

Segurança e Auditoria de Sistemas

Segurança na internet, dispositivos móveis e testes de intrusão

Profª. Ms. Adriane Ap. Loper

- Unidade de Ensino: 3
- Competência da Unidade: Segurança na internet, Proteção para Dispositivos Móveis e Análise de vulnerabilidade e Pentest
- Resumo: Principais definições de segurança na internet e dispositivos móveis.
- Palavras-chave: pentest, internet, dispositivos móveis
- Título da Teleaula: Segurança na internet, dispositivos móveis e testes de intrusão
- Teleaula nº: 3

Contextualização

- Você foi contratado como um **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**.



Fonte: Shutterstock

Contextualização

- E, como a empresa trabalha com **inteligência artificial**, há uma 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 de nuvem na Europa**, você possui 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;



Fonte: Shutterstock

Contextualização

- 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 lista de aspectos que devem ser considerados pela empresa para a definição de uma **estratégia de segurança e privacidade**.



Fonte: Shutterstock

Contextualização

- 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.

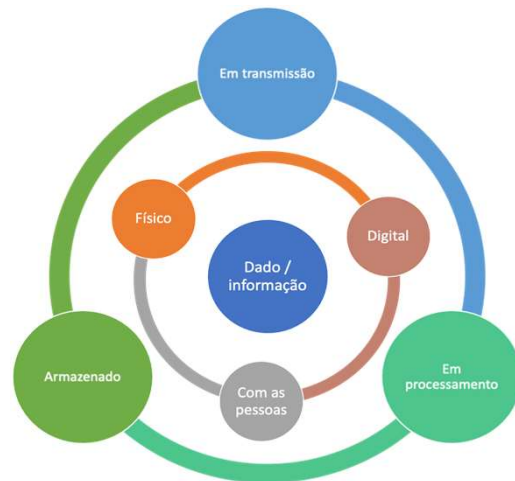


Fonte: Shutterstock

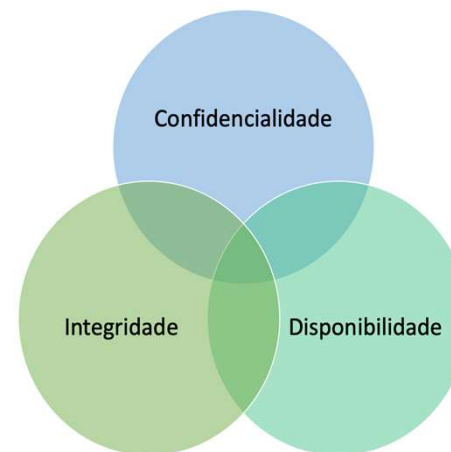
Segurança na internet

Contextualizando

- A segurança e privacidade na internet passa 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.
- Formas e estados do dado e informação/ CID



Fonte: Autora



Transações WEB

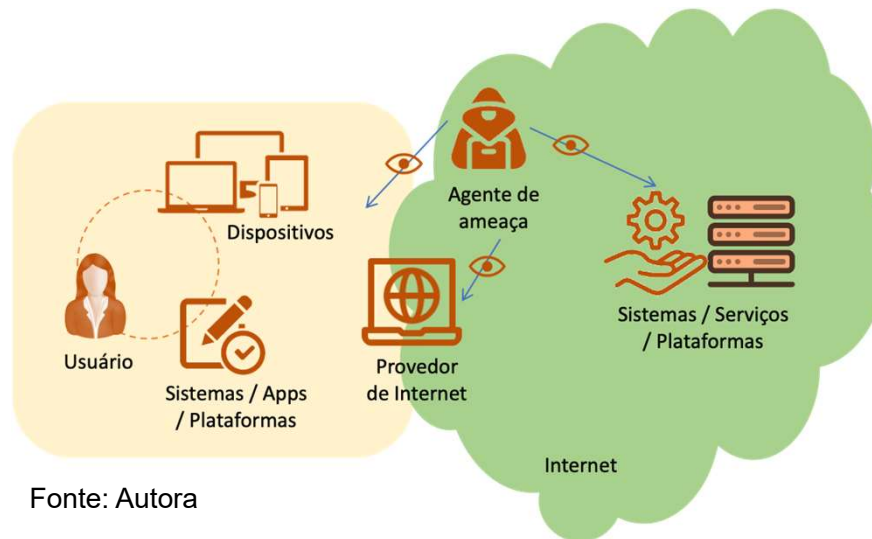
- As transações Web, que partem dos **usuários**, que utilizam seus dispositivos a partir de algum local em que há uma conexão internet, passam por variados componentes até chegar à loja virtual, ao serviço do governo ou o banco.
- Neste caminho, os **agentes de ameaça** estão à espreita em busca de 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, de ter acesso a informações valiosas .



Fonte: Shutterstock

Segurança na internet

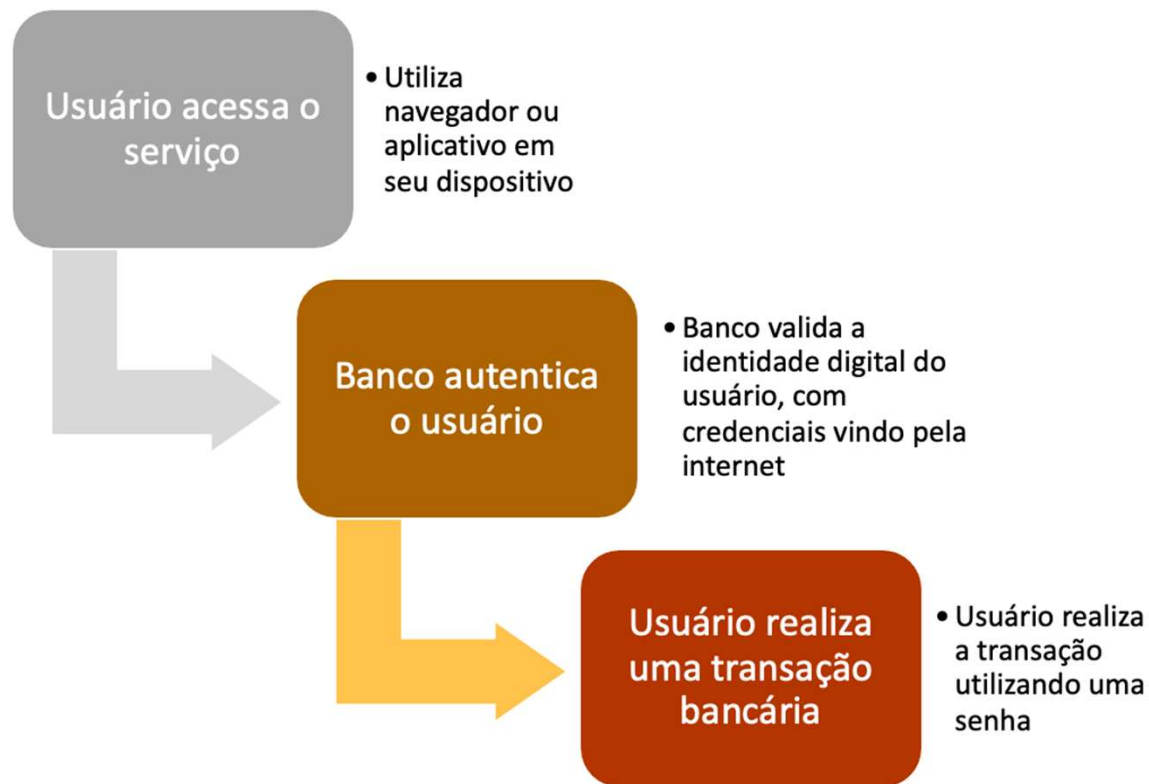
- O agente de ameaça buscando oportunidades em três ambientes: no ambiente do usuário, no ambiente de internet que inclui o provedor de internet, e no ambiente dos provedores de serviços, sistemas e plataformas.



Segurança em transações Web

- As transações Web, realizadas pela internet, envolvem uma série de questões de segurança que parte 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.

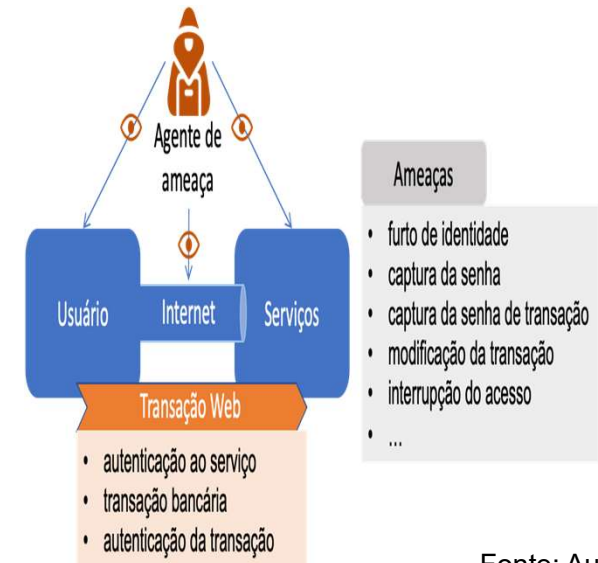
Transação Web em bancos



Fonte: Autora

Transação Web em bancos

- As ameaças no banco, 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.
- Elas podem ocorrer em qualquer um dos três ambientes (usuário, internet e provedor de serviços) e , porém de uma forma diferente, o que leva à necessidade de controles de segurança diferentes, que afetam também as responsabilidades.



Fonte: Autora

Transação Web em bancos

- 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)**.
- 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.

Transação Web em bancos

- 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**.

Golpes na internet



Fonte: Autora

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) (LGPD, 2020), todos devem preservar a privacidade e a proteção de dados pessoais.

Segurança e privacidade

- Para a **segurança em transações Web**, pensar:
- 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 sua 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.
- Usar **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 sua empresa poderá operar com a necessária segurança e privacidade, **minimizando** os problemas de acessos a partir de clientes falsos, resultando em melhores resultados.

Proteção para Dispositivos Móveis

Contextualizando

- **Sua missão:**
- O que deve ser planejado agora é a **expansão para a nova versão da plataforma, baseado 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 e farão o acesso junto com eles na plataforma digital, utilizando dispositivos móveis.

Dispositivos Móveis

- São um dos principais **vetores de ataques**, com os criminosos virtuais buscando 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**.
- E isso implica no aumento da **complexidade de proteção**, além do intrínseco aumento de riscos.
- Ex.: quando um colaborador instala **jogos** em seu dispositivo móvel, mas a partir de fontes não confiáveis.

Dispositivos Móveis

Ano: 2019 Banca: UFMT Órgão: COREN-MT Prova: UFMT - 2019 - COREN-MT - Assistente de Administração

Sobre **segurança da informação** ao utilizar **dispositivos móveis**, assinale a afirmativa correta.

- a) Por se tratar de equipamentos de baixa vulnerabilidade, não é necessária a instalação de um programa antivírus.
- b) Recomenda-se manter interfaces de comunicação, como bluetooth, infravermelho e Wi-Fi sempre ativadas, mesmo quando não utilizadas.
- c) Ao adquirir um dispositivo móvel usado, não é recomendado restaurar as configurações originais de fábrica.
- d) Ao baixar e instalar aplicativos, é aconselhado obtê-los de lojas oficiais ou de sites dos fabricantes.

Ano: 2019 Banca: UFMT Órgão: COREN-MT Prova: UFMT - 2019 - COREN-MT - Assistente de Administração

Sobre **segurança da informação** ao utilizar **dispositivos móveis**, assinale a afirmativa correta.

- a) Por se tratar de equipamentos de baixa vulnerabilidade, não é necessária a instalação de um programa antivírus.
- b) Recomenda-se manter interfaces de comunicação, como bluetooth, infravermelho e Wi-Fi sempre ativadas, mesmo quando não utilizadas.
- c) Ao adquirir um dispositivo móvel usado, não é recomendado restaurar as configurações originais de fábrica.
- d) Ao baixar e instalar aplicativos, é aconselhado obtê-los de lojas oficiais ou de sites dos fabricantes.

Interação

- Entenderam o que podemos ou não podemos fazer com nossos dispositivos móveis?



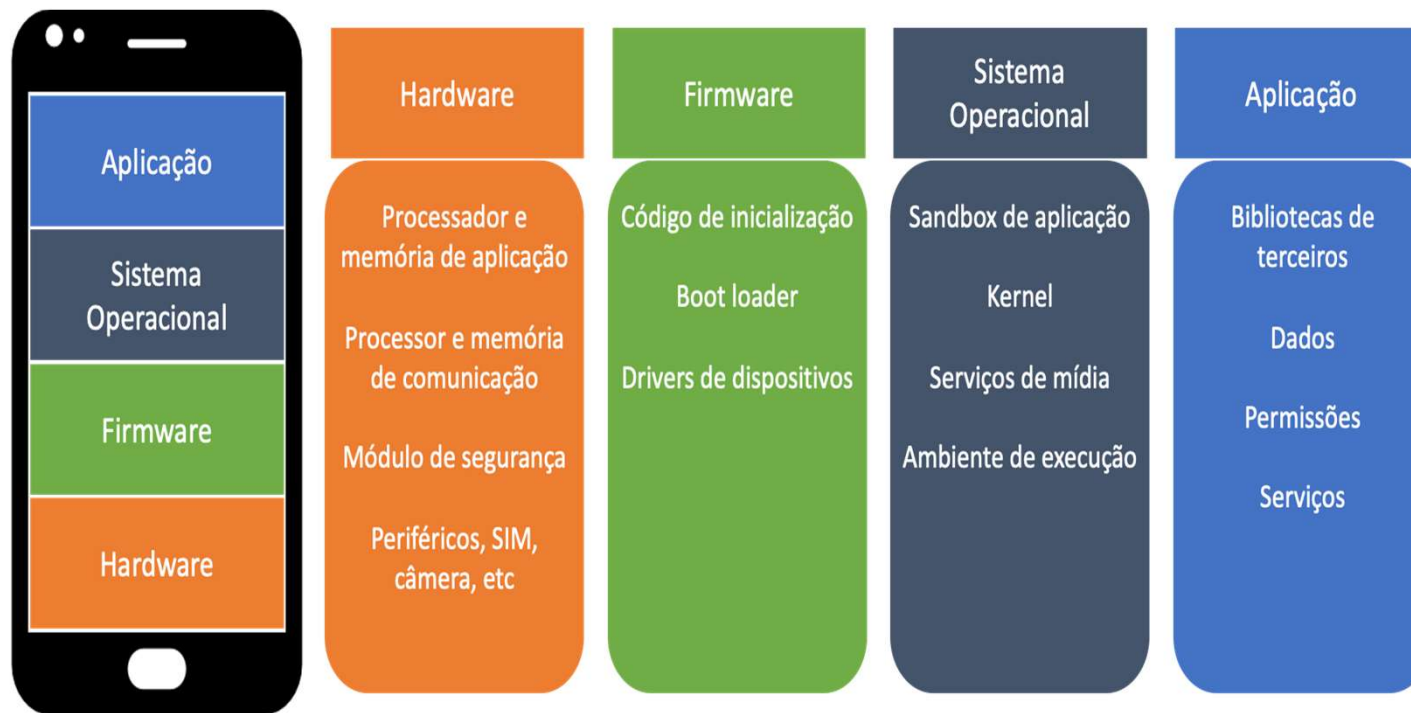
Fonte: <https://gifer.com/en/XIOL9>

Elementos de Segurança para Dispositivos Móveis

Dispositivos Móveis

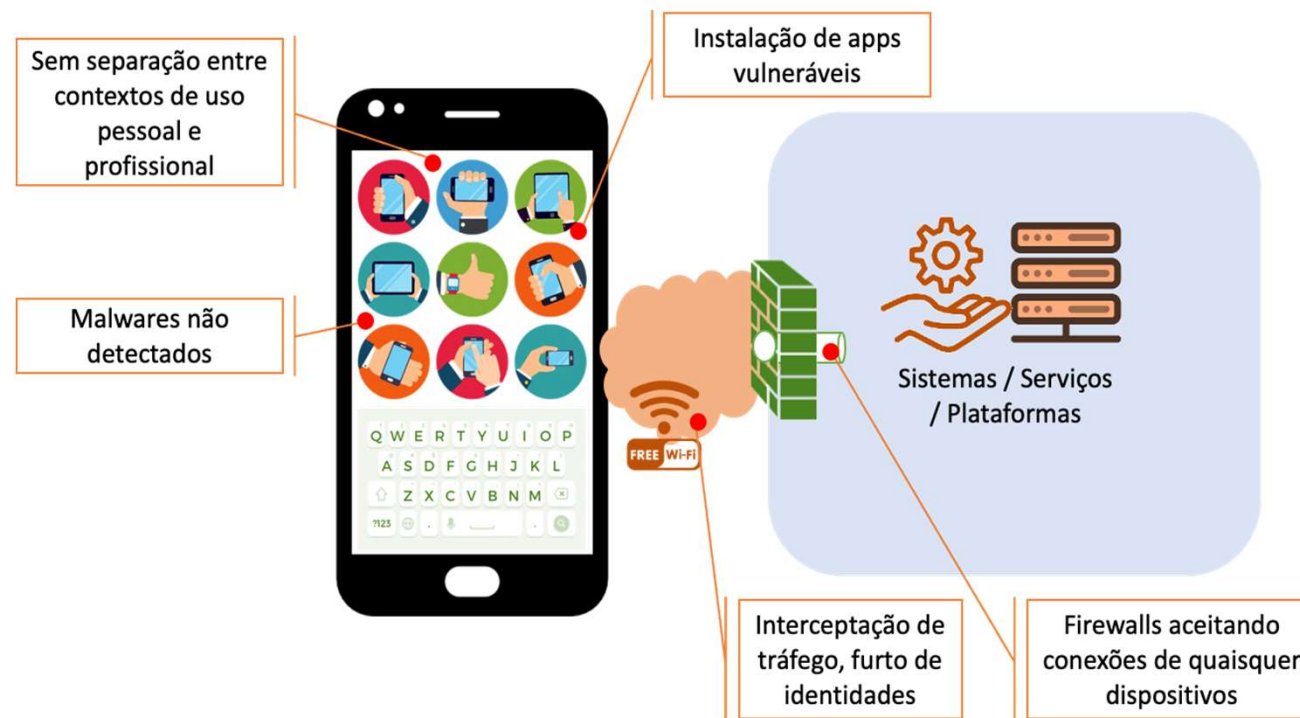
- Os elementos de segurança são diferentes do tradicional, já que os dispositivos móveis possuem características próprias :
- formato - portátil ; expandem o perímetro da empresa, com os dados sendo distribuídos de uma forma ampla e sem limites físicos.
- As políticas e configurações desses dispositivos 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.

Componentes de dispositivos móveis



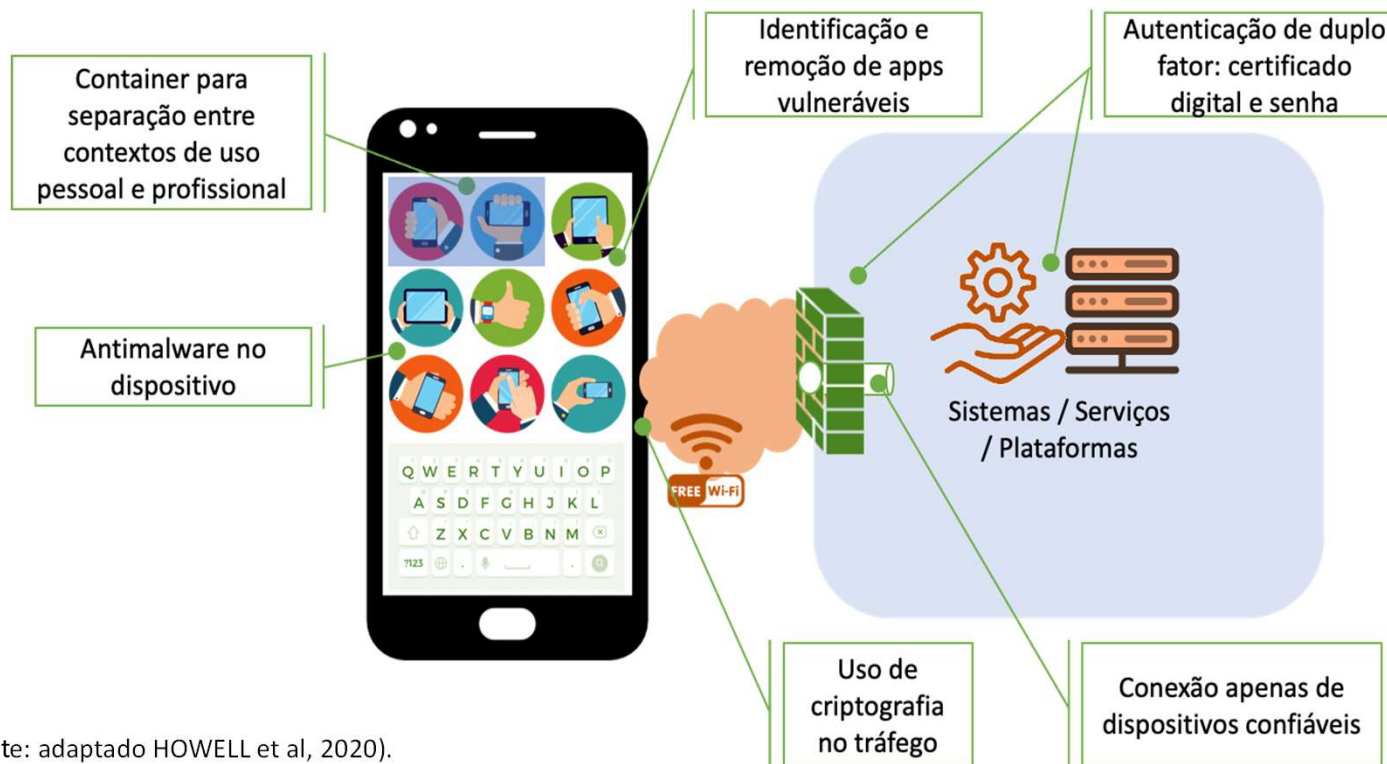
Fonte: adaptado de (FRANKLIN et al, 2020).

Riscos no uso de dispositivos móveis no mundo corporativo



Fonte: adaptado HOWELL et al, 2020).

Objetivos de segurança no uso de dispositivos móveis no mundo corporativo



Fonte: adaptado HOWELL et al, 2020).

Capacidades de segurança necessárias



Fonte: adaptado (NCCoE, 2020).

- 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 da instalação de códigos maliciosos (CERT, 2020).

- Engenharia social (acesso as informações pessoais) de dispositivos móveis
- 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).

- Engenharia social (acesso as informações pessoais) de dispositivos móveis
- 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
- 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 a 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).

Segurança em dispositivos móveis para empresas

- 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;
- Adotar tecnologias de segurança móvel como Enterprise Mobility Management ([EMM](#)), plataformas de defesa contra ameaças móveis ou serviço de veto 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](#).

■ Segurança em dispositivos móveis para empresas

- 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)...
- Ciclo de vida:



Fonte: adaptado de (FRANKLIN et al, 2020).

Relatório

- 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, consumidor e pequenos negócios**. Os servidores e o backend estão em um provedor de 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 inseguro, 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?

- Os modelos possíveis são:
- Uso exclusivamente corporativo de dispositivos móveis providos pela empresa; (COPE) ou (BYOD) ou (CYOD).
- Conduzir uma análise de riscos em dispositivos móveis;
- Adotar tecnologias de segurança móvel como Enterprise Mobility Management / Mobile Device Management (EMM/MDM);
- Manter regularmente a segurança dos dispositivos móveis, realizando avaliações periódicas de segurança e de cumprimento da política de segurança.

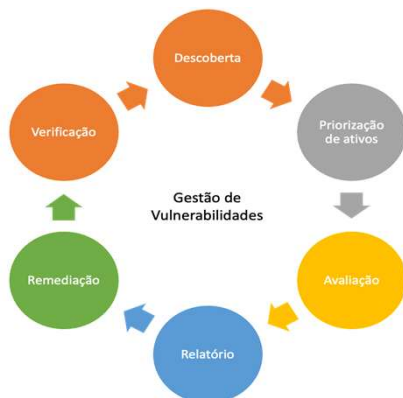
ANÁLISE DE VULNERABILIDADE E PENTEST

Contextualizando

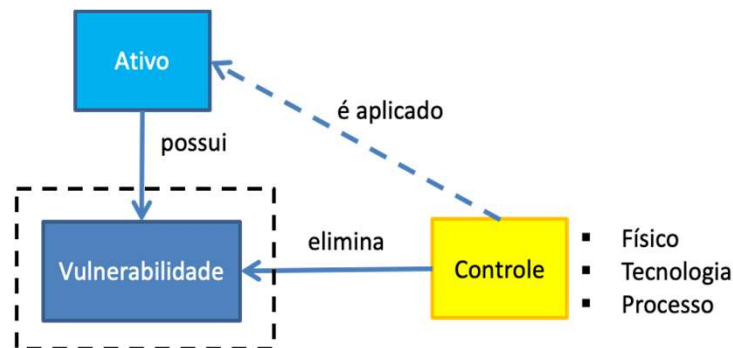
- **Sua missão:**
- O que deve ser planejado agora é a forma como a empresa deve tratar as vulnerabilidades, tanto da plataforma Web quanto da plataforma móvel.
- Mostre as perspectivas envolvidas com a **gestão de vulnerabilidades**, e a razão de precisarem ser tratadas antes das plataformas irem para o ambiente de produção.
- 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.

Processos da gestão de vulnerabilidades

- 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**.



Fonte: adaptado de (CAVALANCIA, 2020).



Fonte: Autor

Testes de segurança

- São importantes para a **gestão de segurança da informação** porque identificam as vulnerabilidades, que podem ser assim serem tratadas. E há diferentes formas de realizar testes de segurança e identificar as vulnerabilidades.
- O objetivo é a sua empresa disponibilizar serviços seguros, sem as 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**, deve disponibilizar o sistema de uma forma segura, seguindo práticas que vão eliminando as vulnerabilidades desde o início do desenvolvimento até após a implantação em ambiente de produção.

Testes de segurança

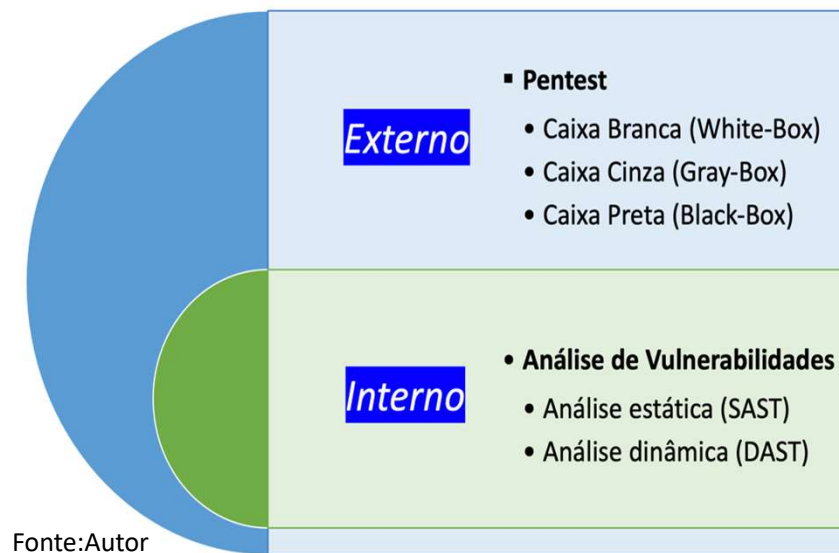
- Se a sua empresa utiliza software de terceiros, deve realizar testes de segurança para garantir que o ambiente da empresa, composta por softwares de diferentes fornecedores e de naturezas diferentes, esteja seguro.
- E os testes de segurança são uma das principais atividades de empresas especializadas em segurança e privacidade, com a oferta de serviços de análise de vulnerabilidades e [pentests](#), por exemplo.

Testes de segurança

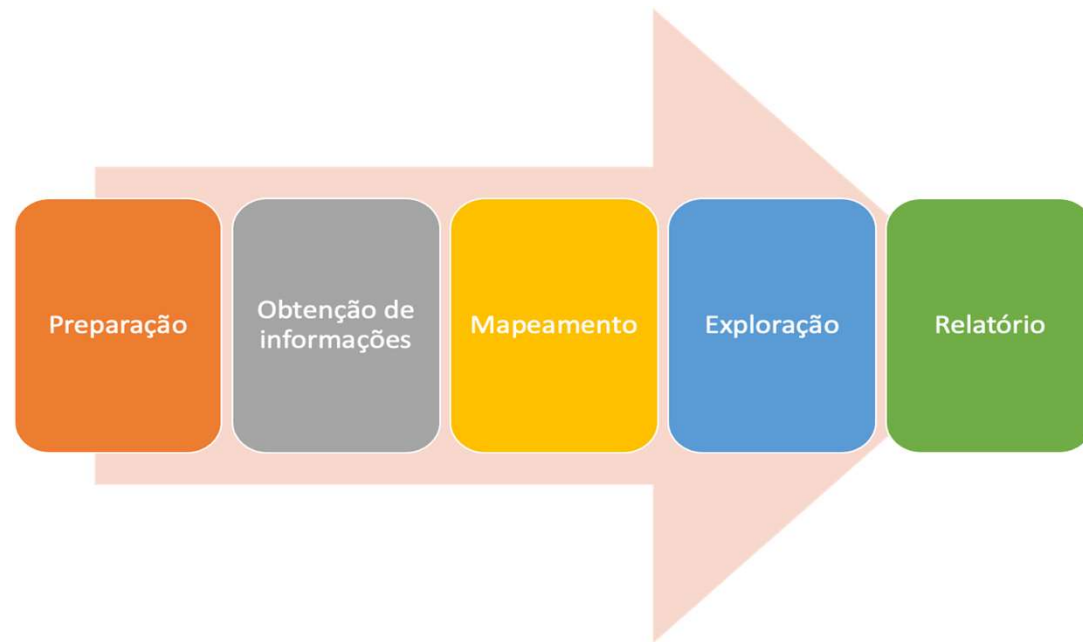
- Há diferentes testes de segurança, como as análises e avaliações de riscos, e as análises de vulnerabilidades, que focam tradicionalmente em aspectos tecnológicos.
- Para a Open Web Application Security Project ([OWASP](#)), que foca em [aplicações Web](#), teste de segurança é o processo de comparar 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).

Testes de segurança

- Os testes de segurança, que 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.



Testes de segurança típico



Fonte: adaptado(OWAST, 2019).

Testes de segurança Interno – 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,

Testes de segurança Interno – Análise de Vulnerabilidades

- 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).
- 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).

Testes de segurança Interno – Análise de Vulnerabilidades

- 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.

Testes de segurança Interno – Análise de Vulnerabilidades

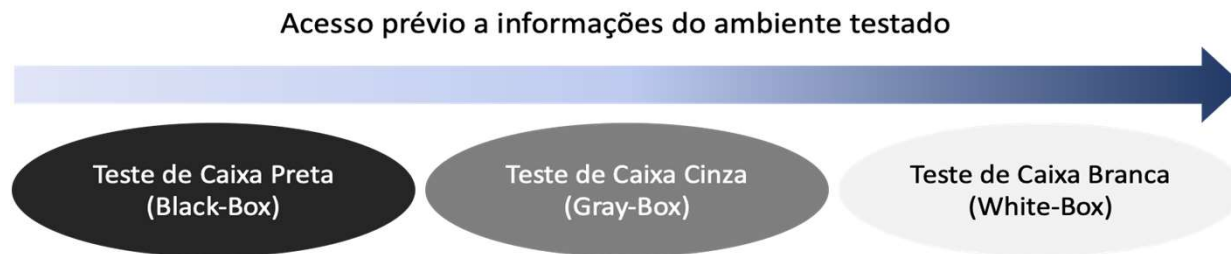
- Os resultados são referentes, principalmente, a problemas de [confidencialidade no trânsito](#), de [autenticação e autorização](#), além de [erros de configuração do servidor](#) (OWASP, 2019).
- O [SAST](#) e [DAST](#) podem ser adotados pelas próprias equipes de desenvolvimento no contexto do [DevSecOp](#), 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).

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 um 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).

Pentest

- Há **três tipos de pentests**, que depende das informações do ambiente obtidas antes dos testes de segurança:



Fonte: adaptado(OWAST, 2019).

- 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 (OWASP, 2019).

Pentest

- 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 o **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).
- 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 que ser descobertas.
- Este teste é bastante comum, devido aos custos, tempo de execução e escopo do teste (OWASP, 2019).

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 de software (Software Development Life Cycle, **SDLC**) 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.



Fonte: adaptado(OWAST, 2019).

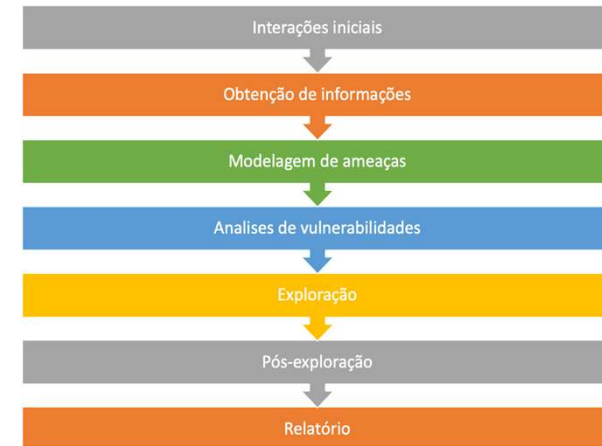
Framework da metodologia da OWASP

1. Antes do desenvolvimento	2. Definição e especificação	3. Desenvolvimento	4. Implantação	5. Manutenção e operações
<ul style="list-style-type: none">1. Definição do SDLC2. Revisão de políticas e padrões3. Desenvolvimento de métricas	<ul style="list-style-type: none">1. Revisão dos requisitos de segurança2. Revisão da especificação e arquitetura3. Criação e revisão dos modelos UML4. Criação e revisão dos modelos e ameaça	<ul style="list-style-type: none">1. Execução simulada do código2. Revisão do código	<ul style="list-style-type: none">1. Pentest da aplicação2. Teste do gerenciamento de configuração	<ul style="list-style-type: none">1. Revisão do gerenciamento operacional2. Checagem periódica3. Verificação das mudanças

Fonte: adaptado(OWAST, 2019).

Metodologia PTES

- A metodologia Penetration Testing Execution Standard (PTES) é composto por sete seções, 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.



Fonte: adaptado(PTES,2014).

Relatório

Os testes internos fazem parte do ciclo de vida de desenvolvimento de software, com atividades de segurança sendo realizados 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 complementar as 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.

Interação

Entenderam a complexidade dos testes de segurança da informação?



Fonte: <https://gifer.com/en/XIOL9>

Recapitulando

- ✓ Segurança na internet
- ✓ Proteção para Dispositivos Móveis
- ✓ Análise de vulnerabilidade e Pentest

