** 2020. Disponível em: <https://bit.ly/39aNXdN>. Acesso em: 26 dez. 2020.

NCCoE, National Cybersecurity Center of Excelence. NIST, National Institute of Standards and Technology. U.S. Department of Commerce. **Mobile Device Security.** Disponivel em:

<https://bit.ly/3vVrkUm>. Acesso em: 22 dez. 2020.

NIST, National Institute of Standards and Technology. U.S. Department of Commerce. NCCoE, National Cybersecurity Center of Excellence. **Mobile Threat Catalogue**. Disponível em:

<https://bit.ly/31eAnl9>. Acesso em: 22 dez. 2020.

NIST, National Institute of Standards and Technology. U.S. Department of Commerce. Joint Task Force. **NIST Special Publication 800-53**

Revision 5 – Security and Privacy Controls for Information Systems and Organizations, set. 2020 Disponível em: <https://bit.ly/39cycmu>. Acesso em: 26 dez. 2020.

OWASP. **OWASP Mobile Top 10**. Disponível em: <https://bit.ly/3rleMSF>. Acesso em: 26 dez. 2020.

OWASP. **Intermediate update 1.1.3** (OSS Release), 4 ago. 2019. Disponível em: <https://bit.ly/3sj3HCN>. Acesso em: 26 dez. 2020.

ROHR, A. O que são phishing, watering hole e golpes on-line: G1 Explica. **G1 Segurança Digital**, 18 ago. 2016. Disponível em: <https://glo.bo/39bMLH2>. Acesso em: 22 dez. 2020.

SECURITY Magazine. **2020: The Year of Mobile Sneak Attacks?**, 9 mar. 2020. Disponível em: <https://bit.ly/2QCgSks>. Acesso em: 26 dez. 2020.

FOCO NO MERCADO DE TRABALHO

PROTEÇÃO PARA DISPOSITIVOS MÓVEIS

Emilio Tissato Nakamura

Ver anotações

QUAIS SÃO OS OBJETIVOS DE SEGURANÇA NO USO DE DISPOSITIVOS MÓVEIS NO MUNDO CORPORATIVO?

Separação do contexto pessoal do profissional, identificação remoção de aplicativos vulneráveis, uso de *antimalware*, uso de criptografia no tráfego, autenticação de duplo fator, conexão apenas de dispositivos confiáveis e política de segurança de instalação de aplicativos.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

O planejamento da nova versão da plataforma digital, baseada em dispositivos móveis, e com a nova função dos colaboradores para a expansão da rede de pequenos negócios parceiros, pode ser dividida em três grandes desenvolvimentos:

1. Desenvolvimento do aplicativo móvel para os consumidores.
2. Desenvolvimento do aplicativo móvel para os colaboradores.
3. Desenvolvimento do aplicativo móvel para os pequenos negócios.

Os aplicativos podem ser agregados, ou seja, pode haver somente um aplicativo que tenha as três funções: consumidor, colaborador e pequenos negócios. Os servidores e o *backend* estão em um provedor em nuvem na Europa.

Para o desenvolvimento do aplicativo móvel para os consumidores e os pequenos negócios, deve-se seguir as boas práticas de segurança, evitando as vulnerabilidades, principalmente aquelas citadas pelo OWASP: uso impróprio de plataforma, armazenamento de dados inseguros, comunicação insegura, autenticação insegura, criptografia insuficiente, autorização insegura, má qualidade de código, modificação de código, engenharia reversa e funcionalidade exposta. Além da prática para a codificação, é preciso estar atento para os demais controles de segurança necessários, como as avaliações de segurança, por exemplo.

Para o desenvolvimento do aplicativo móvel para os colaboradores, além de seguir as recomendações apresentadas, é preciso planejar como o uso do dispositivo móvel será implantado pela empresa.

Um ponto a ser definido pela empresa é o modelo de uso dos dispositivos móveis. De quem será o dispositivo móvel? O colaborador poderá utilizar o dispositivo móvel para fins pessoais? A definição será formalizada em uma política de segurança para dispositivos móveis, e os mecanismos para garantir que ela seja cumprida também precisa ser definida.

Os modelos possíveis são:

- Uso exclusivamente corporativo de dispositivos móveis providos pela empresa.
- Permissão para uso pessoal de dispositivos móveis providos pela empresa, no modelo conhecido como *Corporate-Owned Personally-Enabled* (COPE).
- Uso de dispositivos móveis pessoais dos próprios colaboradores para o uso corporativo, no modelo conhecido como *Bring Your Own Device* (BYOD) ou *Choose Your Own Device* (CYOD).

O uso de dispositivos móveis pelos colaboradores deve também ser definido com a condução de atividades essenciais:

- Conduzir uma análise de riscos em dispositivos móveis e para as informações acessadas por eles, considerando todos os elementos do risco: componentes, vulnerabilidades, ameaças, probabilidade, impacto, e agentes de ameaça.
- Adotar tecnologias de segurança móvel como *Enterprise Mobility Management / Mobile Device Management* (EMM/MDM), plataformas de defesa contra ameaças móveis ou serviço de voto a aplicações móveis, que utiliza uma variedade de técnicas estáticas, dinâmicas e comportamentais para determinar, com o uso de uma pontuação, se uma aplicação ou dispositivo demonstra qualquer comportamento que representa um risco de segurança ou de privacidade. Este serviço de voto pode ser utilizando antes da instalação nos dispositivos móveis.
- Reforçar o ciclo de vida de implantação de dispositivos móveis corporativos, com passos-chave para que os dispositivos cheguem aos colaboradores de uma forma segura, incluindo a análise de riscos, o modelo adotado que pode ou não permitir o uso de dispositivos particulares, inventário, monitoramento e atualizações.
- Implementar e fazer um piloto da solução de dispositivo móvel antes de colocá-la em produção, considerando conectividade, proteção, autenticação, funcionalidades, gerenciamento, registros e desempenho.
- Prover a segurança em cada dispositivo móvel corporativo antes de permitir o acesso a sistemas e informações corporativas, com uso de uma solução de gerenciamento de mobilidade corporativa (EMM/MDM).
- Manter atualizados o sistema operacional e os aplicativos móveis, minimizando as vulnerabilidades.
- Manter regularmente a segurança dos dispositivos móveis, fazendo avaliações periódicas de segurança e de cumprimento da política de segurança.

AVANÇANDO NA PRÁTICA

DADOS CONFIDENCIAIS NOS DISPOSITIVOS MÓVEIS DOS DIRETORES

Em uma análise sobre o ambiente tecnológico da empresa em que você trabalha, você observou que acessos foram sendo concedidos para os diretores, de modo que se perdeu o controle sobre o perímetro da empresa e sobre os dados confidenciais que agora existem fora da empresa, nos dispositivos móveis. O uso do dispositivo móvel tanto para assuntos pessoais quanto para assuntos corporativos é um outro desafio. Cite os principais pontos ou capacidades de segurança que você deve propor para que o uso de dispositivos móveis na empresa possa ser feito de uma forma formal e segura.

RESOLUÇÃO



A formalização do uso de dispositivos móveis na empresa segue o modelo em que é possível usá-los tanto para fins profissionais quanto para fins pessoais. Para os diretores, a empresa disponibiliza o dispositivo móvel, que precisa ser gerenciado com uma solução como o *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM), que aplicará as configurações definidas e manterá atualizados os componentes do dispositivo móvel, tratando as vulnerabilidades.

Uma campanha de conscientização para os diretores também é planejada, para que eles fiquem cientes dos riscos existentes no uso de dispositivos móveis, e também para que entendam como funcionará o gerenciamento e as atualizações. E a conscientização também considera recomendações para que os diretores não sejam vítimas de *phishing* ou *SMiShing*.

Algumas questões de segurança envolvidas com o uso de dispositivos móveis que devem ser consideradas para a definição da sua proposta são:

- Mistura de dados pessoais e dados corporativos.
- Instalação de aplicativos vulneráveis.
- Instalação de *malwares* a partir de fontes não oficiais.
- Interceptação de tráfego a partir de conexões não confiáveis.
- Conexões não confiáveis aceitas pela empresa.

A sua proposta para a defesa de dispositivos móveis, assim, define os seguintes pontos:

- Proteção dos dados armazenados no dispositivo móvel.
- Gerenciamento centralizado para aplicar políticas e configurações aos dispositivos.
- Avaliação da segurança das aplicações móveis.
- Proteção contra o acesso indevido aos dados do dispositivo móvel.
- Configurações de privacidade para proteger os dados dos usuários.
- Proteção contra tentativas de *phishing*.

NÃO PODE FALTAR

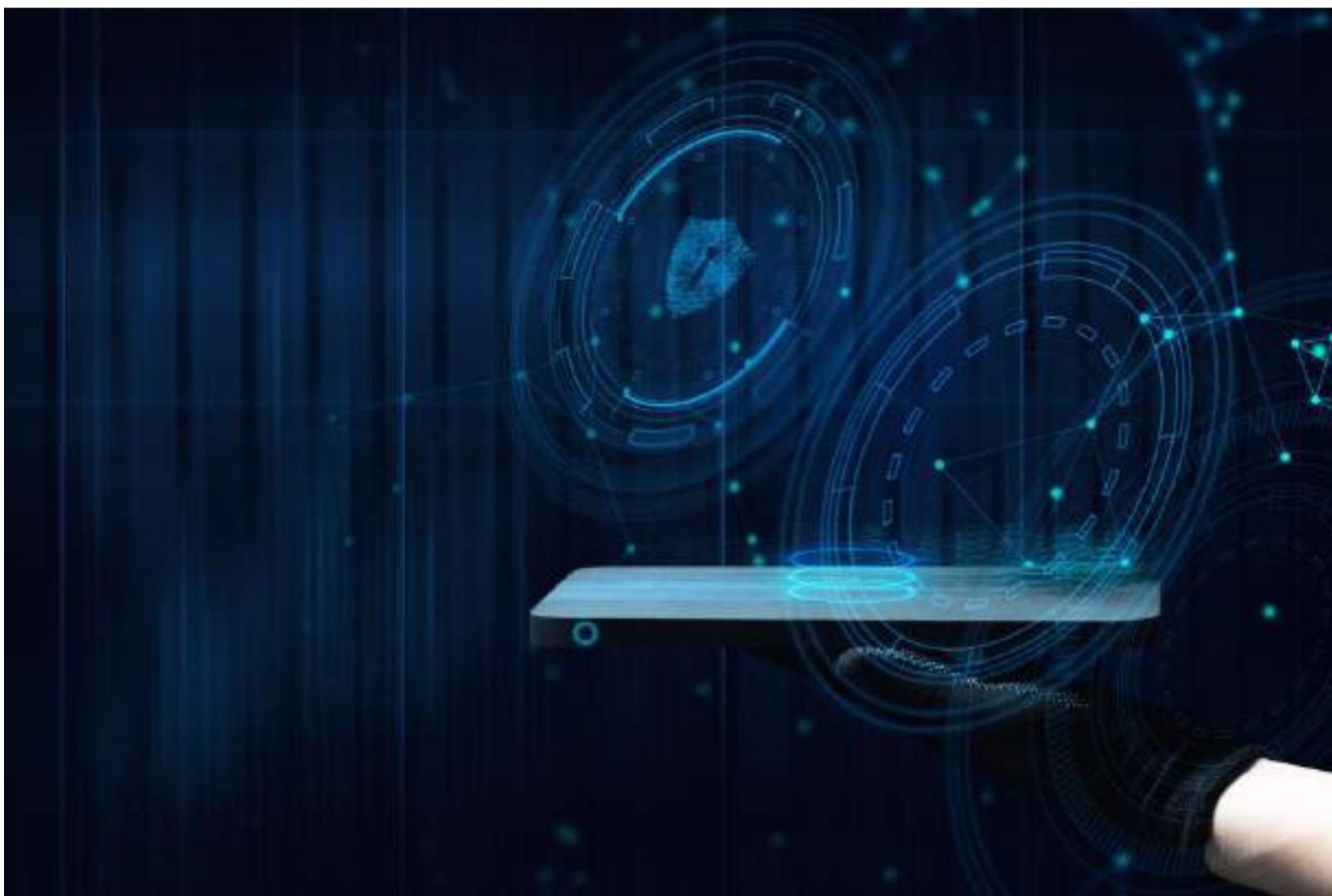
ANÁLISE DE VULNERABILIDADE E *PENTEST*

Emilio Tissato Nakamura

Ver anotações

O QUE É UM TESTE DE SEGURANÇA?

Um teste de segurança é um processo de análises e avaliações de riscos e análises de vulnerabilidades. É o processo de comparar o estado de um sistema ou aplicação de acordo com um conjunto de critérios.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Olá, nesta seção vamos estudar o elemento do risco que é explorado pelos agentes de ameaça nos ataques: a vulnerabilidade. O ambiente das empresas é formado por sistemas, plataformas, aplicações e aplicativos que são utilizados por colaboradores e clientes para acessar diferentes informações e serviços. Há um conjunto de ativos que formam este ambiente e qualquer um destes ativos pode ser atacado e resultar em incidentes de segurança e impactos para a empresa.

Os testes de segurança são importantes para a gestão de segurança da informação porque identificam as vulnerabilidades, que podem ser tratadas. E há diferentes formas de fazer testes de segurança e identificar as vulnerabilidades. O objetivo é a sua empresa disponibilizar serviços seguros, sem vulnerabilidades. Sem os testes de segurança, a sua empresa pode estar expondo informações sigilosas e a privacidade de clientes, colaboradores e parceiros.

Se a sua empresa desenvolve *software*, ela deve disponibilizar o sistema de uma forma segura, seguindo práticas que vão eliminando as vulnerabilidades desde o início do desenvolvimento até o período após a implantação em ambiente de produção.

Se a sua empresa utiliza *software* de terceiros, ela deve fazer testes de segurança para garantir que o ambiente da empresa, composta por softwares de diferentes fornecedores e de naturezas diferentes, esteja seguro.

E os testes de segurança são uma das principais atividades de empresas especializadas em segurança e privacidade, com a oferta de serviços de análise de vulnerabilidades e pentests, por exemplo.

Você é o especialista em segurança e privacidade de um inovador *site* de comércio *online* em que pequenos negócios são conectados com os consumidores em uma plataforma digital baseada no uso de inteligência artificial. A sua função é essencial para a empresa, e você participa de todas as decisões sobre a evolução da plataforma. Há as questões

envolvidas com o desenvolvimento seguro, para que vulnerabilidades não sejam inseridas. Há ainda as questões de segurança e privacidade envolvidas com o uso de provedor de nuvem. E, como a empresa trabalha com inteligência artificial, há necessidade de fazer o desenvolvimento utilizando bases de dados que não interfiram na privacidade dos clientes.

Além da segurança da informação da plataforma da empresa, que está hospedada em um provedor em nuvem na Europa, você tem três preocupações principais:

1. Como diminuir as possíveis fraudes cometidas por usuários falsos que se passam por clientes, com uso de identidades falsas ou uso de recursos financeiros ilícitos.
2. Como diminuir as possíveis fraudes cometidas por pequenos negócios falsos, que podem não cumprir os compromissos comerciais estabelecidos com os clientes que utilizam a plataforma digital.
3. Como proteger os dados pessoais dos clientes principalmente contra vazamentos, que pode levar a sanções previstas na LGPD.

Após já ter mostrado um planejamento sobre os aspectos que devem ser considerados pela empresa para a definição de uma estratégia de segurança e privacidade, com o seu direcionamento quanto à segurança em transações web e para a plataforma móvel, agora vamos para o próximo passo.

O que deve ser planejado agora é a forma como a empresa deve tratar as vulnerabilidades, tanto da plataforma *web* quanto da plataforma móvel. Mostre as perspectivas envolvidas com a gestão de vulnerabilidades e a razão de precisarem ser tratadas antes das plataformas irem para o ambiente de produção.

o

Ver anotações

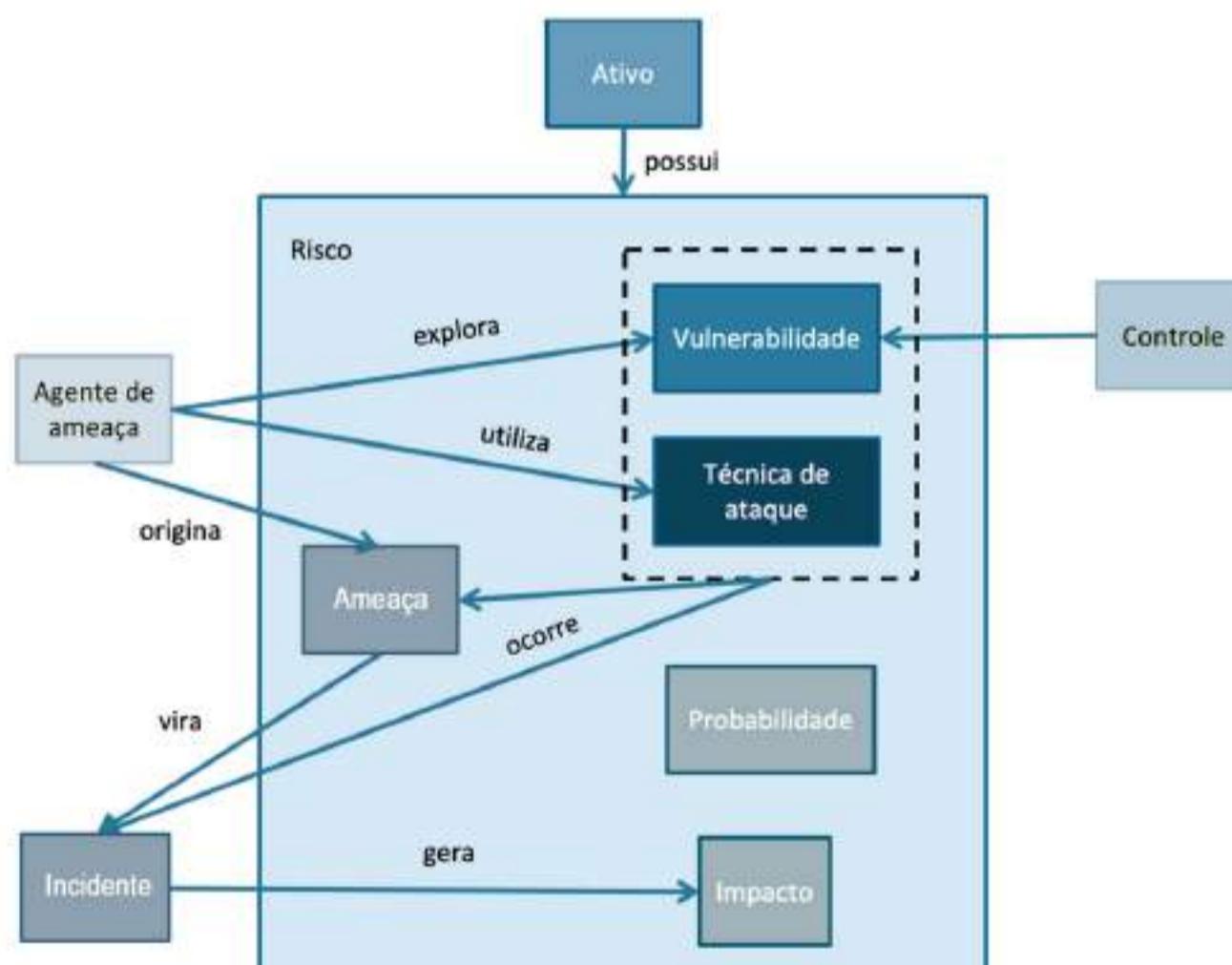
Continuando com o foco nas vulnerabilidades, mostre o que a empresa fará durante as fases do desenvolvimento das plataformas e o que será feito após a implantação.

Nesta aula, você verá que há diversas possibilidades de realização dos testes de segurança, que são baseados na origem dos testes e no nível de conhecimento prévio do ambiente em análise. Você verá que a qualificação e as qualidades técnicas do profissional são essenciais para que bons resultados sejam alcançados. Algumas metodologias estabelecem o que deve ser feito em cada passo dos testes de segurança e são importantes para você aplicar na sua empresa, seja como profissional de segurança ou como consultor.

CONCEITO-CHAVE

Uma das principais atividades dos profissionais de segurança da informação são as atividades relacionadas às vulnerabilidades dos ativos. Quando um ataque ou incidente de segurança acontece, ele é resultado da exploração de vulnerabilidades de ativos por um agente de ameaça (Figura 3.15).

Figura 3.15 | Ativos possuem vulnerabilidades que podem ser exploradas



Fonte: elaborada pelo autor.

O risco é a probabilidade de um agente de ameaça explorar vulnerabilidades de ativos utilizando alguma técnica de ataque, o que faz com que uma ameaça se torne um incidente de segurança,

causando impactos à empresa. Uma das principais formas de reduzir os riscos das empresas é o tratamento das vulnerabilidades, para que elas não possam ser exploradas (NAKAMURA, 2016).

I GESTÃO DE VULNERABILIDADES

As vulnerabilidades têm natureza complexa, já que são descobertas o tempo todo, surgem e são criadas em uma velocidade ainda maior. Com os ambientes mudando o tempo todo e com uso e integração de diferentes tecnologias, há sempre novas vulnerabilidades dos novos ativos das empresas. Assim, é importante que as vulnerabilidades sejam tratadas por um processo de gestão de vulnerabilidades que organiza as ações para a descoberta das inúmeras vulnerabilidades em diferentes ativos, levando em consideração a dinâmica das novas vulnerabilidades e dos ativos das empresas, que estão em constante mudança.

A gestão de vulnerabilidades engloba alguns processos que podem ser vistos na Figura 3.16 (CAVALANCIA, 2020):

- **Descoberta:** não é possível proteger o que não se conhece e este processo envolve o inventário de ativos, incluindo sistema operacional, serviços, aplicações e configurações.
- **Priorização de ativos:** os ativos descobertos precisar ser priorizados de acordo com uma visão de riscos para a empresa.
- **Avaliação:** estabelece uma linha de base para as vulnerabilidades e os riscos.
- **Relatório:** provê a visibilidade para todos da empresa, principalmente os executivos, que precisam entender o estado atual dos riscos e vulnerabilidades.
- **Remediação:** as vulnerabilidades, de acordo com a avaliação, são remediadas com a aplicação de controles de segurança.
- **Verificação:** a remediação é verificada para confirmar que a vulnerabilidade foi tratada corretamente.

Figura 3.16 | Processos da gestão de vulnerabilidades

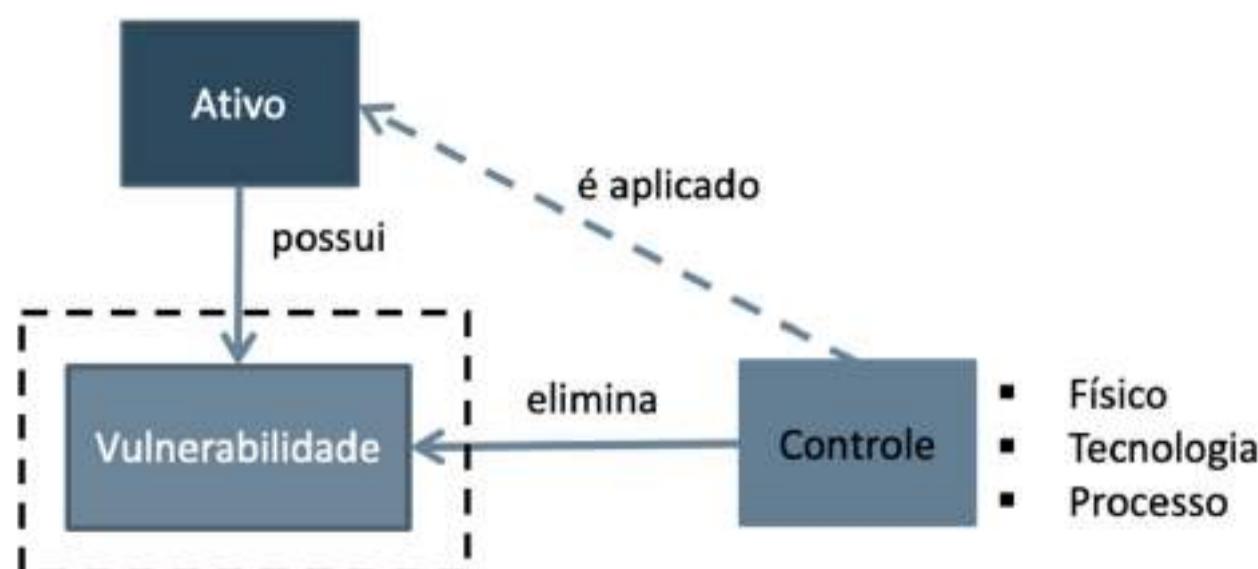


Fonte: adaptado de Cavalancia (2020).

Ver anotações

A identificação de vulnerabilidades é o início dos trabalhos para proteger as empresas e pode ser feita de diferentes formas. Uma vez descoberta e validadas as vulnerabilidades, elas devem ser tratadas com os controles de segurança. Os controles de segurança a serem aplicados na remediação das vulnerabilidades podem ser dos tipos físico, tecnológico ou processual (Figura 3.17).

Figura 3.17 | Controles de segurança



Fonte: elaborada pelo autor.

Há diferentes testes de segurança, como as análises e avaliações de riscos e as análises de vulnerabilidades, que focam tradicionalmente em aspectos tecnológicos. Para a *Open Web Application Security Project* (OWASP), que foca em aplicações *web*, teste de segurança é o processo de comparar o estado de um sistema ou aplicação de acordo com um conjunto de critérios (OWASP, 2014). Eles podem ser feitos no final do desenvolvimento ou fazer parte do ciclo de desenvolvimento desde o início, com a implementação de requisitos e testes de segurança automatizados (OWASP, 2019).

Os testes de segurança refletem diferentes visões, as quais envolvem variáveis como a origem dos testes (interno ou externo), as informações prévias disponíveis para os testes, o uso de ferramentas automatizadas e a qualificação dos profissionais. Estas variáveis são importantes, serão discutidas durante esta seção e indicam os tipos de teste de segurança envolvido, tais como os que podem ser vistos na Figura 3.18.

Figura 3.18 | Testes de segurança mais conhecidos



Fonte: elaborada pelo autor.

REFLITA

É preciso ter a mentalidade correta para os testes de segurança. Testes de segurança requerem um pensamento “fora da caixa”. Casos de uso normais irão testar o comportamento normal da aplicação em que o usuário está

utilizando as funções da forma como é esperado. Em testes de segurança, é preciso ir além das expectativas tradicionais e ter um pensamento de atacante, ou seja, daquele que está tentando quebrar a aplicação. A criatividade pode ajudar a determinar o que um dado não esperado pode causar na aplicação. Há casos em que as premissas não são sempre verdadeiras e podem ser subvertidas. E essa mentalidade faz com que os testes de segurança sejam feitos de acordo com critérios mentais que não são bem definidos ou completos, o que leva os demais a tratarem os testes de segurança como uma arte do mal. O papel do profissional é ainda mais valioso pelo fato das ferramentas automatizadas não terem criatividade, apenas implementando frameworks comuns (OWASP, 2014).

Um teste de segurança típico é estruturado tipicamente de acordo com as seguintes fases (OWASP, 2019), como pode ser visto na Figura 3.19:

- **Preparação:** definição do escopo do teste de segurança, incluindo a identificação dos controles de segurança aplicáveis, objetivos organizacionais do teste, e os dados sensíveis. Envolve ainda o alinhamento com o cliente e as medidas legais para os testes, que incluem a autorização.
- **Obtenção de informações:** análise do ambiente e da arquitetura da aplicação para o entendimento do contexto.
- **Mapeamento:** as informações obtidas até esta fase podem ser complementadas pelo uso de ferramentas automatizadas ou exploração manual. O mapeamento provê o entendimento da aplicação, os pontos de entrada, os dados e as potenciais vulnerabilidades. O mapeamento também inclui a criação dos casos de testes que serão executados, sendo o modelo de ameaças um dos artefatos que podem ser utilizados.

- **Exploração:** o profissional tenta atacar a aplicação explorando as vulnerabilidades identificadas durante a fase anterior, com a intenção de validá-las. Alguns parâmetros a serem considerados são o potencial de dano, a facilidade de reprodução do ataque, a facilidade de executar o ataque, os usuários afetados e a facilidade de descobrir a vulnerabilidade.
- **Relatório:** o profissional relaciona as vulnerabilidades que puderam ser exploradas, incluindo o escopo do comprometimento.

Figura 3.19 | Teste de segurança típico



Fonte: adaptada de OWASP (2019).

REFLITA

Fazer um teste de segurança superficial e considerá-lo completo é tão crítico quanto não fazê-lo, pela falsa sensação de segurança gerada. É importante que as vulnerabilidades encontradas sejam validadas, já que falsos negativos (falhas não encontradas) são fatais e falsos positivos (falhas apontadas que não existem) tiram a credibilidade dos resultados como um todo. Toda a lógica da aplicação deve ser testada e todo cenário de caso de uso deve ser analisado em busca de possíveis vulnerabilidades (OWASP, 2014).

ANÁLISE DE VULNERABILIDADES

A análise de vulnerabilidades compreende a busca por vulnerabilidades nos ativos de uma forma manual ou com o uso de ferramentas automatizadas, como os *scanners*. Os tipos de análise de vulnerabilidades são as análises estática e dinâmica (KOUSSA, 2018) (OWASP, 2019).

A análise estática, ou *Static Application Security Testing* (SAST), envolve a análise dos componentes do sistema sem a sua execução, pela análise manual ou automatizada do código-fonte. A análise manual exige proficiência na linguagem e no framework usado pela aplicação e possibilita a identificação de vulnerabilidades na lógica de negócios, violações de padrões e falhas na especificação, especialmente quando o código é tecnicamente seguro, mas com falhas na lógica, que são difíceis de serem detectados por ferramentas automatizadas. Já a análise automatizada é feita com ferramentas que checam o código-fonte por conformidade com um conjunto pré-definido de regras ou melhores práticas da indústria (OWASP, 2019).

EXEMPLIFICANDO

A revisão manual do código pode ser feita com o uso de métodos mais básicos de busca de palavras-chave no código-fonte, ou com a análise linha a linha do código-fonte.

Também podem ser utilizados os ambientes de desenvolvimento, ou *Integrated Development Environments* (IDEs) (OWASP, 2019).

A análise dinâmica, ou *Dynamic Application Security Testing* (DAST), envolve a análise do sistema durante a sua execução, em tempo real, de forma manual ou automatizada. Normalmente, a análise dinâmica não provê as informações que a análise estática provê, mas detecta elementos sob o ponto de vista do usuário, como os ativos, funções, pontos de entrada e outros. A análise dinâmica é conduzida na camada da plataforma e nos serviços e *Application Programming Interfaces*

(APIs) do *backend*, que são locais em que as requisições e respostas das aplicações podem ser analisadas. Os resultados são referentes, principalmente, a problemas de confidencialidade no trânsito, de autenticação e autorização, além de erros de configuração do servidor (OWASP, 2019).

O SAST e DAST podem ser adotados pelas próprias equipes de desenvolvimento no contexto do DevSecOp, que é um conceito importante que pode ser seguido para o desenvolvimento de *software*, ao integrar os testes de segurança na esteira de desenvolvimento, envolvendo a integração contínua e a entrega contínua (CONSTANTIN, 2020).

o

Ver anotações

REFLITA

Tratar falsos positivos ou alarmes falsos gerados por ferramentas automatizadas é fundamental. Um exemplo é uma vulnerabilidade em um servidor *backend*, que pode ser explorada a partir de um navegador *web*, mas não a partir de um aplicativo móvel. Isso ocorre em caso de ataques de *Cross-site Request Forgery* (CSRF) e *Cross-Site Scripting* (XSS) (OWASP, 2019).

ASSIMILE

SAST deve ser aplicado no código-fonte e é importante para remover as vulnerabilidades do código antes de o *software* entrar em produção. O DAST também deve ser realizado antes de o *software* entrar em produção e o teste é com o *software* funcionando, testando-se as interfaces existentes. Há ainda um teste de segurança conhecido como IAST (*Interactive Application Security Testing*), que faz os testes de segurança de uma forma interativa, combinando os testes estáticos e dinâmicos (SAST e DAST).

REFLITA

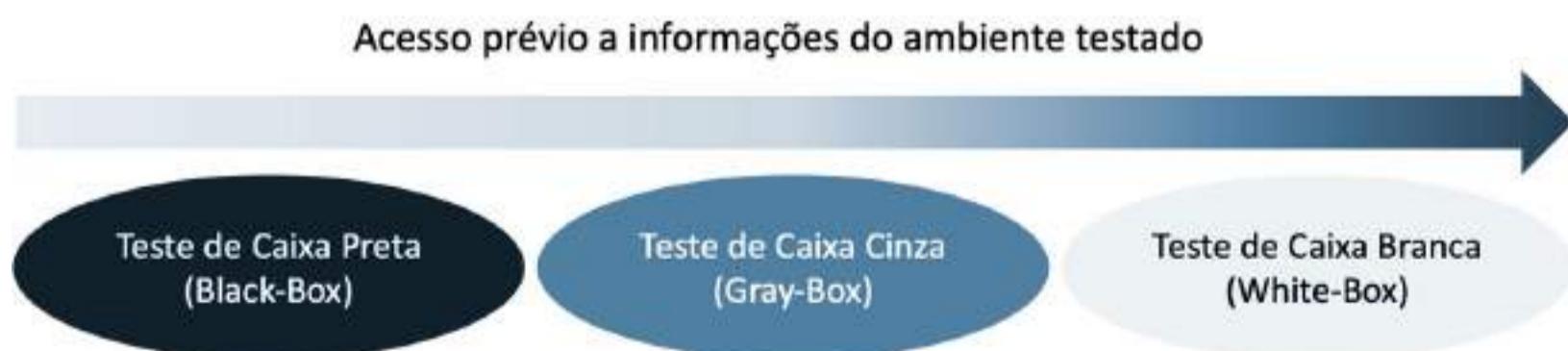
As ferramentas de análise automatizada do SAST geram os resultados com avisos e alertas das violações detectadas e podem funcionar como *plug-ins* nos IDEs. Os resultados dessas ferramentas podem gerar falsos positivos, principalmente se não forem configuradas para o ambiente específico do sistema. Assim, é fundamental que os resultados automatizados sejam sempre revisados por um profissional de segurança (OWASP, 2019).

PENTEST

Os testes de penetração ou *pentests* são também conhecidos como testes de intrusão e *ethical hacking* e são realizados a partir do ambiente externo. Os objetivos são determinar “se” e “como” um agente de ameaça pode obter um acesso não autorizado a ativos que afetam um ambiente, e confirmar se os controles requeridos por padrão, regulamento ou legislação estão implementados. Envolve ainda identificar meios de explorar vulnerabilidades para driblar os controles de segurança dos componentes do sistema (PCI, 2017).

Há três tipos de *pentests*, que depende das informações do ambiente obtidas antes dos testes de segurança, como pode ser visto na Figura 3.20.

Figura 3.20 | Tipos de *pentest*



Fonte: adaptada de OWASP (2019), PCI (2017).

O **teste de caixa preta (Black-Box)** é também conhecido como teste com conhecimento zero, já que é conduzido sem qualquer informação sobre o ambiente que está sendo testado. O objetivo é que o

profissional faça o teste como se fosse um atacante real, explorando o uso de informações públicas e que podem ser obtidas sem restrição por qualquer atacante (OWASP, 2019).

REFLITA

Os resultados dos testes de caixa preta podem impressionar e serem úteis para demonstrar como as vulnerabilidades são exploradas em um ambiente de produção. Porém, não são muito efetivos ou eficientes em tornar a aplicação mais segura. Há dificuldades em testes dinâmicos que exploram todo o código, particularmente quando há uma série de condições interligadas. Assim, se o código-fonte da aplicação estiver disponível, é importante que ele seja disponibilizado para o profissional de segurança para que este possa utilizá-lo no teste (OWASP, 2014).

O **teste de caixa branca (White-Box)** é também conhecido como teste com conhecimento total e é conduzido com todo o conhecimento sobre o ambiente, que engloba código-fonte, documentações e diagramas. Este tipo de teste é mais rápido do que o teste de caixa preta, porque há a transparência e o conhecimento permite a construção de casos de teste mais sofisticados e granulares (OWASP, 2019).

REFLITA

O acesso ao código-fonte no teste de caixa branca (*White-Box*) não simula ataques externos, mas simplifica a identificação de vulnerabilidades, ao possibilitar a identificação de anomalias ou comportamentos suspeitos diretamente no código. A decompilação de aplicações pode ser utilizada no teste de caixa preta (*Black-Box*), porém o código-fonte pode estar ofuscado e revertê-lo pode ser trabalhoso (OWASP, 2019).

Já o **teste de caixa cinza (Gray-Box)** é o teste em que alguma informação é provida para o profissional, como uma credencial de acesso, enquanto outras informações têm de ser descobertas. Este teste é bastante comum, devido aos custos, tempo de execução e escopo do teste (OWASP, 2019).

DICA

Hackathon é um evento que reúne programadores, *designers* e outros profissionais ligados ao desenvolvimento de *software* em maratonas de trabalho com o objetivo de criar soluções específicas para um ou vários desafios (GOMES, 2017). Ele pode envolver aspectos de segurança da informação e há, ainda, o *Capture The Flag* (CTF), que é uma modalidade de competição voltada a desvendar problemas sobre segurança da informação, avaliando, de forma gamificada, habilidades como vulnerabilidade da rede, criptografia e programação, entre outras (MENA, 2018). E há testes públicos de segurança, como o teste público de segurança promovido pelo TSE, visando um conjunto de ações controladas a fim de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do sigilo do voto em uma eleição, com a apresentação de sugestões de melhoria de componentes do sistema eletrônico (TSE, 2017). As empresas também podem criar programas de *Bug Bounty*, em que oferecem prêmios para quem encontrar falhas em seus sistemas, que variam de acordo com o nível de gravidade de cada vulnerabilidade encontrada (WARBURTON, 2020).

| METODOLOGIA OWASP TESTING PROJECT

A OWASP Testing Project foca em aplicações web e visa a construção de aplicações mais confiáveis e seguras. A metodologia segue as premissas de que a prática de testar o *software* deve estar em todo o ciclo de vida

de desenvolvimento do seu desenvolvimento (*Software Development Life Cycle*, SDLC) (Figura 3.21) e que uma das melhores maneiras de prevenir bugs de segurança em aplicações em produção é o SDLC incluir a segurança em cada uma de suas fases.

Figura 3.21 | Ciclo de vida de desenvolvimento de *software* (SDLC)



Fonte: adaptada de OWASP (2014).

A metodologia de testes do OWASP compreende técnicas e atividades para cada fase do SDLC, como pode ser vista na Figura 3.22. Elas são voltadas para serem aplicadas nas empresas que desenvolvem *software*, e trata dos seguintes pontos (OWASP, 2014):

- **Fase 1 - Antes de o desenvolvimento iniciar**
 - **Fase 1.1 - Definição do SDLC:** define em qual estágio a segurança é inerente no processo de desenvolvimento.
 - **Fase 1.2 - Revisão de políticas e padrões:** assegura que as equipes possam desenvolver as atividades de acordo com as políticas, padrões e documentações.
 - **Fase 1.3 - Desenvolvimento de métricas:** dá visibilidade ao processo e ao produto com as métricas a serem medidas.

- **Fase 2 - Durante a definição e especificação**

- **Fase 2.1 - Revisão dos requisitos de segurança:** define como a aplicação deve funcionar na perspectiva de segurança. Os requisitos de segurança precisam ser testados. Os requisitos não devem ser ambíguos e incluem mecanismos como gerenciamento de usuários, autenticação, autorização, confidencialidade de dados, integridade, contabilidade, gerenciamento de sessão, segurança no transporte, segregação em camadas, conformidade com legislação e padrões.
- **Fase 2.2 - Revisão da especificação e arquitetura:** testa artefatos como modelos, documentos textuais e outros documentos, para analisar os requisitos de segurança considerados.
- **Fase 2.3 - Criação e revisão dos modelos UML:** confirma que o entendimento do funcionamento da aplicação é exato após a especificação e arquitetura e modelos *Unified Modeling Language* (UML).
- **Fase 2.4 - Criação e revisão do modelo de ameaças:** utiliza cenários de ameaças realísticos sobre a especificação, arquitetura e modelos UML para a modelagem de ameaças. As ameaças devem ter sido mitigadas, aceitas pelo negócio ou transferidas para terceiros, como empresas de seguros. Caso não haja estratégias de mitigação, a especificação deve ser alterada.

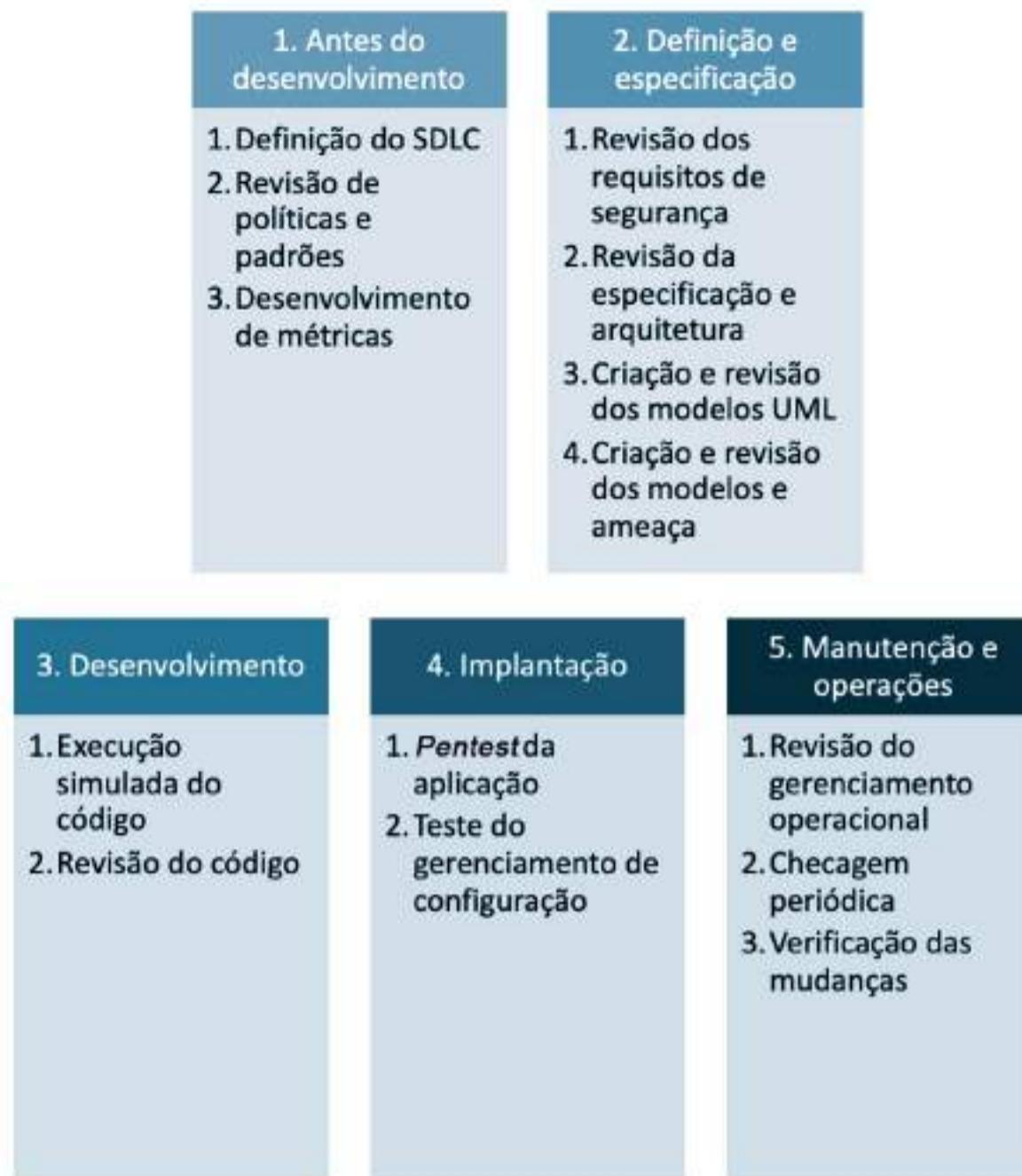
- **Fase 3 - Durante o desenvolvimento**

- **Fase 3.1 - Execução simulada do código:** executa (*walk through*) o código com os desenvolvedores e/ou arquitetos do sistema, em um processo alto nível de execução simulada do código em que os desenvolvedores podem explicar a lógica e o fluxo do código implementado. Esta fase permite o entendimento geral do código e possibilita que os desenvolvedores expliquem a

razão de alguns trechos específicos desenvolvidos. Não é objetivo revisar o código, mas ter um entendimento em alto nível do fluxo, do *layout* e da estrutura do código da aplicação.

- **Fase 3.2 - Revisão do código:** valida o código com a revisão estática, de acordo com alguns objetivos, que incluem os requisitos de negócios para disponibilidade, confidencialidade e integridade, exposição técnica de vulnerabilidades do OWASP Top 10, pontos específicos de linguagens ou *frameworks*, além de requisitos específicos de alguma indústria.
- **Fase 4 - Durante a implantação**
 - **Fase 4.1 - Pентest da aplicação:** provê uma última checagem após os testes dos requisitos, análise da especificação e revisão do código.
 - **Fase 4.2 - Teste do gerenciamento de configuração:** testa a forma como a infraestrutura é implantada e segura, principalmente quanto a instalações-padrão e vulneráveis.
- **Fase 5. Manutenção e operações**
 - **Fase 5.1 - Revisão do gerenciamento operacional:** analisa a forma como a aplicação e a infraestrutura são gerenciadas.
 - **Fase 5.2 - Checagem periódica:** checa a aplicação e a infraestrutura para que novos riscos sejam tratados e o nível de segurança seja preservado. É integrado com a gestão de riscos.
 - **Fase 5.3 - Verificação das mudanças:** checa a mudança para que o nível de segurança não seja afetado após a aprovação e teste da mudança em ambiente de teste e implantação em ambiente de produção. É integrado com a gestão de mudança.

Figura 3.22 | Framework da metodologia da OWASP



Fonte: adaptada de OWASP (2014).

A OWASP prevê algumas análises de segurança (OWASP, 2014):

- **Inspeção e revisão manual:** identifica preocupações de segurança com a análise de documentação e entrevistas, focando em como determinados pontos funcionam e como eles foram implementados. Esta técnica pode analisar o processo de ciclo de vida de desenvolvimento de *software* e assegurar que há uma política adequada e conhecida por todos, além das qualificações necessárias para a especificação e implementação da segurança na aplicação. É recomendado um modelo de “*trust-but-verify*”, já que nem tudo o que é mostrado ou dito é efetivo. As vantagens desta técnica são: não requer tecnologia de suporte; pode ser aplicada em situações variadas; tem flexibilidade; é aplicada no início do SDLC. As desvantagens são: pode consumir tempo; os materiais de suporte nem sempre estão disponíveis; requer competência e qualificação do profissional de segurança.

- **Modelagem de ameaças:** ajuda os arquitetos de sistemas a pensarem nas ameaças para seus sistemas e aplicações, possibilitando a criação de estratégias de mitigação para potenciais vulnerabilidades de uma forma priorizada. Os modelos de ameaças devem ser criados no início do SDLC e revisado conforme o progresso do desenvolvimento. As vantagens são: provê visão do sistema sob o ponto vista do atacante; tem flexibilidade; é aplicado no início do SDLC. As desvantagens são: técnica relativamente nova; modelos de ameaça bons não significam *softwares* bons. O modelo de ameaça pode ser desenvolvido de acordo com os passos do NIST 800-30 (NIST, 2012):

- Decomposição da aplicação: entendimento de como a aplicação funciona, seus ativos, funcionalidades e conectividade.
- Definição e classificação dos ativos: classificação dos ativos e priorização de acordo com a importância de negócio.
- Exploração de vulnerabilidades potenciais: incluindo as técnicas, operacionais e de gerenciamento.
- Exploração de ameaças potenciais: criação de visões de vetores de ataques potenciais com uso de cenários ou árvores de ataques.
- Criação de estratégias de mitigação: controles de segurança para cada ameaça explorável.

- **Revisão de código-fonte:** é uma técnica capaz de detectar muitas vulnerabilidades que outras técnicas não permitem, já que todo problema de segurança está em algum ponto do código. Com a análise do código-fonte, o profissional pode determinar o que está ocorrendo com a aplicação e remover as possibilidades que aparecem em testes de caixa preta. As vantagens são: completude e efetividade; acurácia; rapidez na execução. As desvantagens são: requer qualificação de segurança dos desenvolvedores; pode não identificar problemas em bibliotecas compiladas; não detecta erros

de execução facilmente; necessita de análise de procedimentos operacionais, pois o código implantado pode não ser o mesmo do que está sendo analisado.

- **Teste de penetração ou *pentest*:** realizado de forma remota, do ponto de vista dos usuários, com o profissional atuando como um atacante, a partir de uma conta válida de usuário. Diferentemente de *pentests* em redes ou sistemas operacionais, que têm vulnerabilidades conhecidas e ferramentas automatizadas, os *pentests* em aplicações são mais complexos, já que possuem vulnerabilidades não conhecidas. A recomendação, assim, é que para as aplicações *web*, o *pentest* não seja utilizado como teste primário, apesar de ser útil para detectar algumas vulnerabilidades específicas que podem ser corrigidas. As vantagens são: pode ser rápido (e mais barato); requer menos qualificação do que uma revisão de código-fonte. As desvantagens são: é feito somente no final do SDLC; consegue testar somente a entrada.

REFLITA

Dentre os testes de segurança, o melhor é uma abordagem balanceada, que inclui diferentes técnicas, da revisão manual aos testes técnicos, em diferentes fases do SDLC. Em alguns casos, não há o acesso ao código-fonte, o que faz com que o *pentest* seja melhor do que nenhum teste, que pode ser ainda complementado com outros testes de segurança (OWASP, 2014).

METODOLOGIA OSSTMM

A metodologia *Open Source Security Testing Methodology Manual* (OSSTMM), da *Institute for Security and Open Methodologies* (ISECOM), surgiu em 2000 como um *framework* de melhores práticas e em 2005 evoluiu para uma metodologia. Em 2006, a OSSTMM se tornou um

padrão que foca na segurança, além de poder ser utilizado para a conformidade de acordo com um regulamento ou legislação específica (ISECOM, 2010).

A OSSTMM engloba cinco dimensões ou canais: humano, físico, sem fio, telecomunicações e redes de dados. Eles possibilitam testes de segurança na computação em nuvem, infraestruturas virtuais, *middleware* de mensagens, infraestruturas de comunicação móvel, locais de alta segurança, recursos humanos, computação confiável, e qualquer processo lógico que necessite de testes de segurança. A metodologia ainda tem um conjunto de métricas de superfície de ataque. Os testes podem ser certificados, de acordo com requisitos que incluem a condução dos testes, se todos os canais necessários foram testados, a postura dos testes de acordo com a lei, a mensuração dos resultados de uma forma quantificável, a consistência e repetitividade dos resultados, e se os resultados contêm apenas fatos derivados dos próprios testes (ISECOM, 2010).

Os sete passos para fazer um teste de segurança, segundo a OSSTMM (ISECOM, 2010), são:

- Definir o que será protegido, os ativos e os controles.
- Identificar a área em torno dos ativos que incluem mecanismos de proteção, os processos e serviços. Esta área é a zona de engajamento, onde ocorrem as interações com os ativos.
- Definir tudo o que está fora da zona de engajamento que é necessário para manter os ativos operacionais. Podem ser incluídos elementos que não podem ser influenciados diretamente, como eletricidade, alimento, água, ar, informação, legislação ou regulamentos. Podem ser incluídos ainda elementos que podem ser trabalhados, como a umidade, temperatura, claridade, fornecedores, parceiros, entre outros. E, também, podem ser incluídos processos, protocolos e recursos que mantêm a infraestrutura funcionando. Este é o escopo do teste.

- Definir como o escopo interage entre os elementos e fora dele. Vetores – que são compartimentos lógicos dos ativos que possuem as direções das interações, como de fora para dentro, de departamento A para departamento B, ou de dentro para dentro – devem ser utilizados.
- Identificar os equipamentos necessários para cada teste, em cada vetor, que por sua vez possui diferentes dimensões ou canais: humano, físico, sem fio, telecomunicações e redes de dados.
- Determinar quais informações serão geradas com os testes.
- Assegurar que o teste de segurança está em conformidade com as regras de engajamento, a fim de assegurar que o processo seja executado sem criar mal entendimentos, concepções equivocadas ou falsas expectativas.

Os tipos de testes de segurança previstos e citados no OSSTMM são seis (Figura 3.23), e são baseados na quantidade de informações que os profissionais têm dos alvos, o que o alvo sabe sobre o profissional ou a expectativa do teste e a legitimidade do teste. Alguns irão testar as qualificações do profissional mais do que testar a segurança do alvo (ISECOM, 2010):

- **Blind:** o profissional testa o alvo sem conhecimento prévio sobre a defesa, os ativos e os canais. O alvo é preparado para a análise com o conhecimento dos detalhes da análise. Este teste visa principalmente a qualificação do profissional, já que os avanços da análise podem ir até onde essa qualificação permite. Também é conhecido como *ethical hacking*, ou *war gaming* ou *role playing* no contexto do canal físico.
- **Double Blind:** o profissional testa o alvo sem conhecimento prévio sobre a defesa, os ativos e os canais. O alvo não é notificado sobre o escopo da análise, nem dos canais a serem testados e nem dos vetores de testes. Este teste visa a qualificação do profissional e a preparação do alvo para variáveis desconhecidas. Os avanços da

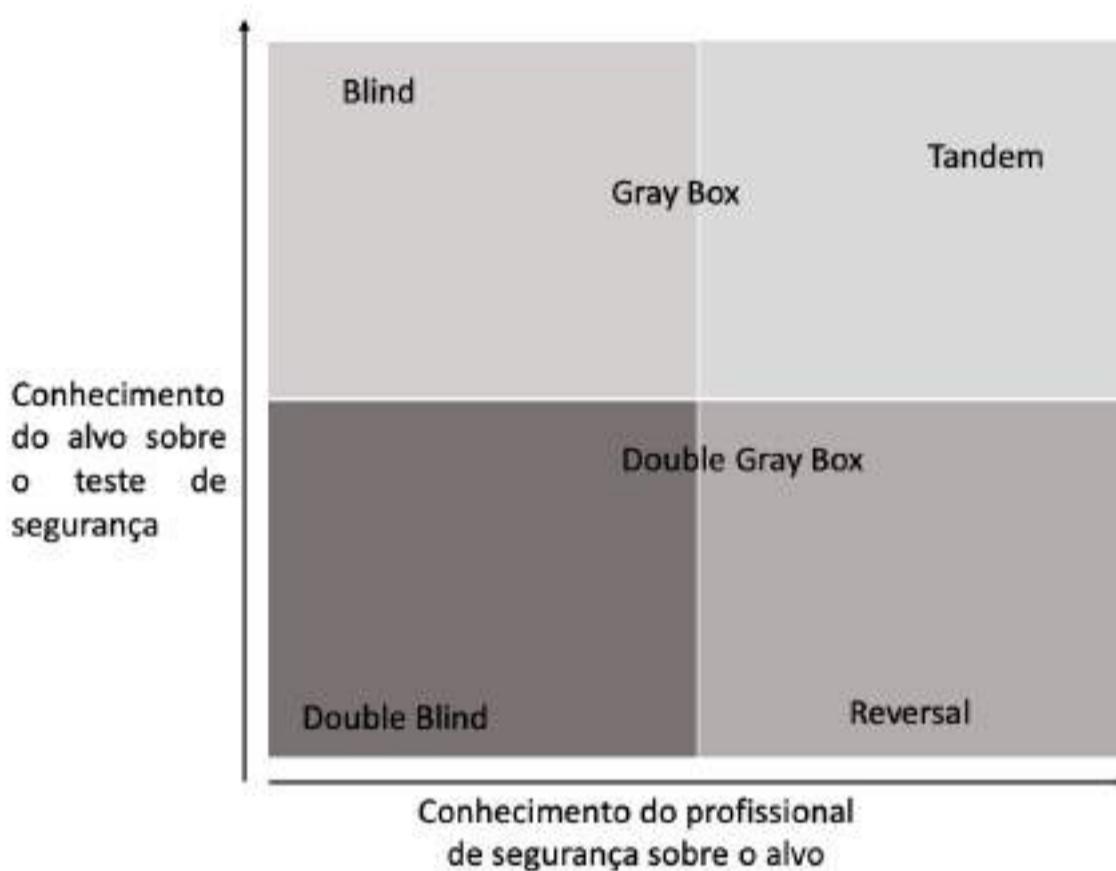
análise podem ir até onde a qualificação do profissional permite.

Também é conhecido como teste de caixa preta ou *pentest*.

- **Gray Box:** o profissional testa o alvo com conhecimento limitado sobre a defesa e os ativos e conhecimento total dos canais. O alvo é preparado para a análise com o conhecimento dos detalhes da análise. Este teste visa a qualificação do profissional. A natureza do teste é a eficiência. Os avanços da análise podem ir até onde a qualificação do profissional permite e dependem da qualidade das informações providas para o profissional antes da análise. Também é conhecido como teste de vulnerabilidade e é iniciado pelo alvo como uma autoavaliação.
- **Double Gray Box:** o profissional visa o alvo com um conhecimento limitado sobre a defesa e os ativos e conhecimento total dos canais. O alvo é notificado sobre o escopo e o período da análise, mas não sobre os canais e vetores de teste. Este teste visa a qualificação do profissional e a preparação do alvo. Os avanços da análise podem ir até onde a qualificação do profissional permite e dependem da qualidade das informações providas para o profissional e para o alvo antes da análise. Também é conhecido como teste de caixa branca.
- **Tandem:** o profissional e o alvo são preparados para a análise, tendo conhecimento sobre os detalhes do teste. Este teste visa a proteção e os controles do alvo. No entanto, não testa o estado de preparação do alvo. A natureza do teste é a meticulosidade, já que o analista não tem a visão completa dos testes e suas respostas. Os avanços da análise podem ir até onde a qualificação do profissional permite, e dependem da qualidade das informações providas para o profissional antes da análise. Também é conhecido como *in-house audit* ou teste de *crystal box*, e o profissional é geralmente parte do processo de segurança.
- **Reversal:** o profissional visa o alvo com conhecimento total sobre os processos e segurança operacional, mas o alvo não sabe sobre o

que, como, e quando o profissional irá fazer o teste. A natureza do teste é a análise do estado de preparação do alvo. Os avanços da análise podem ir até onde a qualificação e criatividade do profissional permitem e dependem da qualidade das informações providas para o profissional antes da análise. Também é conhecido como exercício de *red team*.

Figura 3.23 | Tipos de testes do OSSTMM



Fonte: adaptado de ISECOM (2010).

| METODOLOGIA PTES

A metodologia *Penetration Testing Execution Standard* (PTES) é composta por sete seções (Figura 3.24), que definem as atividades a serem realizadas, desde as interações iniciais até o relatório. De uma forma geral, as atividades são suportadas por uma documentação técnica detalhada, para cada uma das seções do PTES. As seções descrevem como iniciar as atividades, obter informações para a análise, a modelagem de ameaças, as análises de vulnerabilidades, a exploração para passar pelos controles de segurança existentes, o pós-exploração para manter o acesso e controle do alvo e o relatório final.

Figura 3.24 | Metodologia PTES



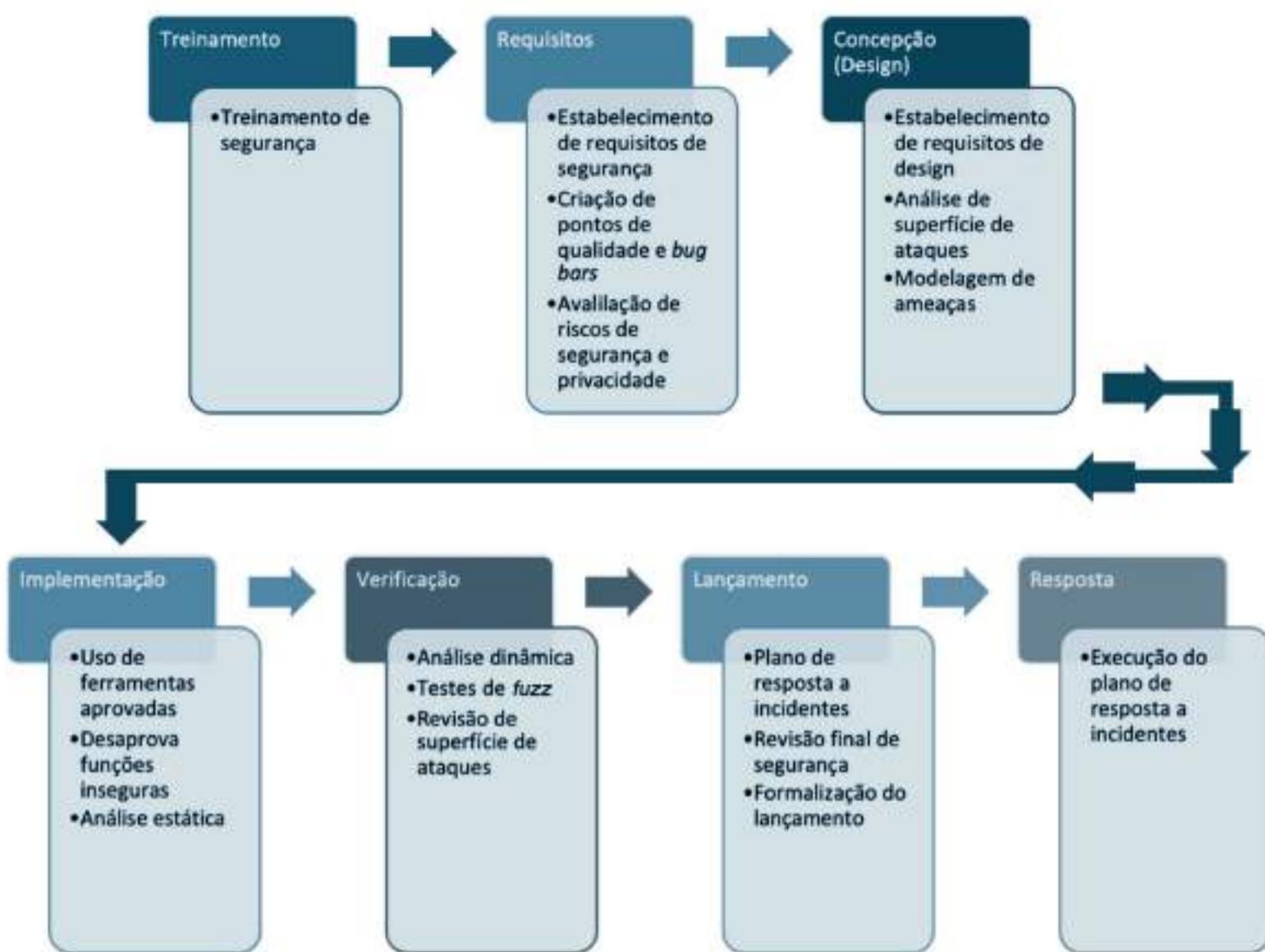
Fonte: adaptada de PTES (2014).

APLICAÇÃO DOS TESTES DE SEGURANÇA

Os testes de segurança são parte importante da gestão de segurança da informação e devem ser feitos por todas as empresas, sejam aquelas que desenvolvem *software* ou aquelas que adquirem sistemas.

A metodologia OWASP *Testing Project* foca na segurança no ciclo de vida de desenvolvimento de *software*, com a inserção de testes de segurança em diferentes pontos do ciclo. O desenvolvimento seguro envolve ainda outros elementos de segurança como o treinamento de segurança, o estabelecimento de requisitos de segurança, a criação de pontos de qualidade, a inclusão de funções de segurança, a avaliação de riscos de segurança e privacidade e o plano de resposta a incidentes após a implantação (Figura 3.25).

Figura 3.25 | Ciclo de vida de desenvolvimento seguro



Fonte: adaptada de Lipner (2010).

SAIBA MAIS

As análises de código-fonte, realizadas no *Static Analysis Security Testing* (SAST) podem ser feitas com o uso de ferramentas ou manualmente. As ferramentas conseguem identificar erros no código, mas dificilmente conseguem identificar falhas na especificação e na lógica.

E o teste de caixa preta pode também ter algumas limitações na identificação de vulnerabilidades. Um exemplo é o uso de um mecanismo criptográfico para autenticar um usuário de diferentes *sites*. Neste exemplo, um usuário autenticado no *site A* pode visitar o *site B* automaticamente. Nesta implementação, essa validação é feita com o uso de um *hash* do nome de usuário e data, que é enviado ao site B pelo site A e pelo usuário. O site B pode então comparar o *hash* para validar o usuário. O problema de segurança é que, uma vez descoberto o funcionamento, qualquer agente de ameaça que capture o *hash* pode chegar ao site B. O teste de caixa

preta enxerga o *hash*, sem saber a sua função, de uma forma direta, que só pode ser identificada com uma análise de código.

PESQUISE MAIS

Aplicações *web* têm características diferentes de aplicações móvel. Os testes de segurança seguem as principais fases de uma forma genérica, mas os testes específicos são diferentes, dependendo do ambiente. E é aí que entra a qualificação do profissional de segurança, que deve fazer os testes condizentes com o ambiente que está sendo analisado. Lembre-se que a qualidade dos testes vai até onde chega a capacidade do profissional, incluindo o limitante do tempo disponível.

A OWASP Testing Project (2014) apresenta exemplos práticos e as atividades de como executar os testes, além da indicação de ferramentas e referências sobre cada teste. Dentre as categorias de testes, estão:

- Obtenção de informação.
- Gerenciamento de configuração e implantação.
- Gestão de identidades.
- Autenticação.
- Autorização.
- Gerenciamento de sessão.
- Validação de entradas.
- Criptografia.
- Lógica de negócio.
- Lado cliente.

Assim chegamos ao final desta seção que trata de testes de segurança. Você já conhece os diferentes tipos de testes que podem ser realizados, tanto para sistemas adquiridos quanto para *software* que é desenvolvido. Menos vulnerabilidades significam menos chances de exploração dos ativos de sua empresa, ou seja, menos incidentes de segurança.

FAÇA VALER A PENA

Questão 1

Testes de segurança são importantes para identificar as vulnerabilidades de um sistema, para que assim possam ser tratadas, antes de serem exploradas por agentes de ameaça. Quando a exploração ocorre, os resultados são incidentes de segurança e impactos para a organização.

O tipo de teste de segurança que é realizado sob o ponto de vista de um usuário ou agente de ameaça, em que nenhuma informação prévia do ambiente é fornecida para o profissional de segurança é o:

- a. Teste de caixa preta.
- b. Teste de caixa cinza.
- c. Teste de caixa branca.
- d. Static Analysis Security Testing (SAST).
- e. Dynamic Analysis Security Testing (DAST).

Questão 2

Sua empresa está finalizando o desenvolvimento de um sistema e você faz parte da equipe de desenvolvimento, focando em aspectos de segurança e privacidade. Você já fez uma análise de código-fonte e agora precisa testar o sistema com ele funcionando.

O teste de segurança que é feito neste estágio do ciclo de vida de desenvolvimento de software, antes da implantação é o:

- a. Teste de caixa preta.

b. Teste de caixa cinza.

c. Teste de caixa branca.

d. *Static Analysis Security Testing (SAST)*.

e. *Dynamic Analysis Security Testing (DAST)*.

Questão 3

Testes de segurança podem ser feitos a partir do ambiente interno ou a partir do ambiente externo. Há testes que analisam o código-fonte e outros que analisam o ambiente em execução. O objetivo é sempre utilizar e desenvolver sistemas com o mínimo de vulnerabilidades, já que são elas que são exploradas em ataques.

Assinale a alternativa que contém os testes de segurança que você pode realizar e que fazem uso de código-fonte.

a. Pentest de caixa preta e *Dynamic Analysis Security Testing (DAST)*.

b. *Static Analysis Security Testing (SAST)* e *Dynamic Analysis Security Testing (DAST)*.

c. Pentest de caixa preta e *Static Analysis Security Testing (SAST)*.

d. Pentest de caixa cinza e *Static Analysis Security Testing (SAST)*.

e. Pentest de caixa branca e *Static Analysis Security Testing (SAST)*.

REFERÊNCIAS

CAVALANCIA, N. Vulnerability management explained, Security Essentials, **AT&T Cybersecurity**, 2 jul. 2020. Disponível em: <http://soc.att.com/3tOIEZi>. Acesso em: 31 dez. 2020.

CONSTANTIN, L. O que é o DevSecOps? Por que é difícil fazer? **SegInfo**, 31 jul. 2020. Disponível em: <https://bit.ly/31sTI7T>. Acesso em: 20 jan. 2021.

GOMES, P. C. T. O que é um hackathon e como pode beneficiar a sua empresa? Inovação e Tecnologia, **OPServices**, 12 jan. 2017. Disponível em: <https://bit.ly/2NNX3We>. Acesso em: 20 jan. 2021

HICKEN, A. Software Safety and Security Through Standards, **Parasoft**, 15 set. 2016. Disponível em: <https://bit.ly/3d22euq>. Acesso em: 2 nov. 2020.

ISECOM, Institute for Security and Open Methodologies. **OSSTMM 3 – The Open Source Security Testing Methodology Manual**. 2010. Disponível em: <https://bit.ly/39b6KWn>. Acesso em: 27 dez. 2020.

KOUSSA, S. What Do Sast, Dast, last And Rasp Mean To Developers? **SoftwareSecured**, 2 nov. 2018. Disponível em: <https://bit.ly/31dI2QP>. Acesso em: 9 dez. 2020.

LIPNER, S. Microsoft Corporation. The OWASP Foundation. **The Security Development Lifecycle**. 24 jun. 2010. Disponível em: <https://bit.ly/2QAHeDs>. Acesso em: 2 nov. 2020.

MENA, I. Verbete Draft: o que é Capture The Flag (CTF). **Draft**, 7 fev. 2018. Disponível em: <https://bit.ly/3vRUrrL>. Acesso em: 20 jan. 2021.

MICROSOFT Corporation. **What are the Microsoft SDL practices?** Disponível em: <https://bit.ly/39fnJgy>. Acesso em: 2 nov. 2020.

NAKAMURA, E. T. **Segurança da informação e de redes**. Editora e Distribuidora Educacional S.A., 2016.

NIST, National Institute of Standards and Technology, U.S. Department of Commerce. Joint Task Force Transformation Initiative. **NIST Special Publication 800-30 Revision 1**. Guide for Conducting Risk Assessments. 12 set. 2020. Disponível em: <https://bit.ly/3lOkKKG>. Acesso em: 31 dez. 2020.

OWASP. **Intermediate update 1.1.3** (OSS Release), 4 ago. 2019. Disponível em: <https://bit.ly/3fcIKuk>. Acesso em: 26 dez. 2020.

OWASP. **Testing Guide 4.0**. Disponível em: <https://bit.ly/3d5Or5U>. Acesso em: 28 dez. 2020.

PCI Data Security Standard (PCI DSS) 1.1. Penetration Test Guidance
Special Interest Group PCI Security Standards Council. **Information**
Supplement: Penetration Testing Guidance. Set. 2017. Disponível em:
<https://bit.ly/3snNtbF>. Acesso em: 30 dez. 2020.

PTES. **Main page.** 16 ago. 2014. Disponível em: <https://bit.ly/3faCkao>.
Acesso em: 30 dez. 2020.

TSE. **TSE realiza teste público de segurança do sistema eletrônico de votação de 28 a 30 de novembro.** 27 nov. 2017. Disponível em:
<https://bit.ly/39dWRqJ>. Acesso em: 20 jan. 2021.

WARBURTON, A. Bug Bounty: como funciona o mundo do *hacking* ético e a caça às vulnerabilidades. **Welivesecurity**, 23 jan. 2020. Disponível em: <https://bit.ly/2PqDtQc>. Acesso em: 20 jan. 2021.

FOCO NO MERCADO DE TRABALHO

ANÁLISE DE VULNERABILIDADE E *PENTEST*

Emilio Tissato Nakamura

0
Ver anotações

O QUE É *PENTEST*?

O teste de intrusão é um método que avalia a segurança de um sistema, determina "se" e "como" um agente de ameaça pode obter um acesso não autorizado a ativos que afetam um ambiente e identifica vulnerabilidades nos controles de segurança dos componentes do sistema.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

As vulnerabilidades são os pontos explorados pelos agentes de ameaça em ataques. As plataformas *web* e móvel que serão desenvolvidas são compostas por diferentes elementos ou ativos, os quais podem conter vulnerabilidades e, portanto, devem ser identificadas e tratadas. Ativos como sistema operacional, componentes de infraestrutura ou bibliotecas de *software* de terceiros também podem conter vulnerabilidades que devem ser eliminadas. As aplicações em si, que serão desenvolvidas, também podem inserir vulnerabilidades no sistema e, portanto, o desenvolvimento do sistema deve considerar a segurança em todo o seu ciclo de vida.

Assim, a gestão de vulnerabilidades da empresa deve prever a descoberta, priorização de ativos, avaliação, relatório, remediação e verificação da remediação em todos os ativos do sistema, incluindo os de terceiros e os que serão implementados. Como o ambiente do sistema muda constantemente, e novas vulnerabilidades são sempre descobertas, a gestão de vulnerabilidades deve ser implementada para acompanhar o dinamismo dos ambientes *web* e móvel.

Dentre os diferentes testes de segurança que podem ser realizados, o plano é adotar os mais completos, o que foi indicado pela avaliação de riscos. Como os testes mais completos são os que requerem mais recursos, incluindo o tempo, o planejamento é fundamental.

O plano prevê, assim, testes de segurança a serem realizados internamente e com o ponto de vista externo, do agente de ameaça.

Os testes internos fazem parte do ciclo de vida de desenvolvimento de *software*, com atividades de segurança sendo feitas nas fases de definição, especificação, desenvolvimento, implantação e manutenção das plataformas *web* e móvel.

A análise de vulnerabilidades no código-fonte, a *Static Analysis Security Testing* (SAST), será feita por sua equipe. A SAST complementará outras atividades de segurança e privacidade importantes durante o desenvolvimento, antes da implantação:

- Treinamento da equipe em segurança e privacidade.
- Revisão de políticas e padrões de segurança e privacidade.
- Uso de métricas para medir a segurança e privacidade das plataformas web e móvel;
- Revisão dos requisitos de segurança, incluindo mecanismos como gerenciamento de usuários, autenticação, autorização, confidencialidade de dados, integridade, contabilidade, gerenciamento de sessão, segurança no transporte, segregação em camadas, conformidade com legislação e padrões.
- Revisão da especificação e arquitetura.
- Criação e revisão integrada dos modelos UML.
- Criação e revisão do modelo de ameaças.
- Execução simulada do código.
- Teste do gerenciamento de configuração.

Outro teste de segurança a ser realizado antes da implantação, com a plataforma *web* e móvel em execução, é a *Dynamic Analysis Security Testing* (DAST). Normalmente, a análise dinâmica não provê as informações que a análise estática provê, mas detecta elementos sob o ponto de vista do usuário, como os ativos, funções, pontos de entrada e outros.

Após a implantação do sistema, o plano é a contratação de uma empresa especializada em *pentest*, para complementar os testes feitos pela sua própria equipe. A empresa contratada fará o teste de caixa preta, com uma visão total do agente de ameaça, enquanto a sua equipe fará o teste de caixa branca, que faz sentido pela sinergia existente com os outros testes de segurança da fase de desenvolvimento, com o acesso ao código-fonte, documentação e diagramas. Estes testes serão complementados pelas atividades necessárias no ambiente de produção:

- Revisão do gerenciamento operacional.
- Verificação das mudanças.

PROJETO NOVO COMEÇANDO, COM SEGURANÇA

A empresa em que você trabalha teve sucesso com investidores e, por isso, foi aprovado um orçamento para o desenvolvimento de um novo projeto, que é um novo sistema de gerenciamento de energia solar.

Você faz parte da equipe e sua responsabilidade como gestor de segurança e privacidade é grande, pois os investidores e executivos da empresa sabem que os ativos envolvidos controlam grandes recursos financeiros que são manipulados pelo sistema. Focando nos testes de segurança, apresente o plano para que a implantação do sistema seja feita de uma forma segura.

RESOLUÇÃO



O ciclo de vida de desenvolvimento de software deve incluir a segurança e privacidade, com a definição dos pontos em que os processos de segurança serão feitos.

O treinamento de desenvolvimento seguro para toda a equipe, visando minimizar a incorporação de vulnerabilidades, é apoiado por políticas, padrões e documentações.

A segurança e privacidade fazem parte dos requisitos de todo o sistema, com requisitos específicos e é realizada revisão da especificação e arquitetura sob essa perspectiva.

Com o uso de modelos de ameaças e alinhamento quanto ao funcionamento de todo o sistema e as implicações de segurança e privacidade, a codificação é acompanhada com a execução simulada e a revisão do código implementado.

São realizadas análises estáticas (SAST) e dinâmicas (DAST) antes da implantação do sistema.

E o *pentest* é realizado no ambiente de homologação uma vez, e outra vez no ambiente de produção, junto dos testes de gerenciamento de configuração.

Após a implantação, é feita a revisão de gerenciamento operacional e as verificações das mudanças, que incluem novas análises de vulnerabilidades.

Novos *pentests* (caixa cinza) são feitos periodicamente, a cada bimestre. Para tanto, uma credencial de usuário será disponibilizada para a empresa especializada contratada.

NÃO PODE FALTAR

Imprimir

FUNDAMENTOS DE AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

Ver anotações 0

O QUE É UMA AUDITORIA DE SISTEMAS?

Auditória é uma inspeção e verificação formal para checar se um padrão ou conjunto de guias está sendo seguido, se os registros estão corretos e se os objetivos de eficiência e eficácia estão sendo alcançados.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

CONVITE AO ESTUDO

Olá, aluno! Nesta unidade avançaremos pela auditoria de sistemas e de segurança da informação, que tem um papel importante para a efetiva proteção das informações da empresa.

A gestão de riscos identifica, analisa, avalia, comunica e trata os riscos em um contexto determinado. Os controles de segurança são definidos e implementados a partir desta visão de riscos e de acordo com padrões e requisitos regulatórios e legais. A auditoria valida a eficiência e eficácia dos controles, com uma análise criteriosa que segue processos e aplica técnicas e ferramentas. O papel do auditor é, assim, fundamental, e o resultado é uma empresa mais segura e em conformidade com padrões, regulações e leis aplicáveis.

A auditoria exerce uma influência positiva para as empresas também no aspecto de comunicação e relações institucionais, melhorando o nível de confiança com todos os atores envolvidos, incluindo funcionários, clientes, fornecedores, parceiros de negócios e investidores. Do ponto de vista de padrão, um exemplo é o *Payment Card Industry Data Security Standard* (PCI DSS), aplicado para empresas que fazem parte do ecossistema de cartões, o qual tem como objetivo melhorar o tratamento de dados de portadores de cartão, o que é benéfico para todo o ecossistema. Um outro exemplo de auditoria é a ISO 27001, que certifica a segurança das empresas em um determinado escopo de auditoria.

Já a análise dos controles das empresas pode ser feita com base em diferentes normas, padrões e frameworks, tais como o *Control Objectives for Information and related Technology* (COBIT) ou *Information Technology Infrastructure Library* (ITIL). Controles de segurança como os relacionados à aquisição, desenvolvimento e manutenção de software ou o controle de acesso podem ser baseados em normas e padrões como a NBR ISO/IEC 27002 ou o NIST 800-53, que definem controles de diferentes tipos, como os administrativos, técnicos e operacionais. Os controles também podem ser classificados como físico, técnico ou lógico e processual.

A forma de executar a auditoria é importante, com o uso das técnicas e ferramentas mais adequadas para cada objetivo. Uma exigência é que, tendo aspectos abrangentes, o auditor precisa definir e utilizar seus conhecimentos e ferramentas para analisar detalhes do ambiente para validar a efetividade dos controles.

As técnicas de auditoria podem ir de entrevistas a testes técnicos com o uso de ferramentas para análise de *logs* e até mesmo de código-fonte, por exemplo.

Com a auditoria, o ciclo de segurança e privacidade fica completo, visando a efetiva segurança das empresas.

Bons estudos!

PRATICAR PARA APRENDER

Olá, nesta seção, você conhecerá o papel do auditor de sistemas e de segurança, que é importante para que a empresa esteja de fato protegida contra os riscos existentes. Você já viu que é a partir dos riscos identificados, analisados e avaliados que os controles de segurança são identificados para serem implantados. Este tratamento dos riscos com os controles de segurança pode resultar em riscos residuais, além daqueles que foram aceitos ou que não foram identificados. Como é possível verificar que a empresa está segura? É preciso analisar se os controles são suficientes para o contexto da empresa, se eles foram implantados de uma forma correta e se estão funcionando de forma adequada.

Este é o papel da auditoria que será discutido nesta aula. A auditoria requer que o auditor busque evidências, avalie as forças e fraquezas de controles internos com base nas evidências coletadas e prepare um relatório de auditoria que apresenta as fraquezas e recomendações para a remediação de uma forma objetiva para apresentar aos atores envolvidos.

As fases do processo de auditoria são importantes, com o planejamento, trabalho em campo e relatórios. O mais importante é, porém, o conhecimento do auditor, que precisa definir as técnicas e as ferramentas para a auditoria, a qual exige conhecimentos amplos e profundos para que seja possível fazer uma análise da eficiência e eficácia dos controles da empresa.

o

Ver anotações

Você trabalha para um provedor de nuvem que está crescendo de uma forma muito rápida e tem recebido como clientes muitas empresas tradicionais, principalmente pelo processo de transformação digital.

Como sua empresa tem clientes de diferentes setores, como financeiro, saúde e governo, há uma exigência para que os serviços sejam seguros e que estejam em conformidade com regulamentos e leis específicas.

Monte um planejamento visando melhorar a segurança da empresa e para fortalecer a imagem do provedor de nuvem diante do mercado quanto ao tratamento das necessidades de segurança e conformidade. Justifique cada ponto do seu planejamento, já que ele será distribuído para a diretoria executiva para que haja a aprovação de seu planejamento.

Uma sugestão de itens do planejamento que não podem faltar são:

- Como é a segurança do provedor de nuvem, em linhas gerais.
- Por que a segurança é importante, focando nos clientes.
- Demanda dos clientes para a conformidade.
- Auditoria de segurança, por que fazer.
- Principais fases da auditoria.
- Conclusão.

A auditoria exige o entendimento de seus conceitos e princípios, que demonstram a importância das competências do auditor, as quais devem ser abrangentes e profundas para serem aplicadas nas fases do processo de auditoria.

Boa aula!

CONCEITO-CHAVE

A auditoria de sistemas é cada vez mais importante para as empresas e tem como papel assegurar que os controles internos sejam eficientes e efetivos. A segurança da informação e privacidade, que é feita a partir

de uma visão de riscos que direciona a definição e implantação de controles de segurança, é uma das áreas em que a auditoria é parte essencial para garantir que a empresa esteja de fato protegida contra as ameaças.

o

INTRODUÇÃO À AUDITORIA E AUDITORIA DE SISTEMAS: CONCEITOS E PRINCÍPIOS

Com a evolução constante do ambiente das empresas, junto do dinamismo dos objetivos de negócios, a auditoria é cada vez mais importante. De uma forma geral, a auditoria tem como objetivo verificar e validar atividades, processos e sistemas das empresas de acordo com o que está estabelecido, incluindo aspectos legais e regulatórios, visando também a eficiência e eficácia. Ela é feita em diferentes contextos, como o ambiental, contábil, financeiro, fiscal, riscos, segurança, sistemas, social, tributário ou trabalhista.

Outro objetivo da auditoria é atestar a conformidade com regulações administrativas, regulatórias e legais. A auditoria visa ainda confirmar para a alta gestão da empresa que o negócio está funcionando bem e está preparado para enfrentar os potenciais desafios. E, principalmente, ela visa assegurar aos diferentes atores envolvidos no negócio sobre a estabilidade financeira, operacional e ética da organização (ISACA, 2016).

Os objetivos da auditoria podem ser vistos na Figura 4.1.

Figura 4.1 | Objetivos da auditoria

Ver anotações

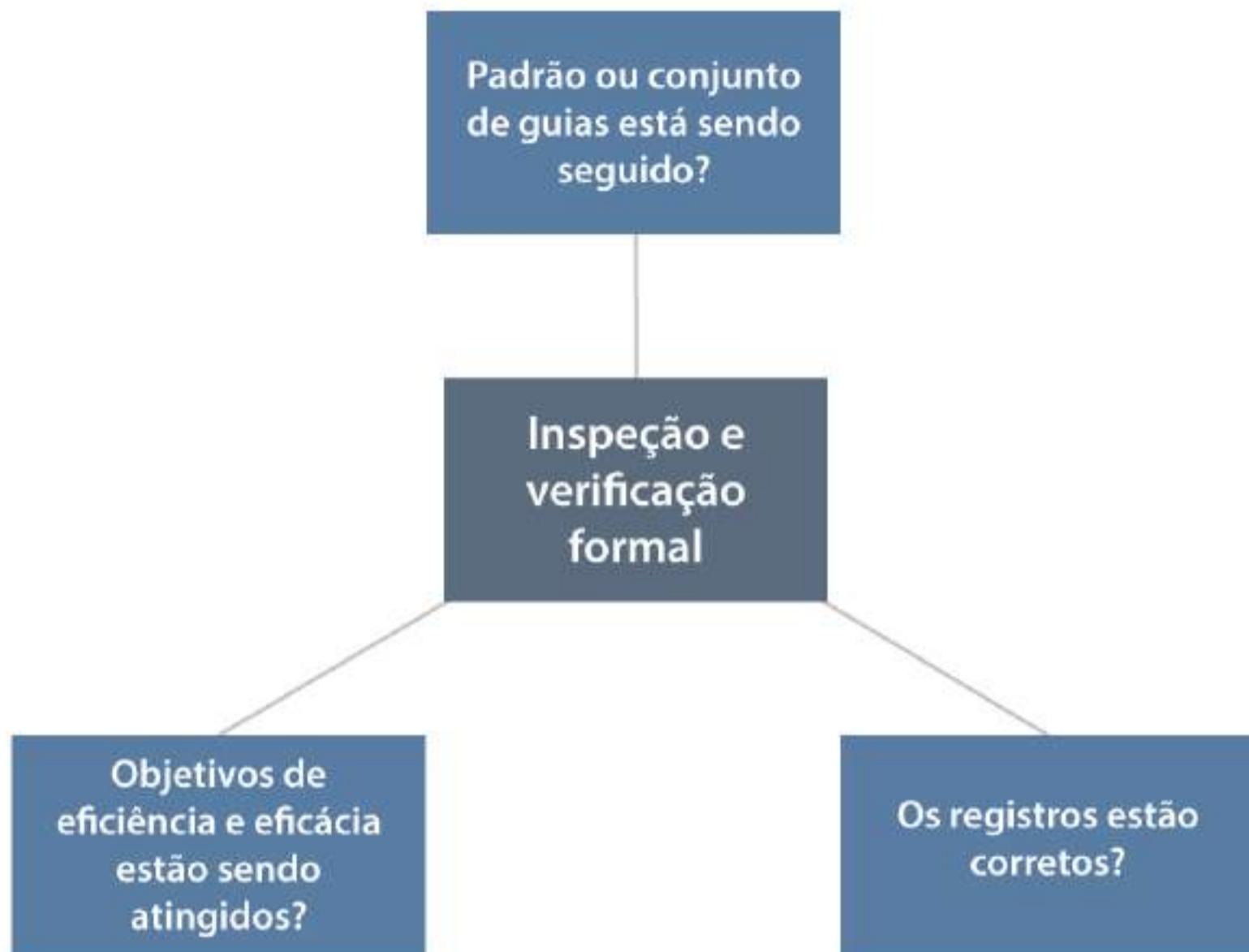


Fonte: adaptada de ISACA (2016, 2017, 2020).

Uma das principais características da auditoria é que ela só pode ser feita por auditores, os quais são profissionais que normalmente têm certificação para exercer esta função. Outra característica é que a auditoria é independente das funções operacionais, o que permite que sejam providas opiniões objetivas e sem viés sobre a efetividade do ambiente de controle interno (ISACA, 2016).

Segundo a *Information Systems Audit and Control Association* (ISACA), que foca em sistemas de informação, a auditoria (Figura 4.2) é uma inspeção e verificação formal para checar se um padrão ou conjunto de guias está sendo seguido, se os registros estão corretos e se os objetivos de eficiência e eficácia estão sendo alcançados (ISACA, 2016).

Figura 4.2 | O que é uma auditoria de sistemas



Fonte: adaptada de ISACA (2016).

A auditoria de sistemas de informação tem foco na informação e nos sistemas relacionados, os quais têm importância cada vez maior, principalmente com a transformação digital. A auditoria de sistemas de informação provê uma série de benefícios para as empresas, tais como a garantia de eficácia, eficiência, segurança e confiabilidade das operações dos sistemas de informação, que são críticos para o sucesso organizacional.

ASSIMILE

A auditoria de sistemas visa garantir que os controles de TI sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz.

Algumas suposições críticas de auditoria de sistemas são (ISACA, 2020):

- O escopo da auditoria é identificável e sujeito à auditoria.
- Há grande probabilidade de sucesso da auditoria ser concluída.
- A abordagem e a metodologia não são enviesadas.
- O projeto de auditoria tem escopo suficiente para os objetivos da auditoria de sistemas.
- O projeto de auditoria irá gerar um relatório objetivo e que não levará a entendimentos dúbios do leitor.

AUDITORIA DE SEGURANÇA E CONTROLES DE SEGURANÇA

Para a segurança e privacidade das empresas, é importante que os processos estejam bem definidos e a equipe responsável tenha as competências para as ações necessárias. A governança garante que as ações do cotidiano sejam tratadas de modo que as ameaças correntes e as emergentes sejam sempre tratadas e alinhadas com a alta gestão (ISACA, 2017).

Ver anotações

EXEMPLIFICANDO

Os principais desafios para as organizações, principalmente em um cenário como o de uma pandemia, são a segurança cibernética, privacidade, dados e resiliência, segundo uma pesquisa feita em 2020. Estes assuntos ganharam importância com a transformação digital e ainda mais com o trabalho remoto e os novos processos de negócios, os quais exigem avaliações de riscos mais estruturadas, com mais frequência, em resposta ao novo contexto. Soma-se a isso a maior conectividade e a Internet das Coisas (*Internet of Things, IoT*), que cresce ainda mais com o advento do 5G. A maturidade digital gera vantagens de negócios e tem acelerado a transformação digital, que exige mais segurança, privacidade e resiliência (ISACA, 2020).

Os investimentos em controles de segurança são necessários para proteger as empresas contra os ataques cibernéticos, que estão crescendo em sofisticação e abrangência. Somada à necessidade regulatória, a segurança da informação e privacidade faz parte da estratégia e *framework* das empresas, o que leva à necessidade de revisão gerencial, avaliação de riscos e auditoria dos controles de segurança (ISACA, 2017).

Os investimentos para melhorar a proteção e as respostas aos incidentes são definidos nos programas de segurança e privacidade das empresas. Do ponto de vista da alta gestão, as questões envolvem os valores investidos, se eles estão adequados e se foram direcionados e implementados corretamente, também em comparação com os concorrentes. Com isso, há dois elementos importantes para as empresas: a avaliação dos riscos atuais e emergentes para a empresa e a auditoria dos controles de segurança atuais e que estão planejados para protegerem os ativos da empresa. Assim, a gestão de riscos é importante para identificar, analisar e avaliar os riscos, que direcionarão a definição dos controles para o tratamento dos riscos. Com a auditoria, a empresa assegura que os controles protegem a empresa de uma forma adequada.

•
Ver anotações

REFLITA

Para as empresas, qual a melhor forma de priorizar investimentos? A gestão de riscos avalia as oportunidades e ameaças, e as ações podem assim ser definidas. No contexto da segurança da informação, os riscos com níveis mais altos, que são produto do cálculo da probabilidade e do impacto, levando em consideração os ativos, vulnerabilidades, agentes de ameaça, ameaças e controles existentes, são naturalmente priorizados. O tratamento dos riscos com a definição e implementação dos controles de segurança, além da proteção, elevam a confiança com os diferentes atores envolvidos, incluindo clientes, público, investidores e a própria gestão interna. A auditoria dá a força e visibilidade sobre a eficácia e efetividade da proteção.

■ O PAPEL DO AUDITOR DE SISTEMAS

O *Information Technology Audit Framework* (ITAF) da ISACA é um framework de auditoria de TI que define padrões para as auditorias de TI relacionadas aos papéis e responsabilidades, ética, comportamento

esperado e conhecimento e qualificação requeridas, além de termos e conceitos específicos ao assunto. Além disso, o ITAF provê guias e técnicas para planejar, executar e reportar auditoria de TI (ISACA, 2020).

Para o auditor, o ITAF estabelece algumas responsabilidades (ISACA, 2020):

- Documentar a função em um estatuto, indicando propósito, responsabilidade, autoridade e a prestação de contas.
- Obter aprovação formal do estatuto pela diretoria executiva e/ou comitê de auditoria.
- Comunicar a alta gestão sobre o estatuto da auditoria.
- Atualizar o estatuto a fim de manter o alinhamento com a missão e estratégia da organização.
- Ser livre de conflitos de interesses e influências indevidas.
- Responder para uma área organizacional que seja livre de influências indevidas.
- Ser objetivo nos assuntos de auditoria.
- Seguir padrões de auditoria e de indústria, além de leis e regulações aplicáveis que levarão a uma opinião ou conclusão profissional.
- Definir um escopo claro e sem limitações, o escopo deve levar a conclusões.
- Deixar clara as obrigações e responsabilidades para que sejam providas informações apropriadas, relevantes e no tempo correto.
- Ter diligência e cuidados profissionais de acordo com código de ética, incluindo a conduta e o caráter, a privacidade e a confidencialidade, e o uso das informações obtidas para fins particulares.
- Ter a competência profissional para executar as atividades requeridas

- Ter conhecimento adequado sobre o assunto em auditoria.
- Manter a competência profissional com educação e treinamento contínuo.
- Revisar as informações obtidas de modo que elas sejam suficientes, válidas e relevantes.
- Selecionar critérios de auditoria objetivos, completos, relevantes, confiáveis, mensuráveis, entendíveis, reconhecidos amplamente, que tenham autoridade e sejam entendidos por todos os envolvidos.
- Considerar a aceitação de critérios reconhecidos, oficiais e disponíveis publicamente.

A efetividade da auditoria depende, em grande parte, da qualidade do programa de auditoria, que será visto a seguir. E as capacidades necessárias para o auditor desenvolver um bom programa de auditoria são (ISACA, 2016):

- Bom entendimento da natureza da empresa e de sua indústria, para identificar e categorizar os tipos de riscos e ameaças.
- Bom entendimento sobre TI e seus componentes, incluindo o conhecimento sobre as tecnologias que afetam o ambiente.
- Entendimento do relacionamento entre riscos de negócios e riscos de TI.
- Conhecimento básico das práticas de avaliação de riscos.
- Entendimento de diferentes procedimentos de testes para avaliar controles de sistemas de informação e identificar o melhor método para a avaliação.

No caso da auditoria de controles de segurança, há a exigência de um conjunto de habilidades que envolvem aspectos especializados, tais como para os *pentests*, as análises de configurações de servidores ou *firewalls*, a revisão de regras de ferramentas de segurança (ISACA, 2017).

O **planejamento** da auditoria é essencial para o sucesso, e o escopo e objetivo da auditoria devem estar claros, entendidos e aceitos pelo auditor e pelo auditado. Uma vez que o propósito da auditoria é definido, o plano de auditoria (Figura 4.3) pode ser criado, englobando o escopo acordado, os objetivos e os procedimentos necessários para a obtenção de evidências que sejam relevantes, confiáveis e suficientes para construir e suportar as conclusões e opiniões da auditoria (ISACA, 2016).

Um componente importante do plano de auditoria é o programa de auditoria, também conhecido como programa de trabalho. O programa de auditoria é composto por procedimentos e passos específicos que serão utilizados para testar e verificar a efetividade dos controles. A qualidade do programa de auditoria possui um impacto significativo na consistência e na qualidade dos resultados da auditoria, de modo que os auditores devem entender como desenvolver programas de auditoria completos e abrangentes (ISACA, 2016).

Figura 4.3 | Plano de auditoria e programa de auditoria



Fonte: adaptada de ISACA (2016).

A auditoria requer que o auditor busque evidências, avalie as forças e fraquezas de controles internos com base nas evidências coletadas, e prepare um relatório de auditoria que apresenta as fraquezas e recomendações para a remediação de uma forma objetiva para os atores envolvidos (ISACA, 2016). As principais fases da auditoria são o planejamento, trabalho em campo e relatórios (Figura 4.4). A fase de planejamento da auditoria tem como resultado o programa de auditoria.

Figura 4.4 | Principais fases de um processo de auditoria e os passos



6

Ver anotações

Fonte: adaptada de ISACA (2016).

■ PLANEJAMENTO

O **objeto** da auditoria pode ser um sistema, uma localidade ou uma unidade de negócio. Um exemplo de **objetivo** da auditoria é determinar se as mudanças no código-fonte de um sistema crítico ocorrem em um ambiente bem definido e controlado. O **escopo** da auditoria, neste exemplo, é o sistema que é composto por diferentes componentes que precisam passar por uma avaliação completa. É o escopo que direciona o auditor a definir o conjunto de testes relevantes para a auditoria, junto de qualificações técnicas e recursos necessários para avaliar diferentes tecnologias e seus componentes.

Na execução do **planejamento de pré-auditória**, a condução de uma avaliação de riscos ajuda na justificativa das atividades e no refinamento do escopo. Além disso, uma entrevista ajuda no entendimento das atividades e áreas que devem ser incluídas no escopo de trabalho, junto da identificação dos requisitos regulatórios de conformidade. Os recursos necessários podem assim ser definidos, incluindo o orçamento necessário para o trabalho, as localidades ou plantas a serem auditadas, as regras e responsabilidades da equipe de auditoria, o tempo determinado para cada estágio da auditoria, as fontes de informação para os testes ou revisões (fluxos, políticas, padrões, procedimentos, documentações), os pontos de contato para necessidades administrativas e logísticas e o plano de comunicação da auditoria.

O planejamento da auditoria é finalizado com a definição dos **procedimentos**, que envolvem a identificação da documentação (políticas, padrões e guias), dos requisitos de conformidade regulatória, da lista de indivíduos para as entrevistas e dos métodos e ferramentas para a avaliação. Além disso, há o desenvolvimento de ferramentas e metodologia para testar e verificar controles. As ferramentas da auditoria podem ser tão simples quanto questionários ou tão complexas quanto scripts que buscam informações em sistemas e devem incluir os critérios para as avaliações. O planejamento inclui também a metodologia para avaliar a acurácia dos testes e resultados.

■ TRABALHO EM CAMPO

Após o planejamento da auditoria, a execução dos passos definidos com o uso dos recursos é feita na fase de trabalho em campo. Esta fase inclui **obtenção dos dados, testes dos controles, realização das descobertas e validações** e a **documentação dos resultados**.

■ RELATÓRIOS

A fase de relatórios representa a entrega da auditoria, com a elaboração, revisão, entrega e acompanhamento dos resultados.

Um exemplo de auditoria tem os seguintes passos (ISACA, 2016):

- Revisão de documentação.
- Entrevista com indivíduos-chave.
- Estabelecimento de critérios de auditoria.
- Condução de visitas ao data center.
- Condução de revisão de áreas de alto risco.
- Documentação dos resultados.
- Preparação do relatório e revisão pelos atores.
- Entrega do relatório final.

É importante que informações técnicas e operacionais sejam identificadas, utilizadas e façam parte da auditoria. Por exemplo: se o escopo da auditoria inclui uma nova tecnologia de autenticação, o auditor deve entendê-la para identificar os riscos, os controles internos e os procedimentos de testes.

0

Ver anotações

TÉCNICAS DE AUDITORIA DE TI

Alguns métodos para avaliar controles são (ISACA, 2016):

- *Software* de auditoria para analisar o conteúdo de arquivos de dados, como os logs de sistemas e a lista de acesso de usuários.
- *Software* especializado para avaliar conteúdo de sistemas operacionais, banco de dados e arquivos de parâmetros de aplicações.
- Técnicas de desenho de fluxos para documentar processos de negócios e controles automatizados.
- *Logs* de auditorias e relatórios para avaliar parâmetros.
- Revisão de documentação.
- Perguntas e observação.
- Simulações passo a passo.
- Execução de controles.

EXEMPLIFICANDO

Exemplos de ferramentas de auditoria são: questionários, *scripts*, banco de dados relacionais, planilhas eletrônicas, ferramentas de auditoria específicas (*Computer-Assisted Audit Tools*, CAATs) e metodologias para coleta de transações (ISACA, 2016).

SAIBA MAIS

Os riscos e os controles devem ser identificados e documentados pelo auditor. A avaliação de riscos é necessária para a auditoria e determina prioridades para a alocação de recursos da auditoria. Algumas informações a serem consideradas:

- Propósito de negócio da auditoria.
- Ambiente em que a empresa opera.
- Resultados de auditorias anteriores.
- Regulações e legislação para conformidade.
- Riscos tecnológicos específicos.

O escopo da auditoria e a estratégia de execução são resultado da avaliação dos objetivos da auditoria, dos riscos identificados e dos controles existentes.

PESQUISE MAIS

O livro de Beneton (2017) *Auditoria e controle de acesso* é uma importante referência sobre auditoria e o capítulo 1 traz conteúdo sobre a auditoria, certificações profissionais de auditores, requisitos e critérios de avaliação, além de frameworks e processos de auditoria NBR ISO 19001 e ABNT NBR ISO/IEC 27007.

BENETON, E. Auditoria e controle de acesso. São Paulo: Editora Senac, 2017.

Chegamos, assim, ao final do entendimento sobre os principais conceitos, necessidades e atividades envolvidos com o processo de auditoria de sistemas e de segurança. O conhecimento amplo e detalhado que o auditor tem sobre a segurança e privacidade é fator crítico para uma auditoria, que exige o uso de diferentes técnicas e ferramentas para a análise dos controles. Avançaremos sobre estes pontos nas próximas aulas. Até lá!

FAÇA VALER A PENA**Questão 1**

A auditoria de sistemas e de segurança é um processo importante para as empresas. Considere as seguintes afirmativas.

- I. Valida atividades, processos e sistemas.
- II. Avalia a eficiência e eficácia dos controles.
- III. Atesta a conformidade administrativa, regulatória e legal.
- IV. Assegura a estabilidade organizacional para a alta gestão e os diferentes atores.

Sobre os objetivos da auditoria, é correto o que se afirma em:

a. II, apenas.

b. II e III, apenas.

c. II, III e IV, apenas.

d. I, II e III, apenas.

e. I, II, III e IV.

Questão 2

Em segurança da informação, um risco é a probabilidade de um agente de ameaça explorar vulnerabilidade de um ativo, fazendo com que uma ameaça se torne um incidente de segurança, o que leva a impactos para a empresa. É entendendo o que é e quais são os riscos que existem na empresa que os controles podem ser definidos e implantados.

Assim, a gestão de riscos é importante para identificar, analisar e avaliar os riscos, que direcionarão a definição dos controles para o tratamento dos riscos. Com a auditoria, a empresa assegura que os controles protegem a empresa de uma forma adequada.

Assinale a alternativa que apresenta qual é a relação entre os riscos de segurança da informação e a auditoria de sistemas e de segurança.

a. Auditoria é feita para validar somente os riscos.

b. Auditoria é feita para implantar os controles.

c. Auditoria é feita para validar os riscos e os controles.

d. Riscos indicam a necessidade de auditoria.

e. Se riscos são avaliados, auditoria não é necessária.

Questão 3

As principais fases de uma auditoria são o planejamento, o trabalho em campo e os relatórios. Considere as atividades listadas a seguir:

I. Define o objetivo da auditoria.

II. Determina os procedimentos.

III. Testa controles.

IV. Realiza descoberta e validação.

V. Documenta resultados.

VI. Elabora relatórios.

Sobre as atividades que fazem parte da fase de trabalho em campo, é correto o que se afirma em:

a. I e II, apenas.

b. III, IV e V, apenas.

c. I, II e V, apenas.

d. I, II, V e VI, apenas.

e. I, II, III, IV, V e VI.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27002:2013** Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2013.

AXELOS. **Building IT and Digital Excellence with ITIL 4**. Disponível em: <https://bit.ly/31ub9PU>. Acesso em: 10 jan. 2021.

BENETON, E. **Auditória e controle de acesso**. São Paulo: Editora Senac, 2017. Disponível em: <https://bit.ly/3rBgWxy>. Acesso em: 13 jan. 2021.

ISACA, Information Systems Audit and Control Association. **COBIT 2019 Framework**. Introduction and Methodology. 2018. Disponível em: <https://bit.ly/31uXeJr>. 2018. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. **COBIT 2019 Framework**. Governance and Management Objectives. 2018 Disponível em: <https://bit.ly/3dnOWbw>. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. **Information Systems Auditing: Tools and Techniques Creating Audit Programs**. 2016. Disponível em: <https://bit.ly/3rx5Cm1>. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. **Auditing Cyber Security: Evaluating Risk and Auditing Controls.** 2017. Disponível em: <https://bit.ly/3sVDgUI>. Acesso em: 9 jan. 2021.

ISACA, Information Systems Audit and Control Association. **IT Audit Framework (ITAF™).** A Professional Practices Framework IT Audit. 4th Edition. Disponível em: <https://bit.ly/2Poo17z>. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. Protiviti. **IT Audit's Perspectives on the Top Technology Risks for 2021.** 2020. Disponível em: <https://bit.ly/3u8Ag6Y>. Acesso em: 4 jan. 2021.

ITIL Process Map & ITIL Wiki. **ITIL 4.** 3 dez. 2019 Disponível em: <https://bit.ly/39poSvt>. Acesso em: 10 jan. 2021.

ITIL Process Map & ITIL Wiki. **IT Service Continuity Management.** 24 jul. 2020. Disponível em: <https://bit.ly/3sBsSkp>. Acesso em: 10 jan. 2021

NAKAMURA, E. T. **Segurança da informação e de redes.** Londrina: Editora e Distribuidora Educacional S.A., 2016.

NATIONAL Institute of Standards and Technology, NIST. **Framework for Improving Critical Infrastructure Cybersecurity.** Version 1.1, 16 abr. 2018. Disponível em: <https://bit.ly/3wm4xBa>. Acesso em: 24 out. 2020.

NATIONAL Institute of Standards and Technology, NIST. Security and Privacy Controls for Information Systems and Organizations. **NIST Special Publication 800-53 Revision 5,** set. 2020. Disponível em: <https://bit.ly/39uqMLr>. Acesso em: 9 jan. 2021.

FOCO NO MERCADO DE TRABALHO

FUNDAMENTOS DE AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

Ver anotações

FASES DO PROCESSO DE AUDITORIA

As principais fases do processo de auditoria são o planejamento, trabalho em campo e relatórios.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você trabalha para um provedor de nuvem em franca expansão, que tem demandas diretas de seus clientes. Eles exigem cada vez mais segurança e precisam estar em conformidade legal e regulatória, o que significa que só se tornarão clientes caso o próprio provedor esteja em conformidade com as melhores práticas de segurança e tecnologia da informação. O planejamento, assim, precisa incluir um elemento que aumente a confiança dos potenciais clientes, os quais precisam de um provedor seguro para operar seus sistemas e dados.

O planejamento segue os itens gerais:

- **Como é a segurança do provedor de nuvem, em linhas gerais:** a segurança segue os processos essenciais de identificação, proteção, detecção, resposta e recuperação. São processos importantes para que a confidencialidade, integridade e disponibilidade dos dados e informações dos clientes sejam maximizados. A segurança é feita com base nos riscos, que é a probabilidade de um agente de ameaça explorar vulnerabilidades de um ativo, fazendo com que uma ameaça se torne um incidente de segurança, o que resulta em impactos para a empresa. Os controles de segurança são identificados e implantados com base nos riscos avaliados, com este tratamento dos riscos envolvendo ainda os riscos aceitos.
- **Por que a segurança é importante, focando nos clientes:** os clientes demandam a segurança porque precisam proteger seus negócios, e o provedor de nuvem operará seus sistemas e dados. Além disso, há a necessidade de conformidade legal e regulatória, exigida para todo o setor.
- **Demandas dos clientes para a conformidade:** a conformidade é baseada em regulamentos e leis, como a do setor financeiro, que exige proteção dos ativos tecnológicos, e a do setor de saúde, que exige a segurança e privacidade dos dados dos pacientes, por exemplo. O conjunto de controles deve ser verificado sob a óptica destas necessidades legais e regulatórias e atestado pelo auditor

- **Auditoria de segurança, por que fazer:** os controles de segurança implantados podem não ser eficientes e eficazes, o que compromete a segurança do provedor de nuvem e de todos os seus clientes. Além disso, riscos não identificados podem não estar sendo tratados. A auditoria é necessária para validar atividades, processos e sistemas; avaliar a eficiência e eficácia dos controles; atestar a conformidade administrativa, regulatória e legal; e assegurar para a alta gestão e diferentes atores a estabilidade organizacional.
- **Principais fases da auditoria:** (1) planejamento, que envolve principalmente a definição do escopo e das técnicas e ferramentas a serem utilizadas na auditoria; (2) trabalho em campo, em que dados são adquiridos e controles são testados e verificados; (3) relatórios, em que os resultados da auditoria são organizados e apresentados.
- **Conclusão:** o provedor de nuvem é seguro com a gestão de riscos e a gestão de segurança da informação, com um processo de melhoria contínua que culmina com a assertividade cada vez maior da visão de riscos e dos controles implantados. As validações dos controles, tanto do ponto de vista da existência de acordo com as necessidades e do ponto de vista da eficiência e eficácia, precisam ser feitas por uma auditoria. Os resultados da auditoria elevam a confiança dos potenciais clientes, já que são realizadas de uma forma independente e formal, com uso de técnicas e ferramentas específicas. Com a auditoria, assim, pode ser confirmada para a alta gestão da empresa que o negócio está funcionando bem e está preparado para enfrentar os potenciais desafios. E, principalmente, ela visa assegurar aos diferentes atores envolvidos, principalmente clientes, sobre a estabilidade financeira, operacional e ética da organização.

CONTRATANDO UM PROVEDOR DE NUVEM DEPOIS DE UMA AUDITORIA

Você é o dono de uma fábrica de peças que está sendo automatizada e que se conecta diretamente com sistemas de fornecedores e clientes.

Você está procurando um provedor de nuvem e busca um alto nível de segurança. Para validar o provedor de nuvem, você irá conduzir uma auditoria em busca de uma inspeção e verificação formal para checar se um padrão ou conjunto de guias está sendo seguido, se os registros estão corretos e se os objetivos de eficiência e eficácia estão sendo alcançados.

Quais são as atividades que você pode seguir para fazer esta auditoria, com escopo nos controles físicos, relacionados à proteção do ambiente quanto a desastres naturais, controle de acesso e riscos de incêndio e enchentes?

RESOLUÇÃO



Uma auditoria tem como fases gerais o planejamento, o trabalho em campo e os relatórios. Para esta auditoria, serão feitas as seguintes atividades:

- Revisão de documentação.
- Entrevista com indivíduos-chave.
- Estabelecimento de critérios de auditoria.
- Condução de visitas ao data center.
- Condução de revisão de áreas de alto risco.
- Documentação dos resultados.
- Preparação do relatório e revisão pelos atores.
- Entrega do relatório final.

NÃO PODE FALTAR

CONTROLES GERAIS DE AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

Ver anotações

QUAIS SÃO OS TIPOS DE CONTROLES DE SEGURANÇA E PRIVACIDADE?

Os controles podem ser físicos (como monitoramento de circuito fechado de TV), tecnológicos (como *firewall*, VPN) ou processuais (como atualização periódica de sistema operacional).



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Olá, aluno. Você sabia que existem diversos tipos de controles? Há os controles lógicos, técnicos ou tecnológicos, que são aqueles corriqueiros de TI. Há os controles processuais, administrativos ou operacionais, que são aqueles que estabelecem pontos de controle a serem executados pelos envolvidos. E há os controles físicos, que são aqueles mais palpáveis, visíveis, como o controle de acesso físico a uma área segura.

E os controles têm objetivos diversos, como para o processo de aquisição, desenvolvimento e manutenção de sistemas, ou para o controle de acesso lógico e físico. Há controles voltados para a segurança e privacidade, como os definidos na norma ABNT NBR ISO/IEC 27002. E há controles voltados para outras finalidades, como para a governança de TI (COBIT) ou para o gerenciamento de serviços (ITIL). O importante é que eles têm relação com a segurança e privacidade, como a continuidade de serviços do ITIL, que é importante para a proteção da disponibilidade da informação.

O auditor precisa conhecer as normas, padrões, *frameworks*, regulações e leis que exigem a implantação de controles, assim como conhecer esses últimos. A auditoria visa garantir que os controles sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz. Assim, a auditoria de sistemas é essencial para a efetiva proteção da empresa, ao analisar a eficiência e eficácia dos controles definidos e implementados.

A definição dos controles a serem implantados é feita a partir de uma visão de riscos, que prioriza as necessidades dos controles de acordo com o cálculo da probabilidade e do impacto, no caso da segurança da informação, de um agente de ameaça explorar vulnerabilidades de um ativo, fazendo com que uma ameaça se torne um incidente de segurança.

Você trabalha para um provedor de nuvem que está crescendo de uma forma muito rápida e tem recebido como clientes muitas empresas tradicionais, principalmente pelo processo de transformação digital.

Como sua empresa tem clientes de diferentes setores, como financeiro, saúde e governo, há uma exigência para que os serviços sejam seguros e que estejam em conformidade com regulamentos e leis específicas.

Você já montou um planejamento para melhorar a segurança da empresa e para fortalecer a imagem do provedor de nuvem perante o mercado quanto ao tratamento das necessidades de segurança e conformidade. Agora, você deve partir para o detalhamento do planejamento, com foco nos controles. Justifique cada ponto de seu material sobre os controles, já ele será distribuído para a diretoria executiva para aprovação.

Uma sugestão de itens do material que você irá desenvolver sobre controles que não podem faltar são:

- Tipos de controles considerados e para que servem.
- Como os controles são definidos.
- Normas ou *frameworks* que podem ser a base para a definição dos controles.
- Controles para aquisição, desenvolvimento e manutenção de sistemas.
- Controle de acesso.
- Auditoria.

O auditor precisa ter conhecimentos e competências para avaliar os controles quanto à eficiência e eficácia. Isto faz com que os controles discutidos nesta aula sejam importantes para a construção deste conhecimento e desta competência. Além disso, normas e frameworks como a ISO 27001, de Sistema de Gestão de Segurança da Informação (SGSI), COBIT e ITIL são frequentemente utilizados nas auditorias.

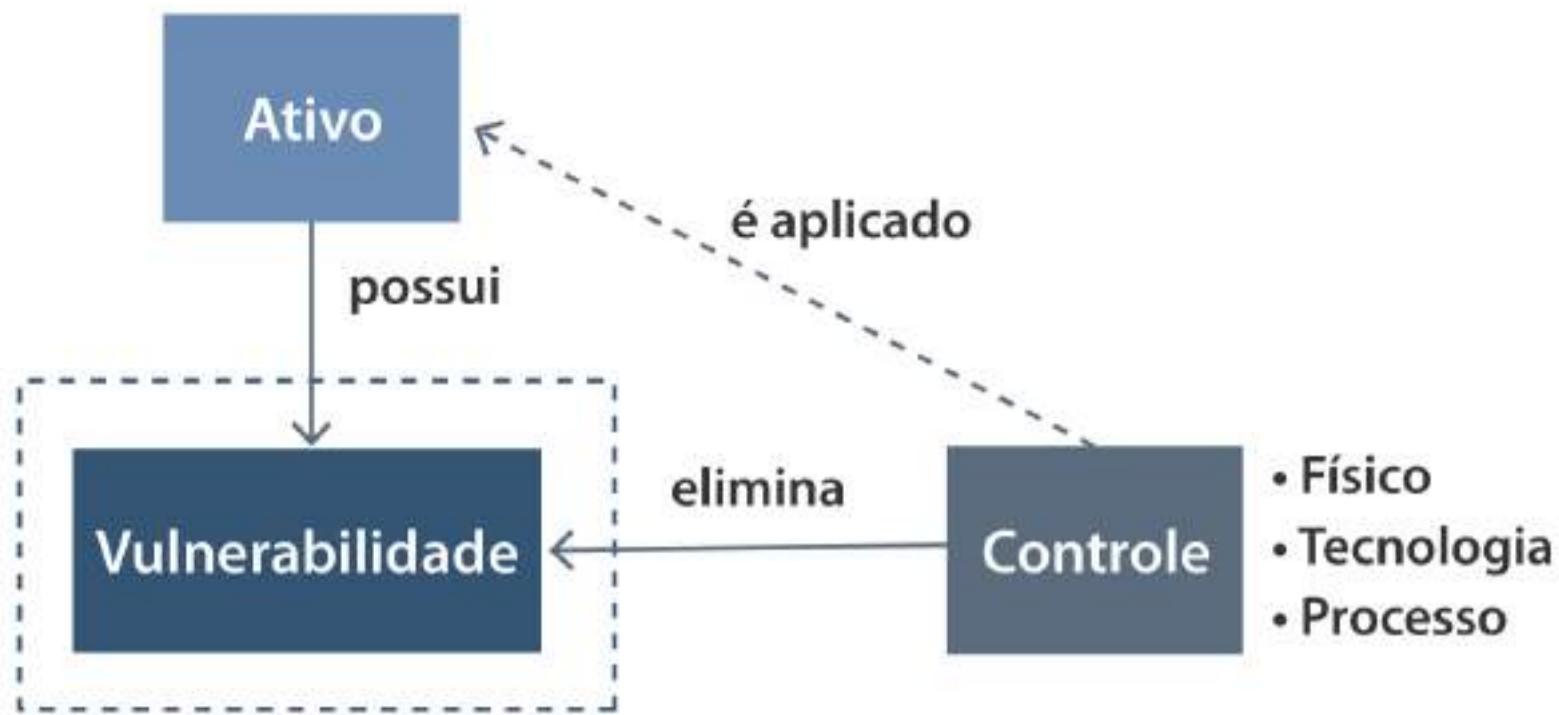
CONCEITO-CHAVE

As empresas evoluem o tempo todo e o papel da segurança e privacidade aumenta cada vez mais com a transformação digital, que traz o uso mais intenso das tecnologias e sistemas de informação. A gestão de riscos é essencial para as empresas ao trazer uma visão de oportunidades e ameaças para o cumprimento da missão, além de possibilitar a priorização de ações e investimentos. Ela também direciona a definição dos controles da empresa, incluindo os de segurança e privacidade. Do ponto de vista de segurança e privacidade, a proteção da empresa contra os riscos identificados na avaliação de riscos é feita após a implementação dos controles definidos. A auditoria de sistemas visa garantir que os controles sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz. Assim, a auditoria de sistemas é essencial para a efetiva proteção da empresa, ao analisar a eficiência e eficácia dos controles definidos e implementados. O foco desta seção está nos controles, que podem ser de diferentes tipos, com variadas finalidades.

CONTROLES DE SEGURANÇA E PRIVACIDADE

No contexto de segurança e privacidade, controles podem ser físicos (como monitoramento de acesso a data center), tecnológicos (como *firewall*) ou processuais (como a atualização das regras do *firewall*) e são aplicados nos ativos para que as vulnerabilidades sejam tratadas. A Figura 4.5 mostra a relação entre estes elementos.

Figura 4.5 | Controles são aplicados nos ativos para tratar as vulnerabilidades



Fonte: elaborada pelo autor.

Os controles de segurança são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança. Os controles de privacidade são salvaguardas administrativas, técnicas e físicas aplicadas em sistemas e organizações para gerenciar riscos de privacidade e para assegurar conformidade com requisitos de privacidade aplicáveis. Os requisitos de segurança e privacidade direcionam a seleção e implementação de controles de segurança e privacidade e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades de missão para assegurar a confidencialidade, integridade e disponibilidade das informações processadas, armazenadas e transmitidas, e também para gerenciar riscos (NIST, 2020).

O NIST *Cybersecurity Framework* (NIST, 2018) define as cinco funções da segurança: identificação, proteção, detecção, resposta e recuperação (Figura 4.6).

Figura 4.6 | NIST *Cybersecurity Framework*



Fonte: adaptada de NIST (2018).

As funções de segurança podem ser executadas com um conjunto de controles que estão divididos em 23 categorias e 108 controles. As categorias dos controles podem ser vistas na Figura 4.7, separadas para cada uma das funções de segurança.

Figura 4.7 | Categorias ou objetivos de controle do NIST *Cybersecurity Framework*

Identificação

- Gestão de ativos
- Ambiente de negócio
- Governança
- Avaliação de riscos
- Estratégia de gestão de riscos
- Gestão de riscos de cadeia de fornecedor

Proteção

- Gestão de identidades e controle de acesso
- Conscientização e treinamento
- Segurança de dados
- Processos e procedimentos de proteção de informação
- Manutenção
- Tecnologia de proteção

Detecção

- Anomalias e eventos
- Monitoramento contínuo de segurança
- Processos de detecção

Resposta

- Planejamento de resposta
- Comunicação
- Análise
- Mitigação
- Melhorias

Recuperação

- Planejamento de recuperação
- Melhorias
- Comunicação

Fonte: adaptada de NIST (2018).

O NIST 800-53 provê um catálogo de controles de segurança e privacidade para sistemas de informação e organizações para proteger as operações e ativos, indivíduos, outras organizações e o país de um conjunto de ameaças e riscos, que incluem ataques hostis, erros humanos, desastres naturais, falhas estruturais, entidades de inteligência estrangeiras e riscos. Os controles são flexíveis e customizáveis e implementados como parte do processo de gestão de

riscos, além de derivados de necessidades de missão e negócios, leis, ordens executivas, diretrizes, regulações, políticas, padrões e guias (NIST, 2020).

CONTROLES ORGANIZACIONAIS E RELAÇÃO COM SEGURANÇA E CONTINUIDADE DO SERVIÇO

A segurança e privacidade fazem parte do contexto das empresas e estão integradas com outros assuntos, como a governança de TI. A governança de TI visa a transformação digital e a relação com a entrega de valor, a mitigação dos riscos de negócios e a otimização de recursos.

A governança tem como principais objetivos (COBIT, 2018):

- Avaliação de necessidades, condições e opções de todos os atores envolvidos, em busca de determinar objetivos corporativos平衡ados.
- Direcionamento para a priorização e tomada de decisão.
- Monitoramento do desempenho e conformidade de acordo com os direcionamentos e objetivos definidos.

REFLITA

Para que a segurança seja efetiva, é importante que os processos estejam bem definidos e a equipe tenha as competências para as ações necessárias. A governança garante que as ações do cotidiano sejam tratadas para que as ameaças correntes e emergentes sejam sempre tratadas e alinhadas com a alta gestão (ISACA, 2017).

COBIT

O COBIT, de *Control Objectives for Information and Related Technology*, é um *framework* de governança de TI que trata de uma visão organizacional, a qual tem relação com a segurança e privacidade. O COBIT define os componentes para construir e sustentar um sistema de

governança, composto por processos, estrutura organizacional, políticas, procedimentos, fluxos de informação, cultura, comportamentos, qualificações e infraestrutura.

Há cinco domínios no COBIT, um para a governança e quatro para o gerenciamento (COBIT, 2018), sendo composto por um total de 40 processos, que podem ser entendidos como controles organizacionais. Os exemplos citados dos 40 processos organizacionais são referentes aos controles de segurança:

- **Avaliar, direcionar e monitorar ou *Evaluate, Direct and Monitor (EDM)*:** é o objetivo da governança e avalia opções estratégicas, direciona a gestão e monitora a execução da estratégia. Exemplos de processos são garantir a definição e manutenção do *framework* de governança (EDM01) e garantir a otimização do risco (EDM04).
- **Alinhar, planejar e organizar ou *Align, Plan and Organize (APO)*:** é o objetivo do gerenciamento e trata de toda a organização, da estratégia e das atividades de suporte para TI. Exemplos de processos são gerenciar a arquitetura corporativa (APO03), gerenciar riscos (APO12) e gerenciar segurança (APO13).
- **Construir, adquirir e implementar ou *Build, Acquire and Implement (BAI)*:** é o objetivo do gerenciamento e trata da definição, aquisição e implementação de soluções de TI e sua integração nos processos de negócios. Exemplos de processos são gerenciar disponibilidade e capacidade (BAI04), gerenciar mudanças de TI (BAI06), gerenciar ativos (BAI09) e gerenciar configuração (BAI10).
- **Entregar serviço e suporte ou *Deliver, Service and Support (DSS)*:** é o objetivo do gerenciamento e trata da entrega operacional e suporte de serviços de TI, incluindo a segurança. Exemplos de processo são gerenciar operações (DSS01), gerenciar requisição de serviços e incidentes (DSS02), gerenciar continuidade (DSS04) e gerenciar serviços de segurança (DSS05).

- **Monitorar, verificar e avaliar ou Monitor, Evaluate and Assess**

(MEA): é o objetivo do gerenciamento e trata do monitoramento do desempenho e a conformidade de TI com os objetivos internos de desempenho, objetivos de controles internos e requisitos externos.

Exemplos de processos são gerenciar monitoramento de desempenho e conformidade (MEA01), gerenciar sistema de controle interno (MEA02) e gerenciar garantia (*assurance*) (MEA04).

Dentre os 40 processos ou objetivos de controle organizacionais definidos no COBIT, estão alguns voltados diretamente para a segurança, que foram destacados nos exemplos acima. Por exemplo, o processo de gerenciar segurança (APO13) está no domínio de alinhar, planejar e organizar (APO) e a condução de auditorias do sistema de gestão da segurança da informação em intervalos definidos é uma das atividades que devem ser feitas (COBIT, 2018).

Além dos controles relacionados com a visão de governança provida pelo COBIT, há a visão relacionada ao gerenciamento de serviços, provido pelo *Information Technology Infrastructure Library* (ITIL). Ambos podem ser utilizados nos processos de auditoria para medir o nível de conformidade das empresas.

ATENÇÃO

A versão atual do COBIT é a 2019, que foi projetada para a criação de estratégias de governança mais flexíveis, colaborativas e voltadas para tecnologias recentes, considerando a TI como negócio da organização e contando com atualizações mais frequentes e fluidas.

ITIL

O ITIL é um *framework* de melhores práticas que visa auxiliar as empresas a entregar e suportar serviços de TI, provendo uma estrutura alinhada com a visão, missão, estratégia e objetivos da organização. Há um sistema de valor dos serviços, composto por (AXELOS, 2018):

- Cadeia de valor de serviços.
- Princípios.
- Governança.
- Melhoria contínua.
- 34 práticas de gerenciamento.

Dentre os benefícios do ITIL para as empresas, estão (AXELOS, 2018):

- Padronização do modelo de operação de TI.
- Cumprimento dos requisitos de clientes e funcionários.
- Maior agilidade e capacidade para inovação.
- Entregas em ambientes em constante mudança.
- Maior controle e governança.
- Demonstração do valor de TI.
- Oportunidade para melhorias.

As 34 práticas do ITIL envolvem guias que são agrupadas em três categorias e estão indicadas no Quadro 4.1 (ITIL, 2019):

- Práticas de gerenciamento geral.
- Práticas de gerenciamento de serviço.
- Práticas de gerenciamento técnico.

Quadro 4.1 | As 34 práticas do ITIL

Práticas de gerenciamento geral		
Gerenciamento de estratégia	Gerenciamento de portfólio	Gerenciamento de arquitetura
Gerenciamento financeiro de serviços	Gerenciamento de força de trabalho e talento	Melhoria contínua

Mensuração e reporte	Gerenciamento de riscos	Gerenciamento de segurança da informação
Gerenciamento de conhecimento	Gerenciamento de mudança organizacional	Gerenciamento de projetos
Gerenciamento de relacionamentos	Gerenciamento de fornecedores	
Práticas de gerenciamento de serviço		
Análise de negócio	Gerenciamento de catálogos de serviços	<i>Design</i> de serviço
Gerenciamento de nível de serviços	Gerenciamento de disponibilidade	Gerenciamento de capacidade e desempenho
Gerenciamento de continuidade de serviços	Gerenciamento de monitoramento e eventos	<i>Service desk</i>
Gerenciamento de incidentes	Gerenciamento de requisição de serviços	Gerenciamento de problemas
Gerenciamento de lançamento	Habilitação de mudanças	Validação e teste de serviços
Gerenciamento de configuração de serviços	Gerenciamento de ativos de TI	
Práticas de gerenciamento técnico		

Gerenciamento de implantação	Gerenciamento de infraestrutura e plataforma	Gerenciamento e desenvolvimento de <i>software</i>
------------------------------	--	--

Fonte: adaptado de ITIL (2019).

O gerenciamento de continuidade de serviços é uma das 34 práticas do ITIL e tem como objetivo gerenciar riscos que podem causar sérios impactos aos serviços de TI. O processo do ITIL assegura que o provedor de serviço de TI possa prover sempre um nível de serviço mínimo, reduzindo os riscos de desastres para um nível aceitável e planejando a recuperação dos serviços de TI (ITIL, 2020). Os subprocessos do gerenciamento de continuidade de serviço são (ITIL, 2020):

- **Suporte:** assegurar que todos os membros com responsabilidades em combater os desastres tenham conhecimento sobre suas obrigações e garantir que toda informação relevante esteja disponível prontamente quando um desastre acontece.
- **Definir os serviços para a continuidade:** definir mecanismos e procedimentos de continuidade apropriados e com custos efetivos, de acordo com os objetivos da continuidade de negócios. Inclui a definição das medidas de redução de riscos e os planos de recuperação.
- **Treinamento e testes:** garantir que todas as medidas preventivas e os mecanismos de recuperação para casos de eventos de desastres sejam testados regularmente.
- **Revisão:** revisar as medidas de prevenção de desastres com relação ao alinhamento com as percepções de risco do ponto de vista do negócio, e verificar se as medidas e procedimentos de continuidade são mantidos e testados regularmente.

O COBIT também trata da continuidade, como o gerenciar continuidade (DSS04) no domínio de entregar serviço e suporte. Além do ITIL e do COBIT, o assunto é tratado também na norma ABNT NBR ISO/IEC 27001:2013 e 27002:2013, em um objetivo de controle específico para aspectos da segurança da informação na gestão da continuidade do negócio. O sistema de gestão de continuidade de negócios é tratado na norma ABNT NBR ISO 22301:2020, que considera a segurança e resiliência. E a norma ABNT NBR ISO/IEC 27031:2015 trata de diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação.

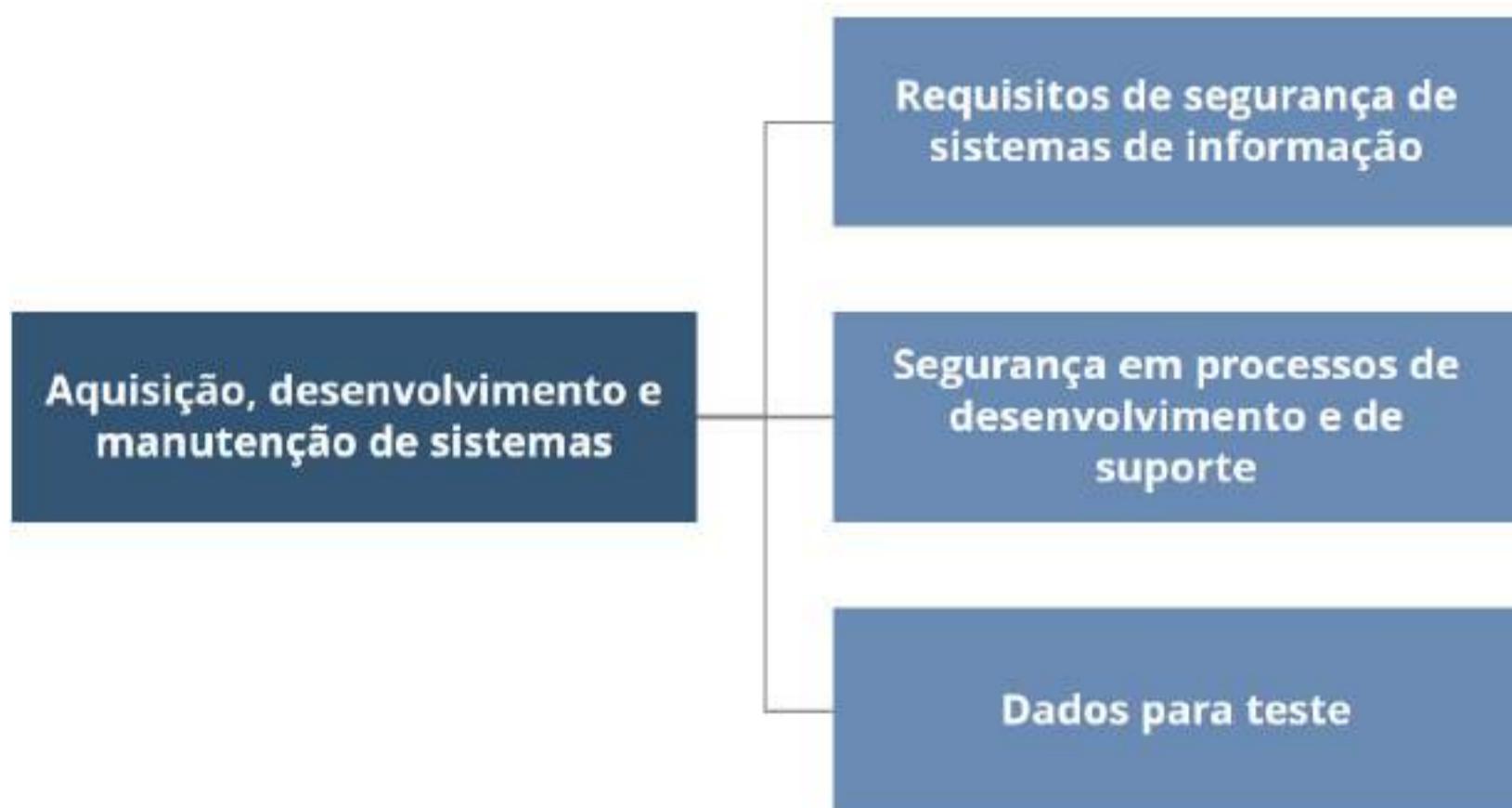
CONTROLES DE SEGURANÇA PARA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

As empresas utilizam *software* de diferentes funções e a abordagem das empresas para o uso é variada. Há empresas que fazem o desenvolvimento do *software* internamente, enquanto há outras empresas que terceirizam o desenvolvimento para uma empresa especializada. E há ainda as empresas que adquirem o *software* a ser utilizado pela empresa. E, uma vez definido o *software*, há outros elementos relevantes, como o modelo de operação do *software*, que pode ser interno, em um provedor de nuvem, ou no modelo de uso direto no fornecedor, no modelo de *Software as a Service* (SaaS). Essa variação de abordagem é cada vez mais abrangente, pois os *softwares* precisam acompanhar a evolução e transformação das empresas e são assim atualizados constantemente. A abrangência de canais atendidos pelo *software* também é importante, uma vez que podem existir para serem utilizados em dispositivos móveis, para acesso via web ou ainda por meio de aplicações instaladas ou aplicativos.

A complexidade envolvida com aquisição, desenvolvimento e manutenção de sistemas é grande e exige um conjunto de controles que precisam ser auditados. E, considerando a essência da segurança, que precisa proteger os ativos contra a exploração de vulnerabilidades que resultam em incidentes de segurança, a verificação da eficiência e eficácia dos controles de segurança e privacidade é fundamental.

A norma ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) define um conjunto de objetivos de controles de segurança e apresenta um conjunto para a aquisição, desenvolvimento e manutenção de sistemas, possuía qual tem os seguintes controles definidos: requisitos de segurança de sistemas de informação, segurança em processos de desenvolvimento e de suporte e dados para teste (Figura 4.8).

Figura 4.8 | Controles da ISO 27002 para aquisição, desenvolvimento e manutenção de sistemas



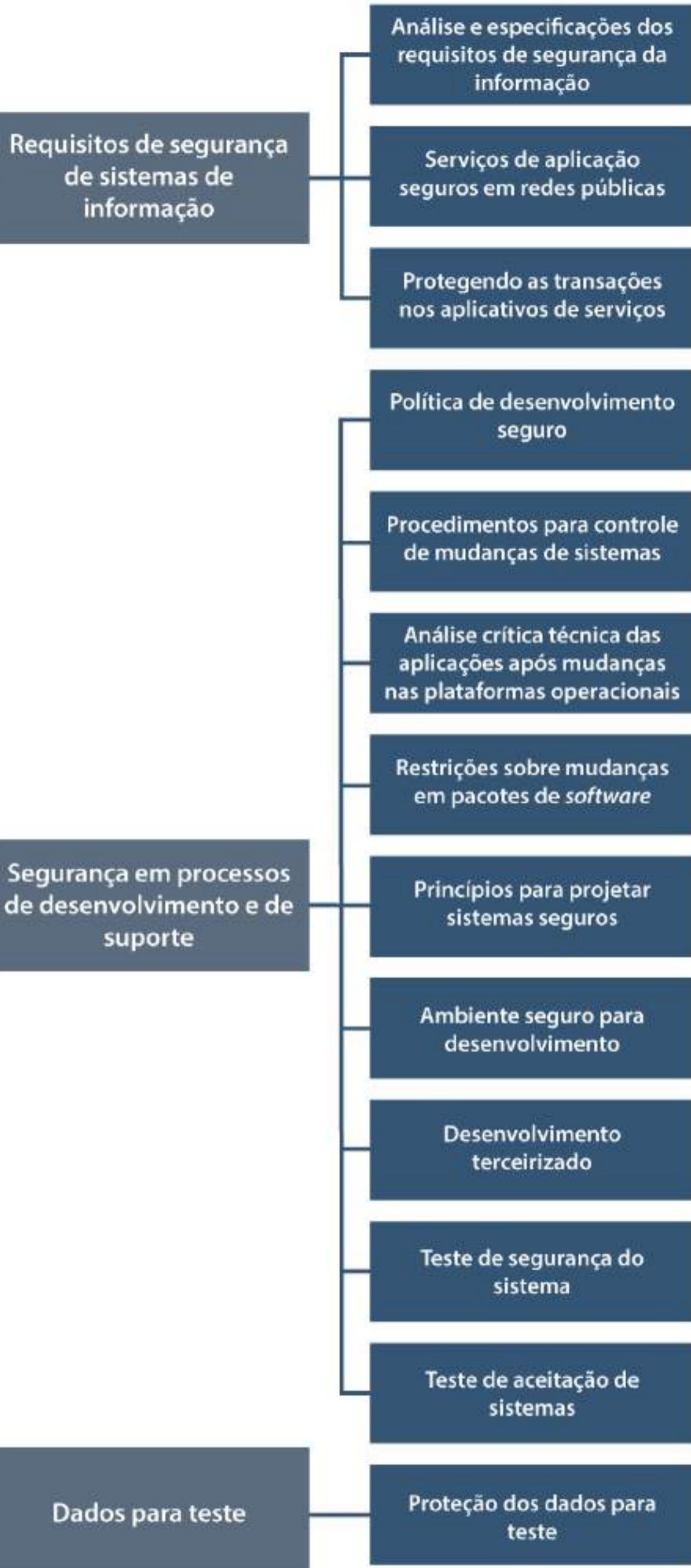
Fonte: adaptada de ISO 27002 (2013).

O objetivo de controle dos requisitos de segurança de sistemas de informação é garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas. Já o objetivo da segurança em processos de desenvolvimento e de suporte é garantir que a segurança

da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. O objetivo dos dados para teste é assegurar a proteção dos dados usados para este fim. O detalhamento destes controles pode ser visto na Figura 4.9.

Figura 4.9 | Controles para aquisição, desenvolvimento e manutenção de sistemas

Aquisição, desenvolvimento e manutenção de sistemas



Fonte: adaptada de ISO 27002 (2013).

Além da ABNT NBR ISO/IEC 27002, o ITIL também define algumas práticas que tratam do desenvolvimento de sistemas (AXELOS, 2018), com os seguintes processos:

- Arquitetura da solução.
- *Design* da solução.
- Teste do *software*.
- Gerenciamento do código.
- Criação do pacote.
- Controle de versão

COBIT também possui um processo específico para construir, adquirir e implementar, ou *Build, Acquire and Implement* (BAI), que tem como objetivo o gerenciamento, tratando da definição, aquisição e implementação de soluções de TI e sua integração nos processos de negócios. Este processo trata do gerenciamento de programas, definição de requisitos, identificação e construção de soluções, disponibilidade e capacidade, mudança organizacional, mudanças de TI, aceitação e transição de mudança de TI, conhecimento, ativos, configuração e projetos (COBIT, 2018).

CONTROLE DE ACESSO

O NIST *Cybersecurity Framework* (NIST, 2020) tem uma família de controles de segurança para o controle de acesso. Estes controles são um dos principais alvos de avaliações em auditorias e envolvem controles relacionados à identificação, autenticação e autorização, como pode ser visto no Quadro 4.2.

Quadro 4.2 | Controles de acesso do NIST *Cybersecurity Framework*

Controle de acesso

Política e procedimentos	Gerenciamento de contas	Aplicação do acesso
Aplicação do fluxo de informação	Separação de deveres	Menor privilégio
Tentativas de acesso sem sucesso	Notificação de uso do sistema	Notificação do acesso anterior
Controle de sessões concorrentes	Bloqueio de dispositivo	Término de sessão
Ações permitidas sem identificação ou autenticação	Atributos de segurança e privacidade	Acesso remoto
Acesso sem fio	Controle de acesso para dispositivos móveis	Uso de sistemas externos
Compartilhamento de informações	Conteúdo acessível publicamente	Proteção contra mineração de dados
Decisões de controle de acesso	Monitor de referência	

Ver anotações

Fonte: adaptado de NIST (2020).

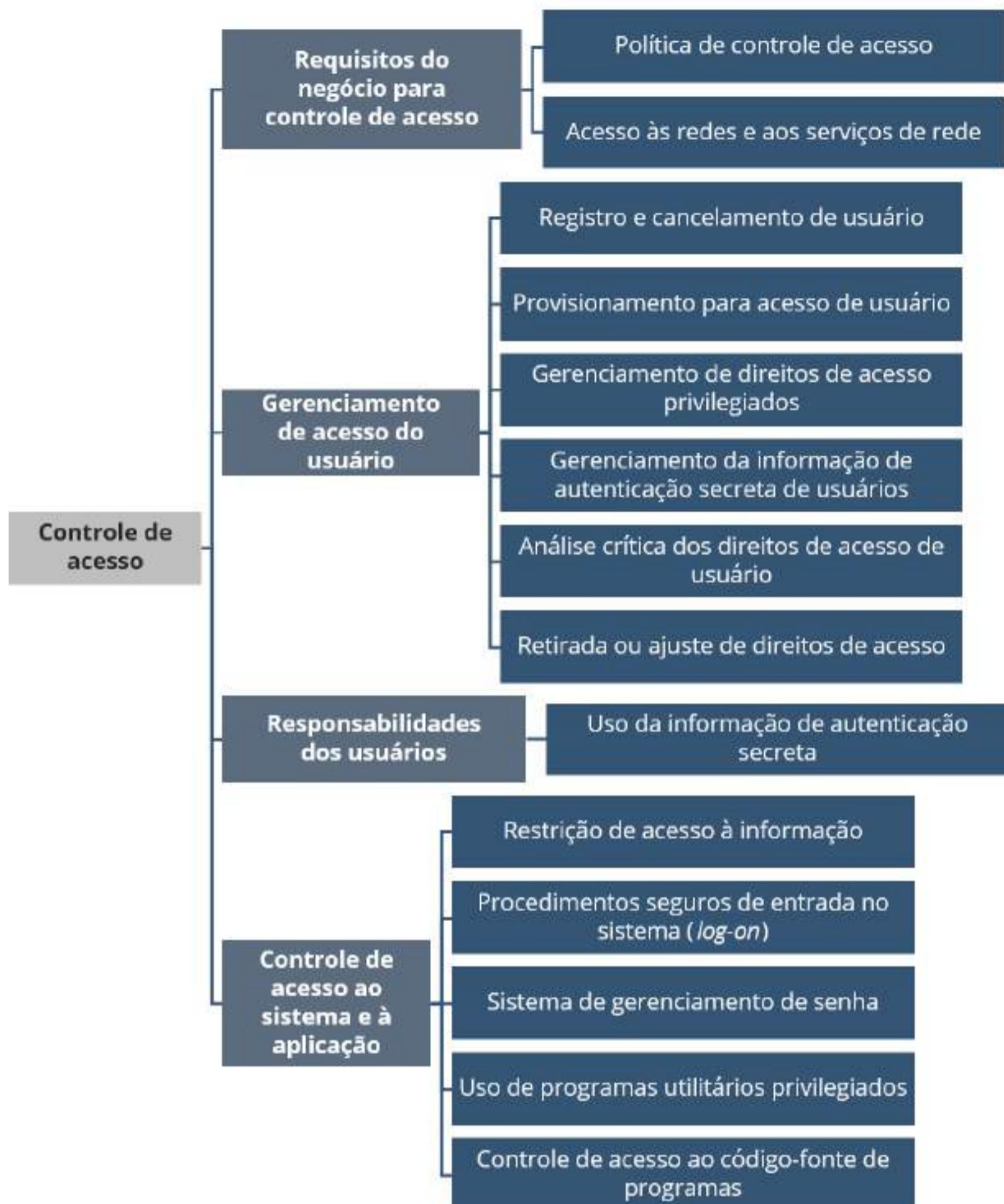
EXEMPLIFICANDO

Os controles de acesso podem ser detalhados, como os referentes ao gerenciamento de contas, que trata de (NIST, 2020): gerenciamento automatizado de contas, gerenciamento automatizado de contas temporárias e emergenciais, desabilitação de contas, ações automatizadas de auditoria, *logout* de inatividade, gerenciamento dinâmico de privilégios, contas de usuários privilegiados,

gerenciamento dinâmico de contas, restrição de uso de contas compartilhadas e de grupos, credenciais de contas compartilhadas e de grupos, condições de uso e monitoramento de contas para uso atípico.

A norma ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) também define um conjunto de objetivos de controles de segurança para o controle de acesso, composto por requisitos do negócio para controle de acesso, gerenciamento de acesso do usuário, responsabilidades dos usuários e controle de acesso ao sistema e à aplicação. O detalhamento do controle de acesso pode ser visto na Figura 4.10

Figura 4.10 | Controles da ISO 27002 para controle de acesso



Fonte: adaptada de ISO 27002 (2013).

CONTROLES LÓGICOS, FÍSICOS E PROCESSUAIS

Os controles podem ser de diferentes tipos, como foi visto nesta aula, com vários exemplos principalmente da ABNT NBR ISO/IEC 27002 (ISO 27002, 2013), COBIT (COBIT, 2018), ITIL (AXELOS, 2018) e NIST 800-53 (NIST, 2020).

Os controles de segurança envolvem investimentos em pessoas, processos e tecnologias, principalmente para o desenvolvimento de uma cultura de segurança, e podem ser administrativos, técnicos ou operacionais. Alguns exemplos são (ISACA, 2017):

- Conscientização.
- Políticas.
- Sistemas de detecção de intrusão.
- Registro de eventos (*logging*).
- Varredura de vulnerabilidades.
- Classificação da informação.
- *Hardening* de arquitetura e de tecnologia.
- *Hardening* de sistemas.

Outra classificação utilizada é os controles de segurança e privacidade serem lógicos ou tecnológicos, físicos e processuais (NAKAMURA, 2016).

REFLITA

Uma empresa pode ter implementado controles de segurança lógicos ou tecnológicos como *firewalls*, *backups* e antivírus. Porém, sem os controles baseados em processos de segurança, as regras do *firewall* podem estar erradas, o antivírus pode estar desatualizado e os *backups* podem não funcionar quando necessário. A auditoria visa avaliar os diferentes tipos de controles, incluindo os processos, para que a empresa esteja de fato segura.

Um ponto que deve ser considerado é que a informação existe em diferentes estados e em diferentes formas, como pode ser visto na Figura 4.11. Os controles lógicos são normalmente complementados com controles processuais em meios digitais. Porém, controles físicos também fazem parte da proteção da informação, como no caso de

dados em equipamentos, que podem ser acessados fisicamente e roubados. Neste caso, o controle de acesso físico é essencial. Outro conjunto de controles físicos diz respeito à proteção contra ameaças externas e do meio ambiente, como um sistema de supressão de incêndio.

o

Ver anotações

Figura 4.11 | Estados e formas da informação, que precisam ser protegidas



Fonte: elaborada pelo autor.

EXEMPLIFICANDO

Um exemplo de controle físico da ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) é para a escolha do local e proteção do equipamento. O controle diz que convém que sejam adotados controles para minimizar o risco de ameaças físicas potenciais e ambientais, tais como furto, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo.

SAIBA MAIS

Níveis de maturidade do COBIT podem ser utilizados para expressar o nível de desempenho da organização. O COBIT estabelece seis níveis de maturidade:

- **0. Incompleto:** trabalho pode ou não pode ser completo para alcançar os objetivos.
- **1. Inicial:** trabalho é completo, mas os objetivos não são alcançados.
- **2. Gerenciado:** há medidas de planejamento e desempenho, porém sem uma padronização.
- **3. Definido:** há padrão corporativo que guia toda a empresa.
- **4. Quantitativo:** a empresa é direcionada a dados, com melhoria de desempenho quantitativo.
- n: a empresa é focada em melhoria contínua.

PESQUISE MAIS

O livro *Auditória e controle de acesso*, de Beneton (2017) apresenta no capítulo 7 um conjunto de controles de acesso lógico, incluindo a forma de auditar pastas e

compartilhamentos, gerência de identidade do usuário, política de senhas e métodos de autenticação e privilégio mínimo.

BENETON, E. **Auditória e controle de acesso**. São Paulo: Editora Senac, 2017.

Chegamos assim ao final desta seção, focando nos controles que podem ter naturezas diferentes, como técnicos ou lógicos; administrativos, processuais ou operacionais; ou físicos. Os objetivos são muitos e dependem dos riscos identificados e avaliados. A verificação da eficiência e eficácia dos controles é feita pela auditoria, que tem papel importante para a segurança das empresas e para a conformidade regulatória e legal. Até a próxima seção, que destaca algumas auditorias importantes para a segurança da informação, as principais técnicas e ferramentas.

Até lá!

FAÇA VALER A PENA

Questão 1

Os controles de segurança são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança. No contexto de segurança e privacidade, controles podem ser físicos (como o controle de acesso a uma área segura), tecnológicos (como autenticação de usuários para acesso a sistemas) ou processuais (como os registros de quem acessa o datacenter).

Assinale a alternativa que contém os elementos em que são aplicados os controles de segurança e privacidade.

- a. Aplicados nos ativos para tratar as vulnerabilidades.
- b. Aplicados nas vulnerabilidades para tratar os ativos.
- c. Aplicados nas ameaças para tratar os agentes de ameaça.
- d. Aplicados nos agentes de ameaça para tratar as ameaças.
- e. Aplicados nas ameaças para tratar as vulnerabilidades.

Questão 2

Os requisitos de segurança e privacidade direcionam a seleção e implementação de controles de segurança e privacidade e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades de missão para assegurar a confidencialidade, integridade e disponibilidade das informações processadas, armazenadas, transmitidas e para gerenciar riscos.

Considere normas e *frameworks* que organizam controles, listadas a seguir.

I. ABNT NBR ISO/IEC 27002.

II. COBIT.

III. ITIL.

As três normas e *frameworks* possuem foco em quais assuntos, respectivamente?

- a. I. Governança / II. Governança / III. Auditoria.
- b. I. Auditoria / II. Governança / III. Auditoria.
- c. I. Segurança da informação / II. Governança / III. Governança.
- d. I. Segurança da informação / II. Governança / III. Gerenciamento de serviços.
- e. I. Auditoria / II. Governança / III. Gerenciamento de serviços.

Questão 3

Considere os seguintes controles: gerenciamento automatizado de contas, gerenciamento automatizado de contas temporárias e emergenciais, desabilitação de contas, ações automatizadas de auditoria, *logout* de inatividade, gerenciamento dinâmico de privilégios, contas de usuários privilegiados, gerenciamento dinâmico de contas, restrição de uso de contas compartilhadas e de grupos, credenciais de contas compartilhadas e de grupos, condições de uso e monitoramento de contas para uso atípico.

Assinale a alternativa que representa a área dos controles citados.

- a. Automatização.
- b. Gerenciamento dinâmico.
- c. Gerenciamento de contas.
- d. Monitoramento.
- e. Restrição de uso.

REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, Associação Brasileira de Normas Técnicas,

2013.

ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2013.

AXELOS. Building IT and Digital Excellence with ITIL 4. 2018.

Disponível em: <https://bit.ly/31A1tDp>. Acesso em: 10 jan. 2021.

BENETON, E. Auditoria e controle de acesso. São Paulo: Editora Senac, 2017. Disponível em: <https://bit.ly/3cFwagE>. Acesso em: 13 jan. 2021.

ISACA, Information Systems Audit and Control Association. COBIT 2019 Framework. Introduction and Methodology, 2018. Disponível em:

<https://bit.ly/31B8Jz6>. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. COBIT 2019 Framework. Governance and Management Objectives, 2018. Disponível em: <https://bit.ly/3cEPTNS>. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. Information Systems Auditing: Tools and Techniques Creating Audit Programs, 2016. Disponível em: <https://bit.ly/3rJ3KXn>. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. Auditing Cyber Security: Evaluating Risk and Auditing Controls, 2017. Disponível em: <https://bit.ly/3rJHtJ2>. Acesso em: 9 jan. 2021.

ISACA, Information Systems Audit and Control Association. IT Audit Framework (ITAF™). A Professional Practices Framework IT Audit. 4th Edition, 2020. Disponível em: <https://bit.ly/3ubsoBG>. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. IT Audit's Perspectives on the Top Technology Risks for 2021. Protiviti, 2020. Disponível em: <https://bit.ly/3m6FU73>. Acesso em: 4 jan. 2021.

ITIL Process Map & ITIL Wiki. **ITIL 4**, 3 dez. 2019. Disponível em:

<https://bit.ly/3wir3La>. Acesso em: 10 jan. 2021.

ITIL Process Map & ITIL Wiki. **IT Service Continuity Management**, 24 jul. 2020. Disponível em: <https://bit.ly/3funAmV>. Acesso em: 10 jan. 2021.

NAKAMURA, E. T. **Segurança da informação e de redes**. Londrina: Editora e Distribuidora Educacional S.A., 2016.

NATIONAL Institute of Standards and Technology, NIST. **Framework for Improving Critical Infrastructure Cybersecurity**. Version 1.1, 16 abr. 2018. Disponível em: <https://bit.ly/3rG9GjV>. Acesso em: 24 out. 2020.

NATIONAL Institute of Standards and Technology, NIST. Security and Privacy Controls for Information Systems and Organizations. **NIST Special Publication 800-53 Revision 5**, set. 2020. Disponível em: <https://bit.ly/3wfcij4>. Acesso em: 9 jan. 2021.

FOCO NO MERCADO DE TRABALHO

CONTROLES GERAIS DE AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

Ver anotações 0

O QUE O AUDITOR PRECISA SABER PARA IMPLANTAÇÃO DE CONTROLES?

O auditor precisa ter conhecimentos e competência técnica para verificar os controles. É preciso conhecer as principais normas e *frameworks* utilizados para a definição de controles.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Você já montou um planejamento para melhorar a segurança do provedor de nuvem e agora irá detalhar o planejamento, com foco nos controles. Os principais tópicos que você pode considerar na elaboração do material são:

- **Tipos de controles considerados e para que servem:** controles são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança, e também para assegurar conformidade com requisitos aplicáveis. Os controles podem ser (i) técnicos, tecnológicos ou lógicos, como o antivírus ou o *backup*; (ii) processuais, administrativos ou operacionais, como a política de segurança ou o processo de revisão de contas de usuários; (iii) físicos, como o cadeado para que o *desktop* utilizado pelo presidente da empresa não seja roubado.
- **Como os controles são definidos:** os controles são definidos pelos riscos existentes na empresa, que direcionam as necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos. Além dos riscos, a definição dos controles pode ser feita a partir de requisitos que direcionam a seleção e implementação de controles, e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa.
- **Normas ou frameworks que podem ser a base para a definição dos controles:** a ABNT NBR ISO/IEC 27002 define um conjunto de objetivos de controle de segurança da informação, e pode ser utilizada para a definição dos controles. COBIT é um *framework* para governança de TI e possui um conjunto de controles mais amplos que podem ser implantados, incluindo os de segurança e privacidade. Já o ITIL é um conjunto de melhores práticas para o

gerenciamento de serviços e estabelece também um conjunto de controles mais amplos que inclui aspectos de segurança.

- **Controles para aquisição, desenvolvimento e manutenção de sistemas:** os controles para este assunto devem incluir os requisitos de segurança de sistemas de informação, para garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. É necessário ainda que controles de segurança sejam definidos em processos de desenvolvimento e de suporte, para garantir que a segurança da informação esteja projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. Os controles de segurança devem ainda abordar os dados para teste, principalmente nos aspectos de privacidade, que devem ser reforçados devido à Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Controle de acesso:** o controle de acesso deve ser tratado pelos requisitos do negócio para controle de acesso, com a política de controle de acesso e o acesso às redes e aos serviços de rede. O gerenciamento de acesso do usuário deve incluir aspectos como o registro e cancelamento de usuário, provisionamento para acesso de usuário, gerenciamento da informação de autenticação secreta de usuários e análise crítica dos direitos de acesso de usuário. O controle para as responsabilidades dos usuários deve envolver o uso da informação de autenticação secreta. O controle de acesso ao sistema e à aplicação deve envolver a restrição de acesso à informação, procedimentos seguros de entrada no sistema (*log-on*), uso de programas utilitários privilegiados e controle de acesso ao código-fonte de programas.
- **Auditória:** a auditoria visa garantir que os controles sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz. Assim, a auditoria de sistemas é essencial para a

efetiva proteção da empresa, ao analisar a eficiência e eficácia dos controles definidos e implementados.

AVANÇANDO NA PRÁTICA

SEGURANÇA É MAIS DO QUE PROTEÇÃO

Você deve definir os controles a serem implantados em sua empresa, mas não deve se restringir à proteção. Considere os processos de segurança: identificação, proteção, detecção, resposta e recuperação. Cite alguns exemplos de controles que podem ser utilizados para cada um destes processos de segurança, que serão depois auditados.

o

Ver anotações

RESOLUÇÃO



Os controles para cada um dos processos de segurança que podem ser implantados na empresa são:

- **Identificação:** gestão de ativos, análise do ambiente de negócio, governança, avaliação de riscos, estratégia de gestão de riscos, gestão de riscos de cadeia de fornecedor.
- **Proteção:** gestão de identidades e controle de acesso, conscientização e treinamento, segurança de dados, processos e procedimentos de proteção de informação, manutenção, tecnologia de proteção.
- **Detectão:** anomalias e eventos, monitoramento contínuo de segurança, processos de detecção.
- **Resposta:** planejamento de resposta, comunicação, análise, mitigação, melhorias.
- **Recuperação:** planejamento de recuperação, melhorias, comunicação.

NÃO PODE FALTAR

TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

Ver anotações 0

QUAIS SÃO OS OBJETIVOS DAS TÉCNICAS E FERRAMENTAS EM AUDITORIA DE SISTEMAS?

Elas devem ser utilizadas para identificar, levantar evidências e para analisar e validar as evidências, além disso, elas devem auxiliar o auditor a organizar e documentar os resultados.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Olá, aluno! Nesta seção focaremos na fase de trabalho em campo, onde serão aplicadas as ferramentas para auditoria de sistemas, com base nos objetivos e escopos de auditoria.

O trabalho em campo é feito a partir do que foi planejado, com a aplicação das técnicas e ferramentas que foram definidas de acordo com os objetivos e o escopo da auditoria, além da pré-auditoria.

Utilizando as técnicas e ferramentas, o auditor poderá fazer a auditoria para verificar se o controle implantado está cumprindo o seu papel e se os controles necessários foram de fato definidos e implantados.

As técnicas e ferramentas podem ser utilizadas para a interação com as pessoas, para análises manuais ou para análises técnicas. Os principais exemplos são as entrevistas, que possibilitam obter informações com a interação com as pessoas, e as análises e revisões de documentação, políticas, procedimentos, processos e configurações, que são técnicas manuais. Outro exemplo é o uso de *softwares* especializados para gerar amostras, importar dados, summarizar e testar os controles, condições e processos implantados nos sistemas a partir de amostras, que correspondem a ferramentas para análises técnicas.

A aplicabilidade da auditoria direciona a escolha das melhores técnicas e ferramentas a serem utilizadas no trabalho em campo, e podem ser baseadas em normas, padrões e *frameworks* como COBIT, ITIL, NIST *Cybersecurity Framework*, CIS *Controls*, PCI DSS e ISO 27001. As auditorias visam a conformidade, o que resulta na segurança e na maior confiança de todos os envolvidos, de clientes a investidores, passando por parceiros, funcionários e fornecedores.

A ISO 27001 possibilita a certificação da empresa do Sistema de Gestão de Informação (SGSI), em um escopo definido de auditoria.

Para finalizarmos a seção, discutiremos alguns cases de auditoria, que reforçam a busca da conformidade e apresentam escopos que variam de acordo com os objetivos da auditoria.

Você trabalha para um provedor de nuvem que está crescendo de uma forma muito rápida e tem recebido como clientes muitas empresas tradicionais, principalmente pelo processo de transformação digital.

Como sua empresa tem clientes de diferentes setores, como financeiro, saúde e governo, há uma exigência para que os serviços sejam seguros e que estejam em conformidade com regulamentos e leis específicas.

Você já montou um planejamento para melhorar a segurança da empresa e para fortalecer a imagem do provedor de nuvem perante o mercado quanto ao tratamento das necessidades de segurança e conformidade. Você também já tem um planejamento detalhado dos controles.

Você deve agora fazer uma auditoria para validar a eficiência e eficácia dos controles. Além disso, a auditoria deve também validar se os controles necessários foram realmente definidos. Apresente as técnicas e ferramentas que você utilizará no trabalho em campo para validar se todos os controles necessários foram definidos, e se os que foram implantados são eficientes e eficazes.

O material que você irá produzir será distribuído para a diretoria executiva para aprovação.

Uma sugestão de objetivo e escopo da auditoria que você irá fazer na empresa para a definição das técnicas e ferramentas que serão utilizadas é o data center do provedor de nuvem, que possui:

- A área segura.
- Os *racks* com os servidores e os equipamentos de comunicação.
- Os administradores de sistemas.
- As máquinas virtuais.
- Sistemas operacionais disponibilizados para os clientes.
- Sistema de provisionamento de acesso aos clientes.

Você verá que a auditoria requer um profissional com várias habilidades e competências, com uma visão abrangente, para definir as técnicas e ferramentas necessárias para a auditoria e para utilizá-las no trabalho em campo. Uma empresa segura de fato precisa da auditoria, então a aplicação de todo o conhecimento é importante.

Boa aula!

o

Ver anotações

CONCEITO-CHAVE

A auditoria é uma inspeção e verificação formal para checar se um padrão ou conjunto de guias está sendo seguido, se os registros estão corretos e se os objetivos de eficiência e eficácia estão sendo alcançados (ISACA, 2016).

Uma auditoria é normalmente feita em três etapas, de planejamento, de trabalho em campo e de relatórios. Na fase de planejamento, de acordo com o objeto, os objetivos, o escopo e a pré-auditoria, os procedimentos, técnicas e ferramentas para a realização dos testes e verificações das evidências são definidos para serem aplicados na fase de trabalho em campo.

Nesta seção discutiremos os principais procedimentos, técnicas e ferramentas que podem ser utilizados em auditorias.

INTRODUÇÃO ÀS TÉCNICAS E TIPOS DE FERRAMENTAS PARA AUDITORIA DE SISTEMAS

O objetivo e o escopo da auditoria podem estar relacionados com a conformidade com normas, padrões, *frameworks*, leis e requisitos de negócios. A auditoria avalia e verifica a eficácia e eficiência dos controles implantados, que são necessários de acordo com a avaliação de riscos e das normas, padrões, *frameworks*, leis e requisitos de negócios relacionados.

EXEMPLIFICANDO

Com o modelo operacional expandindo para a distribuição dos dados e uso mais abrangente dos provedores de nuvens, os dados vão para além das fronteiras da própria empresa. Do lado das empresas, há a necessidade de que o nível de segurança e privacidade dos provedores e fornecedores seja no mínimo equivalente ao que é requerido para os negócios da empresa. Já do lado dos provedores e fornecedores, há a necessidade de demonstrar a conformidade com normas e legislações, para que as oportunidades de negócios possam ser aproveitadas.

Alguns exemplos de abordagens para as auditorias (ISACA, 2017) são:

- **Governança**, com a política de segurança da informação e os procedimentos operacionais técnicos relacionados.
- **Riscos**, com as atualizações dos registros dos riscos, e o tratamento e reporte dos riscos, envolvendo a acurácia, completude e atualizações apropriadas dos registros.
- **Gestão**, com as revisões dos incidentes de segurança, com base nos ataques, brechas e incidentes atuais.
- **Processos de gestão de riscos**, para a eficiência e efetividade.

Estas abordagens podem seguir *frameworks* de governança como o *Control Objectives for Information and Related Technologies* (COBIT), melhores práticas como o *Information Technology Infrastructure Library* (ITIL) ou o sistema de gestão de segurança da informação (ISO 27001).

REFLITA

Com o ambiente tecnológico das empresas sempre evoluindo, como o uso de provedores de nuvem ou a expansão da internet das coisas, o desafio das empresas em manter a segurança e privacidade aumenta, assim como as

auditorias. Somado a essa mudança constante do ambiente tecnológico há o ambiente regulatório e legal que também evoluí e eleva as necessidades de segurança e privacidade.

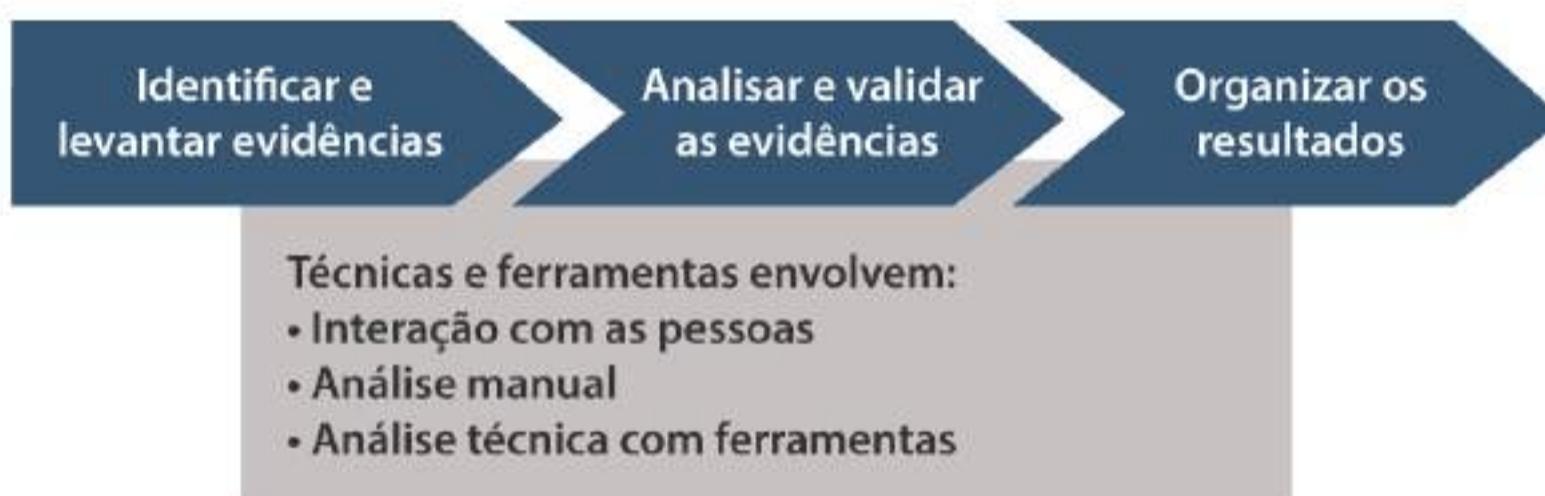
Alguns exemplos de objetivos de auditoria para a segurança e privacidade das empresas, que exigem o planejamento de procedimentos, técnicas e ferramentas específicos, são (ISACA, 2017):

- **Políticas, padrões e procedimentos de segurança adequados e efetivos:** verificar se a documentação está completa e atualizada, confirmar que há aprovação formal e divulgação, verificar se a documentação está cobrindo todos os requisitos de segurança e privacidade e verificar se os controles estão cobrindo tudo o que foi citado em políticas, padrões e procedimentos.
- **Riscos emergentes identificados, avaliados e tratados de uma forma confiável e adequada:** confirmar a confiabilidade do processo de identificação de riscos, avaliar processo, ferramentas, métodos e técnicas de avaliação de riscos utilizados, confirmar que todos os riscos foram tratados de acordo com os resultados, verificar que o tratamento dos riscos está adequado ou se há uma aceitação formal do risco.
- **Ataques e brechas são identificados e tratados no tempo e na forma apropriados:** confirmar soluções de monitoramento e reconhecimento de ataques, avaliar as interfaces para os processos e planos da gestão de incidentes de segurança e de gestão de crises, avaliar o tempo de resposta aos ataques passados.

Assim, a auditoria de controles de segurança e privacidade exige um conjunto de habilidades que envolvem aspectos especializados, tais como para os *pentests*, a análise de configurações de servidores ou *firewalls*, ou revisão de regras de ferramentas de segurança (ISACA, 2017).

As auditorias são normalmente compostas por um conjunto de metodologias, técnicas e ferramentas. Elas devem ser utilizadas para identificar, levantar evidências e para analisar e validar as evidências (Figura 4.12). Além disso, as metodologias, técnicas e ferramentas devem auxiliar o auditor a organizar e documentar os resultados. Há técnicas para interagir com as pessoas em busca das informações, que se complementam às análises manuais e às análises técnicas.

Figura 4.12 | Objetivos das técnicas e ferramentas



Fonte: elaborada pelo autor.

Dentre as técnicas e ferramentas que envolvem **interação com pessoas**, estão (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):

- **Entrevistas:** reuniões com profissionais de áreas-chave para a auditoria.
- **Questionários:** questionários a serem respondidos pelos profissionais de áreas-chave.
- **Pesquisas:** obtenção de dados via pesquisas individuais ou para grupos.
- **Perguntas e observação:** conversas e observações no contexto do cotidiano da empresa.

- **Dinâmicas em grupo:** exercícios ou atividades especializadas direcionadas a grupos.

Já a **análise manual** pode ser feita com (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):

- Análise e revisão de documentação.
- Análise de políticas, procedimentos e processos.
- Análise de configurações.
- Desenho de fluxos para documentar processos de negócios e controles automatizados.
- Simulação de mesa.
- Revisões gerenciais.
- Autoavaliação.
- Análise de código.

A **análise técnica com uso de ferramentas** é um dos principais métodos que exige um conhecimento técnico amplo dos auditores e inclui (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):

- **Planilhas eletrônicas:** organização e análise obtida de diferentes fontes.
- **Scripts:** execução automatizada para obtenção ou filtragem de dados específicos.
- **Software de auditoria** para analisar o conteúdo de arquivos de dados, como os logs de sistemas, lista de acesso de usuários.
- **Ferramentas de auditoria específicas (*Computer-Assisted Audit Tools, CAATs*):** softwares especializados para gerar amostras, importar dados, summarizar e testar os controles, condições e processos implantados nos sistemas a partir de amostras.

- **Software especializado** para avaliar conteúdo de sistemas operacionais, banco de dados e arquivos de parâmetros de aplicações.
- **Logs de auditorias e relatórios** para avaliar parâmetros.
- **Simulações passo a passo**: utiliza as informações do sistema para mapear e construir os passos a serem simulados em outra ferramenta a fim de chegar ao mesmo resultado do sistema.
- **Execução de controles**: submete parâmetros de teste com dados reais, sem impactar na rotina normal de processamento do sistema.
- **Metodologias para coleta de transações**.
- **Pentests ou testes de penetração**: identificação e análise de vulnerabilidades.

ASSIMILE

Os procedimentos, técnicas e ferramentas para auditoria são utilizados para obter dados e informações e para analisar e validar as evidências e os controles existentes. Além disso, são utilizados para organizar os resultados. O conhecimento e a competência técnica do auditor são essenciais para definir procedimentos, técnicas e ferramentas na fase de planejamento da auditoria, e para utilizá-los no trabalho em campo.

APLICABILIDADE DAS TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS

Os procedimentos, técnicas e ferramentas para auditoria de sistemas são utilizadas de acordo com o objetivo e escopo da auditoria, e são definidos no momento de planejamento.

A aplicação das técnicas e ferramentas é feita no trabalho em campo e depende da abordagem da auditoria, que pode ser baseadas em frameworks de governança como o *Control Objectives for Information*

and Related Technologies (COBIT), melhores práticas como o *Information Technology Infrastructure Library* (ITIL) ou o sistema de gestão de segurança da informação (ISO 27001).

No caso da segurança da informação, a auditoria visa assegurar que os controles protegem a empresa de uma forma adequada, com base na gestão de riscos.

EXEMPLIFICANDO

Controles de segurança são implementados para tratar vulnerabilidades. Quando as vulnerabilidades são tratadas, o risco diminui, já que a probabilidade de um agente de ameaça explorá-la diminui ou deixa de existir. Há, porém, o risco residual, que sempre deve ser considerado após a implementação dos controles de segurança. Um exemplo é o controle de segurança que atualiza o sistema com versões de *software* sem vulnerabilidades conhecidas. Porém, novas vulnerabilidades são descobertas o tempo todo e o processo de atualização pode ser definido ou executado de forma incompleta. A auditoria é importante para que a efetividade dos controles seja alcançada.

O universo a ser avaliado em uma auditoria de segurança e privacidade pode ser baseado em três linhas de defesa, que direcionam como as técnicas e ferramentas podem ser aplicadas (ISACA, 2017):

- **Gestão interna:** há o interesse em garantir que os controles de segurança e privacidade estejam presentes e operando efetivamente, com as devidas responsabilidades e cobranças. Algumas atividades são a autoavaliação de controles, testes de penetração, testes funcionais e técnicas, testes sociais e de comportamento, e revisões gerenciais.
- **Gestão de riscos:** as operações da empresa são sustentadas por controles necessários de acordo com uma visão de riscos,

envolvendo os cálculos da probabilidade e do impacto de um agente de ameaça explorar vulnerabilidades de ativos, fazendo com que uma ameaça se torne um incidente de segurança. Controles já implementados são considerados na gestão de riscos, já que diminuem os riscos existentes.

- **Auditoria interna:** para a segurança, é importante que os processos estejam bem definidos e a equipe tenha as competências para as ações necessárias. A governança garante que as ações do cotidiano sejam tratadas para que as ameaças correntes e emergentes sejam sempre tratadas e alinhadas com a alta gestão. A auditoria interna auxilia na comunicação das ações entre as diferentes áreas da empresa, e provê os testes dos controles, a conformidade, a aceitação formal dos riscos e o suporte para as investigações e análises forense.

EXEMPLIFICANDO

O padrão ANSI/TIA-942 trata de infraestrutura de telecomunicações e outros aspectos de datacenters, como a localização, estrutura física e de arquitetura, infraestrutura elétrica e mecânica, além de segurança física e contra incêndios. Os data centers podem ser certificar, de acordo com os requisitos do padrão (TIA, 2020).

CASES DE AUDITORIA EM SISTEMAS DE INFORMAÇÃO

O *Payment Card Industry Data Security Standard* (PCI DSS) é um padrão de segurança de dados da indústria de cartões de pagamento, que estabelece requisitos de segurança que devem ser cumpridos por todos os estabelecimentos e empresas que processam, transmitem ou armazenam dados de cartões de pagamento. As empresas devem cumprir os 12 requisitos de segurança definidos (Quadro 4.3), que são analisados em um processo de avaliação feito por profissionais como assessores e empresas qualificadas.

Quadro 4.3 | Os 12 requisitos de segurança do PCI DSS

Construir e manter a segurança de rede e sistemas	1. Instalar e manter uma configuração de <i>firewall</i> para proteger os dados do titular do cartão. 2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança.
Proteger os dados do titular do cartão	3. Proteger os dados armazenados do titular do cartão. 4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas.
Manter um programa de gerenciamento de vulnerabilidades	5. Proteger todos os sistemas contra <i>malware</i> e atualizar regularmente programas ou <i>software</i> antivírus. 6. Desenvolver e manter sistemas e aplicativos seguros.
Implementar medidas rigorosas de controle de acesso	7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio. 8. Identificar e autenticar o acesso aos componentes do sistema. 9. Restringir o acesso físico aos dados do titular do cartão.

Monitorar e testar as redes regularmente	10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão.
	11. Testar regularmente os sistemas e processos de segurança.
Manter uma política de segurança de informações	12. Manter uma política que aborde a segurança da informação para todas as equipes.

Fonte: adaptado de PCI (2018).

0

Ver anotações

ASSIMILE

As empresas que processam, transmitem e armazenam dados de cartões de pagamento devem estar em conformidade com a PCI DSS, cumprindo os requisitos de segurança definidos que são avaliados pelos assessores qualificados. O objetivo do PCI é proteger a indústria de cartões, uma vez que a confiança no uso dos cartões pode ser comprometida por incidentes de segurança em qualquer ponto da cadeia (comerciantes, processadores, adquirentes, emissores e prestadores de serviço). Assim, quem não está em conformidade com o padrão de segurança pode perder a permissão de utilizar os cartões de pagamento.

Sem a conformidade com a PCI DSS, as empresas ficam sujeitas a não poderem mais participar do ecossistema de cartões de pagamento, por colocar em risco os demais atores da cadeia e prejudicar a confiança no sistema.

REFLITA

O PCI DSS trata o trabalho de avaliação de conformidade como uma avaliação e não uma auditoria. Isso faz com que exista uma característica fundamental no PCI DSS que o

diferença de um potencial conflito de interesses que pode existir nas auditorias: os assessores qualificados podem participar do processo de adequação das empresas ao PCI DSS, não sendo limitados a apenas auditá-los. O resultado, assim, é o relatório de conformidade ou *Report on Compliance* (RoC), que apresenta os resultados dos testes feitos nos controles definidos no padrão.

As empresas podem se certificar em segurança da informação com a ISO 27001, que estabelece um sistema de gestão de segurança da informação, após uma auditoria de certificação.

A ABNT NBR ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação dentro do contexto da organização (Figura 4.13). A norma inclui também requisitos para a avaliação e o tratamento de riscos de segurança da informação voltados para as necessidades da organização. E os requisitos (Figura 4.14) da norma (contexto da organização, liderança, planejamento, apoio, operação, avaliação de desempenho e melhoria) são genéricos e são aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza, e todos devem fazer parte do SGSI (ISO 27001, 2013).

Figura 4.13 | Ciclo PDCA do SGSI

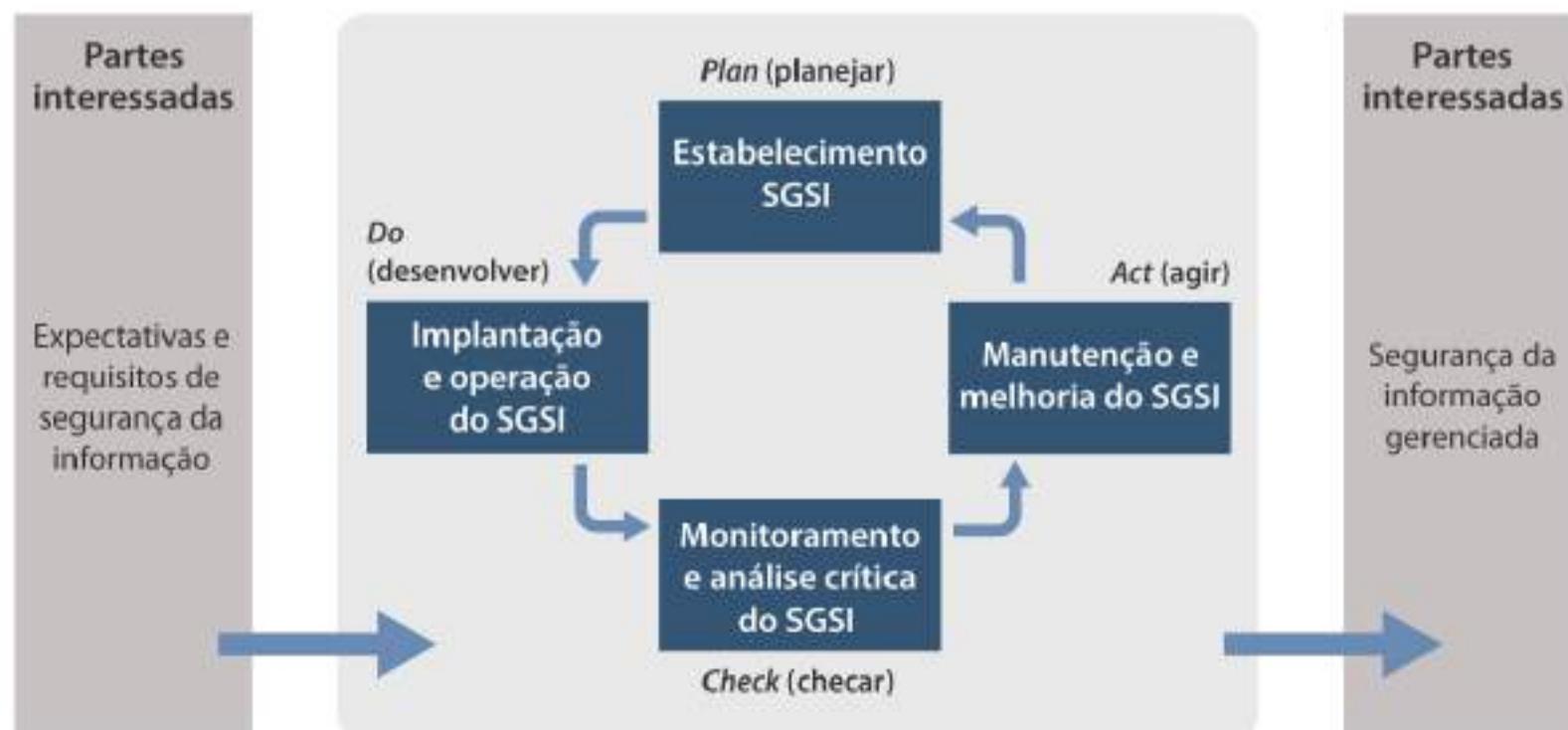


Figura 4.14 | Requisitos da ABNT NBR ISO/IEC 27001



Fonte: elaborada pelo autor.

Em uma auditoria de certificação ISO 27001, que pode ser aplicável para as empresas de diferentes tamanhos e naturezas, a auditoria deve levar em consideração o escopo e os requisitos do SGSI.

ASSIMILE

A certificação ISO 27001 avalia o sistema de gestão de segurança da informação (SGSI), de acordo com um escopo definido. A aplicação dos controles muda de empresa para empresa, dependendo do apetite ao risco, e do escopo envolvido. E ambas as empresas podem obter a certificação ISO 27001, mesmo com controles diferentes implantados.

Para a certificação, a empresa não precisa implantar todos os controles de segurança indicados na norma e detalhados na ABNT NBR ISO/IEC 27002 (ISO 27002, 2013). Os requisitos regulatórios e legais, além dos objetivos de negócios e os resultados da avaliação indicam os controles de segurança necessários. E, para a auditoria, é preciso organizar estas informações.

A declaração de aplicabilidade é um dos principais elementos de uma auditoria da ISO 27001. Ela declara quais controles de segurança são aplicáveis para a empresa, com base nos riscos específicos do ambiente e do escopo que está sendo auditado (HERON, 2019).

Para a criação da declaração de aplicabilidade, os passos são (HERON, 2019):

- Considerar os assuntos, partes interessadas e o escopo do SGSI.
- Identificar os ativos de informação, centros de processamento e dispositivos.
- Analisar os riscos de segurança da informação, considerando a confidencialidade, integridade e disponibilidade.
- Avaliar os riscos e decidir quais dos 114 controles da norma são necessários.
- Entender e avaliar as legislações e contratos aplicáveis.
- Definir a implementação dos controles, incluindo políticas, procedimentos, pessoas, tecnologias etc.
- Criar a declaração de aplicabilidade com as justificativas.
- Relacionar detalhes dos controles, os riscos e os ativos, com o SGSI funcionando.
- Gerenciar.

A auditoria interna é uma parte importante para as empresas e faz parte do processo de avaliação de desempenho do SGSI, o qual indica que elas devem conduzi-las a intervalos planejados para prover

informações sobre o quanto o sistema de gestão da segurança da informação está em conformidade com os próprios requisitos da organização para o seu sistema de gestão da segurança da informação e os requisitos da ABNT NBR ISO/IEC 27001 e que o SGSI está efetivamente implementado e mantido (ISO 27001, 2013).

A ABNT NBR ISO/IEC 27001 define o que a organização deve fazer quanto à auditoria interna (ISO 27001, 2013):

- Planejar, estabelecer, implementar e manter um programa de auditoria, incluindo frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Os programas de auditoria devem levar em conta a importância dos processos pertinentes e os resultados de auditorias anteriores.
- Definir os critérios e o escopo da auditoria, para cada auditoria.
- Selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria.
- Assegurar que os resultados das auditorias são relatados para a direção pertinente.
- Reter a informação documentada como evidência dos programas da auditoria e dos seus resultados.

A auditoria interna é essencial para a avaliação de desempenho do SGSI e é bastante similar com a auditoria de certificação (MCCREANOR, 2020):

- **Definição de escopo e levantamento de pré-auditoria:** condução de uma avaliação de riscos para determinar o foco da auditoria e identificar as áreas que estão fora de escopo. Fontes de informação incluem pesquisas de indústria, políticas e o SGSI. O escopo deve ser relevante para a empresa, incluindo diferentes localidades de unidades de negócios. Durante o levantamento pré-auditoria, a documentação que será revisada durante a auditoria deve ser juntada.

- **Planejamento e preparação:** com o escopo da auditoria de SGSI, o detalhamento envolve o planejamento da auditoria, com a definição do tempo e recursos. Pontos de checagem com a gestão da empresa possibilitam ajustes para agilizar o acesso às informações e pessoas, bem como para a gestão acompanhar o andamento da auditoria e reforçar as preocupações.
- **Trabalho em campo:** o planejamento da auditoria é aplicado, com os auditores coletando evidências com as técnicas definidas, como as entrevistas com equipes, áreas e demais atores envolvidos com o SGSI. Há ainda a revisão de documentação e de dados, com a observância dos processos do SGSI em funcionamento. Os testes das evidências devem ser feitos para validar as evidências coletadas, junto das documentações destes testes.
- **Análise:** as evidências da auditoria devem ser organizadas e revisadas com relação aos riscos e objetivos de controles. A análise pode identificar necessidades de novas evidências ou de novos testes, que devem ser realizados.
- **Reporte:** Os componentes essenciais do relatório consistem em: introdução que justifica escopo, objetivos, tempo e extensão dos trabalhos; sumário executivo indicando os principais resultados, uma análise resumida e uma conclusão; lista de pessoas ou áreas que terão acesso ao relatório, incluindo a classificação da informação e as regras de circulação; resultados e análises detalhadas; conclusão e recomendações; declaração do auditor detalhando as recomendações ou limitações do escopo. O relatório de auditoria deve ser apresentado e discutido previamente com a gestão de projetos, devido a eventuais necessidades de revisões e análises adicionais. A gestão deve se comprometer com o plano de ação.

Uma auditoria de segurança engloba um conjunto de elementos, como as configurações dos sistemas operacionais, compartilhamentos de redes, aplicações e acessos, a validação de processos e do nível de maturidade em segurança dos usuários. Alguns assuntos que são normalmente alvos de auditoria são:

- Proteção de *e-mail*, principalmente contra *phishing* e filtros de *spam*.
- Senhas de usuários, para verificar se estão de acordo com a política de senha da empresa.
- Gerenciamento de usuários, para verificar se há contas ativas que não deveriam, como de ex-funcionários.
- *Backups*, para verificar se é feito e se está íntegro.
- Acesso físico, para evitar acessos indevidos de pessoas não autorizadas.
- Atualização de *software*, para verificar se os sistemas estão em versões livres de vulnerabilidades.
- Vulnerabilidades, para identificar pontos fracos que podem ser explorados em ataques.

PESQUESE MAIS

O livro *Auditoria e controle de acesso*, de Beneton (2017) apresenta no capítulo 5 uma discussão sobre a auditoria de sistema operacional e aplicativos, abordando questões de logs, monitoração de violações, gestão de mudanças e gestão de liberações.

BENETON, E. *Auditoria e controle de acesso*. São Paulo: Editora Senac, 2017.

Chegamos ao fim desta aula, em que a auditoria deve ser planejada com a definição das técnicas e ferramentas a serem aplicadas no trabalho em campo na auditoria. Esta definição depende do objetivo e escopo da auditoria, que pode ser para a conformidade com padrões, normas, leis ou regulações. Em segurança da informação, a auditoria deve validar a eficácia e eficiência dos controles, que são definidos de acordo com a avaliação dos riscos, fechando, assim, o objetivo de tornar a empresa mais segura, de fato. O conhecimento e a competência para definir e utilizar as técnicas e ferramentas é essencial para uma auditoria de sucesso.

FAÇA VALER A PENA

Questão 1

A auditoria é uma inspeção e verificação formal para checar se um padrão ou conjunto de guias está sendo seguido, se os registros estão corretos e se os objetivos de eficiência e eficácia estão sendo alcançados. Ela é realizada em três grandes fases, que são o planejamento, o trabalho em campo e os relatórios.

As técnicas e ferramentas de auditoria são definidas na fase de:

a. Planejamento.

b. Trabalho em campo.

c. Relatórios.

Questão 2

Uma auditoria verifica e inspeciona formalmente a eficiência e eficácia de controles e valida a conformidade de acordo com normas, padrões, *frameworks*, leis ou regulações. Há, assim, auditorias com objetivo de conformidade e outras com objetivo de certificação.

Assinale a alternativa que possibilita uma certificação da empresa.

a. COBIT.

b. ITIL.

c. NIST Cybersecurity Framework.

d. ISO 27001.

e. COSO.

Questão 3

As técnicas e ferramentas para auditoria envolvem interação com pessoas, análise manual e análise técnica. Com base nas técnicas e ferramentas, associe a coluna A com a coluna B.

A	B
I. Perguntas e observação	1. Interação com pessoas
II. Análise de configurações	2. Análise manual
III. <i>Pentest</i>	3. Análise técnica
IV. <i>Scripts</i>	

A seguir, assinale a alternativa que apresenta a associação correta.

a. I-1; II-1; III-3, IV-3.

b. I-1, II-1, III-2, IV-3.

c. I-1; II-2; III-2; IV-3.

d. I-1; II-2; III-3; IV-3.

e. I-1; II-3; III-3; IV-3.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27002:2013** Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2013.

ABNT. **NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.** Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2013.

AXELOS. **Building IT and Digital Excellence with ITIL 4, 2018.**

Disponível em: <https://bit.ly/3dlnll8>. Acesso em: 10 jan. 2021.

BENETON, E. **Auditória e controle de acesso.** São Paulo: Editora Senac, 2017. Disponível em: <https://bit.ly/39uB3rd>. Acesso em: 13 jan. 2021.

HERON, J. The ISO 27001:2013 Statement of Applicability (SoA): The Complete Guide. **ISMS online**, 3 dez. 2019. Disponível em: <https://bit.ly/3sF6VAF>. Acesso em: 14 jan. 2021.

ISACA, Information Systems Audit and Control Association. **COBIT 2019 Framework.** Introduction and Methodology, 2018. Disponível em: <https://bit.ly/3uc08PC>. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. **COBIT 2019 Framework.** Governance and Management Objectives, 2018. Disponível em: <https://bit.ly/3m9CjFc>. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. **Information Systems Auditing: Tools and Techniques Creating Audit Programs,** 2016. Disponível em: <https://bit.ly/39sed3i>. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. **Auditing Cyber Security: Evaluating Risk and Auditing Controls**, 2017. Disponível em: <https://bit.ly/3mdxIC3>. Acesso em: 9 jan. 2021.

ISACA, Information Systems Audit and Control Association. IT Audit Framework (ITAFTM). **A Professional Practices Framework IT Audit**, 4 ed., 2020. Disponível em: <https://bit.ly/3rlJRjk>. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. **IT Audit's Perspectives on the Top Technology Risks for 2021**, Protiviti, 2020. Disponível em: <https://bit.ly/3sGMYK3>. Acesso em: 4 jan. 2021.

ITIL Process Map & ITIL Wiki. **ITIL 4**, 3 dez. 2019. Disponível em: <https://bit.ly/3sRRwNu>. Acesso em: 10 jan. 2021.

ITIL Process Map & ITIL Wiki. **IT Service Continuity Management**, 24 jul. 2020. Disponível em: <https://bit.ly/3wezf4>. Acesso em: 10 jan. 2021.

KAMAL, S.; HELAL, I. M. A.; MAZEN, S. A. Computer-Assisted Audit Tools for IS Auditing – A comparative study. Faculty of Computers and Artificial Intelligence, Cairo University, Giza, Egypt. Disponível em: <https://bit.ly/3fyWg70>. Acesso em 16 jan. 2021.

MCCREANOR, N. The five stages of a successful ISO 27001 audit. **It governance**, 19 maio 2020. Disponível em: [Link](#). Acesso em: 14 jan. 2021.

NAKAMURA, E. T. **Segurança da informação e de redes**. Londrina: Editora e Distribuidora Educacional S.A., 2016.

NATIONAL Institute of Standards and Technology, NIST. **Framework for Improving Critical Infrastructure Cybersecurity**. Version 1.1, 16 abr. 2018. Disponível em: <https://bit.ly/31CTPII>. Acesso em: 24 out. 2020.

NATIONAL Institute of Standards and Technology, NIST. Security and Privacy *Controls* for Information Systems and Organizations. **NIST Special Publication 800-53 Revision 5**, set. 2020. Disponível em: <https://bit.ly/3mbzH9P>. Acesso em: 9 jan. 2021.

PCI Security Standards Council, LLC. **Indústria de cartões de pagamento (PCI) Padrão de Segurança de Dados** – Requisitos e procedimentos da avaliação de segurança – Versão 3.2.1, maio de 2018. Disponível em: <https://bit.ly/2QXgtcv>. Acesso em: 16 jan. 2021.

TELECOMMUNICATIONS Industry Association, **TIA. TIA-942 Certification**. Disponível em: <https://bit.ly/31xLN3y>. Acesso em: 12 fev. 2021.

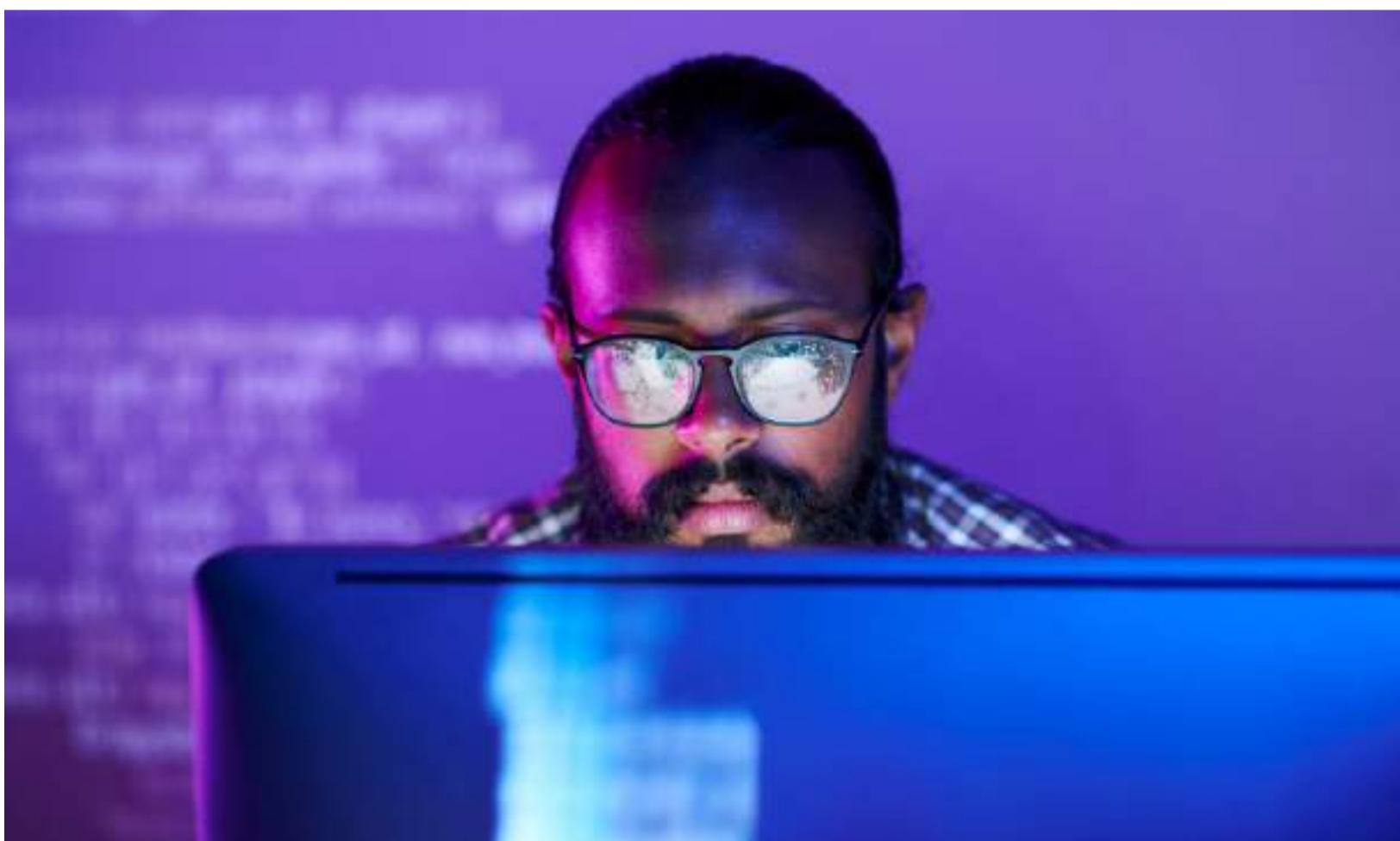
FOCO NO MERCADO DE TRABALHO

TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

QUAIS TÉCNICAS E FERRAMENTAS UTILIZAR EM UMA AUDITORIA?

As técnicas e ferramentas utilizadas em uma auditoria de sistemas envolvem interação com as pessoas, análises manuais e análises técnicas com uso de ferramentas.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

Você já montou um planejamento para melhorar a segurança do provedor de nuvem, que está crescendo de uma forma muito rápida. As ações de implantação dos controles foram adiante e agora você deve planejar as técnicas e ferramentas que serão utilizadas na auditoria.

Os controles implantados no data center foram resultados da avaliação de riscos, que direcionaram as necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos. Além dos riscos, a definição dos controles foi feita a partir de requisitos que direcionam a seleção e implementação de controles e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa, como a norma de certificação de data centers TIA-942, o padrão de segurança PCI DSS da indústria de cartões de pagamento e as melhores práticas de gerenciamento de serviços ITIL.

O primeiro ponto da auditoria é a realização de uma avaliação de riscos, para que todos os riscos do escopo referente ao datacenter tenham sido mapeados. Na avaliação de riscos, devem ser identificados e mapeados ameaças, agentes de ameaças, ativos, suas vulnerabilidades, e calculados a probabilidade e os impactos. Os ativos são:

- A área segura.
- Os *racks* com os servidores e os equipamentos de comunicação.
- Os administradores de sistemas.
- As máquinas virtuais.
- Sistemas operacionais disponibilizados para os clientes.
- Sistema de provisionamento de acesso aos clientes.

Após a avaliação dos riscos, o tratamento dos riscos pode se basear nos controles do TIA-942, PCI DSS, ABNT NBR ISO/IEC 27002, NIST *Cybersecurity Framework*, ITIL e COBIT, entre outros, focando nestes

ativos. Os controles das diferentes normas, padrões e frameworks são equivalentes e complementares.

A verificação dos controles pode ser feita pensando nos controles técnicos, físicos e processuais, que são utilizados pela empresa.

Os principais controles existentes na empresa devem estar cumprindo os objetivos de, pelo menos:

- Políticas de segurança da informação.
- Organização da segurança da informação.
- Segurança em recursos humanos.
- Gestão de ativos.
- Controle de acesso.
- Criptografia.
- Segurança física e do ambiente.
- Segurança nas operações.
- Segurança nas comunicações.
- Aquisição, desenvolvimento e manutenção de sistemas.
- Relacionamento na cadeia de suprimento.

As técnicas e ferramentas para a auditoria no provedor de nuvem podem incluir, pelo menos:

- Análise das políticas, processos e procedimentos de segurança e privacidade.
- Entrevistas com todas as áreas da empresa para percepção sobre se a política de segurança é de conhecimento organizacional e se está sendo seguida.
- Visita ao data center para analisar a segurança física.
- Análise de configuração do *firewall*.

- Análise do fluxo para gestão de identidades.
- *Pentest* para identificar vulnerabilidades do ambiente.
- Análise de *logs* do banco de dados.
- Análise dos relatórios do IDS/IPS.
- Análise dos antivírus.
- Análise de código do sistema corporativo.
- Teste de *phishing*.

Sobre a segurança física, no exemplo do PCI DSS, um requisito é que “haja câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) para monitorar o acesso físico individual a áreas sensíveis. Analise os dados coletados e relate com outras entradas. Armazene, por pelo menos três meses, a menos que seja restringido de outra forma pela lei”.

Os procedimentos de testes recomendados são:

“

Verifique se câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) foram implantados para monitorar os pontos de entrada/saída das áreas sensíveis. Verifique se câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) estão protegidos contra adulteração ou desativação. Verifique se câmeras de vídeo e/ou outros mecanismos de controle de acesso são monitorados, e se os dados são armazenados por, pelo menos, três meses.

— (PCI DSS, 2013, p. 82 -83)

A orientação para a avaliação pelo PCI DSS é:

“

Ao investigar violações físicas, esses controles podem ajudar a identificar indivíduos que acessaram fisicamente as áreas confidenciais, bem como quando eles entraram e saíram. Criminosos que tentam obter acesso físico às áreas confidenciais muitas vezes tentarão desativar ou desviar os controles de monitoramento. Para proteger estes controles contra adulterações, câmeras de vídeo podem ser posicionadas de forma que fiquem fora de alcance e/ou sejam monitoradas para detectar falsificações. Da mesma forma, os mecanismos de controle de acesso podem ser monitorados ou ter proteções físicas instaladas para evitar que sejam danificados ou desativados por indivíduos mal-intencionados. Exemplos de áreas confidenciais incluem salas do servidor do banco de dados corporativo, salas do setor administrativo em local de revenda que armazene dados do titular do cartão e áreas de armazenamento de grandes quantidades de dados do titular do cartão. As áreas confidenciais devem ser identificadas por cada organização para garantir que os controles de monitoramento físicos adequados sejam implementados.

— (PCI DSS, 2013, p. 82 - 83)

AUDITANDO MINHA EMPRESA QUE FOI CONTAMINADA POR UM WORM

Apesar de todos os controles preventivos implantados na sua empresa, ela foi alvo de um ataque de *worm* que paralisou a empresa por várias horas, causando um prejuízo grande. Você irá conduzir uma auditoria no perímetro da rede, mais especificamente no *firewall*, para verificar se o controle está eficiente e eficaz. O que deve ser considerado nesta auditoria, em termos de técnicas e ferramentas?

Ver anotações

RESOLUÇÃO



As técnicas e ferramentas relacionadas ao *firewall* são:

- Avaliar os padrões de configuração do *firewall*.
- Avaliar se há um processo formal para testar e aprovar todas as conexões de redes e alterações nas configurações do *firewall*.
- Conversar com o responsável pelo *firewall* e verificar os registros em busca das aprovações e testes.
- Analisar o diagrama de rede para validar as conexões existentes.
- Analisar se o diagrama de rede está atualizado.
- Analisar o diagrama de rede com as configurações do *firewall*.
- Analisar se o gerenciamento do *firewall* está formalizado quanto às funções e responsabilidades.
- Analisar a documentação em busca das aprovações para cada serviço, protocolo e porta configurada no *firewall*.
- Identificar serviços, protocolos e portas não seguros permitidos.
- Analisar se os recursos de segurança estão implementados para cada porta, serviço e protocolo não seguros.
- Verificar se há uma formalização de que uma revisão e análise das regras do *firewall* devem ser feitas a cada seis meses.

- Conversar com o responsável pelo *firewall* para verificar se ele fez a revisão e análise das regras do *firewall* nos últimos seis meses.
- Analisar os logs do *firewall* em busca de informações específicas do *worm*.