NÃO PODE FALTAR

CULTURA DE SEGURANÇA

Emilio Tissato Nakamura

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.

PRATICAR PARA APRENDER

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

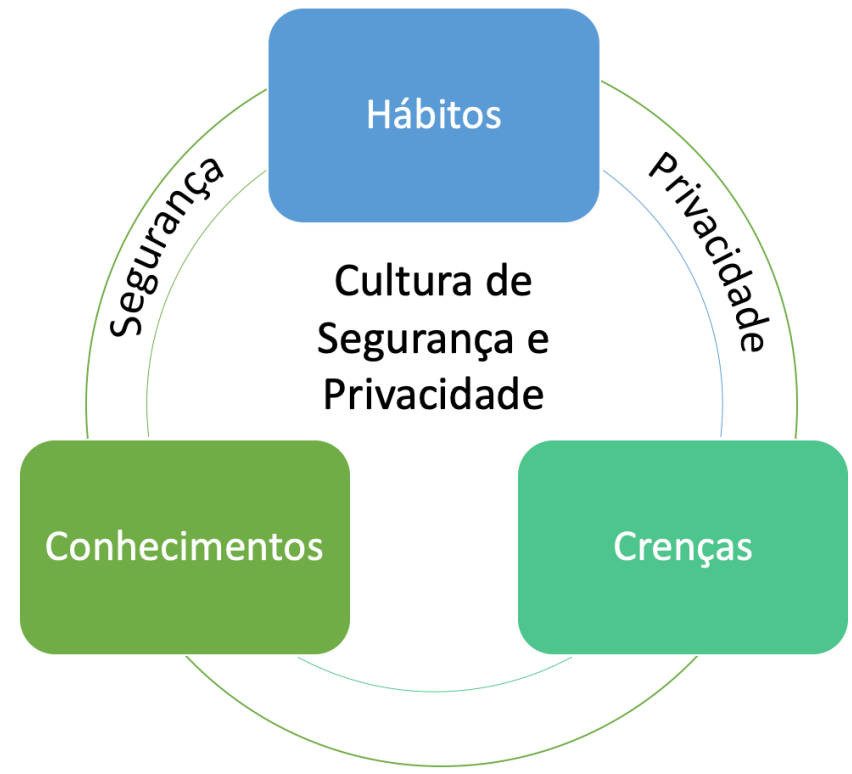
Caro aluno, a cultura de segurança e privacidade é fundamental para as empresas protegerem os seus ativos. Ela é formada pelo conjunto de comportamentos das pessoas no dia a dia das empresas em questões que refletem na proteção das informações e, consequentemente, dos negócios. Um ponto fundamental é 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.

EXEMPLIFICANDO

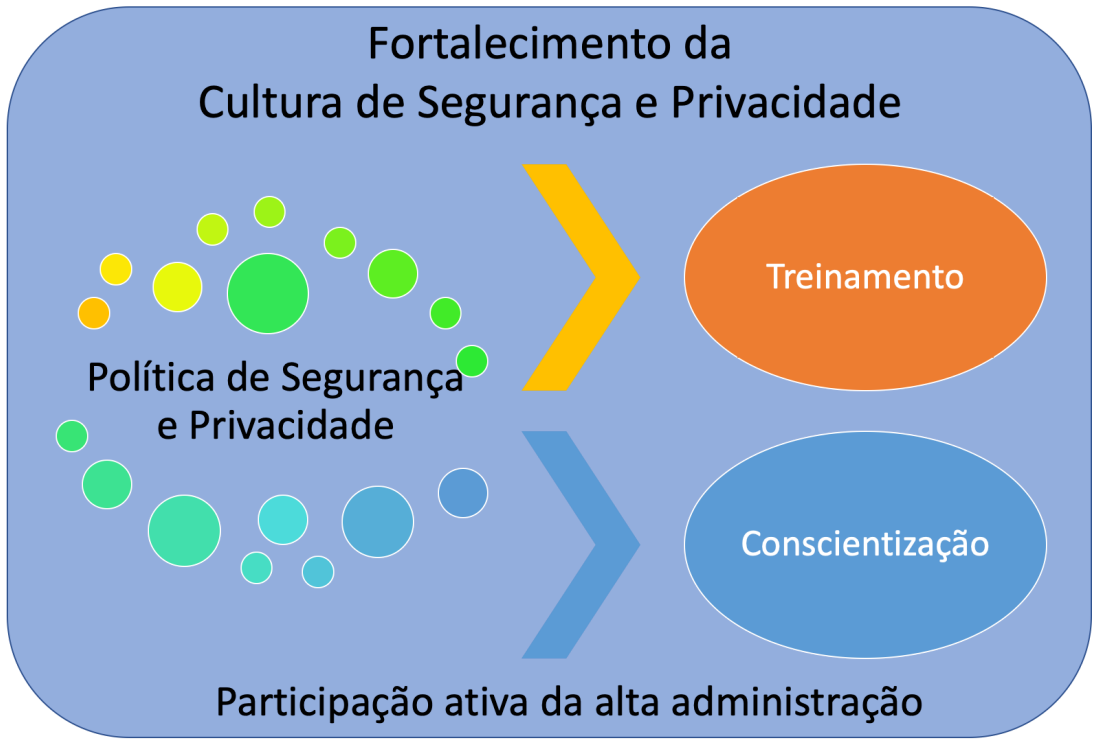
Um exemplo de criação de hábito e de consolidação de conhecimento de segurança é a simulação. Muito utilizado no caso de *phishing*, a simulação pode ser feita também espalhando-se *pendrives* com mensagens sobre a importância de se seguir a política de segurança da empresa.

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

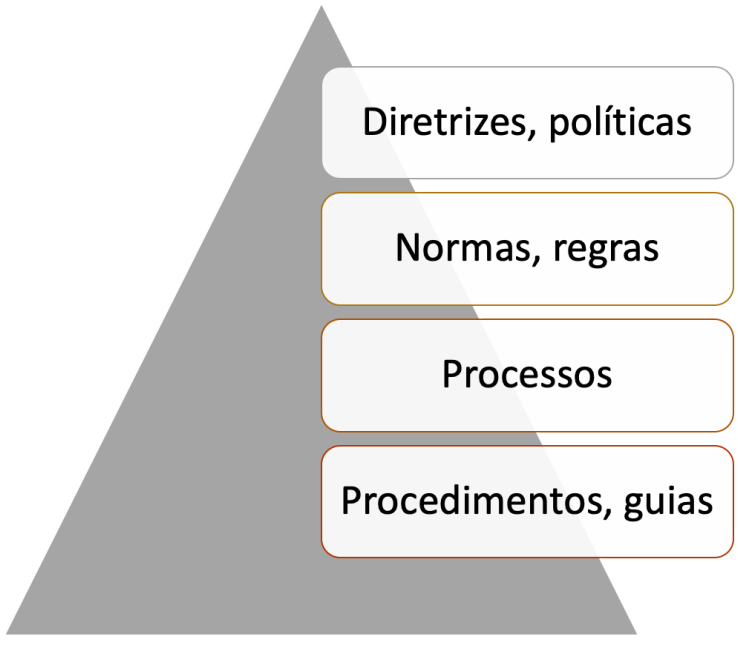
Ver anotações 0

Estar sempre atualizada
Ser comunicada regularmente

Fonte: elaborada pelo autor.

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.

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.

> **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.

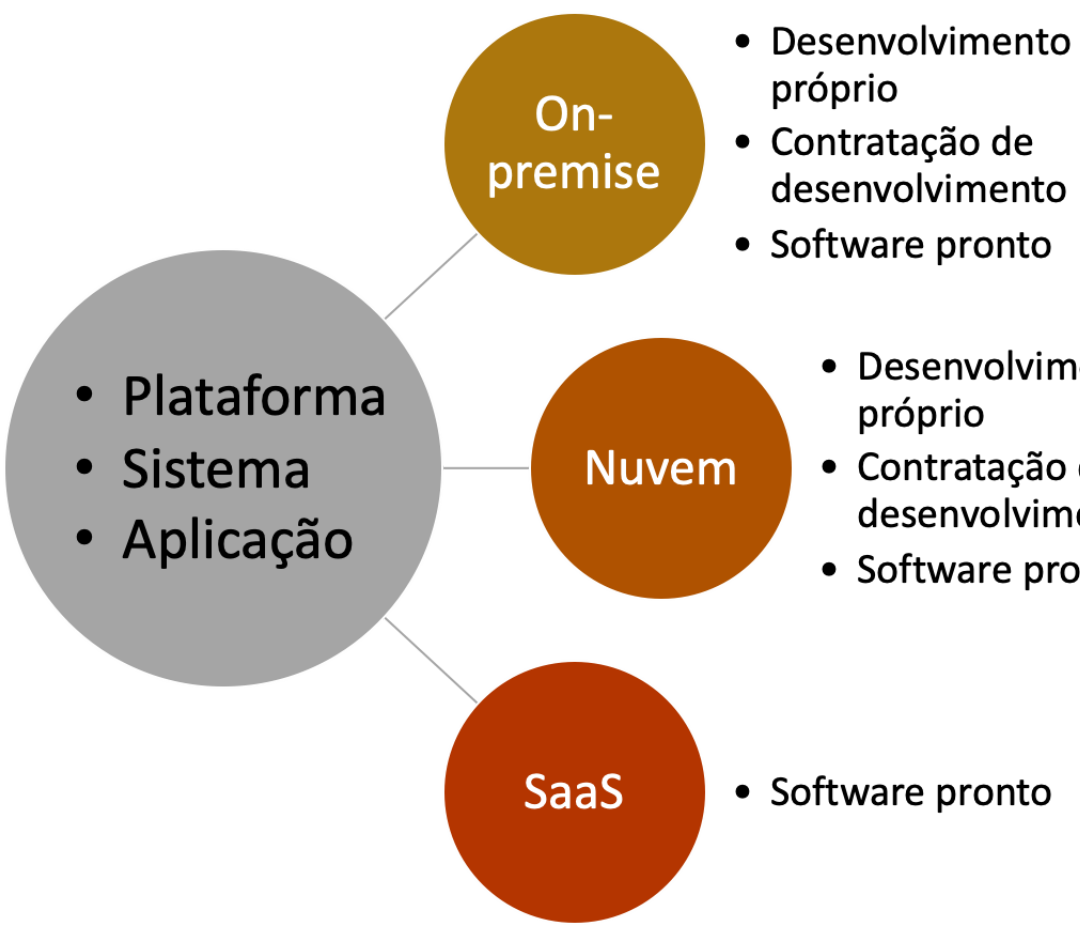
É importante destacar que os termos e contratos, como os de ciência ou de confidencialidade, são importantes para deixar explícito os objetivos e as preocupações com a segurança e privacidade, constituindo instrumentos importantes para as operações de segurança da informação. Eles têm valor legal, sendo 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).

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.

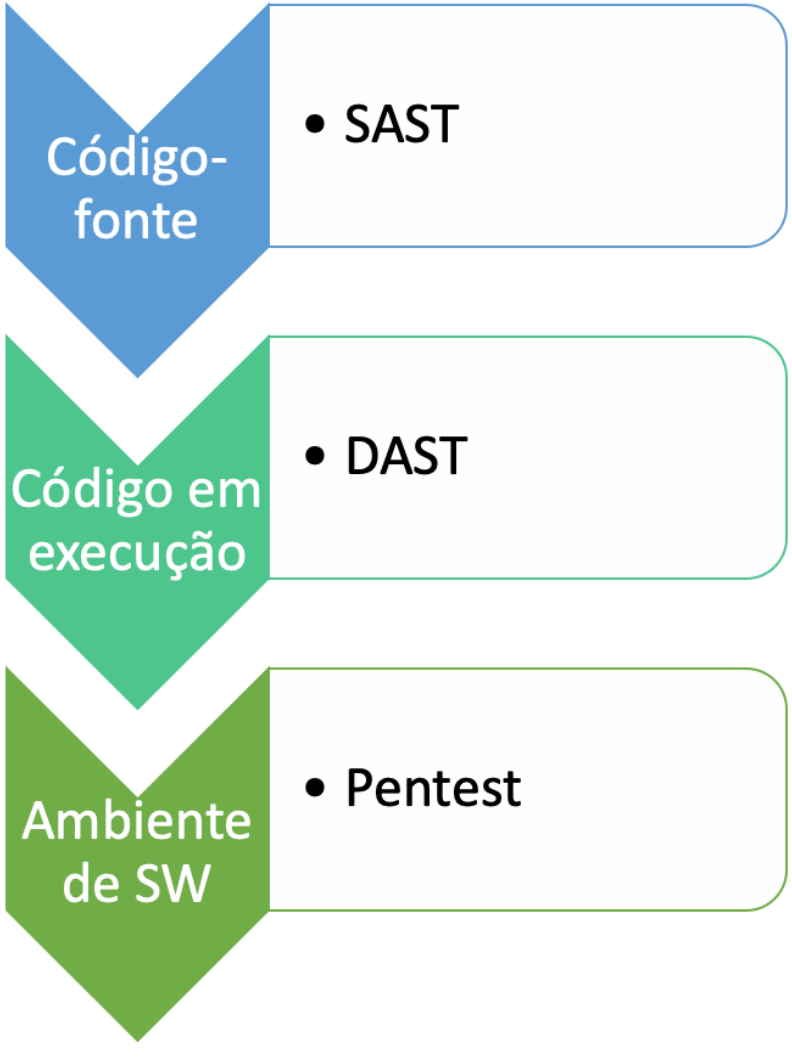
Ver anotações

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



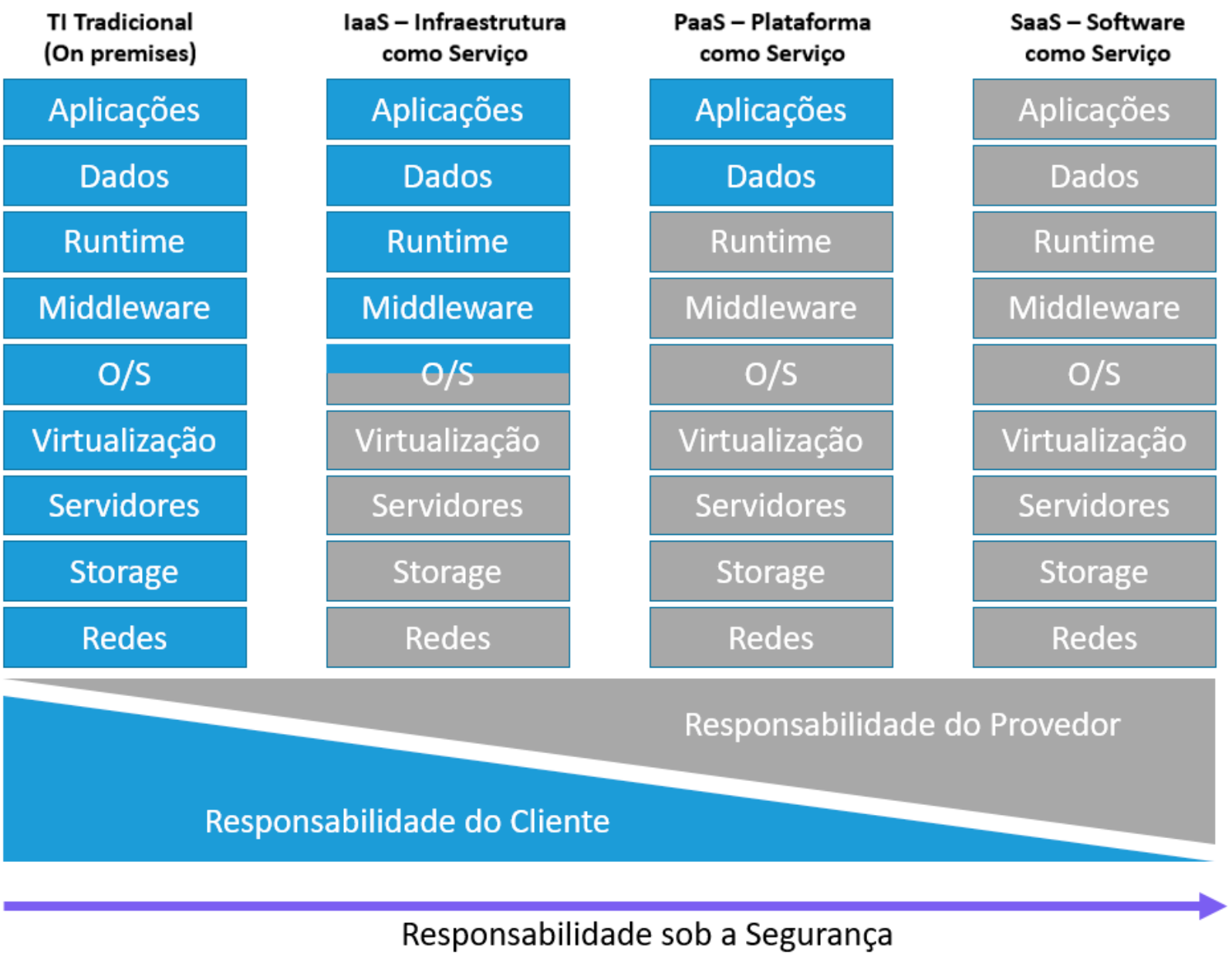
Fonte: elaborada pelo autor.

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 premise*s, 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).

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

Ver anotações

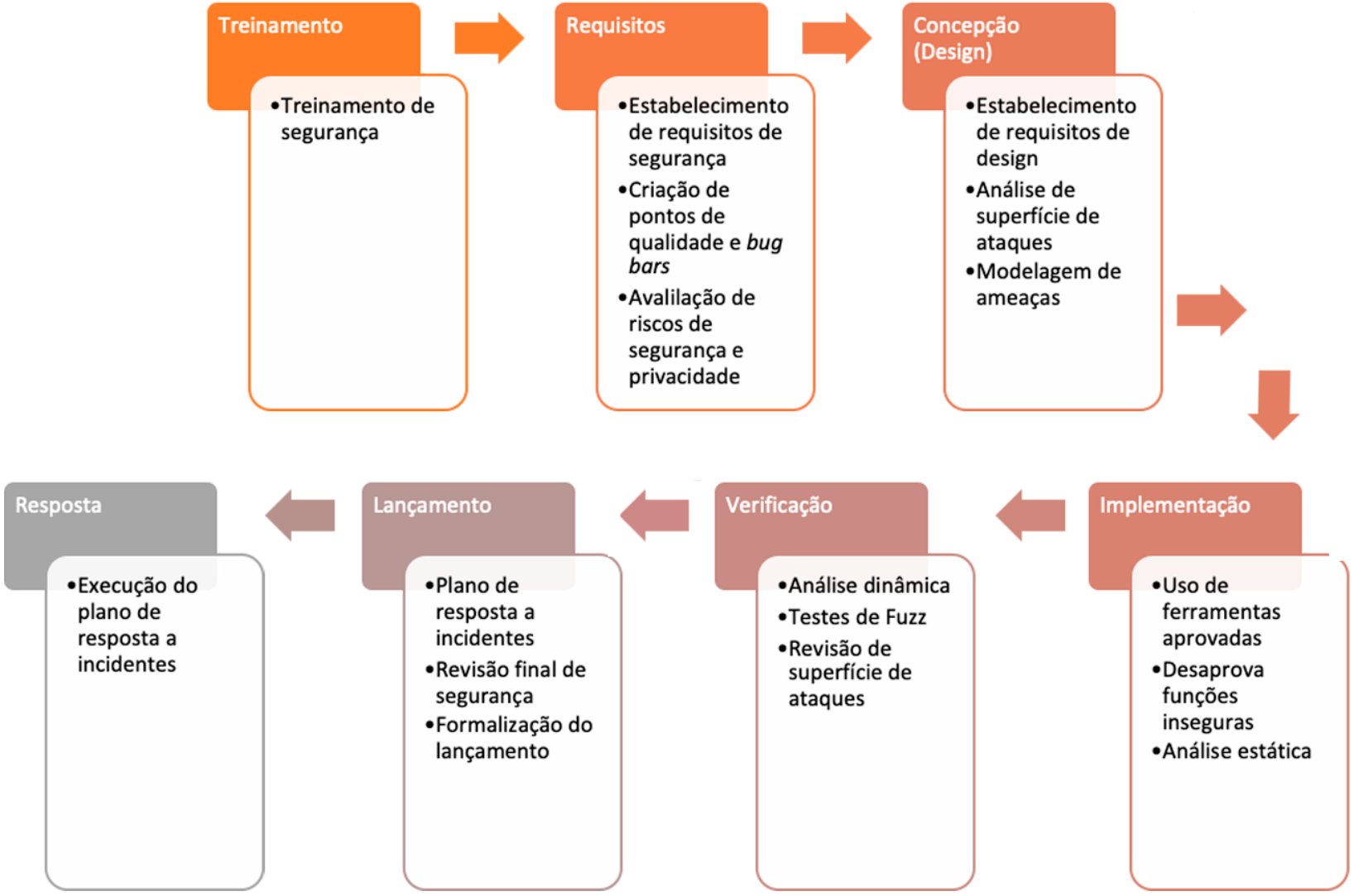
que em caso de vazamento decorrente de um incidente de segurança, há sanções previstas na lei. Assim, as empresas devem desenvolver *softwares* que não sejam a fonte de vazamento de dados pessoais, seja na própria empresa ou nos clientes que utilizam o *software* da empresa. Em caso de incidente de segurança, 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 vazar 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):

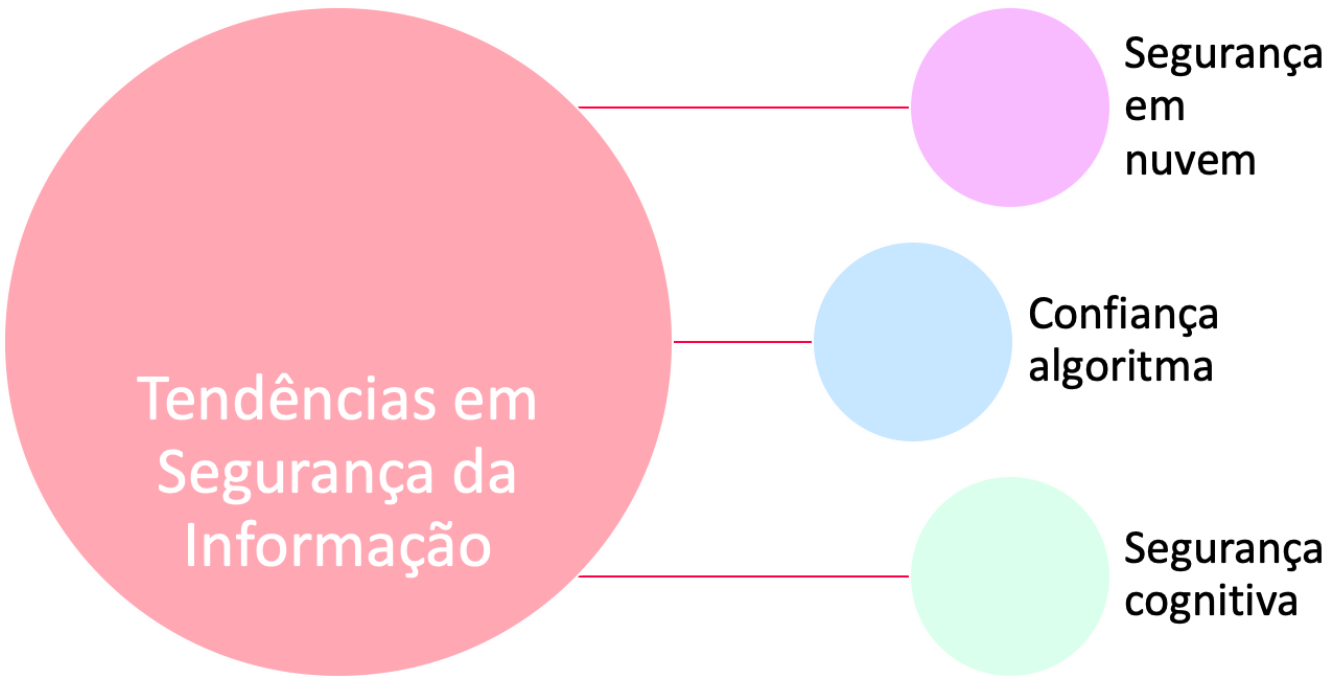
- **Segurança em nuvem** (GARTNER, 2020), incluindo segurança de conexões e acesso remoto ou *Secure Access Service Edge* (SASE), que considera a distribuição e a necessidade de tratar os dispositivos como de confiança zero (*zero trust network access*) e o uso de mecanismos de virtualização de redes. 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.

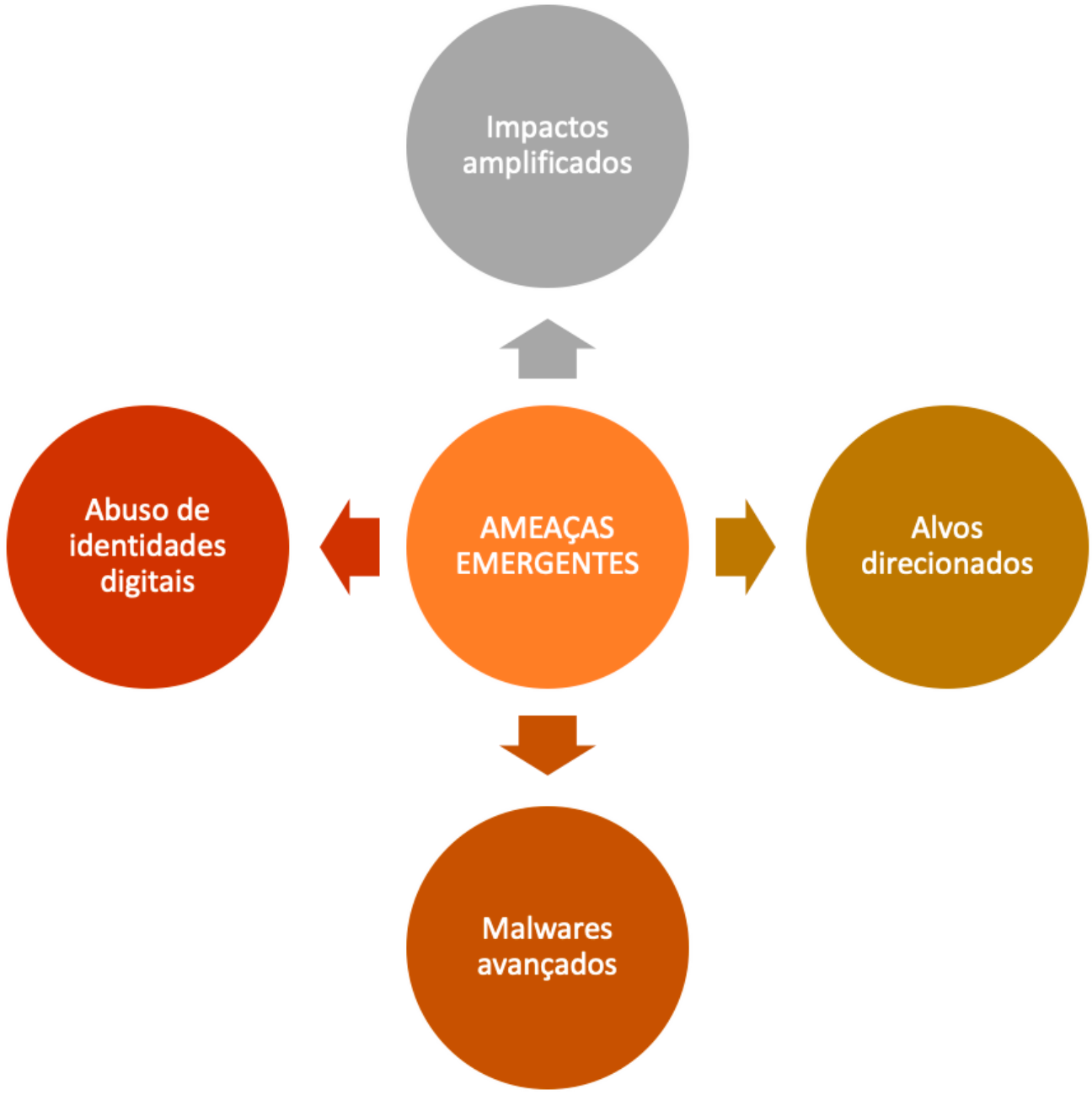
O futuro também nos mostra as ameaças emergentes (Figura 2.22), que deverão ser tratadas. Uma evolução natural das ameaças é o uso de ataques cibernéticos para fins políticos e militares, como um instrumento de instabilidade. Já citamos aspectos relacionados a impactos em fábricas e cidades decorrente 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.

PESQUISE 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.

Ver anotações 0

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. Pentest, resposta a incidentes e *firewall*.

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

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

Ver anotações 0

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/2MIbGtB . 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/3rhcIvH. 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 futur**o. Disponível em: https://bit.ly/3uUmNRk. Acesso em: 8 nov. 2020.

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

LIMA, A. R. 4ª 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 Rede**s. Belo Horizonte: Editora e Distribuidora Educacional S.A., 2016.

OWASP. OWASP Top 10. **Open Web Application Security Project**. 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.