

**Pratique,  
aprenda,  
conquiste.**

 **Proz**  
Viva sua profissão!

Disciplina | Segurança da Informação

**Téc. Desenvolvimento de Sistemas**



**Aqui  
começa  
a sua  
jornada**

**Vamos nessa?**



Disciplina | Segurança da Informação

**Téc. Desenvolvimento de Sistemas**

# SUMÁRIO

<b>A SEGURANÇA DA INFORMAÇÃO.....</b>	<b>4</b>
<b>INTRODUÇÃO.....</b>	<b>4</b>
<b>TEMA 1.....</b>	<b>5</b>
Segurança da Informação e suas características.....	5
<b>TEMA 02.....</b>	<b>11</b>
Políticas de Segurança.....	11
<b>TEMA 03.....</b>	<b>19</b>
Planos de Contingência.....	19
<b>TEMA 04.....</b>	<b>25</b>
Identificação de Vulnerabilidades.....	25
<b>TEMA 05.....</b>	<b>32</b>
Criptografia.....	32
<b>TEMA 06.....</b>	<b>41</b>
Engenharia Social.....	41
<b>TEMA 07.....</b>	<b>50</b>
Segurança em Redes de Computadores e Dispositivos Móveis.....	50
<b>TEMA 08.....</b>	<b>63</b>
LGPD (Lei Geral De Proteção De Dados).....	63
<b>TEMA 09.....</b>	<b>68</b>
Footprint – Descoberta de Informações.....	68
<b>TEMA 10.....</b>	<b>74</b>
Testes de Penetração e Vulnerabilidades.....	74

# A SEGURANÇA DA INFORMAÇÃO



## INTRODUÇÃO

No mundo digital em constante evolução, a segurança da informação tornou-se um tema essencial e uma preocupação fundamental para empresas, organizações e indivíduos. A rápida expansão da tecnologia e a interconexão global aumentaram a quantidade de informações e dados transmitidos e armazenados eletronicamente. No entanto, essa crescente dependência da tecnologia também trouxe consigo uma série de ameaças cibernéticas cada vez mais sofisticadas.

A segurança da informação refere-se à proteção dos dados, informações e sistemas contra acessos não autorizados, uso indevido, alteração, destruição ou qualquer outra forma de comprometimento. O objetivo é garantir a confidencialidade, integridade e disponibilidade das informações, bem como a proteção da privacidade e dos direitos dos indivíduos e organizações.

As ameaças à segurança da informação são diversas e constantemente em evolução. Hackers, crackers, malware, phishing, ransomware e ataques de engenharia social são apenas algumas das ameaças que podem comprometer a segurança dos sistemas e dos dados. Além disso, fatores humanos, como negligência, erro ou má conduta, também podem representar riscos significativos.

Para garantir a segurança da informação, é necessário adotar uma abordagem holística que engloba várias camadas de proteção. Podemos incluir aí a implementação de políticas e procedimentos de segurança, o uso de tecnologias avançadas de criptografia, adoção de práticas seguras de desenvolvimento de software, realização de testes regulares de segurança e a conscientização e treinamento dos usuários.

A segurança da informação não se limita apenas às organizações, inclusive é uma responsabilidade individual. Cada pessoa que utiliza a tecnologia deve estar ciente dos riscos e adotar medidas para proteger suas informações pessoais e digitais.

Nesta era digital, em que a informação é um ativo valioso, a segurança da informação é essencial para garantir a confiança, privacidade e confidencialidade. É uma área em constante evolução, impulsionada pelo avanço tecnológico e pela crescente sofisticação das ameaças cibernéticas. Assim sendo, este módulo possibilitará conhecer os conceitos fundamentais da segurança da informação, e abrange, entre outros assuntos, o acesso a ferramentas e sistemas que facilitarão iniciar o técnicas para garantir a segurança e integridade da informação no âmbito digital.

## TEMA 1

# Segurança da Informação e suas características

### Habilidades:

- Identificar os fundamentos da segurança da informação.
- Entender a importância da informação e dados.
- Operar mecanismos de segurança da informação.



Disponível em: <<https://tinyurl.com/5hb3y7zs>>. Acesso em 16 jul. 2023.

A segurança da informação é um conjunto de medidas e práticas adotadas para proteger os dados, informações e sistemas contra ameaças, dessa forma, garante-se a confidencialidade, integridade e disponibilidade das informações. Essa disciplina visa preservar a segurança dos ativos de informação, sejam físicos ou digitais, e envolve a implementação de políticas, procedimentos, tecnologias e treinamentos. A Segurança da Informação é padronizada pelas normas da família ISO/IEC 27000, que abordam exclusivamente este tema (Sistema de Gestão e Segurança da Informação).

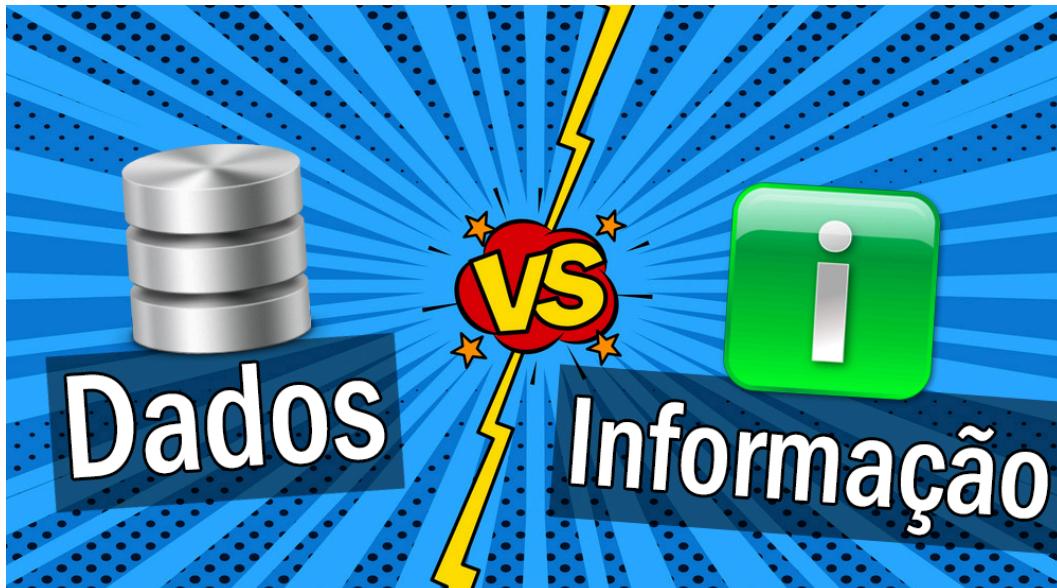
### Cyber Security

A Segurança Cibernética (Cyber Security) contempla a proteção dos dados e informações que

transitam através de um local informatizado, ou seja, é focada na defesa dos dados e informações em meios digitais. Cyber Security é uma das facetas da Segurança da Informação, já que os dados e informações não necessariamente estarão em meios físicos, como contratos físicos (papel), documentos e cartas, por exemplo, mas também em ambientes informáticos.

Tanto a Segurança da Informação quanto a Segurança Cibernética transitam não somente no meio organizacional e corporativo, assim como na nossa rotina. Compartilhamos dados a todo momento e/ou dependemos de serviços externos para requisitar ações em diversos ambientes informatizados no nosso dia a dia. Cabe a nós, da mesma forma, aprendermos a nos prevenir e a remediar os riscos.

### Conceitos-base



Disponível em: <<https://tinyurl.com/yc6c2s5y>>. Acesso em 16 jul. 2023.

Para prosseguirmos, é de extrema importância entendermos alguns conceitos.

#### Dados:

- Os dados são fatos brutos, que podem ser quantitativos ou qualitativos, como números, palavras, símbolos ou valores. Não têm contexto ou significado intrínseco.
- São tipicamente representados de forma objetiva e podem ser coletados, armazenados e processados em diferentes formatos, como planilhas, bancos de dados ou arquivos digitais.
- Podem ser estruturados, como dados organizados em tabelas, ou não estruturados, como textos livres, imagens, áudio e vídeos.

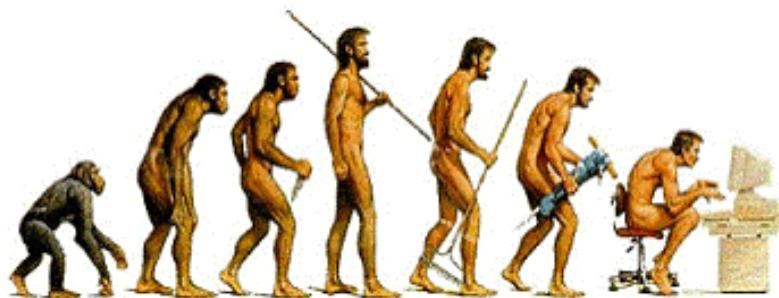
## Informação:

- A informação é o resultado do processamento e interpretação dos dados. Tem significado e contexto atribuídos a ela, o que a torna relevante e útil para as pessoas.
- É o produto da análise, organização, contextualização e interpretação dos dados. Fornece conhecimento, *insights* ou respostas a perguntas específicas.
- É comunicada de forma compreensível e utilizada para tomar decisões, obter entendimento ou fornecer suporte a determinadas ações.

Em resumo, os dados são elementos brutos e objetivos, enquanto a informação é o resultado do processamento dos dados, transformando-os significativos e úteis para as pessoas. São os componentes básicos a partir dos quais a informação é derivada, por meio da aplicação de contextos, análises e interpretações. A transformação dos dados em informação envolve a atribuição de significado, o estabelecimento de relações e a extração de *insights* para gerar conhecimento.

## História da Informação

### DA ARGILA À TELA DIGITAL :OS SUPORTES DA LINGUAGEM



Disponível em: <<https://tinyurl.com/y7evznrt>>. Acesso em 16 jul. 2023.

Na Antiguidade, a informação era transmitida principalmente de modo oral, por meio de narrativas e histórias contadas de geração em geração. Com o surgimento da escrita, por volta de 3500 a.C., a informação pôde ser registrada e preservada de forma mais duradoura. As primeiras formas de escrita incluíam pictogramas e hieróglifos, usados pelos antigos egípcios, sumérios e outros povos.

A invenção do papel, na China, por volta do século II d.C., foi um marco importante na

história da informação, o que permitiu a produção em massa de livros e documentos escritos. A imprensa, inventada por Johannes Gutenberg no século XV, revolucionou a disseminação da informação ao permitir a produção rápida e em grande escala de livros impressos. Isso desempenhou um papel crucial no avanço da Renascença e disseminação do conhecimento científico durante o Iluminismo.

No século XIX, a telegrafia e o telégrafo foram introduzidos, o que possibilitou uma forma rápida de comunicação à distância. Esse desenvolvimento foi seguido pelo telefone, no final do século XIX, e rádio, no início do século XX, e isso ampliou ainda mais as oportunidades de comunicação em tempo real.

Entretanto, a verdadeira revolução na história da informação ocorreu com o advento dos computadores e da internet no século XX. A criação dos primeiros computadores eletrônicos, como o ENIAC, na década de 1940, permitiu o processamento rápido e automatizado de informações. A internet, desenvolvida na década de 1960, conecta computadores em rede e viabilizou a troca de informações em uma escala global.

Desde então, a tecnologia da informação tem avançado rapidamente, com o surgimento de dispositivos cada vez menores e mais poderosos, como smartphones e tablets. A digitalização de informações tornou possível o armazenamento e a transmissão de grandes quantidades de dados de maneira eficiente e acessível.

Atualmente, vivemos na chamada "era da informação", na qual o acesso à informação é amplamente disponível e a comunicação ocorre em tempo real em diferentes plataformas. A inteligência artificial, realidade virtual e computação em nuvem são apenas alguns exemplos das tecnologias que estão moldando o futuro da informação.

Em suma, a história da informação é uma jornada que abrange milênios de desenvolvimento humano, desde a comunicação oral até as tecnologias digitais modernas. Essa evolução tem desempenhado um papel principal na disseminação do conhecimento, avanço científico e transformação da sociedade como um todo.

## Pilares da Segurança da Informação

A segurança da informação é um conjunto de medidas e práticas adotadas para proteger os dados, informações e sistemas contra ameaças, e garantir a confidencialidade, integridade e disponibilidade das informações. Essa disciplina visa preservar a segurança dos ativos de informação, sejam físicos ou digitais, e envolve a implementação de políticas, procedimentos, tecnologias e treinamentos.

Existem algumas características fundamentais da segurança da informação que ajudam a moldar sua abordagem e estratégia:

- Confidencialidade: É a garantia de que as informações estejam acessíveis apenas para

pessoas autorizadas. Isso envolve a proteção contra o acesso não autorizado, o uso indevido e a divulgação não autorizada de informações sensíveis. A criptografia e autenticação são mecanismos normalmente usados para garantir a confidencialidade dos dados.

- **Integridade:** Refere-se à proteção das informações contra alterações não autorizadas ou acidentais. O objetivo é garantir que as informações permaneçam completas, precisas e consistentes ao longo do tempo. Mecanismos de controle, como assinaturas digitais e controle de versões, são usados para verificar a integridade dos dados.
- **Disponibilidade:** Diz respeito à garantia de que as informações e sistemas estejam acessíveis quando necessário. Isso envolve proteger os sistemas contra interrupções, falhas técnicas, desastres naturais e ataques maliciosos que possam afetar a disponibilidade dos serviços e dados. Estratégias de backup, redundância de sistemas e planos de recuperação de desastres são adotados para garantir a disponibilidade dos recursos de informação.
- **Autenticidade:** Remete à validade e origem das informações. É importante garantir que as informações sejam provenientes de fontes confiáveis e que não tenham sido adulteradas. Mecanismos como certificados digitais e assinaturas eletrônicas são usados para verificar a autenticidade das informações.
- **Não repúdio:** Tem o objetivo de evitar que uma pessoa negue a autoria de uma ação realizada. Isso é especialmente importante em transações eletrônicas, nas quais é necessário ter provas irrefutáveis de que uma ação foi realizada por um determinado indivíduo.

Além dessas características, a segurança da informação também envolve a implementação de controles e mecanismos de proteção, como firewalls, antivírus, detecção de intrusões, políticas de acesso e controle de privilégios.

A conscientização e a educação dos usuários também desempenham um papel fundamental na segurança da informação. Todos os envolvidos no uso de informações devem estar cientes dos riscos, conhecer as melhores práticas de segurança e adotar comportamentos seguros, como o uso de senhas fortes, a não divulgação de informações confidenciais e a atualização regular de software e sistemas.



A Segurança da Informação estuda, defende e garante a proteção dos dados e informações, de modo a preservá-las e manter o valor que lhes foi imposto. Cyber Security, ou Segurança Cibernética, tratará desta mesma defesa, porém exclusivamente em meios digitais, ou seja, protegerá as informações e dados armazenados em sistemas, estudando maneiras de prevenção de interrupções de serviços informáticos, ataques hackers, entre outros. A S.I. é baseada em pilares, que são a confidencialidade, integridade, disponibilidade, autenticidade, legalidade e determinam a

organização e padronização do ambiente organizacional.



Link: [https://www.youtube.com/watch?v=d5pl8v\\_CMsM](https://www.youtube.com/watch?v=d5pl8v_CMsM)



### ATIVIDADE DE FIXAÇÃO

**1.** O que é confidencialidade na segurança da informação?

- a) A proteção contra alterações não autorizadas de dados.
- b) A garantia de que as informações estejam acessíveis apenas para pessoas autorizadas.
- c) A validação da origem das informações.
- d) A proteção contra interrupções e falhas técnicas.

**2.** O que é um firewall e qual é sua função na segurança da informação?

**3.** Qual a diferença entre dados e informação?

**4.** Descreva as principais etapas envolvidas na implementação de um programa abrangente de segurança da informação em uma organização.

**5.** Explique o que é criptografia e como ela é utilizada para proteger as informações na comunicação eletrônica.

#### **Atividade em grupo:**

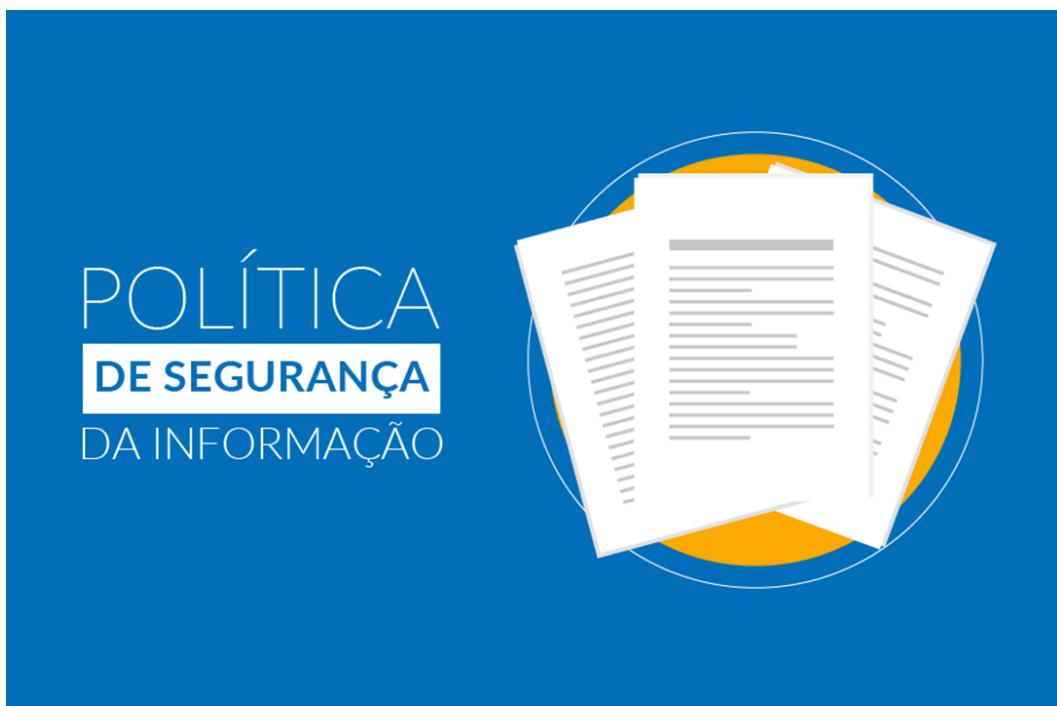
Pesquise na internet, ou outra mídia que preferir, uma notícia que envolva um crime cibernético recente no Brasil. Aponte as características deste ataque e qual ou quais pilares da Segurança da Informação foram afetados (Grupo de até 4 alunos).

## TEMA 02

### Políticas de Segurança

#### Habilidades:

- Identificar a importância de processos e métodos para a segurança digital.
- Elaborar e Planejar Políticas de Segurança.
- Entender as siglas e ferramentas usadas nas Políticas de Segurança.



Disponível em: <<https://tinyurl.com/36xe56cr>>. Acesso em 16 jul. 2023.

#### Políticas de Segurança

As políticas de segurança desempenham um papel fundamental na proteção da segurança da informação de uma organização. Elas estabelecem diretrizes, regras e procedimentos que orientam as práticas e comportamentos relacionados à segurança, enquanto fornecem um quadro de referência à implementação e gestão das medidas de segurança.

Até aqui você já consegui perceber que, nos dias de hoje, os recursos tecnológicos são vitais para qualquer negócio, assim como a informação é o bem mais precioso de qualquer empresa.

A importância que o mercado vem dando à segurança da informação de modo geral está cada vez mais intrínseca e consolidada, visto que os riscos aumentam a cada dia, assim como as exigências das legislações vigentes. Cabe à empresa se organizar e investir em boas práticas para corrigir as falhas e dar a devida proteção para seus ativos.

Segundo o dicionário, **política** é “*a arte ou ciência de governar*”, ou “*arte ou ciência da organização, direção e administração de nações ou estados*”. – Oxford Languages.

Você já deve ter conhecido alguém que diz que “odeia política”, ou até mesmo você pode ser esse alguém. Este termo é muitas vezes tratado com pessimismo, em especial, quando o assunto discutido é associado à corrupção de servidores públicos e outros governantes.

Mas tudo o que fazemos em nossas vidas é baseado em políticas. É através delas que nossa sociedade é regrada e legislada, assim como aperfeiçoamos as tomadas de decisão extremamente delicadas que surgem durante os laços sociais que são pautados e permeados.

Em uma organização também existem políticas, que servem para nortear e organizar as regras que devem ser seguidas pelos colaboradores e categorizar todos os processos de modo geral. As **políticas de segurança da informação (PSI)** vão tratar da padronização das instruções, regras e procedimentos para organizar e aumentar a proteção dos dados contra possíveis vulnerabilidades, ameaças e riscos que possam prejudicar a empresa. Estas diretrizes devem ser seguidas à risca pelos colaboradores do ambiente que reside a organização, seja física, virtual ou ambas.



Disponível em: <<https://tinyurl.com/5dearvrf>>. Acesso em 16 jul. 2023.

Uma boa política de segurança é aquela desenvolvida de acordo com o estudo do ambiente em que ela vai ser implementada. Nenhuma organização é igual a outra. Sendo assim, algumas normas que são importantíssimas para uma empresa podem não funcionar ou não serem necessárias para outra, que atua de forma diferente.

O profissional de Segurança da Informação deve estar sempre muito atento às mudanças e desenvolvimento da empresa, assim como deve estar antenado com a legislação e, principalmente, se a política a ser implantada está devidamente baseada nos pilares da segurança da informação citados anteriormente. As políticas de segurança implementadas devem sempre ser analisadas em

tempos predeterminados a fim de definir possíveis mudanças.

## Mecanismos de Segurança

Antes de qualquer coisa, o profissional de S.I. deve estar munido do conhecimento dos mecanismos de segurança, que são as ferramentas, soluções e ações com o objetivo de implementar a política de segurança, realizar qualquer tarefa relacionada à Segurança da Informação e Cyber Security de maneira correta e garantir que os 5 pilares da S.I. sejam preservados.



Disponível em: <<https://tinyurl.com/3tx9344y>>. Acesso em 16 jul. 2023.

Podemos definir os mecanismos de segurança em 4 partes fundamentais:

- **Prevenção** – É um conjunto de práticas adotadas para impedir que os ataques cibernéticos realmente aconteçam. Por meio dela, o profissional de S.I. irá elaborar barreiras para impedir que pessoas não autorizadas acessem um local físico ou em algum sistema operacional, o que limita o ambiente ao máximo. Podemos dividir a prevenção em dois pilares principais.
- **Identificação** – Pilar responsável por solicitar o login para o usuário em um sistema ou rede. Através dele que o ambiente identifica quem está acessando naquele momento, justamente para evitar que seja um atacante ou outra pessoa indesejada.
- **Autenticação** – Assim que o usuário é devidamente identificado pelo login, o ambiente de controle solicita uma senha de acesso. Caso esta senha seja a mesma que foi armazenada anteriormente no banco de dados, o usuário é autenticado e seu acesso, permitido.

- **Controle de Acessos** – Responsável por barrar quaisquer acessos que não sejam autorizados. É neste pilar onde se concentra a proteção dos dados e informações já que só manuseia o ambiente caso este permita. Um exemplo de controle de acessos é o próprio Firewall, que ainda veremos neste conteúdo.

- **Mitigação** – É a base que tem como objetivo diminuir os impactos dos ataques a um ambiente informático de uma organização. Estes impactos possuem relação com as vulnerabilidades, riscos e ameaças que vimos no tema anterior são um conjunto de práticas e ações contínuas responsáveis por catalogar e notificar os problemas que já existem no ambiente organizacional.

- **Auditoria** – Procedimento base realizado para classificar as atividades onde envolveram algum tipo de ameaça ou uso suspeito para o sistema ou rede, cataloga os eventos, facilita o processo de desenvolvimento ou alteração nas políticas de segurança. Nesta etapa, são realizados testes como os *pentests*, que veremos posteriormente, os quais irão simular ataques cibernéticos realizados por hackers com o objetivo de identificar possíveis falhas ou brechas, e também os scanners de vulnerabilidades, encarregados por realizar uma varredura no ambiente auditado a fim, também, de buscar alguma ameaça.

- **Recuperação** – Este é um dos mais importantes mecanismos de segurança e, por muitas vezes, esquecidos pelos responsáveis. Por mais que exista inúmeras ferramentas importantes para aprimorar a segurança da informação, nenhuma é 100% confiável e vai garantir que o sistema ou rede seja atacado. É necessário estar preparado para uma possível perda de arquivos contendo dados e informações. Por isso que existe a recuperação, capaz de retomar os serviços da organização de maneira ágil através de técnicas de recuperação de dados e informações.

Os meios de recuperação mais comuns são:

**Disaster Recovery** – Recuperação em Desastres é um conjunto de rápidas medidas que devem ser tomadas e foram previamente preparadas com o objetivo de restabelecer o funcionamento do ambiente ou serviço o mais rápido e com o mínimo de investimento e prejuízo possível.

**Backup** – Procedimento de cópia de arquivos importantes para o funcionamento do ambiente, assim como dados e informações críticos. As cópias podem ser armazenadas tanto em dispositivos físicos, como em HDs externos, como também na nuvem (Armazenamento Cloud). Tem como foco preservar estes conteúdos caso aconteça algo com o ambiente que o afete. A rotina de backup pode ser definida através da própria política de segurança, na qual os responsáveis irão avaliar o tempo necessário entre backups. Isso varia para cada organização.

## Planejamento e levantamento de requisitos

Para se implementar uma política de segurança da informação, é necessário a princípio um bom planejamento, juntamente com os mecanismos de segurança. Conforme dito acima, uma empresa é diferente da outra e sempre sofre mudanças.

A equipe de S.I. deve levantar todas as necessidades, problemas, práticas de cada setor e as falhas dos colaboradores do local, de modo a preparar uma PSI entendível e aplicável, além de monitorá-la e alterá-la sempre que necessário.

Para levantar os requisitos, precisaremos identificar os ativos de dados e informação de toda a empresa, assim como analisar as tarefas e procedimentos que já são tomados para ter um real diagnóstico das vulnerabilidades existentes e definir quais mudanças podemos fazer para aperfeiçoar a segurança de cada setor.

### **Alguns exemplos de levantamentos são:**

- Verificar se a empresa realiza backups e caso sim, em qual intervalo de tempo e onde este backup é armazenado;
- Checar a vigilância, monitoramento e controle de acesso em diferentes setores e áreas críticas que envolvem riscos (ex: Sala de servidor, área contendo disjuntores de energia, etc);
- Analisar os softwares e antivírus instalados nos computadores e servidores, além de checar se são originais e se há atualizações disponíveis;
- Como funciona o gerenciamento de logins, senhas e demais credenciais de controle de acesso.

Percebeu como estes levantamentos impactam todos os setores da organização? Por intermédio deles, podemos desenvolver as políticas de segurança para que todos sejam engajados a praticá-las.

## **Classificação de ativos de informação**

Esta etapa aplicará a organização dos dados e informações da empresa por diferentes grupos, nos quais os hierarquiza de acordo com o nível de cada colaborador. Lembre-se que podemos ter mais ou menos grupos, conforme cada organização.

Podemos definir os grupos essenciais como:

**Públicos:** Acessíveis a todos.

**Internos:** Acessíveis apenas ao setor responsável.

**Secretos:** Acessível apenas a um agrupamento seletivo bem definido. Inacessíveis aos demais

**Confidenciais:** Acessíveis apenas a um menor agrupamento também seletivo e bem definido. Inacessíveis aos demais. Tendo esses grupos bem estabelecidos e organizados, será possível criar ou aperfeiçoar os níveis de acesso e reforçar a segurança em grupos críticos. Estes níveis de acesso são pautados na maneira em que o funcionário se desloca a cada área da empresa e, também, em que ele usa a rede.



Link: <https://tinyurl.com/3tr6rpye>

## Desenvolvimento de Regras

Com todo o planejamento elaborado e os dados devidamente classificados e organizados, chegamos na etapa da criação de normas. Esta irá abranger todo o comportamento dos funcionários perante os recursos digitais e não digitais da empresa. As normas poderão, inclusive, serem classificadas de acordo com o setor e nível hierárquico do local. Alguns exemplos de regras que podem ser implementadas:

- Negar acesso em setores críticos;
- Impedir o uso de celulares em setores específicos ou toda a empresa;
- Bloquear sites inadequados;
- Avaliação periódica dos computadores dos funcionários;
- Limitar o uso de programas para cada funcionário e setor.

## Alinhamento final

Finalizada todas as etapas anteriores, chegou a hora de apresentar seu trabalho! É neste momento em que todo o processo será novamente revisado e aprovado pela diretoria e pelo RH. Todo o planejamento deve estar muito bem documentado para os setores críticos analisarem sua implementação juntamente com as políticas já existentes, como as políticas de funcionários e leis trabalhistas vigentes.

## Implementação e treinamento

Com tudo aprovado, será implantada a mais nova Política de Segurança. Esta é uma das mais delicadas etapas, já que a conscientização e comunicação são essenciais para o sucesso.

A política deve ser documentada e divulgada aos setores e devidamente comunicada a todos os colaboradores, explicada de maneira concisa. A abordagem deve apresentar o que está envolvido e as normas e consequências do descumprimento das mesmas, assim como existem nas demais políticas e leis.

É nessa etapa inclusive que a empresa deve se preparar para treinar seus colaboradores à

nova política, assim como preparar tutoriais aos novos que virão. Isso facilitará a propagação e conscientizará o time a seguir todas as normas de segurança, e garantir que todos estejam alinhados. É interessante a diretoria solicitar aos seus funcionários uma assinatura em forma de termo, se comprometendo a cumprir as novas políticas de segurança e dando ciência das consequências de não as seguir.

Durante a implementação e periodicamente após dela, deve-se avaliar os times para sanar eventuais dificuldades e analisar pontos a serem melhorados. Este alinhamento e correção inicial são fundamentais para que estas ocasiões se tornem rotinas futuramente, o que gera vulnerabilidades.

## Controle e Monitoramento

Por fim, compreendemos que a Política de Segurança da Informação é uma das que mais devemos nos atentar. Como está paralelamente ligada à tecnologia e ao meio digital, os profissionais devem se atualizar periodicamente. Novas ameaças surgem todos os dias, assim como novas atualizações e processos.

Nenhuma política é imutável, ou seja, o setor de T.I. deverá atualizar a empresa na mesma proporção que novas tecnologias e ameaças são apresentadas. Desde mudar de antivírus ou até mesmo alterar a periodicidade dos backups, por exemplo. Todas as atualizações vêm para somar e garantir ainda mais a segurança dos ativos de informação.



## RESUMO

As políticas de Segurança da Informação são um conjunto de regras e normas responsáveis por padronizar e diminuir as chances de ataques cibernéticos e acidentes e envolvem os ativos de informação da organização.

Existem as etapas de Planejamento e Levantamento, Classificação, Desenvolvimento, Alinhamento, Implementação e Treinamento e Controle e Monitoramento dos procedimentos, responsáveis por guiar o profissional de S.I. a traçar um plano de política exclusivo e personalizado para cada ambiente organizacional.

## Desafio

Reúnam-se em grupos e imaginem o funcionamento da escola de vocês. Pensando como profissionais de Segurança da Informação, criem novas políticas de segurança para o local em que vocês estudam.



## ATIVIDADE DE FIXAÇÃO

1. O que são políticas de Segurança da Informação e qual é a sua importância em uma organização?
2. Cite três elementos essenciais que devem estar presentes em uma política de Segurança da Informação.
3. Qual é a relação entre as políticas de Segurança da Informação e a proteção dos dados e informações de uma organização?
4. Por que a conscientização e o treinamento dos funcionários são importantes no contexto das políticas de Segurança da Informação?
5. Explique como as políticas de Segurança da Informação contribuem para a conformidade legal e regulatória de uma organização.

## TEMA 03

### Planos de Contingência

#### Habilidades:

- Entender as estruturas dos documentos de contingência.
- Elaborar planos de contingência.
- Compreender e desenvolver relatórios de níveis de risco e prevenir riscos.



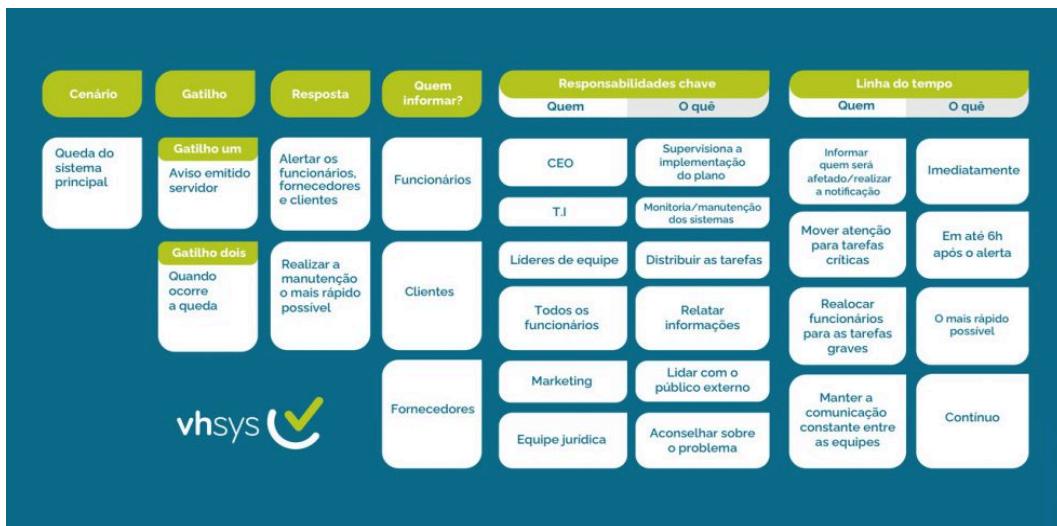
Disponível em: <<https://tinyurl.com/2p825rsb>>. Acesso em 16 jul. 2023.

Planos de contingência na segurança da informação são documentos que estabelecem diretrizes e procedimentos a serem seguidos em casos de incidentes ou situações de emergência que possam comprometer a segurança dos dados e sistemas de uma organização. Estes planos visam minimizar os impactos dos eventos adversos, o que possibilita uma resposta rápida e eficiente para proteger a integridade, confidencialidade e disponibilidade das informações.

Os planos de contingência são essenciais para garantir uma resposta adequada a incidentes de segurança da informação. Eles permitem uma ação rápida e coordenada, o que minimiza os danos causados por incidentes e reduz a interrupção das operações da organização. Ao implementar e manter planos de contingência eficazes, as organizações demonstram seu compromisso com a segurança da informação e sua capacidade de lidar com situações adversas de forma eficiente.

Você pode acompanhar no tema anterior que políticas de segurança são essenciais para a

Segurança da Informação. A prevenção é um dos fundamentos mais importantes para evitar desastres com os ativos de informação.



Disponível em: <<https://tinyurl.com/2uw4djsc>>. Acesso em 16 jul. 2023.

O objetivo de um plano de contingência é traçar estratégias corretivas, ou seja, é definir as atitudes para incidentes correlativos com falhas de segurança, como vazamento de dados, ataques em aplicações e interrupções de serviço indesejadas que trarão prejuízo ao negócio. Do mesmo modo que a política de segurança é moldada para um negócio específico, um plano de contingência será feito na medida das preocupações compreendidas.

O processo de desenvolvimento de planos de contingência se dá, basicamente, por alguns passos básicos: o levantamento, organização e classificação, elaboração dos planos para cada ameaça encontrada, documentação e testes.

**Um plano de contingência geralmente inclui as seguintes etapas:**

- **Identificação de ameaças**: Nessa fase, são identificadas as ameaças potenciais que podem afetar a segurança da informação, como ataques cibernéticos, desastres naturais, falhas de hardware ou software, entre outros.
- **Avaliação de riscos**: Processo que envolve a análise das ameaças identificadas, considerando sua probabilidade de ocorrência e impacto potencial nos sistemas e dados. Com base nessa análise, os riscos são classificados de acordo com sua criticidade.
- **Definição de estratégias de resposta**: Com base na análise de riscos, são estabelecidas estratégias de resposta para cada tipo de ameaça. Isso pode incluir ações de mitigação, como a instalação de firewalls ou sistemas de backup, ou medidas de resposta, como a interrupção de serviços ou a ativação de equipes de resposta a incidentes.
- **Elaboração dos procedimentos de resposta**: Nessa etapa, são definidos os procedimentos detalhados que devem ser seguidos em cada tipo de incidente. Podemos apontar como a designação

de responsabilidades, comunicação de emergência, recuperação de sistemas e dados, e investigação e análise de incidentes.

- Treinamento e conscientização: É fundamental que todos os envolvidos na organização sejam treinados e estejam cientes dos procedimentos de contingência. Isso engloba a realização de exercícios de simulação e treinamentos regulares para garantir que as equipes estejam preparadas para lidar com os incidentes.
- Testes e revisões: Os planos de contingência devem ser testados periodicamente para garantir sua eficácia. Testes de simulação, como exercícios de resposta a incidentes, ajudam a identificar falhas e ajustar os procedimentos, se necessário. Além disso, é importante revisar os planos regularmente para garantir que estejam atualizados e alinhados com as mudanças no ambiente de segurança.



Disponível em: <<https://tinyurl.com/4d3zc552>>. Acesso em 16 jul. 2023.

## Levantamento

Nesta etapa, será realizado todo o levantamento de todos os ativos que podem passar por algum momento de crise e impacte diretamente no ciclo de trabalho, como computadores, servidores, serviços e aplicações, rede de internet, etc. Aqui também é importante acrescentar os fatores humanos, e quais tarefas impactam o meio.

## Classificação e Organização

Com todos os ativos críticos coletados, chegou a hora de organizá-los para definir quais são os mais propensos a serem interrompidos do que outros e definir o nível de risco para cada um, e priorizar as que demandam de mais atenção. Aqui também será descrito de que forma cada falha atua.

MATRIZ DE RISCO					
PROBABILIDADE/ IMPACTO	EXTREMO	ALTO	MODERADO	BAIXO	NULO
EXTREMO	8	7	6	5	4
ALTO	7	6	5	4	3
MODERADO	6	5	4	3	2
BAIXO	5	4	3	2	1
NULO	4	3	2	1	0

REFERÊNCIA	PONTUAÇÃO
EXTREMO	4
ALTO	3
MODERADO	2
BAIXO	1
NULO	0

Elaborado pelo próprio Autor

Uma das ferramentas mais utilizadas para mapearmos os riscos encontrados no cotidiano com os ativos de informação é a matriz de risco. Matriz de risco é uma ferramenta capaz de classificar o nível de risco em pontos, o que permite ao profissional de segurança priorizar cada problema e facilitar o desenvolvimento de um plano de contingência para cada risco identificado.

A matriz é definida a partir de 2 (dois) critérios: a **probabilidade**, que representa a possibilidade de o risco acontecer, e o **impacto**, que é a consequência causada por ele. Enquanto a probabilidade fica na coluna(x), o impacto fica na linha(x). Os atributos vão do nulo ao extremo, e cada um representa uma porcentagem de chance.

- Nulo/Insignificante – 10%
- Baixo – 20%
- Moderado – 50%
- Alto – 70%
- Extremo – 90/100%

A compreensão de riscos é diferente para cada empresa, por isso, cada organização deve fazer a sua e tirar as conclusões cabíveis perante os níveis de probabilidade e impacto.

## Desenvolvimento dos planos de contingência

Agora que temos nossos ativos organizados e classificados, podemos iniciar o processo de desenvolvimento de ações necessárias para mitigar ou impedir que tais falhas aconteçam. Caso, por exemplo, ocorra uma falha que acarrete na exclusão de alguns dados do banco, quais as ações necessárias para que os desenvolvedores consigam realizar o procedimento de backup e retomam o serviço o mais rápido possível.

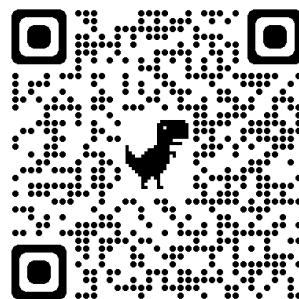
## Documentação

Aqui, elaboramos um documento que abordará o passo a passo de resolução para cada problema classificado, ou seja, o que precisa ser feito se cada falha citada acima for iminente. É

necessário que esta documentação seja muito clara para que cada setor comprehenda perfeitamente o que fazer caso ocorra algo.

## Testes

Nesta última etapa, realizaremos os testes para averiguar se os planos de contingência criados realmente funcionam. Normalmente, simulações das situações-problema são realizadas e os planos de contingência aplicados, analisando se todos os procedimentos, realmente, resolverão o problema.



Link: <https://tinyurl.com/2p8njs6v>



## RESUMO

Os planos de contingência possuem um papel fundamental em todos os contextos institucionais. Eles são competentes para projetar táticas que solucionarão ou irão atenuar circunstâncias críticas no dia a dia, que podem afetar diretamente a proteção dos dados. As estratégias de contingência são absolutamente cruciais em qualquer esfera corporativa. São responsáveis por formular abordagens que enfrentarão ou irão suavizar eventos de crise na rotina, que podem influenciar diretamente na segurança dos dados.

## Desafio

Imagine uma situação em sua sala de aula/laboratório de informática, que pode ocasionar algum tipo de interrupção, prejudicando a você e seus colegas. Crie um plano de contingência para esta situação-problema utilizando os passos que você viu acima.



## ATIVIDADE DE FIXAÇÃO

1. O que é um plano de contingência na segurança da informação e qual é o seu propósito principal?

2. Quais são os elementos-chave que devem ser considerados ao desenvolver um plano de contingência eficaz?
3. Por que é importante treinar e conscientizar as equipes sobre os procedimentos de um plano de contingência?
4. Explique a importância de realizar testes e exercícios de simulação em um plano de contingência.
5. Cite três exemplos de situações de emergência que podem requerer a ativação de um plano de contingência na segurança da informação.

## TEMA 04

### Identificação de Vulnerabilidades

#### Habilidades:

- Entender as principais ameaças e vulnerabilidades atuais.
- Identificar fatores de riscos digitais e humanos.
- Entender sistemas de defesa e resolução de falhas digitais e humanas.



Disponível em: <<https://tinyurl.com/yc6h8yhc>>. Acesso em 16 jul. 2023.

É inevitável não falarmos sobre vulnerabilidades quando mencionamos a Segurança da Informação e Cyber Security. Com o aumento e agressividade dos ataques a cada dia, o profissional de S.I. sempre deve estar atento a todo o ambiente.

A identificação de vulnerabilidades é um processo essencial na área de Segurança da Informação. Por meio desse processo, é possível identificar falhas, fraquezas e lacunas nos sistemas, redes e aplicativos, o que permite que medidas de proteção sejam tomadas antes que sejam exploradas por ameaças maliciosas. Esta apostila fornecerá uma visão geral dos elementos fundamentais da identificação de vulnerabilidades.

É preciso compreender como identificar e categorizar uma vulnerabilidade, pressentir as prováveis ameaças que ela pode trazer, gerando riscos em potencial aos ativos de informação.

## O que são vulnerabilidades?

São pontos fracos em sistemas ou redes que podem ser explorados por ameaças para comprometer a Segurança da Informação. Essas vulnerabilidades podem incluir falhas de software, configurações incorretas, deficiências na infraestrutura de rede e outros fatores que podem ser explorados para obter acesso não autorizado, comprometer a integridade dos dados ou interromper os serviços.

## Importância da identificação de vulnerabilidades

A identificação de vulnerabilidades é crucial para a Segurança da Informação, pois facilita que as organizações ajam proativamente para mitigar riscos e evitar possíveis ataques. Ao identificar e corrigir vulnerabilidades, é possível reduzir as chances de violações de segurança, minimizar impactos negativos e proteger ativos críticos de informações.

## Métodos de identificação de vulnerabilidades

Existem diferentes métodos e ferramentas disponíveis para a identificação de vulnerabilidades.

### Alguns dos métodos comumente utilizados incluem:

- Scanners de vulnerabilidades: Ferramentas automatizadas que examinam sistemas, redes ou aplicativos em busca de vulnerabilidades conhecidas.
- Testes de penetração: Processo controlado que simula um ataque real para identificar e explorar vulnerabilidades existentes.
- Análise de código: Revisão do código-fonte de um software em busca de falhas e vulnerabilidades.
- Análise de configuração: Avaliação das configurações de sistemas e redes para identificar erros de configuração que possam criar vulnerabilidades.

## Ciclo de Identificação de Vulnerabilidades

O ciclo de identificação de vulnerabilidades envolve as seguintes etapas:

- Planejamento: Definição de escopo, objetivos e métodos para a identificação de vulnerabilidades.
- Coleta de informações: Reunião de dados relevantes sobre os sistemas, redes e aplicativos a serem analisados.
- Análise: Avaliação das informações coletadas para identificar vulnerabilidades e determinar seu impacto potencial.

- Classificação: Classificação das vulnerabilidades identificadas com base em sua gravidade e prioridade.
- Relatório: Elaboração de um relatório detalhado que descreve as vulnerabilidades identificadas, suas possíveis consequências e recomendações para mitigação.

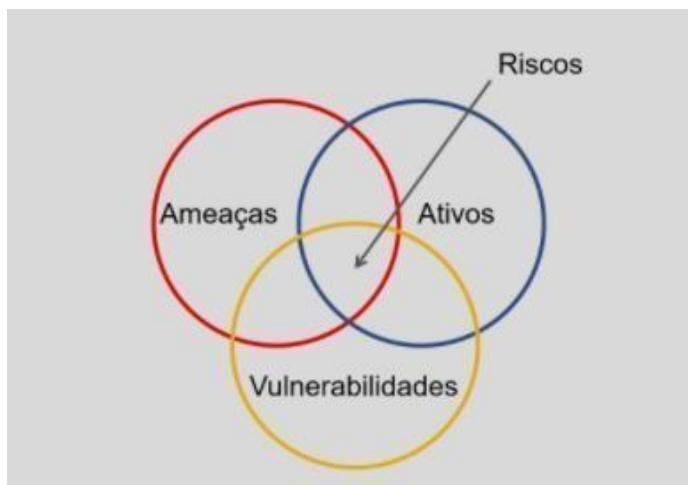
## Ameaças

As **ameaças** são os resultados das vulnerabilidades. Seja de modo intencional ou acidental, elas exploram as brechas, o que pode causar danos aos ativos de informação.

## Riscos

Os **riscos** são as possíveis resultantes das ameaças caso estas sejam realmente iminentes. É a futura concretização do dano, acesso não autorizado ou destruição dos ativos na hipótese que estes não sejam mitigados e tratados.

A lógica é a seguinte: Se você tem um ativo que está sendo ameaçado devido a uma vulnerabilidade, logo o ativo está em risco. A fórmula usada para contextualizar é:



Disponível em: <<https://tinyurl.com/52h3hz3b>>. Acesso em 16 jul. 2023.

Sendo assim, podemos concluir que o risco é o resultado de uma ameaça que abusa de uma vulnerabilidade. Se não existirem vulnerabilidades, dificilmente haverá riscos.

A identificação das vulnerabilidades servirá, justamente, às correções das brechas e falhas que foram antecipadamente analisadas e classificadas pelo profissional de S.I. Estas correções irão partir de uma estratégia operacional e educacional que implementará todas as medidas necessárias para tratar este ambiente e torná-lo mais robusto a novas vulnerabilidades que possam surgir no futuro. Ela garantirá a saúde da infraestrutura e aplicações da empresa de modo geral.

Mas, afinal, como identificamos vulnerabilidades?

## Identificação de Vulnerabilidades

Antes de tudo, devemos nos atentar e estudar as fragilidades do ambiente organizacional. Partimos, a princípio, do levantamento dos ativos de informação e sua análise total. Desde os próprios dados e informações armazenados, como os servidores e outros equipamentos. Após isso, abordaremos o ambiente da organização para identificar as falhas. Alguns apontamentos que podemos realizar são os seguintes:

**Gestão humana** – Uma empresa não é feita simplesmente de equipamentos e aplicações. Precisamos de colaboradores que realizem sua função de maneira segura e exatamente de acordo com o que lhe foi ensinado e instruído. Por isso, devemos nos atentar em alguns pontos:

- Analisar a conduta dos usuários ao utilizarem sistemas operacionais;
- Checar se há um controle hierárquico de acessos, sejam eles virtuais ou físicos;
- Ver se a empresa oferece treinamentos para que os usuários utilizem ferramentas e sistemas;
- Analisar o cotidiano para checar se estas condutas e orientações são realmente feitas ou se há más práticas que devem ser revistas.

**Softwares e Hardwares desatualizados** – A organização deve sempre estar atenta aos sistemas e dispositivos operadores. A falta de reparos e atualizações acarreta em diversas vulnerabilidades, já que, ao longo do tempo, novas tecnologias mais seguras tomam conta do mercado e as antigas perdem suporte e se tornam obsoletas e inseguras. Veja abaixo alguns pontos:

- Checar qual sistema operacional está instalado nos computadores e se estão com as atualizações em dia;
- Avaliar as condições físicas dos equipamentos como computadores e servidores, e se necessitam de reparos, upgrades, limpeza ou substituição;
- Verificar se existe um Firewall e/ou antivírus em todos os equipamentos;
- Analisar se há um monitoramento na infraestrutura de rede;
- Verificar se a empresa está conforme a legislação vigente no âmbito da Segurança da Informação.

## Ambiente

Por incrível que pareça, fatores ambientais podem incidir em vulnerabilidades. Veja alguns levantamentos de ambiente abaixo:

- Analisar as condições de temperatura para o pleno funcionamento de dispositivos informáticos como computadores e servidores;
- Verificar as condições de estrutura do local para desastres naturais como incêndios e enchentes;
- Analisar se a empresa possui algum tipo de controle perante quedas súbitas de energia.

Após identificarmos as vulnerabilidades, devemos categorizá-las para modelar e arquitetar as estratégias às devidas resoluções. Há diversas maneiras de categorizar e avaliar vulnerabilidades. Iremos utilizar o Microsoft Stride, pois é o mais popular

O método Stride utiliza seu nome para definir seu conceito. Cada letra aponta a uma ameaça em potencial causada por uma vulnerabilidade e que traz os riscos de violação.

**S – Spoofing:** falsificação de identidade e dados.

**T – Tampering:** Adulteração de dados e informações.

**R – Repudiation:** Repúdio.

**I – Information Disclosure:** Exposição de dados e informações confidenciais.

**D – Denial of Service:** Ataques voltados à negação de serviço.

**E – Elevation of privilege:** Elevação de privilégio.

Com essa modelagem, os profissionais poderão analisar e enumerar as ameaças e vulnerabilidades e priorizar as que demandam mais urgência.

Após realizarmos o procedimento de identificação e categorização das vulnerabilidades, poderemos remediá-las e tomar medidas de conscientização a partir das políticas de Segurança da Informação, que já aprendemos anteriormente. Assim, os profissionais de T.I. irão conseguir investigar e reduzir as vulnerabilidades, as ameaças e os riscos, e resolvê-los o mais breve possível.

Lembre-se que cada organização possui um ambiente diferente e pendências de segurança diferentes a serem resolvidas, ou seja, as medidas que devem ser tomadas poderão ter o leque aberto ou específico para cada situação.

Algumas medidas que podemos tomar após levantarmos as vulnerabilidades são:

- Criar ou atualizar políticas de segurança com foco em resolver vulnerabilidades
- Investimento no treinamento dos usuários em geral, para nivelar o conhecimento e tratar os maus hábitos;
- Implantar ou rever o monitoramento para controle dos sistemas, aplicações e infraestrutura de redes, com profissionais qualificados;
- Manter os dispositivos e sistemas atualizados com antivírus e firewall de qualidade;
- Padronizar todo o ambiente para que respeite as leis vigentes.

**Desafios cibernéticos:** Através da análise, planejamento e execução de boas práticas, o profissional de S.I. diminui exponencialmente os riscos e ameaças que circundam uma aplicação, infraestrutura ou um ambiente corporativo inteiro. Reúnam-se em grupos e analise sua sala de aula ou seu laboratório de informática. Tente identificar vulnerabilidades, riscos e ameaças neste ambiente e explique com suas palavras o que poderia ser feito para sanar estes problemas.



Link: <https://tinyurl.com/mrx3ujcf>



## RESUMO

Com o avanço da tecnologia e a crescente digitalização, as ameaças e vulnerabilidades têm se intensificado, e variam de invasões cibernéticas, ataques de phishing, ransomware, até a exploração de vulnerabilidades em softwares e hardware. Por outro lado, fatores de risco humano, como a falta de treinamento adequado e comportamentos de risco, como o uso de senhas fracas ou a abertura de e-mails desconhecidos, também permitem o acesso não autorizado aos sistemas. Além disso, a implementação de tecnologias emergentes, como a Internet das Coisas (IoT) e a Inteligência Artificial (IA), aumenta a superfície de ataque, e exigem uma compreensão mais profunda dos riscos digitais associados.

Na luta contra estas ameaças, a adoção de sistemas de defesa robustos é fundamental. Isso inclui a implementação de firewalls, programas antivírus, sistemas de detecção e prevenção de intrusões, bem como a criptografia de dados. Sem contar, estratégias de defesa em profundidade, como a segmentação de redes, podem minimizar o impacto de um ataque. Do lado humano, a educação e o treinamento em segurança cibernética são fundamentais para minimizar os riscos.



## ATIVIDADE DE FIXAÇÃO

1. O que são vulnerabilidades de segurança da informação?
  
2. Qual é a importância da identificação de vulnerabilidades em um ambiente de Segurança da Informação?
  
3. Quais são algumas das principais consequências de não identificar e corrigir vulnerabilidades em um sistema?

4. Explique a diferença entre scanners de vulnerabilidades e testes de penetração.  
Quando cada um desses métodos é mais adequado para identificar vulnerabilidades?

5. Cite três exemplos de informações que podem ser coletadas durante a fase de coleta de informações no processo de identificação de vulnerabilidades. Por que essas informações são relevantes para a análise de vulnerabilidades?

## TEMA 05

# Criptografia

### Habilidades:

- Entender a importância da criptografia para a segurança da informação.
- Aprender a elaborar o pensamento lógico e conhecer as principais cifras.
- Entender sistemas de defesa e resolução de falhas digitais e humanas.



Disponível em: <<https://tinyurl.com/8hvd8x6s>>. Acesso em 17 jul. 2023.

A criptografia desempenha um papel importantíssimo na segurança digital, ao proteger informações sensíveis contra acesso não autorizado e garantir a integridade e confidencialidade dos dados. Envolve o uso de algoritmos matemáticos complexos para transformar os dados originais em uma forma ilegível, conhecida como texto cifrado.

Há dois principais tipos de criptografia utilizados na segurança digital: criptografia simétrica e criptografia assimétrica. Na criptografia simétrica, a mesma chave é usada tanto para criptografar quanto para descriptografar os dados, e exige que o emissor e o receptor compartilhem essa chave. Já na criptografia assimétrica, são empregadas duas chaves diferentes: uma chave pública para criptografar os dados e uma chave privada correspondente para descriptografá-los. Isso permite uma comunicação segura entre duas partes, mesmo que nunca tenham se encontrado antes.

A criptografia desempenha um papel essencial em várias áreas da segurança digital. Por exemplo, é amplamente utilizada em transações financeiras online para proteger informações confidenciais, como números de cartão de crédito. Além disso, é fundamental para garantir a privacidade das comunicações, seja por e-mail, mensagens instantâneas ou chamadas de voz, o que impede que terceiros interceptem e compreendam as informações transmitidas. A criptografia

também é usada em redes privadas virtuais (VPNs) para estabelecer conexões seguras em ambientes de rede não confiáveis.

## História da Criptografia

A criptografia tem uma longa história, que remonta a milhares de anos. Desde os tempos antigos, as pessoas têm usado métodos de criptografia para proteger suas comunicações e informações confidenciais.

Uma das primeiras formas de criptografia conhecidas é a cifra de César, que era usada pelo imperador romano Júlio César. Nessa cifra, cada letra do alfabeto é substituída por outra que esteja três posições à frente no alfabeto. Essa técnica simples de substituição de letras foi usada para ocultar mensagens militares.

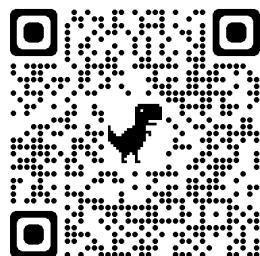
Outra forma de criptografia histórica é a cifra de Vigenère, desenvolvida no século XVI por Blaise de Vigenère. Essa cifra aplicava uma tabela de alfabetos deslocados, na qual a letra-chave determinava qual linha do alfabeto seria usada para cifrar cada letra da mensagem. A cifra de Vigenère era considerada muito segura na época e foi amplamente usada por séculos.

No entanto, o avanço significativo na criptografia ocorreu durante a Segunda Guerra Mundial, quando as máquinas de criptografia foram desenvolvidas. O exemplo mais famoso é a máquina Enigma, utilizada pelos alemães para criptografar suas comunicações militares. A equipe de criptoanalistas, liderada por Alan Turing, no projeto britânico chamado Ultra, conseguiu decifrar as mensagens da Enigma, o que foi essencial ao esforço de guerra dos Aliados.

Após a Segunda Guerra Mundial, a criptografia evoluiu rapidamente com o advento da criptografia de chave pública. Em 1976, Whitfield Diffie e Martin Hellman propuseram o conceito de criptografia assimétrica, em que duas chaves diferentes são usadas para criptografar e descriptografar dados. Essa abordagem inovadora possibilitou um novo nível de segurança e facilitou a troca de chaves em comunicações seguras.

Nos últimos anos, a criptografia desempenha um papel fundamental na segurança digital, especialmente, com o crescimento da internet e comunicações eletrônicas. Sem contar que o desenvolvimento da criptografia de curva elíptica (ECC) e a ascensão das criptomoedas, como o Bitcoin, trouxeram novas aplicações e desafios à criptografia.

Em resumo, a história da criptografia mostra a evolução das técnicas e algoritmos ao longo dos séculos, impulsionada pela necessidade de proteger informações confidenciais. Desde as cifras antigas até a criptografia moderna, essa disciplina tem sido essencial para garantir a segurança das comunicações e a proteção dos dados em várias áreas da sociedade.



Link: <https://tinyurl.com/56s4memf>

## Conceitos

Os métodos para transformar e retomar a informação ao original, respectivamente, denominamos de **encriptação** e **decriptação**, e podemos dividir os ativos de informação que passarão pelo processo de criptografia em três tipos. São eles:

**Texto Claro** - consiste no dado ou informação, o qual qualquer pessoa consegue compreender. **Texto Cifrado** – o qual o dado ou informação que passou pelo processo de cifragem, e foi convertido a um texto não legível.

**Texto Decifrado** – dado ou informação que foi convertido novamente em texto claro.

## Cifra

É um dos termos mais populares quando o assunto é criptografia. A cifra é um conjunto de algoritmos (técnicas e ações) responsáveis pela codificação ou decodificação de uma mensagem. Esta, por sua vez, normalmente envolve o embaralhamento das letras ou palavras do conteúdo da mensagem principal, e este processo pode ser revertido pela pessoa que tem o conhecimento da cifra utilizada.

## Contexto Histórico

Por mais que este termo esteja em destaque, a criptografia definitivamente não é algo novo. Desde a Antiguidade, os seres humanos já viam a necessidade de compartilhar informações com mais privacidade. Podemos separar os períodos de métodos criptográficos de acordo com sua evolução durante o tempo. São eles a **criptografia clássica** e a **criptografia moderna**.

## Criptografia clássica

Em tempos mais remotos, os mensageiros percorriam longas distâncias com o objetivo de transmitir a mensagem que lhes foi confiada. Ocorria que, por muitas vezes, eles eram alvos de pessoas mal-intencionadas no meio do caminho, no intuito de roubar, adulterar ou até mesmo destruir a mensagem a ser entregue. Dessa forma, o homem começou a planejar estratégias que impedissem que essas mensagens aparecessem claras ao atacante e, até mesmo, para o mensageiro, tornando-as inúteis a ele sem a chave para quebrar o enigma que envivia o processo. Uma das criptografias mais antigas e, também, mais populares, sem dúvidas é a Cifra de César.

## Cifra de César

A Cifra de César foi um método extremamente usado pelo exército romano para decodificar mensagens e compartilhar informações com a infantaria e generais. O processo é o seguinte: Cada letra que for escrita deve ser substituída pela 3º letra posterior. Por exemplo, a letra "A", seria substituída pela letra "D".

Veja abaixo uma tabela que mostra o alfabeto e as letras já alteradas pela cifra.

**Alfabeto Normal:**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

**Alfabeto Cifrado:**

D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Disponível em: <<https://www.interop.com.br/blog/como-proteger-pen-drive/>>. Acesso 23 jul 2023

Ao utilizarmos a Cifra de César para criptografar uma frase, ficará desta forma:

“EU ESTUDO NA ESCOLA TECNICA” – Texto claro.

“HX HVWXGR QD HVFROD WHFQLFD” – Texto criptografado pela Cifra de César.

“EU ESTUDO NA ESCOLA TECNICA” – Texto Decifrado.

As letras do alfabeto são equiparadas de acordo com a sua posição na ordem alfabética. O valor da letra "A" é D, o valor da letra "B" é E, e assim por diante. Isso significa que a letra "Z" tem o valor 26. Quando a tabela chega à última letra "Z", ela retorna à letra "A" e continua seguindo a sequência alfabética.

Com o passar do tempo e o surgimento das tecnologias de maquinários eletromecânicos, os métodos de criptografia cresceram junto, e tornaram-se cada vez mais competentes e difíceis de serem decifrados. No século XX e, mais precisamente, na Segunda Guerra Mundial, aumentou mais ainda a popularidade dos métodos de criptografia, já que houve um alto investimento em tecnologia neste período.

Uma das ferramentas mais utilizadas pelo exército alemão, sem dúvidas, foi a máquina comumente chamada de Enigma.

## Enigma



Disponível em: <<https://tinyurl.com/4n3zft8v>>. Acesso em 17 jul. 2023.

Definitivamente o maior desafio de encriptação naquela época, a Enigma era uma máquina capaz de criptografar e descriptografar informações através de seus rotores eletromecânicos. Foi desenvolvida pelo holandês Hugo Alexander Koch e aprimorada por Ritter e Scherbius.

A Enigma se assemelhava a uma máquina de escrever, porém, não era todo mundo capaz de operá-la. O técnico deveria ser cauteloso ao manuseá-la, já que era necessário alterar sua chave todos os dias e ser configurada exatamente de acordo com os manuais. O rotor no seu interior armazenava a mensagem anteriormente digitada em seu teclado, depois, outra pessoa deveria selecionar quais luzes iriam acender caso alguma tecla seja pressionada

Posteriormente, na era da Computação, já com toda sua bagagem milenar, inicia-se o período da Criptografia Moderna.

## Criptografia Moderna

Com o surgimento dos computadores e sua ampla acessibilidade, a criptografia passa a ser utilizada para fins cotidianos, e deixa de ser de uso exclusivo para militares ou de cunho governamental.

A criptografia é hoje o braço direito da S.I., sendo a ferramenta principal contra o vazamento dos ativos de informação, o que contribuiu ao impedimento de fraudes e demais usos inapropriados. É aplicável desde para proteger uma troca de mensagens até mesmo a transações que envolva criptomoedas.

Partindo agora para este contexto do Cyber Security, a criptografia é aplicada praticamente em todos os ambientes informáticos, tanto empresariais, quanto em nossas casas, navegando pela internet e respondendo e-mails. Veja abaixo alguns exemplos em que a criptografia é aplicada

atualmente:

### Criptografia SSL (Secure Sockets Layer – Camada de Soquete Seguro)

É um protocolo de criptografia utilizado em certificados digitais (chamado de Certificado SSL) de um site publicado na Web e cria uma conexão entre o servidor que comporta a aplicação e o navegador de internet. Ele criptografa os dados compartilhados pelo usuário e serviço por meio de algoritmos, o que impede que agentes mal-intencionados em potencial tentam interceptar a comunicação.



Disponível em: <<https://tinyurl.com/muvubdyr>>. Acesso em 17 jul. 2023.

### Assinaturas digitais

As assinaturas digitais são encarregadas por autenticar que uma pessoa está assinando de maneira virtual um documento, o que possibilita que arquivos críticos e demais contratos possam ser reconhecidos juridicamente, sem a necessariamente da assinatura ser física em um papel. Por estarem relacionados a uma identidade real, a criptografia está presente para legitimar a que a pessoa realmente deseja assinar o documento e visa proteger os dados e informações contidas nessa assinatura, o que dificulta que ela sofra alterações e fraudes.

### Aplicativos de troca de mensagens

Os *apps* mensageiros mais utilizados no Brasil não poderiam ficar de fora. O Whatsapp e Telegram, por exemplo, usam um método de criptografia chamado de “ponta a ponta”. Este codifica a mensagem antes de enviá-la. Assim que a mensagem chega ao destinatário, é decifrada e libera a leitura. A mensagem só pode ser decifrada e lida por este destinatário.

### VPN

As VPN's (*Virtual Private Network*) são conexões de rede privadas criadas a partir de redes públicas com o intuito de aprimorar a segurança. A criptografia entra codificando o tráfego de internet do usuário, aumentando sua privacidade enquanto navega.

### Métodos de Criptografia

Existem três tipos de criptografia, sendo que dois deles se baseiam pelas **chaves**. As chaves são os métodos específicos dos algoritmos utilizados para realizar o embaralhamento e a resolução. São elas:

#### Funções Hash

A criptografia do tipo *Hash* emprega algoritmos matemáticos que realizam a função de transformar o dado ou informação em um conjunto de caracteres alfanuméricos de comprimento fixo, e resume consideravelmente seu tamanho. É mais utilizado em métodos de autenticação por possuir alta complexidade.

Veja abaixo três dos algoritmos *Hash* mais utilizados mundialmente:

- **MD (Message Digest)** – É o algoritmo responsável por checar a integridade dos dados. A mais comum é a MD5, que trabalha com 128 bits. Porém, nos dias atuais, não é mais utilizado para criptografia, pois apresenta muitas vulnerabilidades para este fim.
- **RIPEMD** – É considerado a evolução do MD, isso porque apresenta uma quantidade de bits maior (160).
- **SHA (Secure Hash Algorithms)** – Função criptográfica encarregada por mediar a transmissão de dados e informações entre um servidor de aplicações e um cliente.
- 

#### Chave Simétrica/Privada

A chave simétrica usa apenas uma chave para criptografar e descriptografar um dado ou informação dentro do algoritmo, e apresenta uma cadeia de bits proprietária.

Possui um bom desempenho, no entanto, precisa-se substituir a chave caso ocorra alguma implicação, já que tanto o remetente, quanto o destinatário da transmissão usam a mesma chave, além de não possuir uma maneira de autenticar as pessoas envolvidas. Por isso, não é uma alternativa recomendada nos dias de hoje para encriptação de informações críticas.

#### DES

O algoritmo de encriptação simétrico do tipo DES (*Data Encryption Standard*), foi um dos primeiros a serem incluídos na programação de modo geral e instituído nos anos 70. Ele trabalha com uma chave de apenas 56 bits, atualmente, é considerado inseguro, isso porque é facilmente quebrado.

## AES

AES (*Advanced Encryption Standard*) foi uma evolução perante o DES, uma vez que permite a escolha do tamanho da chave. Esta poderia ser de 128, 192 e 256 bits, muito além dos anteriores 56 do DES.

## Chave Assimétrica/Pública

No método de chave assimétrica, a criptografia utiliza duas chaves diferentes: uma pública e outra privada. A chave pública se destina a criptografar a informação e a privada decodificar. Não há necessidade do emissor da mensagem compartilhar e/ou distribuir outras chaves para que o destinatário consiga abrir. Este é o tipo de criptografia mais complexo, porém é o mais seguro e utilizado atualmente.

## RSA

O RSA (**R**ivest, **S**hamir, **A**ndleman) é uma das referências de chave assimétrica, pois é extremamente poderosa. Funciona com a multiplicação de dois números primos para gerar as chaves privadas e públicas. Como resultado, é elaborado um número extenso que dificulta imensamente o processo de decifragem por algum agente externo.

## Diffie-Hellman

Este tipo de criptografia assimétrica foi criado por Whitfield Diffie e Martin Hellman, baseado na confiança da troca de chaves entre o emissor e destinatário de maneira não tradicional, ou seja, ambos sabem a estrutura das chaves.



Link: <https://tinyurl.com/2k62977h>

## Desafio

Decifre a mensagem abaixo com o método da Cifra de César: VHMD EHP YLQGR D HVFROD  
WHFQLFD SURILVVLRQDOLCDQWH



## RESUMO

A criptografia é uma ferramenta essencial à segurança da informação. Funcionando como uma camada protetora contra invasões, codifica dados para que sejam compreendidos apenas por quem possui a chave de decodificação. Desta maneira, é possível prevenir a violação da privacidade, fraudes e outros tipos de ataques cibernéticos, o que torna-se fundamental em um mundo cada vez mais digital e interconectado. A elaboração do pensamento lógico é uma habilidade vital para compreender e utilizar criptografia, e envolve a capacidade de pensar de maneira estruturada e racional para resolver problemas complexos. As cifras são um componente central da criptografia, que abrange técnicas de codificação e decodificação. Além disso, a compreensão dos sistemas de defesa e de como resolver falhas, tanto digitais quanto humanas, é básica para manter a segurança da informação. Esse conhecimento possibilita identificar vulnerabilidades, desenvolver estratégias de proteção eficazes e, em caso de falhas, aplicar soluções apropriadas para minimizar danos e restabelecer a segurança.



## ATIVIDADE DE FIXAÇÃO

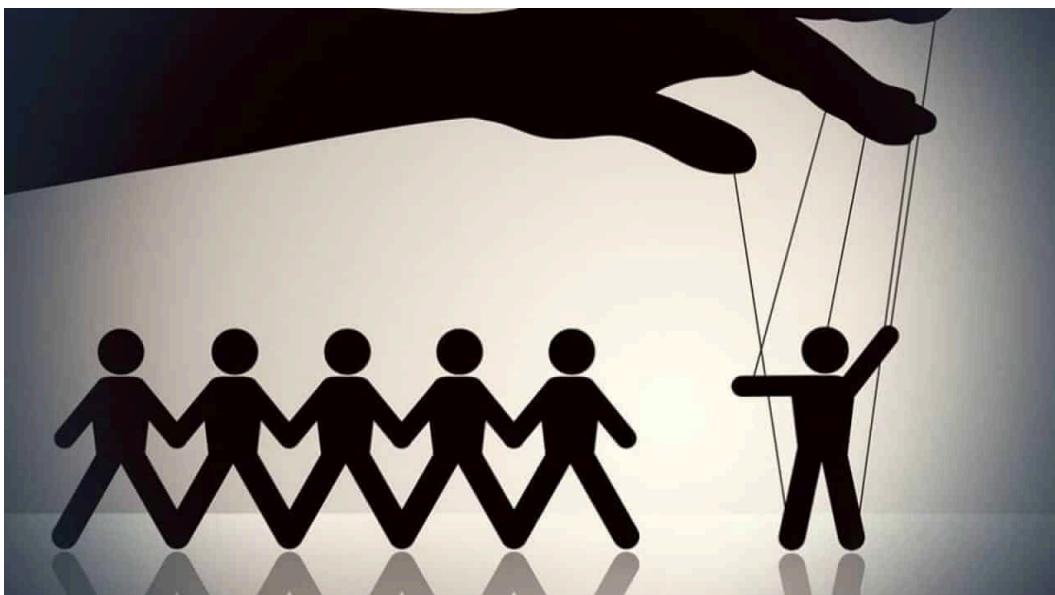
- 1.** O que é criptografia?
  
- 2.** Qual é a finalidade da criptografia na segurança da informação?
  
- 3.** Cite um exemplo de uso comum da criptografia no cotidiano.
  
- 4.** Explique a diferença entre criptografia simétrica e criptografia assimétrica. Quais são as vantagens e desvantagens de cada abordagem?
  
- 5.** Descreva o que é uma chave de criptografia e por que é importante para garantir a segurança dos dados criptografados.

## TEMA 06

# Engenharia Social

### Habilidades:

- Entender a importância da integridade e confidencialidade dos dados.
- Aprender a elaborar e decifrar armadilhas digitais e falsificações.
- Compreender e elaborar perfis para evitar golpes de engenharia social.



Disponível em: <<https://tinyurl.com/5n73h3kd>>. Acesso em 17 jul. 2023.

Até aqui você já pôde ter noção de que os ataques cibernéticos são extremamente perigosos e se tornam mais desafiadores a cada dia. A Engenharia Social, muitas vezes, faz parte deles e é uma das principais artimanhas que definem o sucesso do crime virtual.

A Engenharia Social irá abordar a manipulação psicológica das vítimas (pessoas envolvidas que sofrem o ataque), com o objetivo de adquirir informações confidenciais através do abuso da confiança, ignorância perante determinado assunto e até mesmo da ingenuidade da pessoa.

Por diversas vezes, a vítima mal percebe que está sob ataque ou seus dados se encontram em perigo. O atacante que usa da Engenharia social irá explorar o que o usuário tem de mais vulnerável e atacar esses pontos de diversas maneiras. Costuma ser alguém que se apresenta longe de qualquer suspeita, extremamente comunicativo e persuasivo. Estuda o comportamento da(s) vítima(s) e aplica técnicas psicológicas, sociais e ambientais para conseguir exatamente o que precisa.

### Contexto Histórico

A Engenharia Social é uma prática utilizada para manipular e enganar as pessoas, geralmente,

com foco em obter informações confidenciais, acesso a sistemas ou influenciar comportamentos. Sua história remonta a séculos atrás, e evolui conforme a sociedade e a tecnologia avançam.

No passado, a Engenharia Social era praticada principalmente em ambientes offline, e envolvia técnicas de persuasão e manipulação pessoal. Por exemplo, vigaristas e golpistas utilizavam truques, histórias inventadas e falsas identidades para obter a confiança das pessoas e, assim, realizar fraudes financeiras ou outros tipos de crimes.

Com o avanço da tecnologia da informação e a popularização da internet, a Engenharia Social migrou para o ambiente digital. Através de e-mails fraudulentos, chamados de *phishing*, ou de mensagens em redes sociais, os cibercriminosos tentam enganar os usuários, levando-os a revelar informações pessoais, senhas ou a executar ações prejudiciais.

A história da Engenharia Social está repleta de exemplos marcantes. Um caso famoso é o "Ataque do Cavalo de Troia" da Guerra de Troia, descrito na mitologia grega. Os gregos conseguiram entrar na cidade de Troia enviando um grande cavalo de madeira como um presente, enquanto estavam soldados em seu interior.

Atualmente, a Engenharia Social continua a evoluir e se adaptar às circunstâncias. Os cibercriminosos usam técnicas cada vez mais sofisticadas, como Engenharia Social baseada em informações obtidas de mídias sociais, Engenharia Social reversa em que eles estudam os padrões de comportamento de uma pessoa ou organização antes de lançar um ataque, e Engenharia Social de voz, na qual se utilizam técnicas de manipulação vocal em chamadas telefônicas.

A defesa contra a Engenharia Social envolve a conscientização e o treinamento dos usuários, bem como a implementação de medidas de segurança, como autenticação em dois fatores e políticas de privacidade e segurança rigorosas. Em resumo, tem uma longa história e se adaptou ao longo do tempo, enquanto se adaptava aos avanços tecnológicos. A conscientização sobre as técnicas utilizadas pelos engenheiros sociais e a adoção de medidas de segurança adequadas são fundamentais para se proteger contra esses ataques.



Link: <https://tinyurl.com/mt88bvad>

Geralmente, a pessoa que sofre o ataque se sente tão à vontade que, sem perceber, rompe o sigilo e confidencialidade anteriormente confiadas e entrega diversas informações sigilosas ou deixa a "porta aberta" para este indivíduo.

Abaixo, você verá um simples exemplo do uso da Engenharia Social que, provavelmente, você

já deve ter presenciado algo parecido no seu dia a dia.

Exemplo:

*Um número desconhecido liga para a vítima. Do outro lado da linha, um simpático atendente a parabeniza com a notícia que foi premiada com carro 0km, e que para resgatar, precisa “confirmar” alguns dados como CPF, RG, endereço e, por fim, solicita ao ganhador um depósito de determinado valor em uma conta bancária. A pessoa, ingênuo e acreditando em suas palavras, passa todos os seus dados pessoais e ainda realiza a transferência.*

Percebeu que a Engenharia Social não é algo novo? Esta técnica possui várias vertentes e na grande maioria das vezes, é feita de maneira imperceptível.

Partindo para o contexto da Segurança da Informação e os ataques cibernéticos, a Engenharia Social é empregada em vários crimes digitais, e sempre com os mesmos atributos: ter o poder da persuasão e garantir a confiança do usuário. A diferença para os ataques que não se utilizam da Engenharia social, é que estes atingem o objetivo criminoso sem a necessidade da interação humana, enquanto os ataques que envolvem esta técnica persuadem a vítima para que passe os dados e informações por livre e espontânea vontade.

## Emoções

Todo ser humano apresenta “gatilhos” psicológicos que são acionados em determinadas situações e podem deixá-lo vulnerável e aberto para expor algo confidencial. São estes gatilhos que os atacantes se aproveitam para conseguir o que querem. Conforme dito anteriormente, as vítimas demoram para desconfiar da situação de perigo que está inserida. O atacante, capacitado em Engenharia Social, utiliza do emocional das pessoas e pode criar cenários baseados neles para garantir o sucesso.

## Tipos de ataques cibernéticos envolvendo Engenharia Social

### Phishing



Disponível em: <<https://tinyurl.com/yc296ea4>>. Acesso em 17 jul. 2023.

É um dos ataques mais populares hoje em dia. A tradução remete a “pescaria”, ou seja, é arquitetado um ambiente para que as vítimas “comam a isca” e se sintam confiantes. O *phishing* apresenta diversas variações que veremos a seguir. A mais comum é aplicada pelo envio em massa de e-mails, com mensagens fortes e que chamam a atenção da vítima, normalmente para resolução imediata. De modo geral, os *phishings* tem como objetivo usar as métricas da Engenharia Social para persuadir e conseguir a confiança da vítima através de um contato que é ambientado para parecer autêntico. Normalmente, neste contato haverá formulários, confirmação de dados cadastrais, links, solicitações de instalação de softwares entre outros. A inocência, falta de atenção aos detalhes e a confiança são as metas que a Engenharia Social almeja para ter sucesso no ataque.

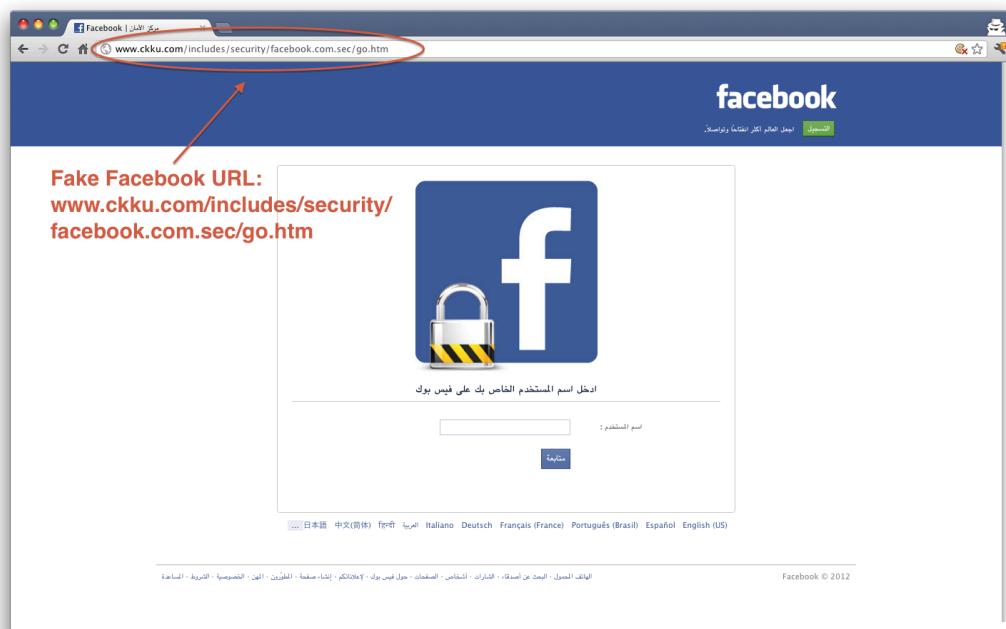
### Smishing



Disponível em: <<https://tinyurl.com/y3mhn2tb>>. Acesso em 17 jul. 2023.

O *smishing* é uma variante do *phishing*, que utiliza aplicativos mensageiros e SMS para se propagarem. De modo geral, são baseados em mensagens de texto impactantes com um link malicioso encurtado. A recomendação é de não clicar em nenhum tipo de link vindo de SMS de números desconhecidos e checar a veracidade da mensagem por outros meios.

### Phishing de sites

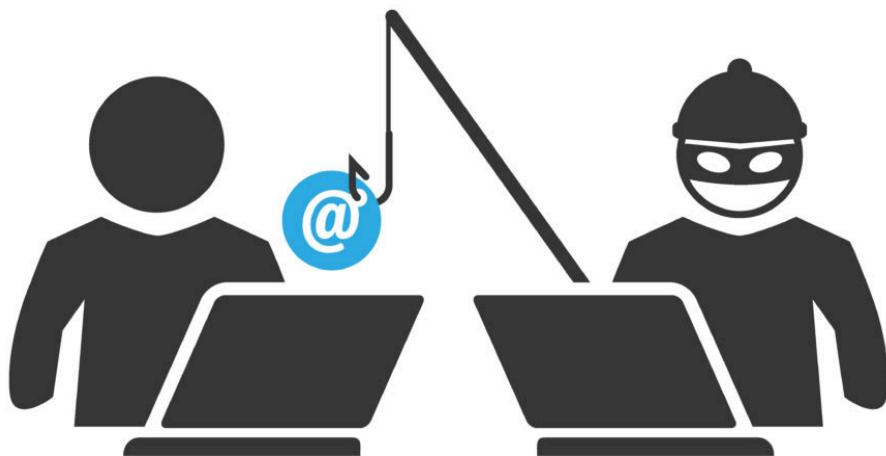


Link:

<https://www.eff.org/deeplinks/2012/04/new-wave-facebook-phishing-attacks-targets-syrian-activists>

Neste tipo de *phishing*, o ambiente malicioso está caracterizado como um site de bancos, escolas e até mesmo de redes sociais, no qual, o usuário realmente acredita estar em um ambiente seguro. Veja abaixo este exemplo: Aparentemente é a página inicial da rede social Facebook, não é mesmo? Agora, observe bem na url do site. O que é para ser <https://www.facebook.com>, é outro link completamente diferente e que mal utiliza o domínio. Esta é uma amostra do *phishing* de sites. Uma cópia muito fiel a página original, pronta para roubar seu usuário e senha.

## Pretexting

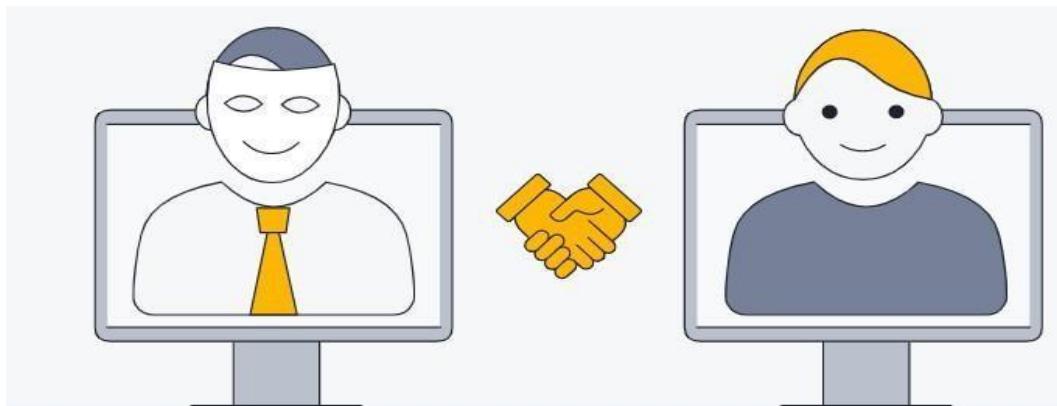


Disponível em: <<https://tinyurl.com/2s3pn7cw>>. Acesso em 17 jul. 2023.

O *pretexting*, ou *pretexto*, é um tipo de ataque que prepara uma relação com a vítima para que se sinta à vontade com ele. Essas relações, via de regra, são criadas no momento do golpe, no qual o atacante finge ser alguém do ciclo social dessa vítima ou alguém que denota uma superioridade.

O criminoso pode vestir várias “carapuças”. Isso pode acontecer tanto pessoalmente, quanto por telefonemas e e-mails. Exemplificando, o atacante pode fingir ser um novo colega de trabalho e pedir ajuda em algum procedimento de acesso ao computador, se passar por um superior na empresa, solicitar dados confidenciais e até mesmo se vestir como um agente público, como um policial ou bombeiro e exigir entrar em algum setor, pressionando a vítima a aceitar imediatamente.

## Quid Pro Quo



Disponível em: <<https://tinyurl.com/2s3pn7cw>>. Acesso em 17 jul. 2023.

Partindo da tradução livre “algo por algo”, o método *Quid Pro Quo* é baseado em uma premissa: “Se você fizer algo por mim, farei algo para você”. Basicamente, o atacante virá com a pretensão de ajudar ou dar algum tipo de assistência à vítima e tudo o que ele precisa são de alguns dados ou informações para que isso seja feito.

Para ilustrar, em nosso cotidiano, você já pode ter presenciado algum suposto técnico de alguma operadora ou colega de trabalho que pede acesso remoto ao seu computador ou desativar o antivírus, na premissa de realizar algum tipo de reparo. Pode acontecer também do criminoso pedir algum tipo de credencial de recursos críticos que, em mãos erradas, pode comprometer todo o ambiente pelo roubo ou exclusão de dados.

## Baiting

Esta técnica de “isca” vai abusar da curiosidade da vítima. Um dos exemplos mais comuns para exemplificar o *baiting* é a pessoa mal-intencionada deixar um dispositivo de mídia, como um pendrive, CD, ou HD propositalmente em algum local, seja público ou privado. Uma hora ou outra, alguém verá aquele dispositivo no chão e se sentirá atraído a pegá-lo e ver o que tem dentro. Nestas mídias, haverá softwares maliciosos como malwares só esperando o “curioso” inserir o dispositivo em sua máquina ou no computador da empresa para infectar a rede ou conceder acesso total a seus arquivos e documentos confidenciais.

## Como evitar ataques envolvendo Engenharia Social?

Para evitar ataques envolvendo engenharia social, é importante adotar algumas práticas e medidas de segurança.

### Aqui estão algumas orientações:

- Conscientização e treinamento: Eduque-se e conscientize-se sobre os diferentes tipos de ataques de Engenharia Social, suas técnicas e os sinais de alerta. Participe de treinamentos e workshops para entender melhor como identificar e lidar com esses ataques.
- Desconfie de solicitações não solicitadas: Esteja atento a solicitações de informações

pessoais ou confidenciais, especialmente quando forem inesperadas ou originadas de fontes não confiáveis. Nunca forneça informações sensíveis por e-mail, telefone ou mídias sociais, a menos que possa verificar a autenticidade do solicitante.

- Valide a identidade: Sempre que receber uma solicitação de informações ou ação, cheque a identidade da pessoa ou organização envolvida. Entre em contato diretamente com a pessoa ou empresa, e use informações de contato confiáveis, para confirmar se a solicitação é legítima.
- Esteja atento a redirecionamentos de URL: Ao clicar em links recebidos por e-mail ou mídias sociais, apure cuidadosamente o URL antes de inserir informações confidenciais. Certifique-se de que o site seja legítimo e seguro. Evite clicar em links suspeitos ou desconhecidos.
- Fortaleça as senhas: Utilize senhas fortes e exclusivas para cada conta. Evite senhas óbvias ou fáceis de adivinhar. Considere o uso de gerenciadores de senhas para criar e armazenar senhas complexas de forma segura.
- Mantenha os softwares atualizados: Mantenha seu sistema operacional, aplicativos e programas antivírus atualizados. As atualizações geralmente incluem correções de segurança que ajudam a proteger contra ameaças conhecidas.
- Cuidado com informações compartilhadas nas mídias sociais: Seja cauteloso ao compartilhar informações pessoais ou detalhes sobre sua vida pessoal nas mídias sociais. As informações publicamente disponíveis podem ser usadas por atacantes para criar perfis falsos ou personalizar ataques de engenharia social.
- Esteja atento a solicitações de ajuda financeira ou urgência: Fique ligado a solicitações de transferências de dinheiro, doações ou pedidos de urgência que não possam ser verificados. Sempre confirme a autenticidade de tais solicitações antes de agir.
- Mantenha um ambiente de trabalho seguro: Em ambientes profissionais, seja cauteloso ao compartilhar informações sensíveis, especialmente com pessoas que não estão autorizadas a acessá-las. Não deixe dispositivos eletrônicos desbloqueados ou informações confidenciais à vista.
- Relate incidentes suspeitos: Se suspeitar de um ataque de Engenharia Social ou identificar atividades suspeitas, relate imediatamente ao departamento de segurança da informação ou equipe responsável pela segurança da sua organização.

Lembre-se de que a Segurança da Informação é um esforço contínuo e envolve tanto aspectos técnicos quanto comportamentais. Ficar atualizado sobre as últimas técnicas de engenharia social e adotar medidas de prevenção adequadas são essenciais para se proteger contra esses ataques.



A necessidade de permanecermos em constante estado de vigilância em relação a novas variantes de fraudes em Engenharia Social é incontestável. A Engenharia Social refere-se a um conjunto de técnicas que se concentram na exploração de aspectos humanos para influenciar o comportamento de indivíduos, manipulando-os a realizar ações ou divulgar informações que não deveriam. Em outras palavras, esses ataques têm como objetivo principal a alteração psicológica do

alvo.

As táticas empregadas pelos fraudadores em engenharia social são sutis e engenhosas. Eles usam várias estratégias de persuasão para convencer suas vítimas a revelar, de maneira voluntária, suas informações pessoais e sensíveis. Isso pode incluir detalhes como senhas, informações bancárias, dados de cartões de crédito, entre outros. De fato, o mais alarmante é que muitas vítimas não percebem que suas informações foram comprometidas até que seja tarde demais.

Frequentemente, os ataques de Engenharia Social são tão bem orquestrados que a vítima, sem sequer perceber, acaba sendo conduzida a acreditar que a divulgação dessas informações confidenciais é de seu próprio interesse. Deste modo, muitas vezes, as vítimas nem sequer têm consciência de que estão caindo em uma armadilha.

Assim, é de suma importância que continuemos vigilantes, educando-nos e a outros sobre a natureza desses ataques e como podemos nos proteger deles. Em um mundo cada vez mais conectado, a emergência de novas estratégias de Engenharia Social é inevitável. Portanto, é crucial reconhecer as maneiras pelas quais esses golpes podem ocorrer, e tomar medidas proativas para se proteger contra esses tipos de fraudes.

## Desafio

Reúnam-se em grupos (máximo 4 pessoas) e realizem um seminário para o restante da turma, encenando uma das Engenharias Sociais citadas acima, simulando uma situação real. O desenvolvimento da situação é livre.



### ATIVIDADE DE FIXAÇÃO

1. O que é Engenharia Social?
2. Qual é o objetivo principal da Engenharia Social?
3. Cite três exemplos comuns de técnicas de Engenharia Social.
4. Explique a importância da conscientização e treinamento dos usuários para prevenir ataques cibernéticos. Como essas práticas podem fortalecer a segurança da informação de uma organização?
5. Discuta a importância de validar a identidade de um solicitante antes de fornecer informações confidenciais. Cite três métodos que podem ser usados para verificar a autenticidade de uma solicitação.

## TEMA 07

# Segurança em Redes de Computadores e Dispositivos Móveis

### Habilidades:

- Entender a importância da integridade e confidencialidade dos dados.
- Aprender a elaborar e decifrar armadilhas digitais e falsificações.
- Compreender e elaborar perfis para evitar golpes de engenharia social



Disponível em: <<https://tinyurl.com/2p9bewtf>>. Acesso em 17 jul. 2023.

Segurança em redes de computadores e dispositivos móveis é um conjunto de práticas e medidas implementadas para proteger informações e sistemas contra ameaças cibernéticas. Isso envolve a aplicação de técnicas como criptografia, autenticação, controle de acesso e monitoramento para garantir a confidencialidade, integridade e disponibilidade dos dados.

Em redes de computadores, são utilizados firewalls, antivírus e detecção de intrusões para prevenir e detectar ataques. Em dispositivos móveis, são adotadas medidas como atualizações de software, autenticação forte, proteção contra malware e backup de dados para garantir a segurança dos dispositivos e das informações armazenadas neles. A segurança em redes de computadores e dispositivos móveis é fundamental para proteger dados pessoais e corporativos, evitar violações de privacidade e assegurar um ambiente digital seguro.

A popularidade dos dispositivos móveis como smartphones, notebooks, tablets e wearables (dispositivos vestíveis como relógios inteligentes) nunca esteve tão alta no nosso cotidiano. Através deles, é possível desempenhar boa parte das tarefas de trabalho, estudo e entretenimento, que há alguns anos atrás apenas PC's faziam e com muito esforço.

Da mesma maneira que protegemos nossos dispositivos físicos e a rede que se conectam,

não podemos deixar de dar a devida atenção à segurança dos dispositivos móveis, já que passam pelos mesmos riscos. O objetivo é basicamente o mesmo da segurança em redes de computadores: impedir que pessoas mal-intencionadas acessem os dados e informações contidos nestes aparelhos por meio da rede e aplicações indesejadas e evitar a perda destes dados por qualquer tipo de acidente.

Para os métodos de segurança de redes surtirem efeito de fato, as políticas de segurança da informação devem estar em plena sintonia, pois reforçará o controle hierárquico de acesso aos usuários e a devida instrução. Tanto os usuários comuns como os colaboradores de uma empresa devem estar atentos às orientações referentes a todos os métodos e adotar as boas práticas de segurança para não ficarem vulneráveis e sofrerem prejuízos.

Existem alguns riscos e ameaças que reforçam a importância de uma implementação da segurança de rede em qualquer lugar. Todos irão explorar algum tipo de vulnerabilidade ou falta de atenção do usuário. São eles:



Link: <https://tinyurl.com/y9z9895n>

## Malwares

Malwares são softwares ou trechos de códigos desenvolvidos com um intuito malicioso por trás. São feitos com o objetivo de invadir sistemas, espionar, roubar dados e informações e até mesmo destruir por completo um sistema. Ele pode afetar computadores, servidores e até mesmo smartphones e podem ser transmitidos através de uma rede.

Existem diversos tipos de malwares. Dentre os mais populares, podemos citar

Vírus – Como o próprio nome sugere, o vírus é um software capaz de se multiplicar e infectar, desde documentos, até mesmo outras aplicações instaladas no dispositivo. Ele fica dentro do arquivo e ao ser aberto, o vírus se espalha ainda mais, o que pode comprometer totalmente uma rede de computadores.

Ransomware – Vem ganhando popularidade devido ao grande número de ataques atualmente. É uma ameaça que realiza, literalmente, o sequestro de todos os dados e informações de um sistema operacional ou aplicação através de uma criptografia de alta complexidade.

Geralmente uma mensagem ao usuário é exibida, o que impede o uso do equipamento e informa sobre o ataque juntamente com o passo a passo de resgate. Caso o usuário não realize o pagamento deste resgate, todos os arquivos e documentos são definitivamente apagados.

Spyware – É um software que tem como objetivo analisar e coletar os dados e informações

da vítima, sem a sua autorização. O atacante, através do spyware, consegue receber essa coleta de maneira remota.

De modo geral, os spywares aparecem na forma de screenloggers, o qual captura imagens da tela do usuário, e indica ao atacante onde a vítima está clicando, ou keyloggers, que capturam as teclas digitadas pela vítima. Através destas ferramentas, o hacker consegue obter acesso a senhas e outros dados confidenciais

Backdoor – Backdoor ou “porta dos fundos” é um código que explora falhas já existentes no sistema e é capaz de criar novas brechas de segurança a partir delas. A finalidade é fragilizar o ambiente para que se torne vulnerável a ataques maiores.

Cavalo de Troia – É um software que o próprio usuário instala, e acredita (técnicas de Engenharia Social) ser uma aplicação original/legítima e vai lhe trazer alguma utilidade. São capazes de liberar o acesso aos dados e informações pertinentes ao atacante.

Rootkit – É um malware dedicado a conceder ao atacante o acesso total a um dispositivo, de modo remoto e sem ser detectado.

Bot – São códigos capazes de conceder o acesso remoto de computadores e outros dispositivos ao atacante. Através dele, é possível inserir outros códigos maliciosos que podem comprometer o funcionamento ou coletar dados e informações da vítima.

Worm – Semelhante ao vírus, os Worms são softwares capazes de criar cópias de si de maneira autônoma e se espalhar pela rede de computadores ou internet. A diferença dele para o vírus é que ele não precisa se hospedar em nenhum arquivo, ou seja, não depende de que o usuário interaja com ele para se propagar e causar danos.

## Engenharia Social

Procedimento o qual os hackers manipulam o psicológico das vítimas para realizar transações, compartilhar dados e instalar aplicativos maliciosos.



Link: <https://tinyurl.com/mu758e3c>

## Injection SQL



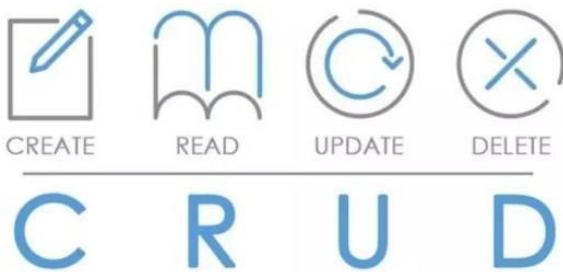
Disponível em: <<https://tinyurl.com/munwjkvr>>. Acesso em 17 jul. 2023.



Até aqui compreendemos que a organização e proteção dos dados e informações são primordiais ao estabelecimento de estratégias e métricas que a organização segue de modo a atingir seus objetivos. Partindo do contexto digital, atualmente, nenhuma empresa vive sem pelo menos um Banco de Dados. É através deles que armazenamos os dados e informações estruturadas e os organizamos da melhor forma possível para consultá-los posteriormente.

Uma só empresa ou aplicação pode ter diversos bancos de dados. Cada um destinado a um ativo de informação específica e, em sua maioria, interligados. Um banco bem estruturado é aquele o qual a criação, leitura, atualização e exclusão dos dados são bem estipulados e controlados por profissionais capacitados. Lembre-se que todos os ativos de informação estão neles, e podem ser poucos, ou milhões. Portanto, exige-se muita cautela para controlá-lo e hierarquizar o seu acesso.

A linguagem mais comum na qual grande parte dos bancos de dados se baseia é a SQL (*Structured Query Language*, ou Linguagem de Consulta Estruturada), onde os comandos do banco de dados serão executados a partir dela. Com este recurso, podemos realizar o que chamamos de CRUD (*Create, Read, Update, Delete*), ou seja, criar, ler, atualizar/modificar e deletar as informações contidas no banco de dados associados a alguma aplicação.



Disponível em: <<https://tinyurl.com/nhva5zm9>>. Acesso em 17 jul. 2023.

Dito isso, precisamos ter muita cautela ao manusear e passar o controle, seja parcial ou total a um banco de dados. Ademais, devemos garantir que a segurança dele perante ataques internos e externos seja preservada.

Por ser uma linguagem internacional e a mais popular, como consequência, é uma das que mais sofrem com ataques e falhas. E uma das mais conhecidas que, ainda podem ocorrer a um banco de dados, e ocasiona sérios problemas é o **SQL Injection (Injeção SQL)**, uma técnica na qual o indivíduo imputa um trecho código SQL (conhecido como Query) manipulado maliciosamente de algum campo vulnerável da aplicação que interage com o banco de dados a fim de realizar consultas para obter dados e informações sigilosas, ou até mesmo alterar ou apagar o que está armazenado no banco.

Como resultado deste ataque, diversos dados confidenciais como credenciais, senhas, e outras informações críticas e sigilosas são expostas e, muitas vezes violados, e ferem os princípios, principalmente dos pilares da Integridade e Confidencialidade da Segurança da informação, o que resulta em prejuízos e danos à imagem e reputação de uma empresa, muitas vezes irreparáveis. Esta falha não tem relação com as ferramentas usadas para desenvolver a aplicação ou banco, mas sim com o próprio desenvolvedor que não adotou tratativas para impedir o SQL Injection.

Você aprenderá dois dos tipos de ataques mais comuns de SQL Injection. O por meio de formulários e de URL's.

## SQL Injection em formulários

Para exemplificar o SQL Injection, neste primeiro momento, vamos imaginar um formulário de autenticação de usuário em um site qualquer, como este abaixo.

JÁ SOU CLIENTE

Usuário  
Senha

**CONTINUAR**

[Esqueceu Usuário/Senha?](#)

Elaborado próprio autor

Este formulário solicita duas variáveis para o cliente: o usuário e a senha. Assim que estes dados forem inseridos e o botão “CONTINUAR” for clicado, a aplicação fará uma consulta no banco de dados para procurar estes atributos e permitir o acesso caso encontre.

Vamos supor que inserimos o usuário **josemoura** e a senha **010203**.

JÁ SOU CLIENTE

josemoura  
010203

**CONTINUAR**

[Esqueceu Usuário/Senha?](#)

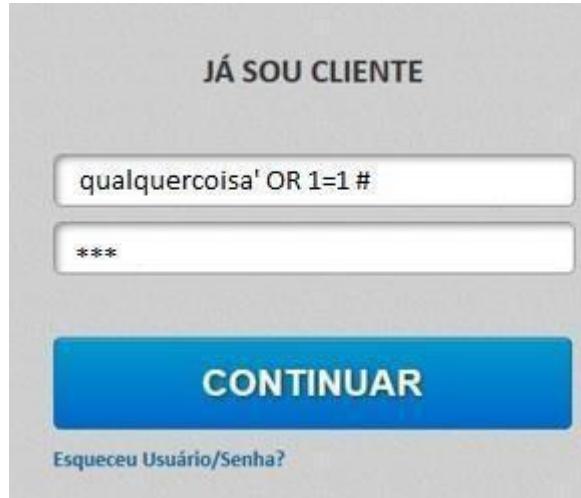
Usuário logado com sucesso

Elaborado próprio autor

A query(consulta) ficaria desta forma:

```
SELECT * FROM usuários WHERE usuário = 'josemoura' AND senha = '010203'
```

Aqui, o código solicita todos os resultados que estejam na tabela de usuários, em que o usuário for igual a **josemoura** e a senha seja **010203**. Agora, imagine que algum criminoso, na tentativa de obter acesso aos dados, colocasse esses comandos nos campos:



Elaborado próprio autor

Na consulta, ficou desta forma:

```
SELECT * FROM usuários WHERE usuário = 'qualquercoisa' * / OR 1=1; # AND senha = '010203'
```

No campo usuário, o atacante digitou um texto qualquer para indicar um usuário e colocou uma condicional “ou” de 1=1. O número 1 sempre será igual a 1, então, o sistema viu que havia nenhum usuário “**qualquercoisa**” dentro do banco e partiu para a segunda condicional **OR**, que simplesmente ignorou o campo usuário. O símbolo “#” transformou o restante da consulta, que está em verde em um comentário, ou seja, na hora da consulta, este campo será ignorado e ele conseguirá logar no sistema.

## SQL Injection em URL

Por incrível que pareça, há a possibilidade de atacar sites apenas por meio da URL. A URL em si, ou *Uniform Resource Locator* (Localizador Uniforme de Recursos) é o endereço da aplicação disponível em uma rede, isto é, o endereço de um site que esteja na Web.

O método de invasão por SQL Injection via URL tem como objetivo atacar a aplicação a partir de uma vulnerabilidade encontrada em seu endereço.

Vamos usar como exemplo esta URL:

<http://www.supercyberbrasil.com/noticias.php?cat=3>

É possível identificar visualizando o final deste link que há um dado sendo transmitido de uma página para outra dentro da aplicação. Sabemos disso através do “?” e este dado pode ser tanto um número, igual o exemplo acima, como também letras ou palavras. Neste caso, o “**cat**” representa uma categoria de notícias e o link pede que seja a categoria de número **3**.

O código em SQL que podemos prever é:

```
SELECT * FROM noticias WHERE codigo='$cat'
```

Em outras palavras, ele busca uma notícia em que o código da categoria seja o mesmo do número que se encontra no endereço URL.

Para identificar se este site está vulnerável, podemos simplesmente remover o parâmetro de categoria. Caso o site apresente uma mensagem de erro de sintaxe de SQL, já é um sinal que há uma falha de segurança. Ficaria dessa forma:

<http://www.supercyberbrasil.com/noticias.php?cat=>

E retornaria no site algo parecido como:

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1

Um dos usos deste ataque é, por exemplo, reunir informações de várias tabelas do banco de dados através do comando **UNION**.

Pode ser inserido desta forma no navegador:  
<http://www.supercyberbrasil.com/noticias.php?cat=3 UNION ALL SELECT 1,2,3,4>. Ou seja, solicita a consulta de todos as informações nas tabelas e colunas especificadas. Em posse destas informações, o criminoso conseguirá ir muito mais fundo e realizar outros procedimentos de invasão.

Apesar o SQL Injection não estar mais com tanta força como era há alguns anos, justamente pela evolução nos meios de proteção, não se deve baixar a guarda para manter o ambiente seguro.

## NEGAÇÃO DE SERVIÇO – DoS e DDoS

Dentre os ataques web mais conhecidos, não podemos deixar de citar o DoS (*Denial of Service* – Negação de Serviço) e o DDoS (*Distributed Denial of Service* – Negação de Serviço Distribuída). De modo geral, não funcionam para roubar ou invadir dados e informações, mas para tirar do ar uma aplicação e/ou os servidores que a mantém ativa, e a sobrecarrega temporariamente por meio de várias métricas. São os ataques que exploram a Disponibilidade, um dos pilares da Segurança da Informação.

E são vários os motivos pelos quais esta abordagem é feita. Uma interrupção de alguma aplicação, ainda que rápida, pode causar prejuízos incalculáveis para a organização. Pode ser utilizada tanto para extorquir o proprietário da aplicação, pedir um resgate para a normalização do serviço, como também como estratégia para derrubar aplicações e outros serviços de concorrentes a fim de prejudicá-los em algum momento em específico.

Os ataques DoS e DDoS irão realizar diversas requisições a um servidor, aplicação ou até uma rede ou infra de maneira proposital com o intuito de exceder a capacidade de processamento a ponto de não conseguir realizar mais nenhum outro tipo de tarefa, o que derruba o serviço

temporariamente. Isso faz com que até os usuários legítimos não consigam acessar os dados.

Os atacantes realizam toda uma investigação e planejamento nesta investida. Eles conseguem avaliar qual é o melhor alvo e o momento certo para atacar. Desde um hardware e sua capacidade, como até mesmo uma vulnerabilidade na aplicação ainda não resolvida e que, forçando-o para acontecer, trará instabilidades e interrupções comprometedoras. Como fazê-lo consumir todo o processamento ou memória RAM de um servidor Web, e interromper e derrubar totalmente a aplicação.

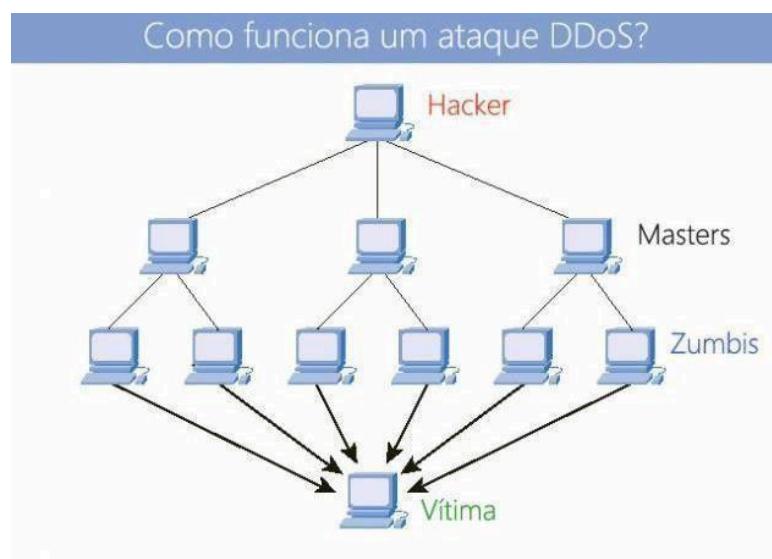
## DoS

Nos ataques DoS, as requisições realizadas irão partir apenas do computador do criminoso direto para o servidor de aplicação. São comumente utilizados em dispositivos mais simples e fracos.



Disponível em: <<https://tinyurl.com/32ddpfuw>>. Acesso em 17 jul. 2023.

## DDoS



Fonte: canaltech

Disponível em: <<https://tinyurl.com/3pmnvcvx>>. Acesso em 17 jul. 2023.

Do DDoS, o cibercriminoso estará munido de mais máquinas para realizar o ataque. Ele conseguirá, através de ataques de malwares, se apossar de computadores que controlam outros, e produzir uma ação de “escravidão” a outros computadores para fazer o “serviço sujo”. Normalmente,

chamamos estas máquinas controladoras de Mestre, enquanto as escravas chamamos de Zumbis.

A diferença do Dos para o DDoS é, sem sombra de dúvidas, o poder de fogo. Com mais máquinas trabalhando para ele, o atacante consegue realizar ataques de larga escala a serviços mais parrudos.

Há três métodos de ataque de negação de serviço mais comuns.

São eles:

- *Negação de serviço por excesso ou volume* - Ataques que envolvem, exclusivamente, o excesso de requisições, o que resulta em um congestionamento no serviço.
- *Negação de serviço por amplificação* - Ataques que compreendem a falsificação do endereço IP do atacante para realizar requisições a inúmeros servidores simultaneamente.
- *Negação de serviço por protocolos* – Ataques feitos através de inúmeras solicitações de conexão simultâneas por meio de algum protocolo ou falha na infraestrutura.

Com a popularidade destes tipos de ataques, fica cada vez mais difícil estabelecer métricas fixas e padronizadas para DoS e DDoS. Como já aprendemos, a educação e a prevenção são fundamentais para combater os crimes cibernéticos.

Para as organizações, de modo geral, uma boa política de segurança baseada na prevenção de anomalias e controle de tráfego de dados e firewall, além dos contínuos testes de penetração, juntamente com a identificação e correção rápida de bugs irão reduzir drasticamente a probabilidade de novos ataques. No entanto, se o ataque for iminente e, realmente, sobrecarregar o serviço a ponto de interrompê-lo, que existam estratégias predefinidas no escopo da política para corrigir e ter o controle da disponibilidade de volta e evitar que isso ocorra novamente.

## Varredura e Análise

Para manter uma infraestrutura e um ambiente seguros, além da implantação das políticas de segurança, é necessário o uso de ferramentas de varredura e análise da rede, sistemas operacionais e aplicações. Elas são capazes de auxiliar no encontro de vulnerabilidades, detecção e eliminação de ameaças, e realizar o vasculhamento aprofundado de diversas áreas e é responsável pela emissão de relatórios úteis para a gestão de T.I.

Todas essas devem ser adquiridas e utilizadas de acordo com a real necessidade de cada um, ou seja, ferramentas de varredura e análise são necessárias para realizar um levantamento de todos os requisitos necessários para estabelecer a segurança no ambiente.

## Firewall



Disponível em: <<https://tinyurl.com/rmj9bv7c>>. Acesso em 18 jul. 2023.

Firewall é uma das principais ferramentas de proteção a redes de computadores e sistemas. Traduzindo do inglês, “paredes corta-fogo”, é um dispositivo físico (hardware), software ou híbrido (hardware + software) capaz de filtrar e barrar agentes nocivos dentro de redes domésticas e corporativas computadores/servidores, e evitar que estes agentes se propaguem no ambiente e causem danos e prejuízos.

Estes agentes nocivos podem ser tanto dados mal-intencionados, como também malwares, capazes de se espalharem como verdadeiras pragas.

Quando falamos em **firewall por hardware**, são dispositivos físicos conectados juntamente com a rede para gerir uma quantidade maior de computadores. Ele é mais recomendado nesses ambientes devido a grande quantidade de tráfego de dados e informações

O firewall físico tende a ser mais caro do que o software. Isso porque soma-se o custo do equipamento, instalação e implementação e também o controle/manutenção, porém é bem mais otimizado e entrega maior segurança no ambiente.

Normalmente, estes dispositivos vêm de fábrica pré-configurados com algumas políticas genéricas de segurança, mesmo assim, há a personalização de entrada e saída de pacotes ou portas da rede da organização, podendo assim ter um controle maior do que é trafegado e as requisições.

Vale ressaltar que fica sob responsabilidade da equipe de T.I./S.I. manter este dispositivo devidamente atualizado e conforme as políticas de segurança do local.

Já o **firewall via software** é o mais popular. Visam o custo mais baixo e oferecem proteção regular às máquinas pessoais de usuários comuns ou organizações pequenas. Geralmente, são renovados através de licenças anuais e recebem atualizações frequentes do desenvolvedor. Entretanto, este método é bem mais limitado comparado ao firewall por hardware, pois, de um modo geral, possui menos ferramentas de controle e dependem de o usuário querer atualizá-la, além de consumir o hardware do próprio computador, juntamente com os demais programas utilizados.

Vale ressaltar que nenhum método de segurança é 100% seguro e de nada adianta adquirir qualquer tipo de firewall ou outra ferramenta, se não houver a conscientização do real motivo deste recurso ser implantado. Por isso, em caso de ambientes organizacionais, os colaboradores devem ser devidamente instruídos a utilizar a rede e sistemas operacionais de maneira segura e de acordo com as políticas de segurança, assim como o usuário comum deve se atentar ao que acessa. Quanto mais ferramentas tivermos e com a devida orientação, aprimoramos a segurança dos ativos de informação em qualquer ambiente.

## Tipos de Firewall

Os firewalls são componentes essenciais da segurança de rede, pois atuam como barreiras entre a rede interna de uma organização e a Internet externa, permitindo o controle do tráfego de rede e bloqueando o acesso indesejado. A escolha de um firewall dependerá de uma variedade de fatores, incluindo a configuração da rede, os usuários, as necessidades específicas, os hardwares e sistemas operacionais envolvidos, além das políticas de segurança em vigor. Vejamos alguns dos tipos mais populares e utilizados de firewalls:

### Firewall de Filtro de Pacotes (Packet-Filtering Firewalls)

Este é o tipo mais básico de firewall. Ele atua no nível de rede do modelo OSI e decide se os pacotes de dados podem passar com base em endereços IP, portas e direção (entrada ou saída). Embora sejam eficazes, não possuem a capacidade de filtragem de conteúdo.

### Firewalls de Inspeção de Estado (Stateful Inspection Firewalls)

Esse firewalls mantêm um registro de todas as conexões ativas. Ao receber um pacote, o firewall verifica se o pacote pertence a uma conexão existente e, em caso afirmativo, permite que o pacote passe sem qualquer inspeção adicional.

### Firewalls de Proxy (Proxy Firewalls)

Também conhecidos como gateways de aplicação, esses firewalls atuam como intermediários para o tráfego de rede. Eles filtram pacotes em nível de aplicação do modelo OSI e oferecem mais recursos de segurança, como registro de conteúdo e verificação de autenticidade do usuário.

### Firewalls de Próxima Geração (Next-Generation Firewalls - NGFWs)

Os NGFWs são uma combinação de vários tipos de firewalls que incluem funções como filtragem de pacotes, inspeção de estado, inspeção profunda de pacotes, IPS (sistema de prevenção de intrusões) e identificação de usuário. Eles são mais complexos, mas oferecem segurança avançada.

## Firewalls Unificados de Ameaças (Unified Threat Management - UTM)

Os UTMs são dispositivos de segurança multifuncionais. Eles combinam as funções de um firewall com outros recursos de segurança, como antivírus, prevenção de intrusões e controle de aplicativos.

A escolha do tipo de firewall a ser usado em uma organização depende de uma variedade de fatores, como a natureza do negócio, o tamanho e a configuração da rede, e o nível de segurança necessário. A decisão deve ser tomada levando em consideração a necessidade de equilíbrio entre segurança, desempenho e custo.



### RESUMO

A segurança em redes de computadores é o estudo das ameaças em potencial para computadores conectados na internet e quais são as ferramentas e atenções necessárias para termos mais segurança no meio digital. Todo cuidado é pouco na hora de configurar e utilizar qualquer dispositivo conectado à internet.

Com boas práticas de políticas de segurança e ferramentas adequadas ao local de aplicação, diminui-se consideravelmente o risco de ocorrerem novas ameaças e possibilitará a mitigação e correção mais certeira.



### ATIVIDADE DE FIXAÇÃO

1. Explique o que é um firewall e qual é o seu papel na segurança de redes de computadores. Cite dois tipos de firewalls e discuta suas diferenças.
2. Discuta a importância da autenticação em redes de computadores. Explique como a autenticação em dois fatores pode fortalecer a segurança dos sistemas.
3. Descreva o que é criptografia e qual é o seu papel na segurança das comunicações em redes de computadores. Cite dois algoritmos de criptografia amplamente utilizados e explique suas características principais.
4. Discuta as diferenças entre uma rede local (LAN) e uma rede virtual privada (VPN). Explique como uma VPN pode fornecer segurança adicional para as comunicações em uma rede.
5. Explique o conceito de detecção de intrusões em redes de computadores. Descreva dois métodos comuns de detecção de intrusões e discuta suas vantagens e desvantagens.

## TEMA 08

### LGPD (Lei Geral De Proteção De Dados)

#### Habilidades:

- Conhecimento sobre legislação de proteção de dados LGPD.
- Habilidades de conformidade com a LGPD.
- Competência em gestão de riscos de privacidade.
- Sensibilidade para a proteção de dados e privacidade.



Disponível em: <<https://tinyurl.com/3rn64kj>>. Acesso em 18 jul. 2023.

No percorrer deste material, você pôde acompanhar os diversos perigos que circulam entre nossos dados e informações. Apesar dos esforços, muitas vezes, é difícil identificarmos a maneira que eles são coletados, além de poderem ser vendidos sem nosso consentimento, o que resulta na exposição e diversas dores de cabeça. Foi nesse propósito que a LGPD foi sancionada no ano de 2018.

A LGPD (Lei Geral de Proteção de Dados – Lei nº13.709) é uma das leis brasileiras mais importantes atualmente quando o assunto é Segurança da Informação. Tem como inspiração a GDPR da União Europeia e foi desenvolvida no intuito de fiscalizar a forma com que as empresas e órgãos públicos coletam e tratam os dados de pessoas brasileiras ou que moram no Brasil, concedendo a este dono, direitos perante a privacidade de seus ativos de informação.

Existem algumas pessoas envolvidas no processo de tratamento de dados da Lei Geral de Proteção de Dados que precisam ser mencionados:

- **Titular:** Proprietário do dado coletado;
- **Operador:** Responsável pela manipulação destes dados para realizar algum fim;

- **Controlador:** Responsável pela gestão da utilização dos dados manipulados pelo operador. É possível que um controlador também seja um operador.

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que estabelece diretrizes e regras para o tratamento de dados pessoais por organizações públicas e privadas. Seu principal objetivo é garantir a privacidade e a proteção dos dados dos indivíduos, além de estabelecer direitos e deveres para os responsáveis pelo tratamento dessas informações.

### Pontos principais sobre a LGPD:

- Abrangência: A LGPD se aplica a qualquer organização que realize o tratamento de dados pessoais no território brasileiro ou que forneça bens e serviços no país.
- Consentimento: O tratamento de dados pessoais deve ser baseado no consentimento explícito do titular dos dados. A organização precisa obter consentimento de forma clara e específica, e informar sobre a finalidade e a forma como os dados serão tratados.
- Direitos dos titulares: A LGPD estabelece diversos direitos para os titulares dos dados, como o direito de acessar, corrigir, excluir e portar seus dados, bem como o direito de revogar o consentimento.
- Princípios do tratamento de dados: A lei define princípios que devem ser seguidos pelas organizações, como o princípio da finalidade, necessidade, transparência e segurança.
- Proteção de dados sensíveis: A LGPD trata de forma específica os dados sensíveis, como informações sobre raça, orientação sexual, convicções religiosas, entre outros. O tratamento desses dados requer consentimento específico e proteção adicional.
- Responsabilidade e segurança: As organizações são responsáveis por adotar medidas de segurança adequadas para proteger os dados pessoais, o que garante sua integridade, confidencialidade e disponibilidade.
- Autoridade Nacional de Proteção de Dados (ANPD): A LGPD estabelece a criação da ANPD, que é responsável por supervisionar, orientar e aplicar sanções em caso de violações à lei.
- Sanções e penalidades: Em caso de descumprimento da LGPD, as organizações estão sujeitas a sanções administrativas, que podem incluir advertências, multas, suspensão das atividades de tratamento de dados e até mesmo proibição do tratamento de dados.

Em resumo, a LGPD tem como objetivo principal proteger a privacidade e os direitos dos indivíduos em relação ao tratamento de seus dados pessoais. Estabelece princípios, direitos e deveres às organizações que tratam dados pessoais, e procura promover a transparência, a segurança e a responsabilidade no uso dessas informações. A conformidade com a LGPD é fundamental para garantir a proteção dos dados e evitar sanções legais.

Um dos seus pontos mais importantes é o consentimento, ou seja, impõe às empresas de informar ao cliente/titular que está havendo uma coleta e uso de dados e o motivo pelo qual isto é solicitado, e também, o concede acesso ao que foi cedido, o que possibilita o usuário corrigir ou excluir dados e informações.

## Não cumprimento

Como toda lei, o não cumprimento resulta em sanções administrativas contra a empresa que não está de acordo com a LGPD. Estas sanções podem partir de advertências a até mesmo multas diárias severas e interrupção do serviço/aplicação através de ordens judiciais. O teto de uma multa voltada a LGPD é de 50 milhões de reais. Todas as empresas que realizam qualquer tipo de tratamento de dados devem estar adequadas à LGPD.

O órgão fiscalizador da LGPD é a ANPD, Autoridade Nacional de Proteção de dados, ou seja, será este o órgão responsável por auditar e analisar as organizações por meio de documentações que demonstraram algum tipo de falha e punir de acordo com o que não está de acordo com a lei. Ela também é responsável por organizar campanhas de conscientização para que as pessoas tenham acesso à informação sobre a privacidade de seus dados pessoais.

## Ciclo de tratamento de dados

O ciclo de tratamento de dados é o estágio de vida de dados coletados. A LGPD visa tratar estes dados de maneira segura, desde sua chegada, até o seu descarte.

**Coleta** – Procedimento de recebimento dos dados de um titular para determinado fim. Pode ser recebida por meio de documentos físicos e digitais, contratos, formulários, entre outros. A LGPD entra analisando a maneira que estes dados chegam, em outras palavras, se são dados e informações recebidos de maneira legítima, sem a intervenção de terceiros.

**Armazenamento/Organização** - Após a coleta, estes arquivos devem ser armazenados de maneira segura em um banco de dados. Nesta fase, ocorre a organização dos dados de acordo com os procedimentos das políticas de segurança, tendo em mente que existem dados de titular mais sensíveis do que outros. Isso diz respeito à cor, religião, saúde, entre outros.

**Uso** – Nesta etapa, ocorre a concatenação de dados para desenvolver o objetivo previamente proposto para eles. É a real utilização dos dados.

**Transmissão** – Dependendo da necessidade, os dados podem ser transmitidos após o tratamento.

**Descarte/Reciclagem** – É a última análise dos dados existentes para avaliar se ainda há algum tipo de utilidade ou se está atrelado a algum outro serviço que dependa dele. Caso não tenha, estes são descartados totalmente do banco de dados.



Link: <https://tinyurl.com/5n6j3t2j>

## Fundamentos da LGPD

A Lei Geral de Proteção de Dados é baseada em dez fundamentos principais que norteiam e fazem com que os profissionais de Segurança da Informação moldem suas políticas e práticas de segurança de dados. Estes princípios estão localizados no Art.6º da LGPD.

**Adequação** – Diz respeito à real finalidade do dado, ou seja, o dado deve ser tratado a partir do real objetivo.

**Necessidade** – Diz respeito à captação de dados exclusivamente para o fim determinado. Coletar os dados essenciais, e armazenar no banco de dados apenas o que for necessário.

**Livre acesso** – Remete ao direito de o titular dos dados conseguir consultar tudo o que lhe foi captado, além de explicitar a ele de que maneira seus dados estão sendo tratados.

**Qualidade** dos dados – Diz respeito à fidelidade dos dados coletados. Se são reais e se estão devidamente atualizados.

**Transparência** – Diz respeito à honestidade da empresa referente a forma de como os dados são tratados para os titulares.

**Segurança** – Diz respeito à adoção de práticas e soluções de tecnologia para evitar ataques e agentes maliciosos.

**Prevenção** – Diz respeito às precauções anteriormente padronizadas no intuito de remediar possíveis situações-problema.

**Não Discriminação** - Diz respeito a impedir que um titular seja discriminado por seus dados. Tem correlação com os dados sensíveis.

**Responsabilização e Prestação de Contas** – Diz respeito às tratativas e evidências necessárias para que a lei seja cumprida.

**Finalidade** – Diz respeito à justificativa pela qual este dado está sendo coletado e ao informe previamente feito para o titular.



O conhecimento da Lei Geral de Proteção de Dados (LGPD), legislação brasileira que se assemelha ao GDPR europeu, é fundamental no mundo digitalizado atual. A LGPD tem como objetivo principal proteger os direitos fundamentais de liberdade e privacidade dos indivíduos, e estabelecer regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo um padrão mais elevado de proteção e penalidades significativas para o não cumprimento. Portanto, uma compreensão completa da LGPD é essencial para qualquer organização que lida com

dados pessoais de indivíduos localizados no Brasil.

Habilidades de conformidade com a LGPD envolvem a capacidade de implementar e monitorar práticas de proteção de dados que estejam de acordo com as exigências da legislação. Isso abrange a implementação de medidas de segurança adequadas, garantia de transparência na coleta e uso de dados, e o respeito aos direitos dos titulares dos dados. Paralelamente, a competência em gestão de riscos de privacidade significa a habilidade de identificar, avaliar e diminuir riscos associados à privacidade dos dados em diferentes contextos, uma capacidade que se torna cada vez mais importante na era digital. Além disso, a sensibilidade para a proteção de dados e privacidade significa a consciência e a valorização da importância do respeito à privacidade e à proteção de dados, um componente crucial para a cultura de proteção de dados dentro de uma organização.



## ATIVIDADE DE FIXAÇÃO

1. Explique o que é a LGPD e qual é o seu objetivo principal na proteção de dados pessoais. Por que essa legislação é importante para os indivíduos e as organizações?
2. Discuta os principais direitos conferidos aos titulares de dados pela LGPD. Explique a importância desses direitos e como impactam o tratamento de dados pelas organizações.
3. Descreva as responsabilidades das organizações em relação à proteção de dados pessoais, conforme a LGPD. Quais são as medidas que as organizações devem adotar para garantir a conformidade com a lei?
4. Explique o que é o princípio da finalidade no contexto da LGPD. Como as organizações devem aplicar esse princípio no tratamento de dados pessoais?
5. Discuta a importância da segurança da informação e das medidas de proteção de dados pessoais em conformidade com a LGPD. Quais são as melhores práticas de segurança que as organizações devem adotar para proteger os dados pessoais?

## TEMA 09

### Footprint – Descoberta de Informações

#### Habilidades:

- Conhecimento sobre legislação de proteção de dados LGPD.
- Habilidades de conformidade com a LGPD.
- Competência em gestão de riscos de privacidade.
- Sensibilidade para a proteção de dados e privacidade.



Disponível em: <<https://tinyurl.com/bde8vw98>>. Acesso em 18 jul. 2023.

Footprint (pegada, em inglês) é a primeira etapa que um invasor, seja ético ou não, realiza em um ataque. Este é o momento em que ele faz o reconhecimento e o estudo do alvo, além de levantar as informações necessárias com o auxílio de ferramentas públicas ou privadas, com o objetivo de analisar as possibilidades e preparar sua estratégia e ideias sem o perigo de detecção. Chamamos esta técnica, inclusive, de pré-ataque.

São diversas as opções de informações a serem exploradas por um hacker/cracker, como a arquitetura de uma rede, banco de dados, softwares e hardwares, configurações de back e front-end, entre outros.

O footprint (ou rastreamento) é uma prática que visa coletar informações e dados sobre uma entidade-alvo, e usa fontes disponíveis publicamente.

Aqui estão alguns tópicos importantes relacionados ao Footprint:

- Definição: O Footprint é o processo de rastrear e coletar informações sobre uma

entidade, como uma pessoa, organização, sistema ou marca, por meio de fontes abertas, como registros públicos, mídias sociais, sites, fóruns e outras fontes de informação disponíveis publicamente.

- Objetivos: O objetivo do Footprint é obter uma visão abrangente e detalhada da entidade-alvo, enquanto coleta informações relevantes que podem ajudar na tomada de decisões informadas, análise de riscos, investigações ou qualquer outra atividade que exija conhecimento prévio sobre a entidade.

- Fontes de informações utilizadas: Durante o processo, várias fontes de informações são exploradas, como registros públicos, diretórios, sites de busca, redes sociais, blogs, fóruns, bancos de dados públicos, entre outros recursos disponíveis publicamente.

- Métodos de coleta de informações: Existem diferentes métodos para coletar informações durante o Footprint, incluindo pesquisa manual em sites e fontes relevantes, uso de ferramentas de busca especializadas, consulta a registros públicos, análise de perfis de mídias sociais e interação com a entidade-alvo para obter informações adicionais.

- Tipos de informações coletadas: No decorrer do Footprint, várias informações são coletadas, como nomes, endereços, números de telefone, endereços de e-mail, registros profissionais, histórico de empregos, relacionamentos, atividades nas mídias sociais, participação em fóruns, eventos passados e qualquer outra informação relevante disponível publicamente.

- Análise e correlação de informações: Após coletar as informações, é importante realizar uma análise cuidadosa e correlacionar os dados coletados para obter uma visão mais completa da entidade-alvo. Isso envolve a identificação de padrões, relacionamentos e qualquer outra informação que possa ser útil para entender a entidade em questão.

- Importância do Footprint em diferentes áreas: Ele é usado em diversas áreas, como segurança da informação, investigação digital, inteligência de negócios, análise de riscos, due diligence, marketing digital, entre outros. Ele fornece uma base sólida de informações para orientar decisões e atividades nessas áreas.

O Footprint é uma prática fundamental para obter informações relevantes sobre uma entidade-alvo por meio de fontes disponíveis publicamente. A coleta e a análise de informações durante o Footprint fornecem uma visão abrangente e embasada da entidade, o que possibilita tomar decisões mais informadas e realizar atividades de forma mais eficiente.

## Métodos de Footprint

Para a obtenção dessas informações, o atacante pode usar de diversas ferramentas e pesquisas, específicas ou públicas. Há vários métodos e cabe ao hacker/cracker definir o que usar de acordo com a complexidade do alvo. Vamos aprender alguns destes métodos?

### Fingerprint

Definitivamente um dos pontos de partida quando falamos de Footprint. O Fingerprint (impressão digital) é a técnica que tem como objetivo identificar qual sistema operacional, versão e distribuição o alvo utiliza, além de identificar brechas nos protocolos de comunicação dos dispositivos

que estão em uma rede, conhecidos como TCP/IP. Ao reconhecer essas informações, o atacante conseguirá optar quais ferramentas para que apresentem um melhor desempenho e compatibilidade.

As ferramentas utilizadas para este método são chamadas de Scanner de Fingerprint, que são separadas entre **Fingerprint ativo** e **Fingerprint passivo**.

O Fingerprint passivo atuará como farejador na rede do alvo para identificar o sistema operacional, analisando o formato dos pacotes, detectando a informação. Uma das ferramentas baseadas nesse Fingerprint é a **POF**, que realiza o reconhecimento do sistema sem precisar enviar nenhum pacote e é capaz de retornar ao atacante a estruturação da rede.

Já o Fingerprint ativo é um pouco mais complexo, já que o mesmo encaminha pacotes anteriormente manipulados e analisará como a rede responde, que retorna informações para definir qual o sistema operacional a aplicação utiliza

O mais conhecido fingerprint ativo, sem dúvidas, é o **NMap(Network Mapper – Mapeador de Rede)**, um programa que, além de detectar o sistema operacional, também é capaz de identificar os dispositivos conectados na rede e os serviços que estão sendo executados. Ele também consegue identificar se há portas abertas nesta rede, o que por si só já facilitaria bastante para o atacante.

## Whois

O Whois é uma ferramenta pública de consultas de domínios que pode ser acessada via terminal/console ou até mesmo via site. Você pode conferir esta ferramenta facilmente em <https://registro.br/tecnologia/ferramentas/whois/>.



Disponível em: <<https://registro.br/tecnologia/ferramentas/whois/>>. Acesso em 18 jul. 2023.

Elas permitem a rápida obtenção de dados do titular do domínio, como nome completo, endereços, telefones e e-mails. Definitivamente um prato cheio para os atacantes, já que a ferramenta retorna informações de maneira rápida e sem deixar rastros.

## IP Location

Funciona basicamente da mesma forma que o Whois, as ferramentas de localização via endereço IP permitem a realização de consultas de IP retornando à localização aproximada de endereços públicos. Você pode conferir esta ferramenta em <https://iplocation.com>.

The screenshot shows the results of an IP location search for the IP address 192.168.1.3. The interface includes a 'CHANGE' button for the IP input field, a map of São Paulo with a blue marker indicating the location, and a table of location details:

Your IP address	192.168.1.3 - your IP	CHANGE
Latitude	-23.5494	
Longitude	-46.6350	
Country	Brazil	
Region	Sao Paulo	
City	São Paulo	
Organization	TIM Brasil	

Disponível em: <<https://tinyurl.com/ye237cbv>>. Acesso em 18 jul. 2023.

## DIG

A Domain Information Groper, ou pesquisador de informações de domínio, é uma ferramenta para consultar registros de DNS, abreviação de Domain Name System, traduzindo, Sistema de Nome de Domínio e são responsáveis por traduzir os endereços IP dos sites

## TraceRoute

Ferramenta que realiza um mapeamento das rotas e topologia de uma rede específica. No Windows, ela vem com o nome de tracert, e pode ser facilmente utilizada através do console do Prompt de Comando.

```
PS C:\Users\Lucas Moura> tracert google.com
Rastreando a rota para google.com [142.250.79.206]
com no máximo 30 saltos:

  1   1 ms    8 ms    1 ms MyRouter [192.168.1.1]
  2   *        5 ms    6 ms 186-230-221-202.ded.intelignet.com.br [186.230.221.202]
  3   6 ms    6 ms    4 ms 10.40.14.0
  4   5 ms    6 ms    8 ms 10.40.67.91
  5   12 ms   7 ms    7 ms 10.223.238.238
  6   8 ms    7 ms    7 ms 72.14.215.93
  7   7 ms    7 ms   14 ms 142.250.58.65
  8   7 ms    6 ms    8 ms 108.170.235.255
  9   12 ms   9 ms    7 ms gru06s59-in-f14.1e100.net [142.250.79.206]

Rastreamento concluído.

C:\Users\Lucas Moura>
```

Elaborado pelo autor

## Engenharia Social

Já vimos este nome antes, certo? Definitivamente a Engenharia Social não poderia ficar de fora da lista de ferramentas mais comuns para Footprint. Através da manipulação psicológica contra funcionários de uma empresa, por exemplo, o atacante consegue pegar as minúcias e informações valiosas para um ataque futuro.

## Fotoprint

Footprint representa uma coleção de instrumentos que possibilitam a um invasor digital, seja ele hacker ou cracker, coletar dados adicionais acerca do seu objetivo. Utilizando-se do Footprint, o indivíduo será capaz de entender a mecânica de determinados serviços e softwares, o que possibilita a ele um aprimoramento de sua estratégia ofensiva.

Em outras palavras, Footprint é uma série de recursos que dão ao ciberinvasor, seja hacker ou cracker, o poder de extrair mais detalhes sobre a sua meta. Por meio do Footprint, ele tem a capacidade de decifrar a funcionalidade de várias aplicações e serviços, permitindo, dessa forma, o aperfeiçoamento de seu plano de ataque.

## Desafio

Realize uma consulta através do Whois, inserindo um domínio de site que você costuma navegar. Depois, insira este mesmo domínio na ferramenta IP Location para descobrir outras características.



## ATIVIDADE DE FIXAÇÃO

**1.** Explique o conceito de Footprint e qual é o seu objetivo principal na coleta de informações sobre uma entidade-alvo. Por que o Footprint é uma prática relevante em diversas áreas?

**2.** Discuta as diferentes fontes de informações utilizadas no processo de Footprint. Cite exemplos de fontes disponíveis publicamente que podem ser exploradas para obter informações relevantes sobre uma entidade.

**3.** Descreva os métodos de coleta de informações durante o processo de Footprint. Quais são as técnicas e ferramentas comumente utilizadas para extrair informações de fontes públicas?

**4.** Explique a importância da análise e correlação de informações durante o Footprint. Como essa etapa contribui para obter uma visão mais completa e precisa da entidade-alvo?

**5.** Discuta os desafios éticos e legais associados ao Footprint. Quais são as considerações éticas que devem ser levadas em conta ao realizar a coleta de informações de fontes públicas? Há restrições legais que regem a prática do Footprint?

## TEMA 10

### Testes de Penetração e Vulnerabilidades

#### Habilidades:

- Identificação de vulnerabilidades.
- Exploração de vulnerabilidades.
- Análise de riscos.
- Relatórios técnicos e comunicação efetiva.



Disponível em: <<https://encurtador.com.br/glvP3>>. Acesso em 18 jul. 2023.

Testes de Penetração/PenTest/Testes de Intrusão, são métodos e técnicas realizadas por profissionais da área de cibersegurança com o intuito de identificar e avaliar a segurança operacional de uma infraestrutura de redes e aplicações de uma organização.

Os testes de penetração (também conhecidos como *PenTests*) são atividades de avaliação de segurança que têm como objetivo identificar e explorar vulnerabilidades em sistemas, redes, aplicativos e infraestruturas de TI. O propósito é simular um ataque realista para avaliar a eficácia das medidas de segurança existentes e reconhecer as áreas de melhoria. Aqui estão os principais tópicos relacionados aos testes de penetração e vulnerabilidades:

- Definição de Testes de Penetração: Explicação sobre o que são testes de penetração e como são conduzidos para identificar vulnerabilidades e avaliar a segurança de sistemas e redes.
- Objetivos dos Testes de Penetração: Discussão sobre os principais objetivos dos testes de penetração, incluindo a identificação de vulnerabilidades, avaliação da postura de

segurança, redução de riscos e melhoria contínua da segurança.

- Fases dos Testes de Penetração: Explicação das etapas comuns de um teste de penetração, como o levantamento de informações, identificação de vulnerabilidades, exploração, obtenção de acesso e documentação dos resultados.
- Metodologias e Abordagens: Apresentação das metodologias e abordagens normalmente utilizadas em testes de penetração, como as metodologias OSSTMM, OWASP e PTES, e a importância de adaptá-las para atender às necessidades do ambiente alvo.
- Tipos de Testes de Penetração: Exploração dos diferentes tipos de testes de penetração, incluindo testes de caixa-preta, caixa-cinza e caixa-branca, e como eles se diferenciam em termos de acesso à informação do sistema.
- Ferramentas de Teste de Penetração: Visão geral das ferramentas comumente usadas em testes de penetração, como scanners de vulnerabilidades, ferramentas de exploração, sniffers e ferramentas de análise de tráfego.
- Documentação e Relatórios: Discussão sobre a importância da documentação e relatórios em testes de penetração, e abrange a descrição dos testes realizados, as vulnerabilidades identificadas, os riscos associados e as recomendações para mitigação.
- Ética e Legalidade: Exploração das considerações éticas e legais envolvidas nos testes de penetração, incluindo a obtenção de autorização prévia, o respeito às políticas e leis de privacidade, e a importância de manter a confidencialidade dos dados obtidos.
- Benefícios dos Testes de Penetração: Destaque dos benefícios de realizar testes de penetração, como a melhoria da postura de segurança, a identificação proativa de vulnerabilidades e a redução do risco de ataques cibernéticos.
- Melhores Práticas em Testes de Penetração: Apresentação de algumas melhores práticas a serem seguidas em testes de penetração, como a definição de escopo claro, o envolvimento das partes interessadas, a comunicação eficaz dos resultados e a realização de testes regulares para garantir a segurança contínua.

Os testes de penetração são uma parte importante da avaliação e melhoria da segurança, mas devem ser realizados por profissionais experientes e seguindo as melhores práticas e considerações éticas.

Os **hackers éticos**, normalmente, são desenvolvedores de alto nível que contam com habilidades com infraestrutura de redes e sistemas de informação em geral. Estes profissionais usam de suas destrezas para algo que impactará positivamente à organização e de modo geral prestam serviços de forma autônoma.

A função do hacker não é apenas realizar os testes, mas canalizar e imaginar como um criminoso agiria vendo este sistema e de quais artimanhas usaria para realizar algum ataque. Ele deve pensar de que maneira um usuário pode encontrar e percorrer diversos caminhos que não poderiam ser utilizados e notados por eles.

## Níveis de Testes de Penetração

Existem três níveis de *PenTests* que poderão ser definidos e usados conforme a necessidade e tem como objetivo preparar os procedimentos da forma que um atacante enxerga a empresa. Cada um possui uma aplicabilidade diferente. São elas:

### White Box

Nesta abordagem, os testes serão realizados com todas as informações de infraestrutura e aplicações disponíveis. É o processo mais completo e por ter o acesso de todas as operações e costuma ser realizado pelos próprios analistas de T.I. e S.I. da organização, no intuito de testar um agente interno tentando realizar algum tipo de crime cibernético.

### Black Box

Aqui, os testes irão partir do princípio de que o ataque virá de um agente externo, ou seja, que não tem conhecimento da estrutura da organização e tentará atacar “às cegas”.

### GrayBox

A GrayBox utiliza dos dois métodos citados acima, o Black e o White box. Ele parte da premissa de que o atacante conseguiu alguma informação relevante a ponto de conseguir uma permissão de acesso e conseguir realizar um ataque. Ele não tem acesso a tudo como na White Box, mas esta informação ou nível de acesso já consegue ser minimamente suficiente para invadir.

## Procedimentos de um Pentest

Existem etapas para se realizar um procedimento de *Pentest*. São elas:

### Discovering(Descoberta)

Nesta etapa, o profissional irá planejar seu ataque e levantar seu escopo junto com o cliente. É neste momento que as métricas e estratégias dos testes serão traçadas e o atacante tentará adquirir informações pertinentes à empresa, de modo também a identificar vulnerabilidades a partir daí.

Um dos métodos de descoberta mais utilizados pelos hackers é o **FootPrint**, que você já aprendeu no tema anterior.

### Escaneamento

Assim que o hacker finaliza seu planejamento, segue à segunda fase, que é chamada de escaneamento. São estratégias que tem como objetivo de encontrar vulnerabilidades dentro dos

códigos da aplicação, partindo de dois tipos de análise

Análise Estática – Avaliação do código da aplicação de modo genérico, para identificar alguma brecha ou falha.

## Conseguindo Acesso

Planejamento feito e codificação analisada, finalmente chegou a hora de realizar os testes de penetração baseados nas falhas encontradas. Eles irão explorar todas as vulnerabilidades para conseguir sucesso na simulação de invasão.

## Manter o Acesso

Neste estágio, o atacante irá averiguar o andamento de seu ataque, ou seja, vai acompanhar se o ambiente de segurança consegue detectar que houve uma invasão e como ele reage. Caso isso não aconteça, é uma evidência de que a aplicação pode ser violada por tempo suficiente para o agente conseguir informações sigilosas.

## Análise e Documentação

Assim que os testes de penetração forem concluídos, o profissional irá documentar todas as vulnerabilidades encontradas no ambiente e anexar todas os comprovantes que validam suas afirmações em um relatório

Além disso, neste arquivo também conterá todos os motivos pelos quais estas falhas acontecem, seja por algum defeito na infraestrutura, colaboradores não cumprindo as políticas de segurança, falta de atualização de sistemas operacionais, ausência de softwares antivírus entre outros.

## Correção e Controle

Nesta última fase, serão realizados os procedimentos cabíveis para sanar todas as vulnerabilidades encontradas, como correções em trechos de códigos da aplicação, mudanças na infraestrutura de redes alterações nos filtros de pacotes no firewall, atualizações de sistemas e softwares, inserção e correção de políticas de segurança e orientação dos colaboradores. Feito isso, o *PenTester* irá realizar novamente os testes para assegurar que as correções surtiram efeito.

## Tipos de PenTest

Existem diversos tipos de PenTests, cada um para um tipo de aplicação, infraestrutura e ambiente. Veja abaixo os mais comuns:

## Na rede:

Serão realizadas simulações de invasão em firewalls e outras ferramentas de segurança que a organização possui. Caso a invasão seja bem-sucedida, qualquer dispositivo que esteja conectado a esta rede-vítima, estará vulnerável e passível de acesso.

### Pentests em uma aplicação Web

Em posse da coleta de informações pelo método de Footprint, o atacante consegue ter uma noção de como uma aplicação Web foi desenvolvida e consegue dimensionar um ataque certeiro às vulnerabilidades encontradas nos firewalls, servidores e endereços IP.

Dois exemplos de ataques comuns e que podem ser realizados por hackers éticos são oSQL Injection e o Ataque de Negação de Serviço DoS e DDoS, vistos nos temas anteriores.

### Pentests Client Side

Nestes testes, o atacante irá analisar a perspectiva de um usuário comum utilizando a aplicação e se ele consegue usar o ambiente com segurança. A proposta é realizar simulações de invasões que não afetem a aplicação em si, mas o usuário/cliente que a utiliza.

### Pentests com engenharia social

Neste tipo de teste, o hacker ético abordará o ambiente com métricas de engenharia social no intuito de analisar o comportamento dos colaboradores de um ambiente organizacional.

## Ferramentas de Pentest

Existem inúmeras ferramentas de testes de penetração existentes, desde dispositivos físicos, para simulação de ataques em hardware, até softwares e sistemas. Neste tópico, você verá o conceito de ambas e exemplos das mais utilizadas atualmente.

### Ferramentas de dispositivos físicos (Hardware Hacking)

As ferramentas físicas de testes de penetração são equipamentos de grande valia na exploração e subtração de informações dentro da empresa. Veja abaixo alguns exemplos:

#### Hardware Keylogger

O Keylogger de hardware é um dispositivo físico, comumente prototipado em portas USB, que é desenvolvido para captar todas as teclas digitadas pelo usuário. Ele funciona plugado ao teclado da vítima na porta USB fêmea do dispositivo e ao USB macho no computador. Tem a vantagem de não ser detectado por antivírus, já que funciona como um extensor do teclado e ser pequeno, podendo passar despercebido. O log das teclas digitadas pode tanto ser armazenado no dispositivo, quanto transmitido por Wi-Fi, dependendo do modelo.

#### USB Rubber Ducky

O Rubber Ducky é um dispositivo que tem semelhança com um pen drive, com uma ponta

USB macho, e consegue simular um teclado. Tem como o objetivo de simular diversos ataques. No seu interior, há um script que pode ser editado conforme a necessidade. É possível inserir instruções para tentar roubar informações de redes, injetar teclas que possam causar algum tipo de dano ao sistema ou deixar um backdoor.

### Shark Jack

Shark Jack é um dispositivo voltado para ataques de rede. Possui uma porta rj45 na extremidade e tem como objetivo coletar diversas informações referentes a infraestrutura e firewall e até mesmo realizar injeções de comandos ao inseri-la em algum ponto de rede.

### Cabo O.MG

Este cabo que aparenta ser um simples carregador de celular, na verdade, é um cabo malicioso que, caso conectado a um computador, consegue capturar tudo o que for digitado e encaminhado para o hacker a partir de um ponto de acesso Wi-Fi em uma interface web.

### RaspBerry

O Raspberry é um microcomputador totalmente modular, capaz de ser atrelado a outros componentes e realizar diversas funções através de uma codificação. Consegue realizar ataques de rastreamento, captação de ondas de rádio e até hackear redes Wi-Fi.

## Ferramentas de Softwares/Sistemas

Grande parte das ferramentas de penetração virtual podem ser encontradas em distribuições do Linux. Estas distribuições foram totalmente otimizadas para realizar os mais diversos testes de invasão, além de serem seguras para o hacker ético.

Vale ressaltar que a escolha de uma distribuição depende da necessidade de cada projeto e também varia de gosto pessoal de cada profissional, já que muitas distribuições, ainda que diferentes, conseguem rodar os mesmos testes.

Dentre as distros mais conhecidas para fins de pentests, podemos citar:

## Kali Linux



Disponível em: <<https://l1nk.dev/a0A2J>>. Acesso em 18 jul. 2023.



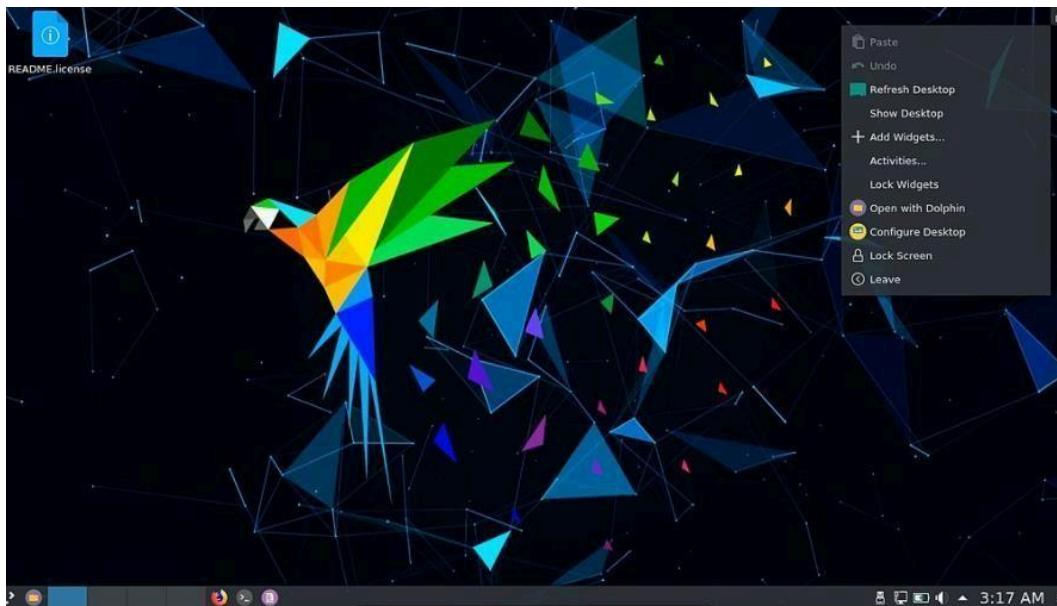
A mais famosa e querida entre os hackers éticos, a Kali é uma distro baseada no Debian e reúne mais de 600 ferramentas forenses e pentest pré-instaladas disponíveis para o atacante utilizar e sempre recebem atualizações continuamente. Possui a ferramenta NetHunter, capaz de realizar testes de invasão em dispositivos Android.

## Pentoo

A Pentoo é uma distro conhecida por ter uma gama de testes de invasão e avaliações específicas para redes e infraestruturas. Foi desenvolvida baseando-se na Gentoo e possui versões de 32 e 64 bits.

## Parrot Security OS

A Parrot é uma distro mais leve e amigável que, assim como o Kali, é baseada no Debian e possui inúmeros pentests e ferramentas específicas de mitigação de vulnerabilidades e de computação forense.



Disponível em: <<https://tinyurl.com/352hs9kx>>. Acesso em 18 jul. 2023.

Ela utiliza repositórios do Kali para rodar as ferramentas, apesar de vir com em menor quantidade. Diferente da Kali, a Parrot não possui suporte para dispositivos Android.

Dentro destas distribuições e de outros sistemas operacionais, podemos encontrar e instalar inúmeras ferramentas de pentest. Veja abaixo algumas das mais populares.

## NMap

Já mencionado anteriormente no Footprint, é uma ferramenta extremamente rápida e eficaz capaz de mapear toda a rede e dispositivos, além da utilização do firewall.

## Wireshark

A Wireshark é uma das ferramentas com foco em redes mais populares no Linux. Ela consegue realizar uma monitoração dos pacotes de dados que estão trafegando pela rede em tempo real, emitir logs mais complexos e analisar os protocolos de rede.

## Nessus

Esta ferramenta é capaz de escanear e detectar vulnerabilidades em um computador de maneira remota. Ela não tem como objetivo acabar com a falha, mas sim realizar mais de 1200 verificações predefinidas, identificando problemas e reportando.

## John The Ripper

É uma ferramenta desenvolvida para quebrar senhas(cracking). É possível realizar ataques de força bruta contra as senhas criptografadas e trabalhar com dicionários. Seu ataque é focado em serviços offline.

### Hydra

A Hydra permite realizar procedimentos de ataque de força bruta contra serviços de autenticação online, tendo suporte a dezenas de protocolos, como por exemplo os FTP's, HTTP, Banco de dados, SSH, entre outros.

### Fern Wifi Cracker

É uma ferramenta que tem como objetivo quebrar a segurança de redes sem fio do tipo WPS, WEP e WPA, executando ataques de força bruta e com dicionários.



A identificação de vulnerabilidades é um processo crítico em qualquer sistema de segurança da informação, que consiste em descobrir, catalogar e analisar pontos fracos em um sistema que podem ser explorados por invasores. O objetivo é identificar essas vulnerabilidades antes que um invasor possa fazê-lo, permitindo que as organizações tomem medidas proativas para mitigá-las. Isso pode envolver o uso de ferramentas automatizadas, bem como inspeções manuais e auditorias de segurança.

A exploração de vulnerabilidades refere-se ao processo de aproveitar esses pontos fracos identificados para ganhar acesso não autorizado a um sistema ou dados. Uma vez explorada, a vulnerabilidade pode permitir ao invasor executar comandos arbitrários, acessar informações confidenciais ou mesmo comprometer todo o sistema. A análise de riscos, por outro lado, é o processo de identificar e avaliar os riscos associados a estas vulnerabilidades, considerando a probabilidade de um ataque e o impacto potencial para a organização. Finalmente, a elaboração de relatórios técnicos e a comunicação efetiva são vitais para documentar os resultados e as recomendações dessas análises. Esses relatórios ajudam as partes interessadas a entender os riscos e a tomar decisões informadas sobre como abordá-los, seja implementando medidas de segurança adicionais, aceitando o risco ou transferindo-o para outra parte.

### Desafio

Faça uma pesquisa detalhada sobre os principais ataques ocorridos e vulnerabilidades expostas dos últimos anos, mapeie as soluções encontradas e faça uma apresentação aos colegas de sala (Grupo de até 4 alunos).



## ATIVIDADE DE FIXAÇÃO

**1.** Explique o que é um Teste de Penetração e qual é o seu objetivo principal na área de segurança da informação. Por que o Pentest é considerado uma prática importante para identificar vulnerabilidades em sistemas e redes?

**2.** Discuta as etapas principais de um Teste de Penetração. Descreva cada uma delas e explique a importância de seguir um processo estruturado durante a realização do Pentest.

**3.** Descreva as diferenças entre um Pentest de Caixa Preta, Caixa Cinza e Caixa Branca. Quais são as vantagens e desvantagens de cada abordagem?

**4.** Explique a importância da coleta de informações na fase de reconhecimento de um Teste de Penetração. Quais são as fontes comuns de informações utilizadas nessa etapa?

**5.** Discuta os tipos de testes que podem ser realizados durante um Teste de Penetração. Cite exemplos e explique como eles contribuem para identificar vulnerabilidades e avaliar a segurança de um sistema ou rede.



## REFERÊNCIAS

ANDERSON, R. J. **Security Engineering: A Guide to Building Dependable Distributed Systems.** 3. ed. Indiana: Wiley, 2020.

BEJTLICH, R. **The Practice of Network Security Monitoring: Understanding Incident Detection and Response.** San Francisco: No Starch Press, 2013

MITNICK, K. D. ; SIMON, W. L. **The Art of Deception: Controlling the Human Element of Security.** Indiana: Wiley, 2002.

STALLINGS, W.; BROWN, L. **Segurança da Informação:** Como proteger ativos de informação. 2 ed. São Paulo: Elsevier Editora, 2014.

STEWART, J. M. **CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide.** 8 ed. Indiana: Sybex, 2018.

STUTTARD, D. PINTO, M. **The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.** Indiana: Wiley, 2011.

WHITMAN, M. E.; MATTORD, H. J. **Princípios de Segurança da Informação.** Boston: Cengage Learning, 2017.



Viva sua profissão!