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.

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.

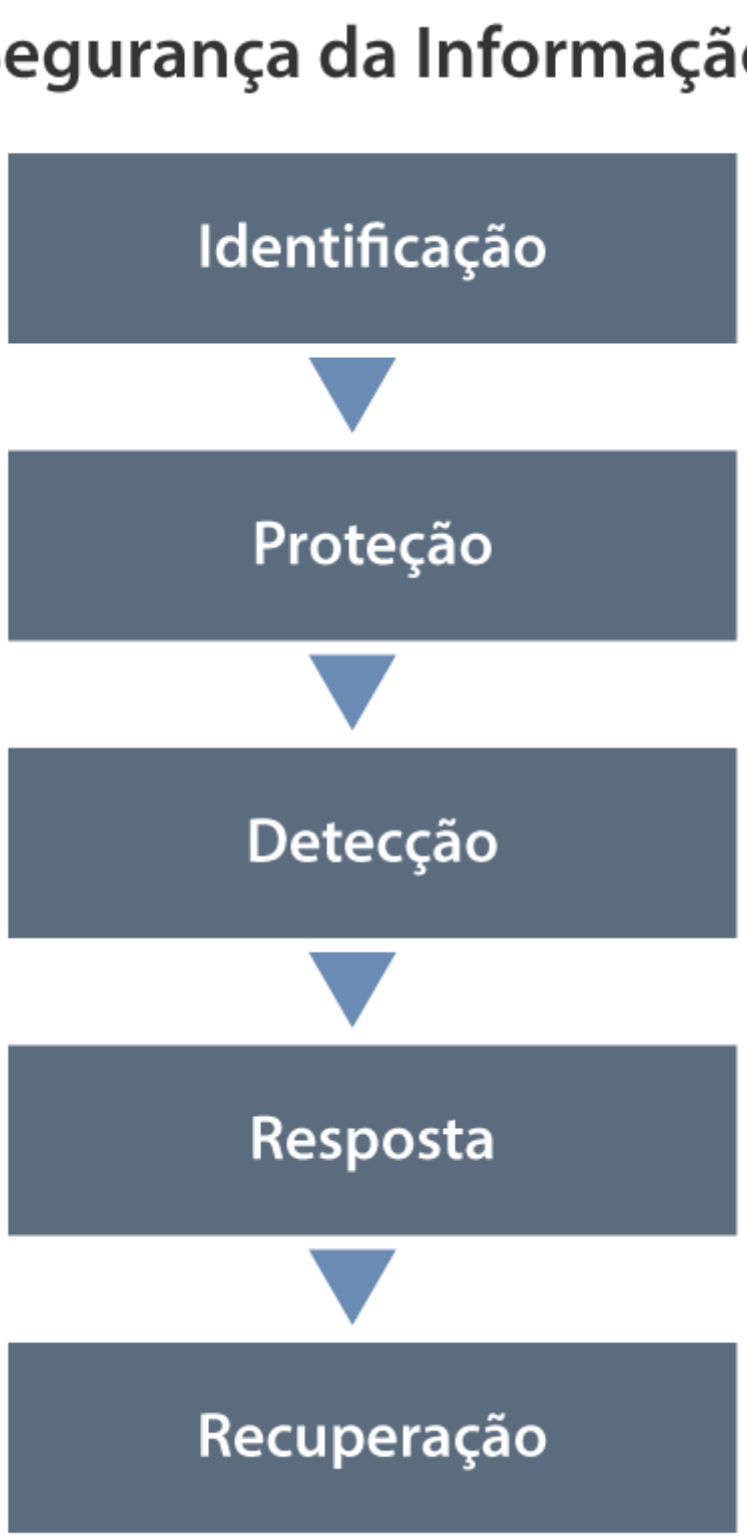
CONCEITO-CHAVE

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

devem ser realizadas atendendo aos princípios da CID.

Para visualizar o objeto, acesse seu material digital.

Ver anotações

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.

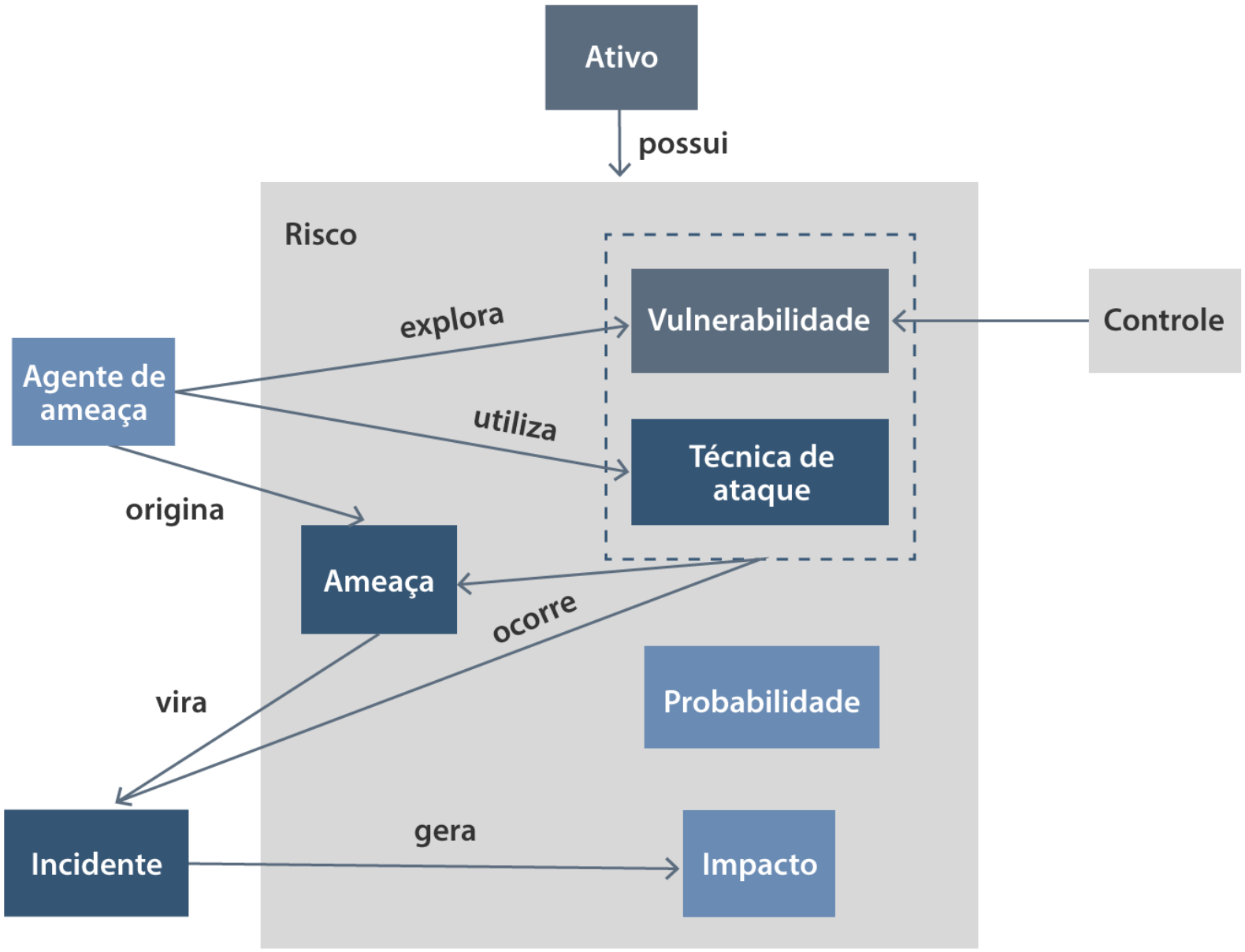
ELEMENTOS DO RISCO

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.

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.

Ver anotações

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 possiblidade 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).

> **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).

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.

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:

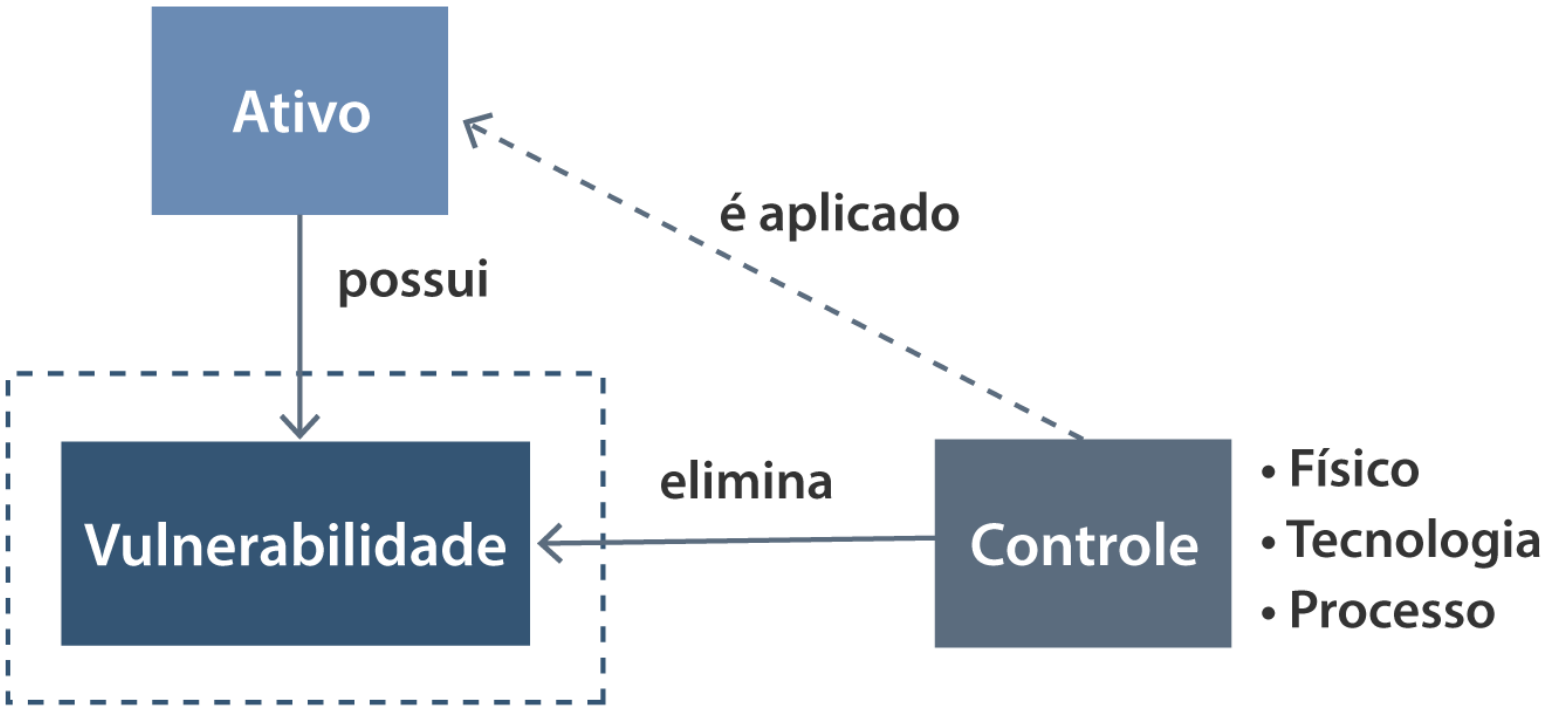
- Vazamento de projeto de novo produto ou de estratégia de marketing.
- Acesso não autorizado às informações confidenciais.
- Negação de serviço aos sistemas de TI da empresa.
- Alteração de informações-chave da estratégia de marketing.

CONTROLES DE SEGURANÇA

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

Ver anotações

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.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉNICAS. **ABNT NBR ISO/IEC 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/3pHlltl. 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.

Ver anotações 0