



# Introdução à cibersegurança



**Aula 1 – O que é hacker e seus tipos**

**Aula 2 – Conceito de ética**

**Aula 3 – Profissões em cibersegurança**

**Aula 4 – Conceitos iniciais**

**Aula 5 – Como se proteger**

# Aula 1 – O que é hacker e seus tipos

# Definição de hacker

Primeiro, vamos definir o que é ser um hacker. Em termos gerais, um **hacker** é um **indivíduo que tem grande habilidade e conhecimento em computação e tecnologia** e usa essas habilidades para encontrar soluções criativas e inovadoras para problemas relacionados a essas áreas.

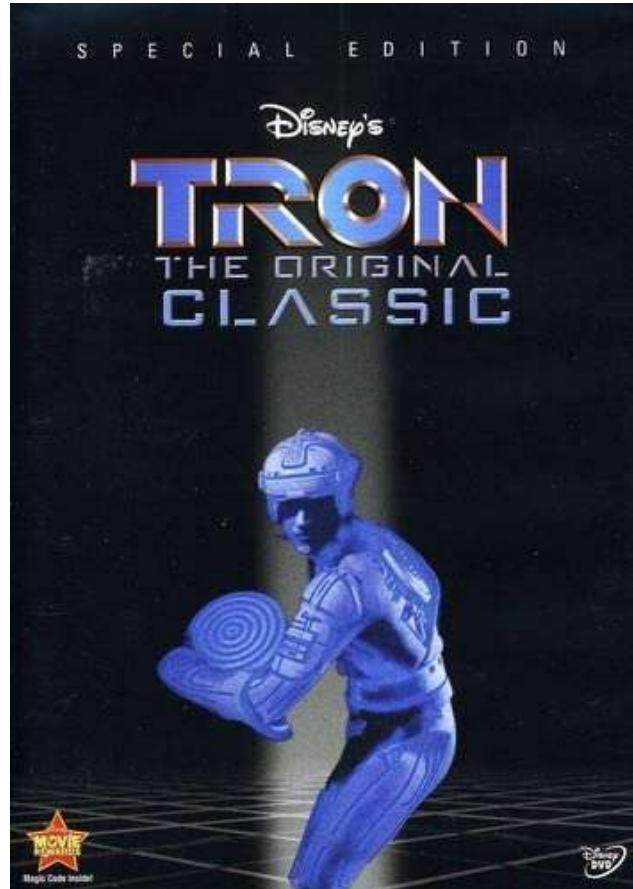


Fonte: Hacking.  
Disponível em: <https://unsplash.com/pt-br/fotografias/dYEuFB8KQJk>. Acesso em 4 Maio, 2023

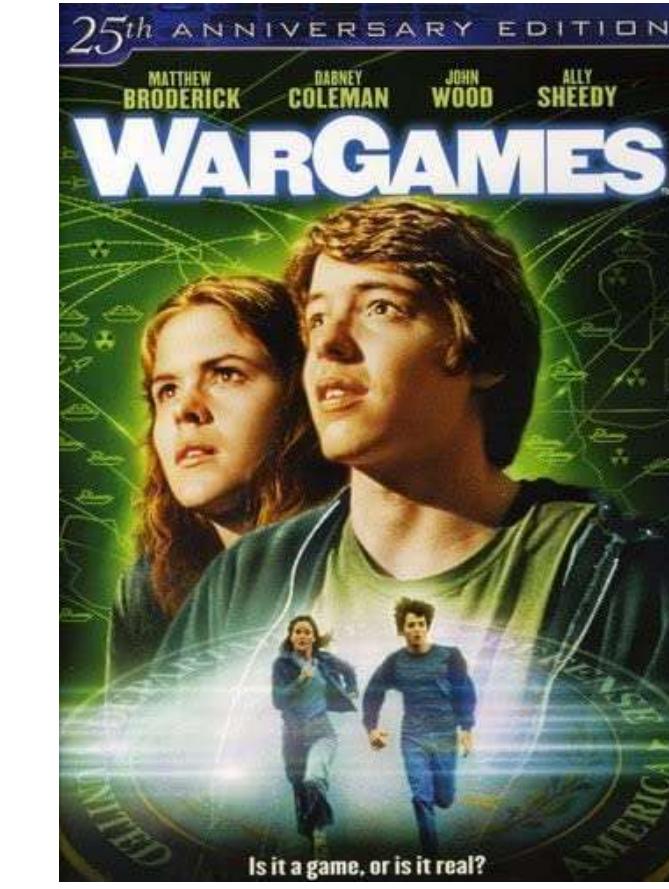
# “Hacking”

Hacking também pode ser definido como: **o ato de comprometer dispositivos e redes digitais por meio de acesso não autorizado a uma conta ou sistema de computador**. O termo hacking apareceu pela primeira vez na década de **1970**, mas se tornou mais popular na década seguinte, com o lançamento de filmes como Tron e WarGames, que mostravam personagens invadindo sistemas de computador. Nessa época, também ocorreram os primeiros casos de ataques cibernéticos a grandes organizações, como o **Laboratório Nacional de Los Alamos** e o **Sloan-Kettering Cancer Center**. Foi então que o Congresso dos Estados Unidos aprovou as primeiras leis sobre crimes de informática e que a palavra hacker passou a ter uma conotação negativa.

# “Hacking”



Fonte: Capa DVD do filme Tron.  
Disponível em: [https://m.media-amazon.com/images/I/41syZaRegHL.\\_AC\\_.jpg](https://m.media-amazon.com/images/I/41syZaRegHL._AC_.jpg). Acesso em 10 fev. 2023

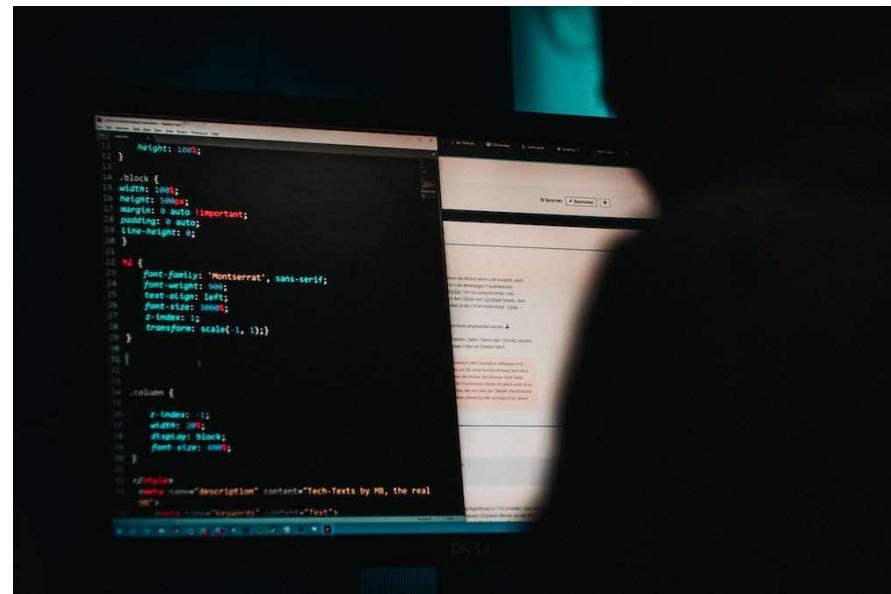


Fonte: Capa DVD do filme WarGames.  
Disponível em: [https://m.media-amazon.com/images/I/51aLtscr+FL.\\_AC\\_.jpg](https://m.media-amazon.com/images/I/51aLtscr+FL._AC_.jpg). Acesso em 10 fev. 2023

# Origem do termo hacker

A palavra "hacker" surgiu nos anos 70, quando os primeiros programadores começaram a **criar softwares e sistemas mais complexos.**

No entanto, com o passar do tempo, o termo acabou sendo associado a atividades ilegais e criminosas, como **invasão de sistemas e roubo de informações**, por exemplo. É importante ressaltar que nem todo hacker é um criminoso e que essa visão equivocada tem gerado muita confusão.

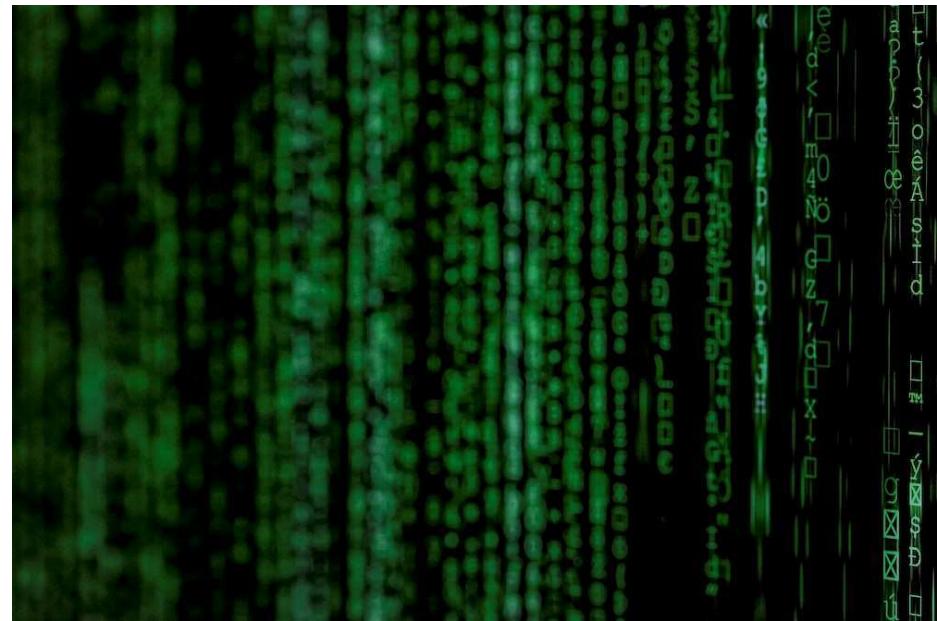


Fonte: Desenvolvimento de scripts para hacking.  
Disponível em: <https://unsplash.com/pt-br/fotografias/J5yoGZLdpSI>. Acesso em 4 Maio, 2023

# Diferença entre hacker e cracker

A diferença entre hacker e cracker é bastante sutil, mas importante.

Enquanto o termo hacker se refere a um **indivíduo que possui grande habilidade e conhecimento em computação e tecnologia** e usa essas habilidades para encontrar soluções criativas e inovadoras para problemas relacionados a essas áreas, o termo cracker é usado para se referir a um **indivíduo que usa suas habilidades em computação para atividades ilegais e mal-intencionadas**, como invasão de sistemas e roubo de informações.



Fonte: Código fonte estilo Matrix.  
Disponível em: [https://unsplash.com/pl-br/fotografias/gcgves5H\\_Ac](https://unsplash.com/pl-br/fotografias/gcgves5H_Ac). Acesso em 4 Maio, 2023.

# Ética



Fonte: Eu sou o bom guia - placas.  
Disponível em: <https://unsplash.com/pt-br/fotografias/yRDSiNdfNJc>. Acesso em 4 Maio, 2023

A ética é o ramo da filosofia que lida com questões de moralidade, ou o que é **considerado comportamento certo e errado**. Preocupa-se em examinar e avaliar os princípios e valores que orientam a conduta humana e a tomada de decisão.

# Ética



Fonte: Eu sou o bom guia - placas.  
Disponível em: <https://unsplash.com/pt-br/fotografias/yRDsiNdfNJc>. Acesso em 4 Maio, 2023

O comportamento ético é o comportamento consistente em princípios e valores. Envolve tomar decisões e agir de acordo com princípios morais como **honestidade, integridade, justiça, respeito** pelos direitos humanos e preocupação com o bem-estar dos outros.

# Ética

Em termos práticos, o comportamento ético envolve a adesão a códigos de conduta ou diretrizes éticas em várias áreas da vida, como negócios, saúde, direito e educação. Também envolve considerar o impacto potencial das ações de alguém sobre os outros e **tomar decisões justas e corretas.**



Fonte: Trabalho em equipe.  
Disponível em: <https://unsplash.com/pt-br/fotografias/Y5bvRlcCx8k>. Acesso em 4 Maio. 2023

# Ética

Em última análise, o comportamento ético é fazer o que é certo, **mesmo quando é difícil ou inconveniente**. Requer o compromisso de defender os princípios e valores morais e a disposição de assumir a responsabilidade pelas próprias ações e suas consequências.



Fonte: Trabalho em equipe.  
Disponível em: <https://unsplash.com/pt-br/fotografias/Y5bvRlcCx8k>. Acesso em 4 Maio. 2023

# Quais são os tipos de hackers

## Hats – chapéus

Podemos classificar em três categorias os tipos de hackers, são eles: **black hat, grey hat e white hat**. Alguns hackers usam seus conhecimentos para ajudar empresas e instituições a se protegerem contra as ameaças cibernéticas, enquanto outros hackers usam seus conhecimentos para causar danos e roubar dados.



Fonte: Autor.

# White hat hackers (hackers éticos)



White hat

Fonte: Autor.

Hacker Ético



Fonte: Autor.

O primeiro tipo que vamos abordar é o White Hat hacker, também conhecido como hacker ético. Os hackers éticos, que são especialistas em segurança da computação que atuam fazendo testes de invasão e outras metodologias para garantir que os sistemas de informação de uma empresa sejam seguros. **Eles têm** autorização para acessar os sistemas e procurar por vulnerabilidades que possam ser corrigidas. Eles são os “mocinhos” da cibersegurança e são contratados por empresas e instituições para melhorar sua proteção.

# Exemplos de ataques feitos por White hat hackers (hackers éticos)



Fonte: Autor.

- A descoberta do bug Heartbleed no OpenSSL em 2014, que permitiu que hackers roubassem informações sensíveis de sites que usavam o software. Os Hackers éticos descobriram a vulnerabilidade e a reportaram aos desenvolvedores para que ela pudesse ser corrigida.
- A descoberta das vulnerabilidades Meltdown e Spectre nos processadores de computador em 2018. Os Hackers éticos descobriram as vulnerabilidades e as reportaram aos fabricantes para que elas pudessem ser corrigidas.

# Grey hat hackers (hackers neutros)



Fonte: Autor.

Grey hat

Hacker neutro



Fonte: Autor.

Por fim, temos o Grey Hat hacker, que é uma mistura dos dois tipos anteriores. Eles às vezes agem legalmente, com boa vontade, e às vezes não. Eles não têm autorização para acessar os sistemas, mas também não têm intenções maliciosas. Eles podem invadir sistemas por curiosidade, desafio ou para alertar sobre falhas de segurança. Eles podem ocasionalmente cometer crimes durante o curso de suas explorações.

# Exemplos de ataques feitos por Grey hat hackers (hackers neutros)



Fonte: Autor.

- Em 2018, um hacker neutro invadiu uma máquina de votação em uma conferência de hacking para demonstrar como era fácil fazê-lo. O hacker reportou a vulnerabilidade ao fabricante para que ela pudesse ser corrigida

# Black hat hackers (mal-intencionados)



Fonte: Autor.

Hacker Malicioso



Fonte: Autor.

O segundo tipo é o Black Hat hacker. São os hackers criminosos, que obtêm acesso não autorizado a um sistema de computador ou rede com más intenções. Eles podem usar computadores para atacar sistemas visando lucro, diversão, motivações políticas ou como parte de uma causa social. Eles geralmente envolvem modificação ou destruição de dados, distribuição de vírus, worms e spam. Eles são os vilões da cibersegurança e estão sujeitos a punições legais.

# Exemplos de ataques feitos por Black hat hackers (mal-intencionados)

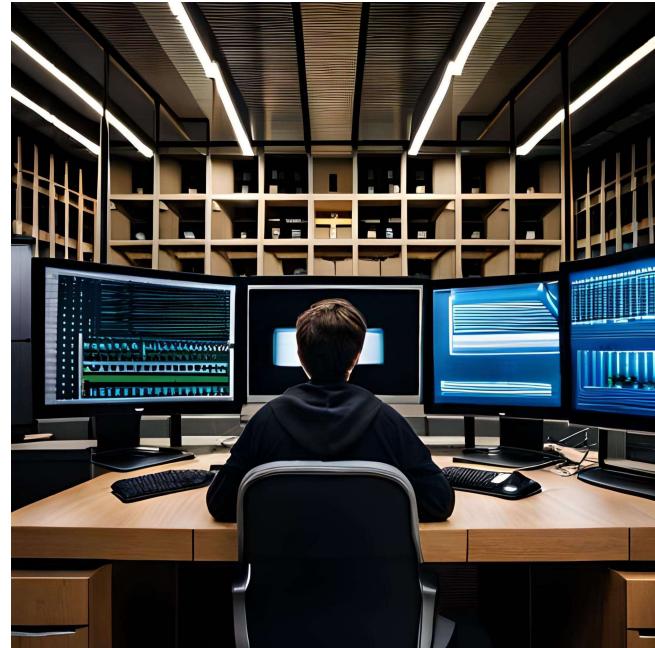


Fonte: Autor.

- O ataque de ransomware WannaCry em 2017, que afetou mais de 200 mil computadores em 150 países e causou bilhões de dólares em danos.
- A violação de dados da Equifax em 2017, que expôs as informações pessoais de mais de 147 milhões de pessoas.
- A violação de dados da Target em 2013, que expôs as informações de cartão de crédito e débito de mais de 40 milhões de clientes.

## Script Kiddies ou “Iniciantes”

Os script kiddies são hackers inexperientes que dependem de ferramentas e scripts desenvolvidos por outros para realizar seus ataques. Eles têm um conhecimento limitado e geralmente não possuem uma compreensão profunda dos sistemas que estão atacando. Eles geralmente copiam e colam códigos ou scripts que encontram na internet sem entender como eles funcionam. Os ataques realizados por script kiddies são geralmente motivados pelo desejo de se exibir, diversão e aprendizado.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Hacktivistas



Dentro da comunidade hacker, encontramos também os "hacktivistas", cujo nome surge da junção das palavras "hacker" e "ativista". Esses hackers têm motivações políticas ou sociais e utilizam suas habilidades em ataques cibernéticos para promover causas em que acreditam. Eles podem ter diferentes visões ideológicas e podem apoiar ou se opor a governos, organizações ou movimentos sociais. Eles podem ser vistos como heróis ou vilões, dependendo do ponto de vista do público.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Conclusão



É importante lembrar que as atividades de hackers, especialmente as dos **black hats, são ilegais e devem ser evitadas.** No entanto, os white hat hackers são uma exceção e podem ser usados para proteger empresas e governos de ataques cibernéticos.

À medida que a tecnologia continua a evoluir, o papel dos hackers se tornará **cada vez mais importante** para garantir um ambiente digital seguro e protegido.

# Aula 2 – Conceito de ética



# Hackers éticos

## Definição do conceito de Ética

A ética pode ser definida como um **código moral pelo qual uma pessoa vive**, orientando seu processo de tomada de decisão e comportamento. No contexto da segurança da informação, a ética refere-se a um **conjunto de princípios e diretrizes** que os profissionais seguem ao trabalhar com dados, sistemas e tecnologias sensíveis (geralmente de terceiros).



Fonte: Imagem criada por Inteligência Artificial no Bing.

Isso é crucial porque os profissionais de segurança cibernética têm acesso a informações **confidenciais** e o poder de **protegê-las** ou **explorá-las**.

# A importância da ética na segurança da informação



Na área da segurança da informação, a ética é fundamental para a proteção dos dados, garantindo a **privacidade** e a **confidencialidade** das informações.

A ética na segurança da informação envolve questões como:

- O uso ético de dados pessoais;
- A avaliação dos reguladores em relação à proteção de dados;
- A confiança do cliente em relação à privacidade dos dados.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# A importância da ética na segurança da informação

É importante que as organizações desenvolvam suas bases de dados em atenção a LGPD, prezando pela privacidade e proteção dos dados pessoais dos titulares, para resultados que não sejam uma ameaça à confiança da marca e à fidelidade do cliente.

A ética também é fundamental na inteligência artificial e nas tecnologias de análise de dados, onde é necessário garantir que as tecnologias sejam usadas de maneira justa e igualitária, promovendo a equidade, a tomada de decisões corretas e o uso honesto dos dados.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Princípios e construção de uma cultura ética

Um aspecto importante da ética na segurança da informação é o estabelecimento de princípios éticos comuns. Alguns princípios chaves são:

- **Confidencialidade**
- **Integridade**
- **Responsabilidade**



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Princípios e construção de uma cultura ética

- **Confidencialidade:** Profissionais de segurança lidam com informações pessoais, privadas ou proprietárias sensíveis que devem ser mantidas confidenciais. Garantir a confidencialidade é vital para manter a confiança entre organizações e clientes.
- **Integridade:** Profissionais de segurança devem agir com honestidade e transparência, aderindo aos mais altos padrões éticos. Isso inclui evitar conflitos de interesse, garantir relações justas e imparciais e promover uma cultura de responsabilidade.
- **Responsabilidade:** Os profissionais de cibersegurança têm o dever de proteger as informações e sistemas com os quais trabalham, além de relatar e abordar quaisquer vulnerabilidades ou riscos que descobrirem. Eles também devem estar preparados para enfrentar os dilemas éticos que surgem em seu ambiente de trabalho.

# Para ser ter sucesso na construção de uma cultura ética

Construir uma cultura ética no campo da segurança da informação envolve incorporar esses princípios aos valores, políticas e programas de treinamento da organização e dos colaboradores.

A tomada de decisões éticas deve ser promovida em todos os níveis da organização, desde diretoria até os colaboradores operacionais.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Benefícios da cultura ética na segurança da informação

## Benefícios da cultura ética

Promover uma cultura ética na segurança da informação tem vários benefícios como:

**Confiança:** Práticas éticas ajudam a construir confiança entre organizações e seus clientes e parceiros. Essa confiança é crucial para manter relacionamentos de longo prazo e garantir o **sucesso** da organização.

**Conformidade:** Adotar princípios éticos pode ajudar as organizações a cumprir requisitos **legais e regulatórios**, evitando penalidades e possíveis **danos à reputação**.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Benefícios da cultura ética

**Mitigação de riscos:** A tomada de decisões e práticas éticas podem ajudar a identificar e mitigar riscos potenciais, como **violações de dados ou ciberataques**, protegendo a organização e seus stakeholders.

**Engajamento dos funcionários:** Fomentar uma cultura ética pode aumentar o **engajamento e a satisfação dos funcionários**, levando a um melhor desempenho e retenção.

**Reputação:** Uma organização com uma forte cultura ética é mais propensa a ser **percebida positivamente** por seus stakeholders, incluindo clientes, parceiros e o público em geral.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Exemplo de ética em hacking

# Hacking ético – estudo de caso



Um hacker ético foi contratado por uma instituição financeira para realizar um teste de penetração em seu sistema bancário online. Nesse cenário, o hacker ético recebe permissão explícita para tentar violar os sistemas, redes ou aplicativos da organização, a fim de identificar vulnerabilidades e potenciais pontos de exploração.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Hacking ético

Durante o teste, o hacker ético segue um estrito e rigoroso código de ética, que contempla os seguintes princípios:

**Permissão:** O hacker ético opera somente **dentro dos limites definidos** pela organização e com autorização adequada. Eles obtêm consentimento por escrito e definem claramente o escopo e as limitações do engajamento.

**Confidencialidade:** O hacker ético respeita a confidencialidade de qualquer informação ou dados sensíveis que possam ser encontrados durante o processo de teste. Eles **não divulgam** nem usam as informações para ganho pessoal ou para prejudicar a organização.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Hacking ético

**Integridade:** O hacker ético mantém o mais alto nível de integridade durante todo o engajamento. Eles **não modificam, roubam ou destroem** dados ou sistemas além do necessário para demonstrar vulnerabilidades e riscos potenciais.

**Conformidade:** O hacker ético **cumpre todas as leis** e regulamentações aplicáveis, garantindo que suas ações **não violem** quaisquer limites legais ou éticos.



# Hacking ético

**Relatório:** O hacker ético fornece relatórios detalhados e precisos à organização, delineando as vulnerabilidades descobertas e recomendações para remediação. Eles comunicam suas descobertas de **maneira responsável**, garantindo que as informações sejam **compartilhadas com segurança e somente com indivíduos autorizados**.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Hacking ético



Ao aderir a esses princípios éticos, o hacker ético profissional ajuda as organizações a melhorar sua postura de segurança, identificando fraquezas **antes que atores mal-intencionados possam explorá-las.** Seu trabalho, em última análise, aprimora as defesas de cibersegurança da organização e as protege contra ameaças potenciais, garantindo a privacidade e a integridade de informações sensíveis.

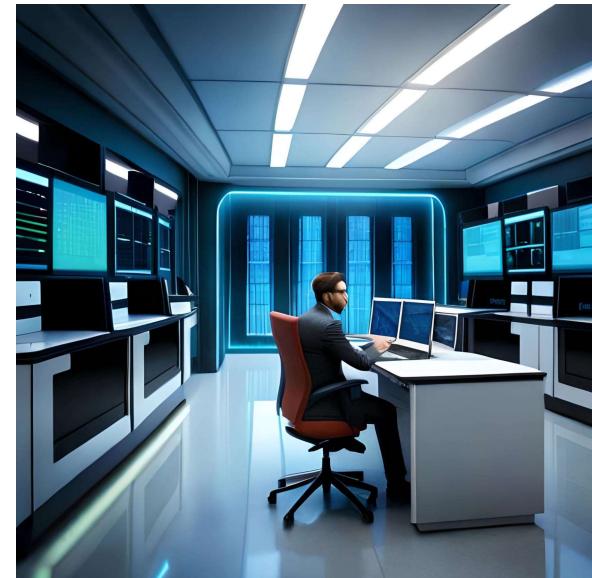


Fonte: Imagem criada por Inteligência Artificial no Bing.

# Conceito de Hacking Ético

# O que é hacking ético

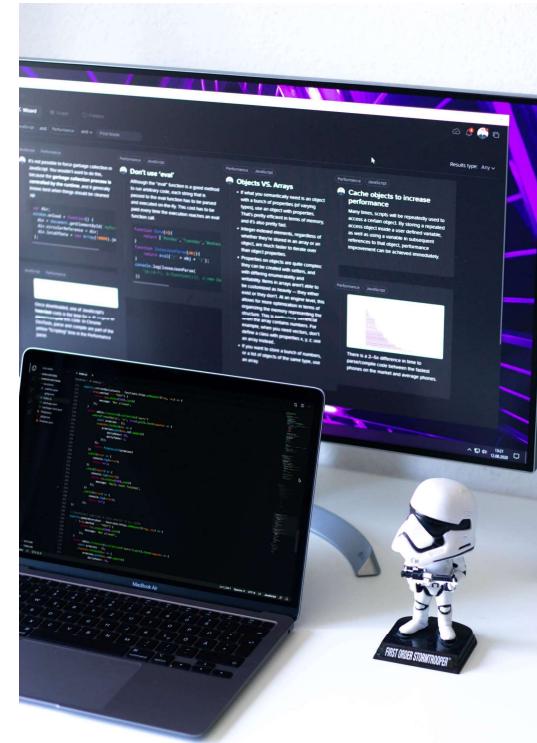
Hacking ético é o processo de tentativas **autorizadas** de obter acesso não autorizado a um sistema de computador, aplicativo ou dados. Hackers éticos são responsáveis por **testar sistemas e identificar vulnerabilidades** que poderiam ser exploradas por hackers maliciosos. Eles usam as mesmas ferramentas e técnicas que os hackers maliciosos, mas param antes de realmente realizar um ataque. Em vez disso, eles **relatam quaisquer vulnerabilidades ou preocupações** e buscam contramedidas para reforçar as defesas do sistema.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# O que é hacking ético

Um profissional que domina o **conhecimento técnico** usado em ataques a sistemas de tecnologia da informação, mas que o utiliza para **encontrar e corrigir vulnerabilidades de segurança**, com o **consentimento** de uma empresa ou do proprietário da aplicação / dispositivo de computação.



Fonte: Projetos de desenvolvimento de software.  
Disponível em: <https://unsplash.com/pt-br/fotografias/SQIpFNb0Nk4>. Acesso em 4 Maio. 2023

# O que é hacking ético

Hackers éticos são profissionais vitais no mundo atual, pois ajudam a desenvolver novas formas de combater as ameaças cibernéticas e são a principal **linha de defesa contra spam, phishing, malware, vírus e outras ameaças à cibersegurança.**



Fonte: Desenvolvimento de scripts para hacking.  
Disponível em: <https://unsplash.com/pt-br/fotografias/vJP-wZ6hGBg>. Acesso em 4 Maio, 2023

# Atuação de um hacker ético

O papel de um hacker ético é importante dentro da indústria de cibersegurança. Hackers éticos são responsáveis por **proteger a infraestrutura de TI, os dispositivos de borda, as redes e os dados**. Eles são especialistas em corrigir ameaças e as vulnerabilidades potenciais de um sistema.



Fonte: Atuação hacker ético.  
Disponível em: <https://unsplash.com/pt-br/fotografias/3C0SWyusdS8>. Acesso em 6 Maio. 2023



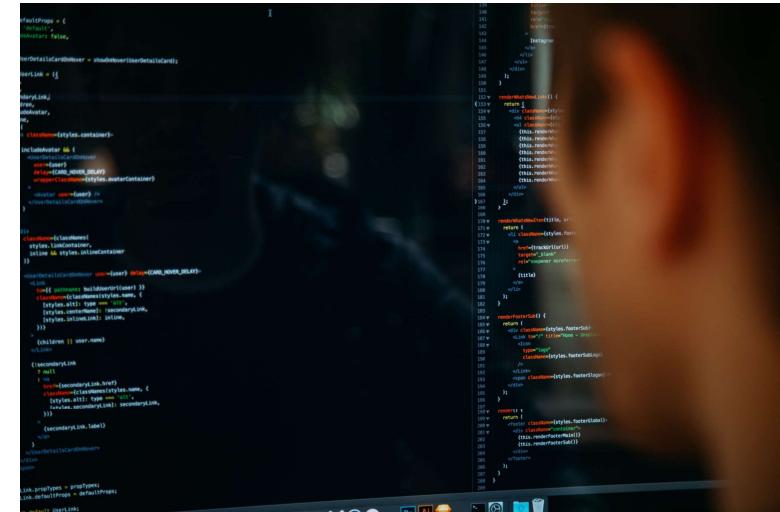
# Como se tornar um hacker ético

# Habilidades de um hacker ético

Para se tornar um hacker ético, é preciso ter conhecimentos avançados em:

- **Sistemas de segurança de computação e internet;**
- **Habilidades de alto nível de hacking;**
- **Capacidade de criar relatórios claros e concisos.**

Um hacker ético profissional é capaz de identificar rapidamente as falhas de segurança e fornecer conselhos úteis sobre como melhorar o sistema. Hackers éticos devem ser capazes de encontrar os métodos de ataque para acessar conteúdos sensíveis de uma organização.



Fonte: Habilidade de desenvolvimento de software.  
Disponível em: <https://unsplash.com/pt-br/fotografias/pjAH2Ax4uWk>. Acesso em 6 Maio. 2023

# Habilidades de um hacker ético

Eles devem ser capazes de invadir sistemas e devem estar bem familiarizados com as ameaças e **vulnerabilidades potenciais** que podem ocorrer nos sistemas organizacionais. Eles devem estar sempre acompanhando **atualizações e novidades no campo da computação e segurança**. Como em qualquer profissão, a paixão pela tecnologia é um dos **aspectos-chave do sucesso**. Isso, combinado com um sólido conhecimento de redes e programação, ajudará um profissional a ter sucesso na área de cibersegurança.



Fonte: Habilidades hacker ético.  
Disponível em: <https://unsplash.com/pt-br/fotografias/3TU34jaW88k>. Acesso em 6 Maio. 2023

# Habilidades de um hacker ético

Para se tornar um hacker ético, é necessário ter uma combinação de **habilidades técnicas e não técnicas** (hard skills e soft skills). Algumas das habilidades técnicas são:

Domínio dos conceitos de informática;

Habilidades em programação;

Habilidades de banco de dados (SQL);

Conhecimento avançado em Linux;

Conceitos e técnicas de Criptografia;

Habilidades de engenharia social;



```
myProgrammingSkills(){  
    ul.skills  
        +skill('programming', '98%', '(htmls - Java, swift - React, node, typescript, etc.)')  
        +skill('planning', '80%', '(I can plan very well every task or project)')  
        +skill('organisation', '77%', '(I am good with organizing projects)')  
        +skill('visual design', '75%', '(I am really handling with visual designs)')  
    li(style="margin: 0")  
        #my[personal="skills"]  
            ul.skills  
                +skill('creativity', '98%', '(creative thinking about design or ideas)')  
                +skill('learning', '93%', '(I would describe myself as fast learner)')  
                +skill('communication', '89%', '(I understand and speak English fluently)')  
            li
```

Fonte: Código fonte em detalhe.  
Disponível em: <https://unsplash.com/pt-br/fotografias/GI1hwOGqGtE>. Acesso em 6 Maio. 2023

# Habilidades de um hacker ético



- Arquitetura e funcionamento de aplicações web;
- Habilidades de rede de computadores;
- Proficiência em sistemas operacionais.

As habilidades não técnicas incluem **comunicação, solução de problemas, criatividade, habilidades analíticas e paixão por tecnologia**.

```
myProgrammingSkills(){
  ul.skills
    +skill('programming', '98%', '(htmls - Java, CSS3 - MySQL, Node.js, React, Angular, Python, C/C++, etc)')
    +skill('planning', '80%', '(I can plan very well every kind of project')
    +skill('organisation', '77%', '(I am good with organizing projects')
    +skill('visual design', '75%', '(I am really handling with UI/UX designs')
  li[style="margin: 0"]
  #my[personal="skills"]
  ul.skills
    +skill('creativity', '98%', '(creative thinking about design and problem solving')
    +skill('learning', '93%', '(I would describe myself as fast learner')
    +skill('communication', '89%', '(I understand and speak English fluently')
```

Fonte: Código fonte em detalhe.  
Disponível em: <https://unsplash.com/pt-br/fotografias/GI1hwOGqGtE>. Acesso em 6 Maio. 2023



# Atividades de um hacker ético

# Atividades de um hacker ético

Os hackers éticos, também conhecidos como hackers de chapéu branco, são profissionais que usam suas habilidades e conhecimentos de hackers para **identificar e solucionar vulnerabilidades em sistemas e redes de computadores**. A seguir, alguns exemplos de atividades que estes profissionais exercem.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Atividades de um hacker ético

**Teste de penetração:** hackers éticos realizam testes de penetração, que envolvem a tentativa de explorar vulnerabilidades em um sistema ou rede para identificar possíveis **pontos fracos e recomendar contramedidas**. Isso ajuda as organizações a identificar e lidar com vulnerabilidades **antes** que possam ser **exploradas por agentes mal-intencionados**.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Atividades de um hacker ético

**Teste de engenharia social:** os hackers éticos também podem testar as defesas de uma organização contra técnicas de engenharia social, como phishing ou golpes sociais, tentando induzir os funcionários a revelar **informações confidenciais**. Isso ajuda as organizações a identificar **pontos fracos** em seus programas de treinamento de conscientização de segurança e desenvolver **estratégias para mitigar** os riscos de engenharia social.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Atividades de um hacker ético

**Avaliação de vulnerabilidade:** hackers éticos realizam avaliações de vulnerabilidade para identificar possíveis pontos fracos nos sistemas e redes de uma organização. Isso envolve a verificação de **portas abertas**, o estudo das **vulnerabilidades** de cada porta e a **recomendação de ações corretivas**. O objetivo é identificar possíveis pontos fracos que possam ser explorados por agentes mal-intencionados.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Atividades de um hacker ético

**Avaliação de risco:** hackers éticos realizam avaliações de risco para identificar riscos potenciais aos sistemas e redes de uma organização e recomendar contramedidas. Isso envolve a análise da probabilidade e o impacto de diferentes tipos de ameaças cibernéticas e o desenvolvimento de estratégias para mitigar esses riscos.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Atividades de um hacker ético

**Auditoria de segurança:** hackers éticos realizam auditoria de segurança para avaliar a **postura geral de segurança de uma organização**. Isso envolve revisar as políticas e procedimentos de segurança, testar os controles de segurança e fazer recomendações para melhorias.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Atividades de um hacker ético

**Pesquisa de segurança:** hackers éticos se envolvem em pesquisas de segurança para identificar novas vulnerabilidades e desenvolver novas ferramentas e técnicas para identificar e lidar com ameaças cibernéticas. Isso ajuda a manter as organizações à frente das ameaças cibernéticas emergentes.



Fonte: Imagem criada por Inteligência Artificial no Bing.

## Melhoria contínua

O ciclo **PDCA** é um método para melhoria contínua de processos e produtos. Ele significa **Planejar, Executar, Verificar, Agir**. Em termos de cibersegurança, pode ajudar a estabelecer e manter uma segurança efetiva das informações seguindo alguns passos.



12

Fonte: Autor.

## Melhoria contínua

**Planejar:** Identificar um problema ou objetivo relacionado com a cibersegurança, como criar **consciencialização entre equipe**, implementar uma nova política de segurança, ou evitar o roubo de dados. **Definir os recursos, ações e indicadores** que tornarão o seu plano bem-sucedido.



Fonte: Autor.

**Executar:** Colocar em prática o seu plano e monitorar os **indicadores**. Esteja preparado para enfrentar alguns desafios ou problemas inesperados ao longo do caminho. Se possível, teste o **seu plano em pequena escala** antes de aplicá-lo a toda a organização.

## Melhoria contínua

**Verificar:** Avaliar os resultados e dados do seu plano.

Compará-los com os **resultados esperados** e ver se há **lacunas ou discrepâncias**. Identificar as causas raiz de quaisquer problemas e aprender com os erros.

**Agir:** Com base na sua avaliação, decidir se precisa ajustar o plano ou implementá-lo como está. Se precisar fazer alterações, volte à fase de **planejamento** e repita o **ciclo**. Se estiver satisfeito com os seus resultados, **padronize** o seu plano e **comunique-o** aos seus stakeholders.



Fonte: Autor.

# Conclusão

# Conclusão

A ética é um dos maiores requisitos para se tornar um profissional de cibersegurança, pois envolve lidar com informações sensíveis das empresas e dos usuários, bem como prevenir e combater crimes cibernéticos. Um hacker ético deve agir de forma responsável e legal, respeitando as normas e os direitos dos outros, e utilizando seus conhecimentos para proteger e melhorar a segurança cibernética.

As principais habilidades de um hacker ético são: conhecimentos técnicos sobre sistemas operacionais, redes, protocolos, aplicações, vulnerabilidades e ferramentas de segurança; ter capacidade de análise, raciocínio lógico, criatividade e persistência para encontrar e explorar falhas; ter habilidades de comunicação, escrita concisa e reporte para apresentar os resultados dos testes de invasão e as recomendações de mitigação; e ter atitude proativa, curiosa e colaborativa para aprender constantemente e compartilhar conhecimentos.

## Conclusão

A importância de se manter atualizado sobre conceitos de segurança cibernética se deve ao fato de que as ameaças e os **riscos são dinâmicos e evoluem rapidamente**, exigindo dos profissionais uma adaptação constante às **novas tecnologias, regulamentações e cenários**. Além disso, a cibersegurança é uma área **multidisciplinar** que envolve **aspectos técnicos, jurídicos, sociais e éticos**, que devem ser considerados na hora de criar soluções inteligentes e eficazes para ambientes cada vez mais conectados.

# Aula 3 – Profissões em cibersegurança



# Red Team

## Red Team (equipe vermelha) – o que é

Os profissionais de Cibersegurança Red Team atuam com simulações de ataques cibernéticos contra empresas e organizações, com o objetivo de **identificar e eliminar vulnerabilidades nos sistemas de defesa**. Esse profissional precisa ter um alto conhecimento sobre as principais ameaças e técnicas de invasão existentes e atuais, e ser capaz de usar ferramentas e metodologias de hackers éticos.



Fonte: Imagem criada por Inteligência Artificial no Bing.

## Red Team (equipe vermelha) – o que é

O principal objetivo de um profissional Red Team, é **melhorar a segurança cibernética das empresas**, demonstrando os impactos de ataques bem-sucedidos e o que funciona para os defensores (ou seja, a equipe azul – Blue Team) em um ambiente operacional.



Fonte: Imagem criada por Inteligência Artificial no Bing.

## Red Team - atividades

O trabalho do Red Team pode ser dividido em quatro etapas principais: planejamento, execução, análise e recomendação.

**Planejamento:** o Red Team define o escopo, os objetivos, as regras e os limites do teste de ciberataque. Eles devem levar em conta as características da empresa, os sistemas envolvidos, os riscos associados, e as expectativas dos contratantes.



Fonte: Imagem criada por Inteligência Artificial no Bing.

## Red Team - atividades

O planejamento também envolve a coleta de informações sobre o alvo, como **endereços IP, domínios, portas abertas, serviços rodando, vulnerabilidades conhecidas**, entre outros. Esses dados são usados para mapear a superfície de ataque e escolher as melhores estratégias para explorá-las.

**Execução:** o Red Team coloca em prática as ações planejadas para tentar invadir os sistemas da empresa. Eles podem usar diferentes métodos de ataque, como **phishing, brute force, SQL injection, cross-site scripting**, entre outros.



Fonte: Imagem criada por Inteligência Artificial no Bing.

## Red Team - atividades

O Red Team também pode usar técnicas de **engenharia social** para enganar ou persuadir os funcionários da empresa a fornecerem informações ou acessos privilegiados. Por exemplo, eles podem se passar por clientes, fornecedores ou colegas de trabalho para enviar e-mails maliciosos ou fazer ligações falsas.

O Red Team deve **documentar** todas as suas **atividades durante a execução do teste**, registrando as evidências das vulnerabilidades encontradas, os impactos causados e as dificuldades enfrentadas.



Fonte: Imagem criada por Inteligência Artificial no Bing.

## Red Team - atividades

**Análise:** o Red Team analisa os resultados obtidos durante a execução do teste. Eles devem verificar se conseguiram **atingir os objetivos definidos no planejamento**, quais foram as falhas mais críticas e frequentes nos sistemas de defesa da empresa, e quais foram as **lições aprendidas** com a experiência.

A análise também envolve a classificação das vulnerabilidades encontradas de acordo com o seu **nível de gravidade, probabilidade e urgência**. Assim, eles podem priorizar as correções mais importantes e efetivas.

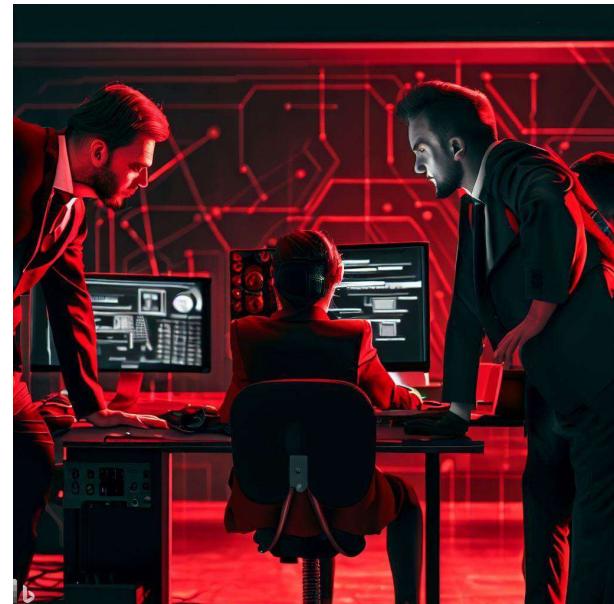


Fonte: Imagem criada por Inteligência Artificial no Bing.

## Red Team - atividades

**Recomendação:** o Red Team elabora um **relatório detalhado** com as conclusões da análise. O relatório deve conter uma descrição **clara e objetiva** das vulnerabilidades encontradas, as evidências coletadas, os impactos gerados e as recomendações para mitigá-las.

O relatório deve ser apresentado aos contratantes do teste de ciberataque, que podem ser gestores ou responsáveis pela segurança da informação na empresa. O Red Team deve explicar os resultados obtidos e esclarecer as dúvidas que possam surgir.



Fonte: Imagem criada por Inteligência Artificial no Bing.

## Red Team - atividades

O relatório também deve servir como base para a **implementação das correções** sugeridas pelo Red Team. Essas correções podem envolver desde a atualização de softwares e sistemas operacionais até a mudança de políticas e procedimentos internos.



Fonte: Imagem criada por Inteligência Artificial no Bing.

## Red Team – habilidades

Para se tornar um profissional de Cibersegurança que atua como Red Team, é preciso ter algumas **habilidades** e certificações **específicas**. Entre elas, podemos destacar:

Conhecimento avançado sobre redes, sistemas operacionais, protocolos, serviços e ferramentas de segurança;

Conhecimento sobre as principais técnicas de ataque e invasão cibernética, como exploração de vulnerabilidades, injeção de código, spoofing, sniffing, entre outras;



Fonte: RedTeam – Equipe Vermelha.  
Disponível em [https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000\\_F\\_547993174\\_6SRwBS1T8YVVnu6JIdT7L2ixIJDh4K5.jpg](https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000_F_547993174_6SRwBS1T8YVVnu6JIdT7L2ixIJDh4K5.jpg). Acesso em 10 Maio, 2023.

## Red Team – habilidades

Conhecimento sobre as principais técnicas de engenharia social, como phishing, vishing, baiting, entre outras;

Capacidade de planejar, executar, analisar e reportar testes de ciberataque de forma eficiente e ética;

Capacidade de se comunicar de forma clara e objetiva com os contratantes e os demais membros da equipe;



Fonte: RedTeam – Equipe Vermelha.  
Disponível em [https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000\\_F\\_547993174\\_6SRwBS1T8YVVnu6JIdT7L2ixHJDh4K5.jpg](https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000_F_547993174_6SRwBS1T8YVVnu6JIdT7L2ixHJDh4K5.jpg). Acesso em 10 Maio. 2023

## Red Team – habilidades

Capacidade de trabalhar em equipe e colaborar com outros profissionais da área;

Capacidade de se atualizar constantemente sobre as novidades e ameaças do cenário cibernético.



Fonte: RedTeam – Equipe Vermelha.  
Disponível em [https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000\\_F\\_547993174\\_6SRwBS1T8YVVnu6JIdT7L2ixHJDh4K5.jpg](https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000_F_547993174_6SRwBS1T8YVVnu6JIdT7L2ixHJDh4K5.jpg). Acesso em 10 Maio. 2023

## Red Team – desafios e benefícios

O trabalho do Red Team é desafiador por vários motivos. Primeiro, porque exige um alto nível de conhecimento técnico sobre as diversas formas de ataque cibernético existentes. Segundo, porque exige uma capacidade de adaptação e criatividade para lidar com as diferentes situações que podem surgir durante o teste. Terceiro, porque exige uma ética profissional e um compromisso com a confidencialidade dos dados e informações acessados.



Fonte: RedTeam – Equipe Vermelha.  
Disponível em [https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000\\_F\\_547993174\\_6SRwBS1T8YVVnu6JIdT7L2ixHJDh4K5.jpg](https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000_F_547993174_6SRwBS1T8YVVnu6JIdT7L2ixHJDh4K5.jpg). Acesso em 10 Maio. 2023

## Red Team – desafios e benefícios

Por outro lado, o trabalho do Red Team também traz muitos benefícios. Primeiro, porque contribui para a melhoria contínua da segurança da informação na empresa, reduzindo os riscos de ataques reais e seus prejuízos. Segundo, porque proporciona um aprendizado constante sobre as novas tendências e tecnologias do mercado de cibersegurança. Terceiro, porque oferece uma oportunidade de crescimento profissional e reconhecimento na área.



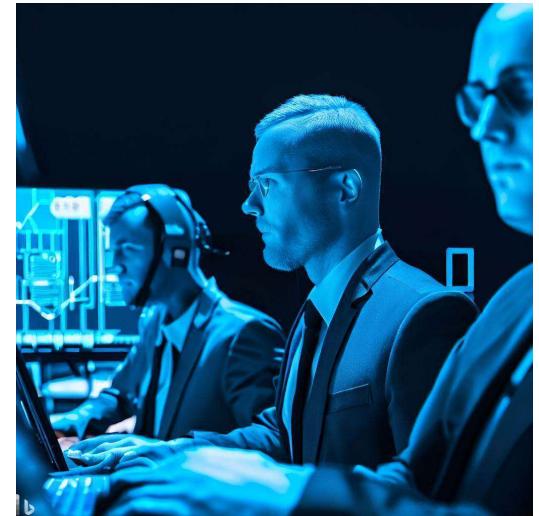
Fonte: RedTeam – Equipe Vermelha.  
Disponível em [https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000\\_F\\_547993174\\_6SRwBS1T8YVVnu6JIdT7L2ixHJDh4K5.jpg](https://as2.ftcdn.net/v2/jpg/05/47/99/31/1000_F_547993174_6SRwBS1T8YVVnu6JIdT7L2ixHJDh4K5.jpg). Acesso em 10 Maio. 2023



# Blue Team

## Blue Team (equipe azul) – o que é

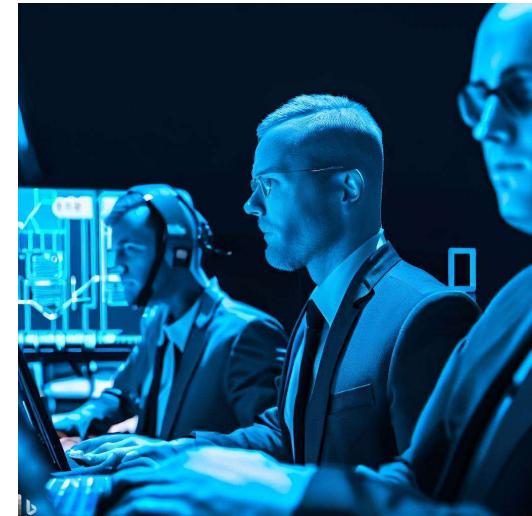
Um profissional de cibersegurança da equipe azul é um especialista em segurança responsável por defender os sistemas de informação de uma organização e garantir sua segurança contra possíveis ameaças cibernéticas. Eles concentram-se em **manter e melhorar a postura de segurança** da organização, identificando falhas de segurança, verificando a eficácia das medidas de segurança e garantindo que essas medidas **permaneçam eficazes após a implementação**. Eles usam seus conhecimentos e habilidades para fins legítimos e benéficos.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Blue Team – o que é

O objetivo do Blue Team é fortalecer as barreiras e os mecanismos de proteção da empresa, e reagir rapidamente aos incidentes de segurança que possam ocorrer. Assim, eles ajudam a garantir a **confidencialidade, a integridade e a disponibilidade** das informações, e evitar os prejuízos causados por ataques cibernéticos.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Blue Team – atividades

Alguns exemplos de atividades realizadas por profissionais de cibersegurança Blue Team incluem:

**Monitoramento:** Blue Team acompanha constantemente o funcionamento dos sistemas e das redes da empresa, verificando se há algum sinal de **anomalia ou intrusão**. Eles usam ferramentas como firewalls, antivírus, IDS (Intrusion Detection System ou Sistema de Detecção de Intrusão), IPS (Intrusion Prevention System ou Sistema de Prevenção de Intrusão), entre outras.



Fonte: Blue Team—Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/TyT4KoFCEaU>. Acesso em 25 Maio. 2023

## Blue Team – atividades

O monitoramento também envolve a coleta e a análise de dados sobre o tráfego e o comportamento dos usuários na rede, como **endereços IP, portas abertas, serviços rodando, logs de acesso**, entre outros. Esses dados são usados para identificar padrões normais e anormais de atividade, e alertar sobre possíveis ataques.



Fonte: Blue Team— Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/TyT4KoFCEaU>. Acesso em 25 Maio. 2023

## Blue Team – atividades

**Detecção:** Blue Team verifica se há alguma evidência de ataque cibernético em andamento ou concluído. Eles usam técnicas como **análise forense, engenharia reversa, análise de malware**, entre outras.

O Blue Team deve validar se os alertas recebidos são verdadeiros ou falsos positivos, e **classificar** os ataques de acordo com o seu **nível de gravidade, probabilidade e urgência**. Assim, eles podem priorizar as respostas mais adequadas e eficazes.



Fonte: Blue Team— Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/TyT4KoFCEaU>. Acesso em 25 Maio. 2023

## Blue Team – atividades

**Resposta:** Blue Team executa as ações necessárias para conter e neutralizar os ataques cibernéticos detectados. Eles usam ferramentas como **isolamento de rede, bloqueio de acesso, remoção de malware, restauração de backup**, entre outras.

O Blue Team deve **documentar** todas as suas atividades durante a resposta ao incidente, registrando as evidências dos ataques sofridos, os impactos causados e as soluções aplicadas.



Fonte: Blue Team— Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/TyT4KoFCEaU>. Acesso em 25 Maio. 2023

## Blue Team – atividades

**Mitigação:** Blue Team analisa os resultados obtidos durante a **resposta ao incidente**. Eles devem verificar se conseguiram **eliminar ou minimizar** os danos causados pelos ataques cibernéticos, quais foram as falhas mais críticas e frequentes nos sistemas de defesa da empresa, e quais foram as lições aprendidas com a experiência.



Fonte: Blue Team— Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/TyT4KoFCEaU>. Acesso em 25 Maio. 2023

## Blue Team – atividades

A mitigação também envolve a **implementação das correções** sugeridas pelo Blue Team. Essas correções podem envolver desde a atualização de softwares e sistemas operacionais até a mudança de políticas e procedimentos internos.



Fonte: Blue Team— Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/Ty4KoFCEaU>. Acesso em 25 Maio. 2023

## Blue Team – habilidades

Algumas das principais habilidades necessárias para um profissional de cibersegurança Blue Team incluem:

Conhecimento avançado sobre redes, sistemas operacionais, protocolos, serviços e ferramentas de segurança.

Conhecimento sobre as principais técnicas de defesa e prevenção cibernética, como firewall, antivírus, criptografia, backup, entre outras.



Fonte: Blue Team – Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/3TiNowmZluA>. Acesso em 25 Maio, 2023.

## Blue Team – habilidades

Conhecimento sobre as principais técnicas de resposta e mitigação cibernética, como análise forense, engenharia reversa, análise de malware, entre outras.

Capacidade de monitorar, detectar, responder e mitigar ameaças virtuais de forma eficiente e ética.

Capacidade de se comunicar de forma clara e objetiva com os contratantes e os demais membros da equipe.



Fonte: Blue Team – Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/3TiNowmZluA>. Acesso em 25 Maio. 2023.

## Blue Team – habilidades

Capacidade de trabalhar em equipe e colaborar com outros profissionais da área.

Capacidade de se atualizar constantemente sobre as novidades e ameaças do cenário cibernético.



Fonte: Blue Team– Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/3TiNowmZluA>. Acesso em 25 Maio, 2023.

## Blue Team – desafios e benefícios

O trabalho do Blue Team é desafiador por vários motivos. Primeiro, porque exige um alto nível de conhecimento técnico sobre as diversas formas de defesa e prevenção cibernética existentes. Segundo, porque exige uma capacidade de reação rápida e eficiente diante dos ataques cibernéticos que possam ocorrer. Terceiro, porque exige uma ética profissional e um compromisso com a confidencialidade dos dados e informações protegidos.



Fonte: Blue Team– Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/3TiNowmZluA>. Acesso em 25 Maio, 2023.

## Blue Team – desafios e benefícios

Por outro lado, o trabalho do Blue Team também traz muitos benefícios. Primeiro, porque contribui para a manutenção da segurança da informação na empresa, garantindo a confiança e a reputação do negócio. Segundo, porque proporciona um aprendizado constante sobre as novas tendências e tecnologias do mercado de cibersegurança. Terceiro, porque oferece uma oportunidade de crescimento profissional e reconhecimento na área.



Fonte: Blue Team – Equipe Azul.  
Disponível em <https://unsplash.com/pt-br/fotografias/3TiNowmZluA>. Acesso em 25 Maio. 2023



# Forense

# Forense Cibernético – o que é

Um profissional de cibersegurança forense, também conhecido como analista de forense digital ou analista forense de computador, é um especialista que analisa **evidências digitais e investiga incidentes de segurança** cibernética para extrair informações úteis em apoio à mitigação de vulnerabilidades de sistemas e redes. O objetivo do Forense Digital é **identificar e rastrear** os autores e as vítimas desses crimes ou incidentes, coletando evidências que possam ser usadas em **processos judiciais ou administrativos**. Assim, o Forense Digital contribui para a aplicação da lei e da justiça no âmbito digital.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Forense Cibernético – o que é

O Forense Digital é uma ciência que **aplica métodos científicos** para analisar dados e dispositivos digitais relacionados a **crimes cibernéticos** ou **incidentes de segurança**. Esses crimes podem envolver desde fraudes, extorsões, invasões, sabotagens, espionagens, até violações de direitos autorais, pornografia infantil, cyberbullying, entre outros.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Forense Cibernético – atividades



**Coleta:** o Forense Digital realiza a busca e a apreensão dos dados e dispositivos digitais que possam estar relacionados ao crime ou incidente investigado. Esses dados e dispositivos podem estar em diferentes locais, como computadores, celulares, tablets, pendrives, cartões de memória, servidores, nuvens, redes sociais, entre outros.



Fonte: Forense Digital.  
Disponível em <https://pixabay.com/pt/illustrations/dedo-impress%C3%A3o-digital-seguran%C3%A7a-2081169/>. Acesso em 28 Maio. 2023

# Forense Cibernético – atividades



O Forense Digital deve **seguir os protocolos legais** para realizar a coleta dos dados e dispositivos digitais, respeitando os direitos e as garantias dos envolvidos. Além disso, o Forense Digital deve **documentar** todas as suas ações durante a coleta, registrando as informações sobre os locais, as datas, as horas, as pessoas, os equipamentos e os procedimentos utilizados.



Fonte: Forense Digital.  
Disponível em <https://pixabay.com/pt/illustrations/dedo-impress%C3%A3o-digital-seguran%C3%A7a-2081169/>. Acesso em 28 Maio. 2023

# Forense Cibernético – atividades



**Preservação:** o Forense Digital realiza a proteção dos dados e dispositivos digitais coletados contra alterações ou **perdas acidentais ou intencionais**. Essa proteção é essencial para garantir a **integridade** e a **autenticidade** das evidências digitais.



Fonte: Forense Digital.  
Disponível em <https://pixabay.com/pt/illustrations/dedo-impress%C3%A3o-digital-seguran%C3%A7a-2081169/>. Acesso em 28 Maio. 2023

# Forense Cibernético – atividades

O Forense Digital deve usar técnicas como selagem física (proteger fisicamente os ativos de tecnologia da informação), etiquetagem digital, criptografia, hash ou checksum para preservar os dados e dispositivos digitais coletados. Além disso, o Forense Digital deve armazenar os dados e dispositivos digitais coletados em **locais seguros e controlados**.



Fonte: Forense Digital.  
Disponível em <https://pixabay.com/pt/illustrations/dedo-impress%C3%A3o-digital-seguran%C3%A7a-2081169/>. Acesso em 28 Maio, 2023.

# Forense Cibernético – atividades



**Análise:** o Forense Digital realiza a extração e a interpretação dos dados e dispositivos digitais preservados. Essa extração e interpretação visa **encontrar as evidências** que possam esclarecer o que aconteceu, quando aconteceu, como aconteceu, quem fez e quem foi afetado pelo **crime ou incidente investigado**.



Fonte: Forense Digital.  
Disponível em <https://pixabay.com/pt/illustrations/dedo-impress%C3%A3o-digital-seguran%C3%A7a-2081169/>. Acesso em 28 Maio. 2023

## Forense Cibernético – atividades

O Forense Digital deve usar técnicas como duplicação de imagem forense, recuperação de dados apagados, análise de arquivos, análise de logs, análise de rede, análise de malware, entre outras. Além disso, o Forense Digital deve usar ferramentas confiáveis e validadas para realizar a análise dos dados e dispositivos digitais preservados.



Fonte: Forense Digital.  
Disponível em <https://pixabay.com/pt/illustrations/dedo-impress%C3%A3o-digital-seguran%C3%A7a-2081169/>. Acesso em 28 Maio. 2023

# Forense Cibernético – atividades

**Apresentação:** o Forense Digital realiza a comunicação e a divulgação dos resultados da análise dos dados e dispositivos digitais preservados. Essa comunicação e divulgação visa fornecer as evidências e as conclusões que possam auxiliar na tomada de decisão dos responsáveis pelo caso.



Fonte: Forense Digital.  
Disponível em <https://pixabay.com/pt/illustrations/dedo-impress%C3%A3o-digital-seguran%C3%A7a-2081169/>. Acesso em 28 Maio. 2023

# Forense Cibernético – atividades

O Forense Digital deve **elaborar um relatório técnico** que contenha as informações sobre o caso, os métodos e as ferramentas utilizados, as evidências e as conclusões encontradas. Além disso, o Forense Digital deve estar preparado para apresentar e defender o seu relatório perante os **órgãos competentes, como juízes, promotores, advogados ou gestores**.



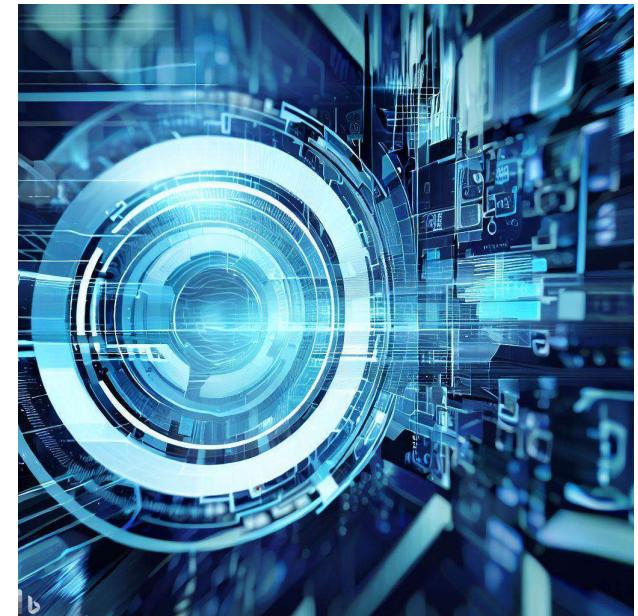
Fonte: Forense Digital.  
Disponível em <https://pixabay.com/pt/illustrations/dedo-impress%C3%A3o-digital-seguran%C3%A7a-2081169/>. Acesso em 28 Maio. 2023

## Forense Cibernético – habilidades

Para se tornar um profissional de Cibersegurança que atua como Forense Digital, é preciso ter algumas habilidades e certificações específicas. Entre elas, podemos destacar:

Conhecimento avançado sobre sistemas operacionais, redes, protocolos, serviços e ferramentas digitais;

Conhecimento sobre as principais técnicas e ferramentas de análise forense digital, como duplicação de imagem forense, recuperação de dados apagados, análise de arquivos, análise de logs, análise de rede, análise de malware, entre outras;

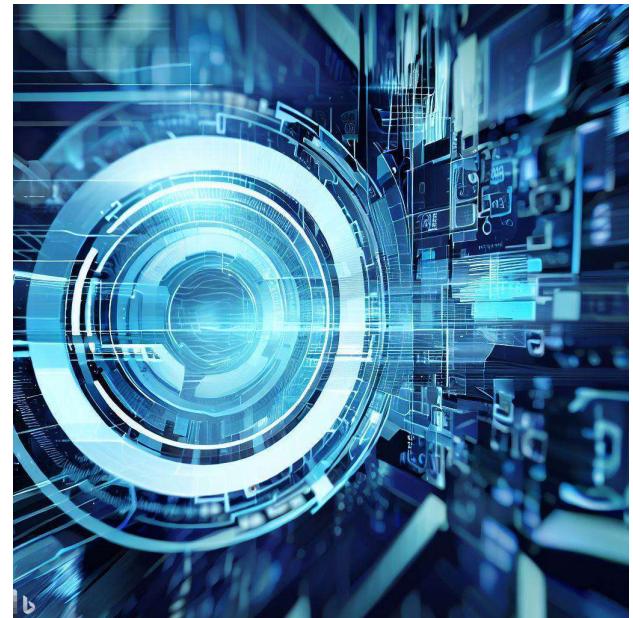


Fonte: Imagem criada por Inteligência Artificial no Bing.

## Forense Cibernético – habilidades

Capacidade de coletar, preservar, analisar e apresentar evidências digitais de forma válida e confiável;

Capacidade de se comunicar de forma clara e objetiva com os contratantes e os demais envolvidos no caso;

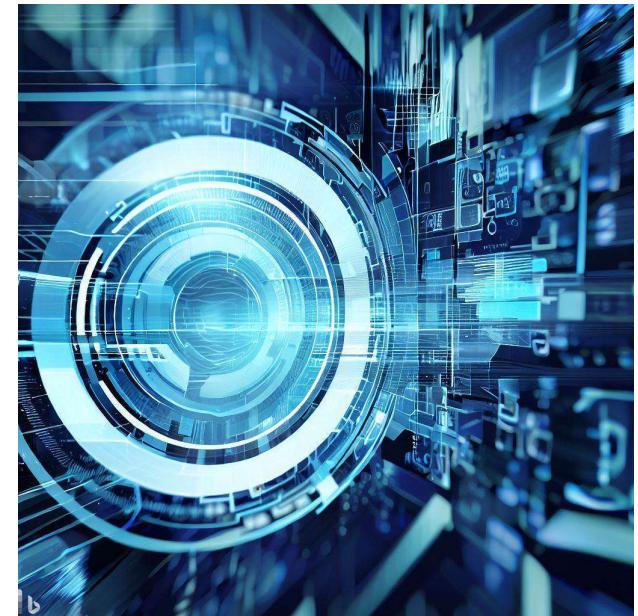


Fonte: Imagem criada por Inteligência Artificial no Bing.

## Forense Cibernético – habilidades

Capacidade de trabalhar em equipe e colaborar com outros profissionais da área;

Capacidade de se atualizar constantemente sobre as novidades e ameaças do cenário digital.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Forense Cibernético – desafios e benefícios



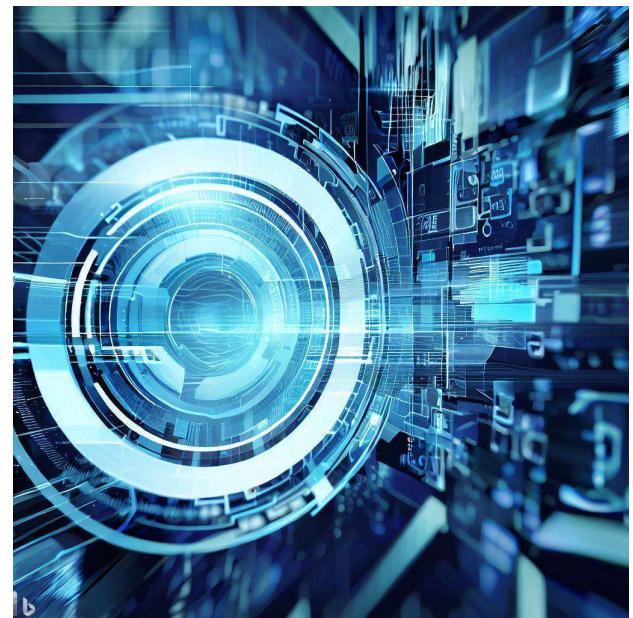
O trabalho do Forense Digital é desafiador por vários motivos. Primeiro, porque exige um alto nível de conhecimento técnico sobre as diversas tecnologias e ferramentas envolvidas no cenário digital. Segundo, porque exige uma capacidade de raciocínio lógico e analítico para solucionar problemas complexos e dinâmicos. Terceiro, porque exige uma ética profissional e um compromisso com a verdade e a justiça.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Forense Cibernético – desafios e benefícios

Por outro lado, o trabalho do Forense Digital também traz muitos benefícios. Primeiro, porque contribui para a elucidação de crimes cibernéticos ou incidentes de segurança que afetam milhares de pessoas e organizações. Segundo, porque proporciona um aprendizado constante sobre as novas tendências e ameaças do mundo digital. Terceiro, porque oferece uma oportunidade de crescimento profissional e reconhecimento na área.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# GRG - governança, risco e conformidade

## GRG cibernético – o que é

Governança, Risco e Conformidade (GRG), é um conjunto de conceitos que visa **integrar e otimizar** os processos de cibersegurança nas empresas. O objetivo é assegurar que as empresas estejam **protegidas contra ataques cibernéticos**, em **conformidade** com as **normas e os regulamentos de cibersegurança**, e alinhadas com as suas metas e valores.



Fonte: GRC – Governança Risco e Compliance.

Disponível em:

[https://as1.ftcdn.net/v2/jpg/01/33/86/84/1000\\_F\\_133868469\\_sK9gZlXOADD4kSBT9L0BhmhBhHsihb.jpg](https://as1.ftcdn.net/v2/jpg/01/33/86/84/1000_F_133868469_sK9gZlXOADD4kSBT9L0BhmhBhHsihb.jpg). Acesso em 30 Maio. 2023

O papel do profissional de Cibersegurança que atua como GRG é coordenar e supervisionar esses processos, garantindo que eles sejam **eficientes, eficazes e transparentes**.

# GRG cibernético – o que é

Os profissionais de GRC trabalham em estreita colaboração com as equipes de TI e segurança para criar uma estratégia abrangente de cibersegurança que esteja alinhada aos objetivos de negócios, gerenciando efetivamente os riscos cibernéticos e atendendo aos **requisitos regulatórios.**

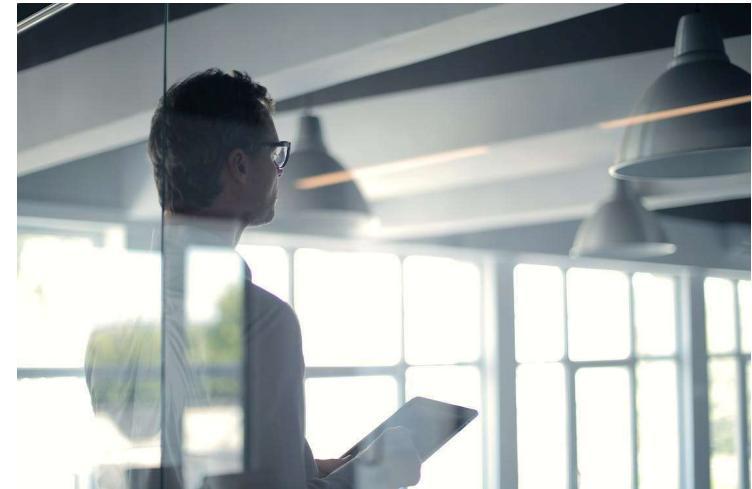


Fonte: GRC – Governança Risco e Compliance.  
Disponível em:  
[https://as1.ftcdn.net/v2/jpg/01/33/86/84/1000\\_F\\_133868469\\_sK9gZltXOADD4kSBT9L0BhmhBhHtsihb.jpg](https://as1.ftcdn.net/v2/jpg/01/33/86/84/1000_F_133868469_sK9gZltXOADD4kSBT9L0BhmhBhHtsihb.jpg). Acesso em 30 Maio. 2023

## GRG cibernético – atividades

Na área de governança, o GRG é responsável por definir e implementar as políticas, os procedimentos, os papéis e as responsabilidades relacionados à cibersegurança na empresa. Ele também deve estabelecer e monitorar os indicadores de desempenho e qualidade da cibersegurança, bem como **comunicar e reportar** os resultados aos stakeholders internos e externos.

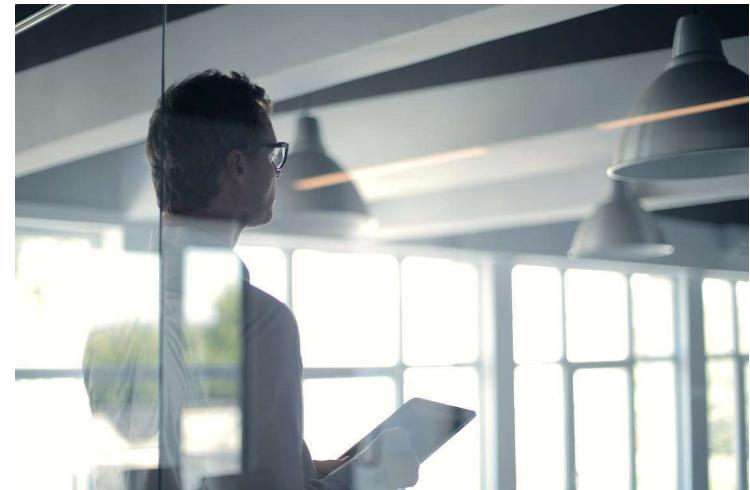
O objetivo da governança é garantir que a cibersegurança esteja **alinhada com a estratégia, a cultura e a missão** da empresa, bem como com as expectativas dos clientes, dos parceiros e da sociedade.



Fonte: Governança Risco e Compliance.  
Disponível em: <https://unsplash.com/pt-br/fotografias/pYysG78E-Zs>, Acesso em 30 Maio. 2023

## GRG cibernético – atividades

Na área de risco, o GRG é responsável por **identificar, avaliar, tratar e monitorar** os riscos relacionados à cibersegurança na empresa. Ele também deve desenvolver e implementar planos de contingência e recuperação em caso de incidentes ou crises de cibersegurança.



O objetivo do risco é garantir que a empresa esteja preparada para enfrentar as ameaças virtuais, minimizando os impactos negativos sobre a sua reputação, a sua operação e o seu resultado.

Fonte: Governança Risco e Compliance.  
Disponível em: <https://unsplash.com/pt-br/fotografias/pYysG78E-Zs>, Acesso em 30 Maio. 2023

## GRG cibernético – atividades

Na área de conformidade, o GRG é responsável por verificar e garantir que a empresa esteja em **conformidade com as leis, os regulamentos, as normas e os padrões** de cibersegurança aplicáveis ao seu setor ou mercado. Ele também deve realizar auditorias internas e externas para avaliar a eficácia dos controles de segurança implementados na empresa.

O objetivo da conformidade é **garantir** que a empresa esteja **protegida contra sanções legais ou regulatórias**, bem como contra perdas financeiras ou processuais decorrentes de violações ou falhas na cibersegurança.



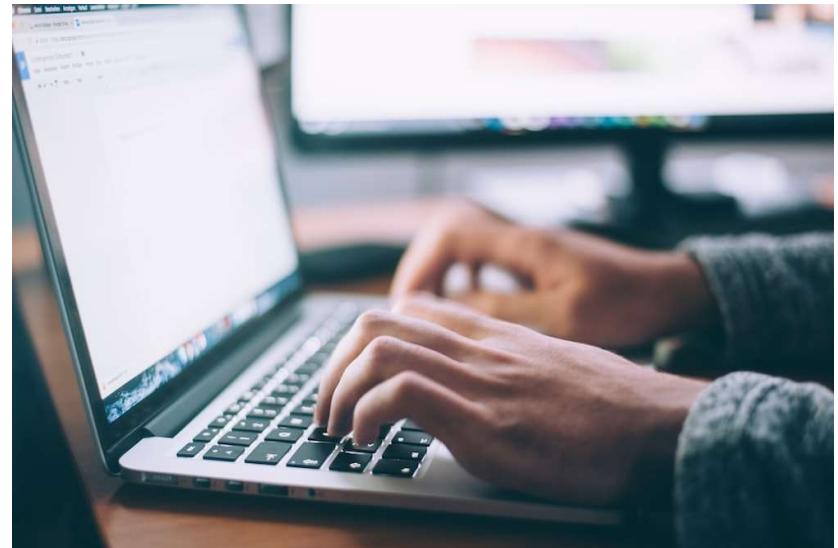
Fonte: Governança Risco e Compliance.  
Disponível em: <https://unsplash.com/pt-br/fotografias/npxXWgQ33ZQ>, Acesso em 30 Maio. 2023

## GRC cibernético – habilidades

Para se tornar um profissional de Cibersegurança que atua como GRC, é preciso ter algumas habilidades e certificações específicas. Entre elas, podemos destacar:

Conhecimento avançado sobre as leis, os regulamentos, as normas e os padrões de cibersegurança aplicáveis ao setor ou mercado da empresa;

Conhecimento sobre as melhores práticas e metodologias de governança, risco e conformidade em cibersegurança;



Fonte: Governança Risco e Compliance.  
Disponível em: <https://unsplash.com/pt-br/fotografias/npxXWgQ33ZQ>, Acesso em 30 Maio. 2023

## GRC cibernético – habilidades

Capacidade de definir e implementar políticas, procedimentos, papéis e responsabilidades em cibersegurança na empresa;

Capacidade de identificar, avaliar, tratar e monitorar os riscos em cibersegurança na empresa;

Capacidade de verificar e garantir a conformidade da empresa com as leis e os regulamentos de cibersegurança;



Fonte: Governança Risco e Compliance.  
Disponível em: <https://unsplash.com/pt-br/fotografias/npxXWgQ33ZQ>, Acesso em 30 Maio. 2023

# GRC cibernético – habilidades



Capacidade de estabelecer e monitorar os indicadores de desempenho e qualidade da cibersegurança na empresa;

Capacidade de comunicar e reportar os resultados da cibersegurança aos stakeholders internos e externos da empresa;

Capacidade de realizar auditorias internas e externas em cibersegurança na empresa;



Fonte: Governança Risco e Compliance.  
Disponível em: <https://unsplash.com/pt-br/fotografias/npxXWgQ33ZQ>, Acesso em 30 Maio. 2023

## GRC cibernético – habilidades

Capacidade de desenvolver e implementar planos de contingência e recuperação em caso de incidentes ou crises de cibersegurança na empresa;

Capacidade de trabalhar em equipe e colaborar com outros profissionais da área.



Fonte: Governança Risco e Compliance.  
Disponível em: <https://unsplash.com/pt-br/fotografias/npxXWgQ33ZQ>, Acesso em 30 Maio. 2023

# GRG cibernético – desafios e benefícios



O trabalho do GRC é desafiador por vários motivos. Primeiro, porque exige um alto nível de conhecimento sobre as diversas leis, regulamentos, normas e padrões de cibersegurança que afetam a empresa. Segundo, porque exige uma capacidade de gerenciar e coordenar múltiplos processos e projetos de cibersegurança, envolvendo diferentes áreas e pessoas da empresa. Terceiro, porque exige uma habilidade de se comunicar e negociar com os diversos stakeholders internos e externos da empresa, como clientes, fornecedores, auditores, reguladores, entre outros.



Fonte: Governança Risco e Compliance.  
Disponível em: <https://unsplash.com/pt-br/fotografias/npxXWgQ33ZQ>, Acesso em 30 Maio. 2023

# GRG cibernético – desafios e benefícios



Por outro lado, o trabalho do GRC também traz muitos benefícios. Primeiro, porque contribui para a proteção da empresa contra ataques cibernéticos, que podem causar danos irreparáveis à sua imagem, à sua operação e ao seu resultado. Segundo, porque contribui para a conformidade da empresa com as leis e os regulamentos de cibersegurança, que podem evitar sanções legais ou regulatórias, bem como perdas financeiras ou processuais. Terceiro, porque contribui para o alinhamento da cibersegurança com a estratégia e a cultura da empresa, que podem aumentar a sua competitividade e o seu valor no mercado.



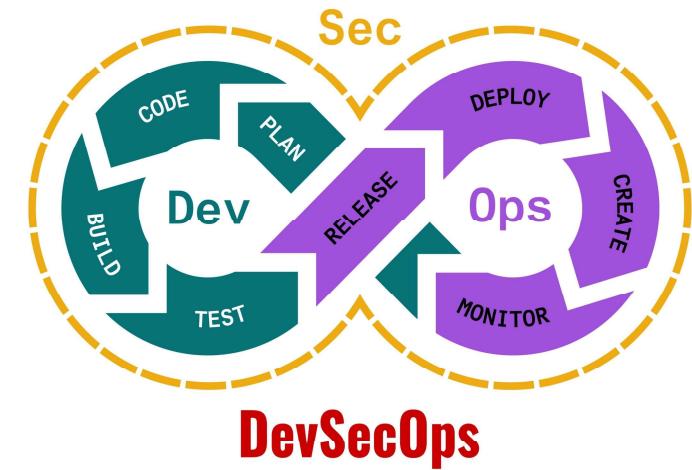
Fonte: Governança Risco e Compliance.  
Disponível em: <https://unsplash.com/pt-br/fotografias/npxXWgQ33ZQ>, Acesso em 30 Maio. 2023



# DevSecOps

# DevSecOps – o que é

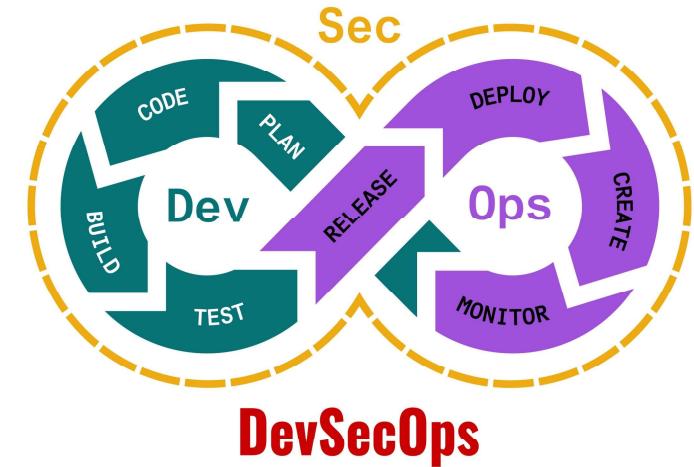
**DevSecOps** é uma abreviação de Development, Security e Operations, ou seja, **Desenvolvimento, Segurança e Operações**. Esse termo representa uma evolução do DevOps, que é uma abordagem para o desenvolvimento de software que **visa integrar e agilizar os processos entre as equipes de desenvolvimento e operações**.



Fonte: Forense Digital.  
Disponível em [https://as2.ftcdn.net/v2/jpg/03/86/17/23/1000\\_F\\_386172307\\_CtawKu2XgGIJZZKvcOnei4bFmegDYMca.jpg](https://as2.ftcdn.net/v2/jpg/03/86/17/23/1000_F_386172307_CtawKu2XgGIJZZKvcOnei4bFmegDYMca.jpg).  
Acesso em 29 Maio. 2023

# DevSecOps – o que é

O DevSecOps acrescenta a segurança como um elemento essencial nessa **integração e agilização, automatizando a incorporação da segurança** em todas as fases do ciclo de vida de desenvolvimento de software. O objetivo é garantir que o software seja desenvolvido com qualidade, segurança e eficiência, reduzindo os riscos de ataques cibernéticos ou falhas na entrega.



Fonte: Forense Digital.

Disponível em [https://as2.ftcdn.net/v2/jpg/03/86/17/23/1000\\_F\\_386172307\\_CtawKu2XgGlJZZKvcOnei4bFmegDYmca.jpg](https://as2.ftcdn.net/v2/jpg/03/86/17/23/1000_F_386172307_CtawKu2XgGlJZZKvcOnei4bFmegDYmca.jpg).  
Acesso em 29 Maio. 2023

O papel do profissional de Cibersegurança que atua como **DevSecOps** é coordenar e executar as atividades de segurança em conjunto com as equipes de **desenvolvimento e operações**, garantindo que elas sejam realizadas de forma contínua, colaborativa e transparente.

## DevSecOps – atividades

Na área de desenvolvimento, o **DevSecOps** é responsável por aplicar as práticas e os princípios de desenvolvimento **ágil e contínuo**, como Scrum, Kanban, Lean, entre outros. Ele também deve usar as ferramentas e os frameworks adequados para cada projeto, como Java, Python, Ruby on Rails, entre outros.

O objetivo do desenvolvimento é criar softwares que atendam às necessidades e às expectativas dos clientes, com **qualidade, funcionalidade e usabilidade**.



Fonte: Forense Digital.  
Disponível em: <https://www.pexels.com/photo/hands-on-a-laptop-keyboard-5483071/>. Acesso em 29 Maio. 2023

## DevSecOps – atividades

Na área de segurança, o **DevSecOps** é responsável por aplicar as práticas e os princípios de segurança por design e por padrão, como OWASP Top 10, SANS Top 25, entre outros. Ele também deve usar as ferramentas e os métodos adequados para cada projeto, **como análise estática ou dinâmica de código, teste de penetração ou vulnerabilidade, entre outros.**



Fonte: Forense Digital.  
Disponível em: <https://www.pexels.com/photo/hands-on-a-laptop-keyboard-5483071/>. Acesso em 29 Maio. 2023

O objetivo da segurança é proteger os softwares contra **ameaças cibernéticas ou falhas internas**, com qualidade, confidencialidade e integridade.

# DevSecOps – atividades

Na área de operações, o DevSecOps é responsável por aplicar as práticas e os princípios de **operações ágeis e contínuas**, como integração contínua, entrega contínua, infraestrutura como código, entre outros. Ele também deve usar as ferramentas e os serviços adequados para cada projeto, como Docker, Kubernetes, AWS, Azure, entre outros.



Fonte: Forense Digital.  
Disponível em: <https://www.pexels.com/photo/hands-on-a-laptop-keyboard-5483071/>. Acesso em 29 Maio. 2023

O objetivo das operações é implantar e manter os softwares em ambientes de produção ou de teste, com **eficiência, disponibilidade e escalabilidade**.

## DevSecOps – habilidades

Para se tornar um profissional de Cibersegurança que atua como DevSecOps, é preciso ter algumas habilidades e certificações específicas. Entre elas, podemos destacar:

Conhecimento avançado sobre as técnicas e as ferramentas de desenvolvimento ágil e contínuo;

Conhecimento avançado sobre as técnicas e as ferramentas de segurança por design e por padrão;



Fonte: Imagem criada por Inteligência Artificial no Bing.

# DevSecOps – habilidades



Conhecimento avançado sobre as técnicas e as ferramentas de operações ágeis e contínuas;

Capacidade de integrar e automatizar as técnicas e as ferramentas de desenvolvimento, segurança e operações em um fluxo de trabalho contínuo e colaborativo;



Fonte: Imagem criada por Inteligência Artificial no Bing.

## DevSecOps – habilidades

Capacidade de se adaptar às mudanças constantes nas demandas dos clientes e nas ameaças cibernéticas;

Capacidade de se comunicar e trabalhar em equipe com outros profissionais da área.



# DevSecOps – desafios e benefícios



O trabalho do DevSecOps é desafiador por vários motivos. Primeiro, porque exige um alto nível de conhecimento sobre as diversas técnicas e ferramentas de desenvolvimento, segurança e operações. Segundo, porque exige uma capacidade de integrar e automatizar essas técnicas e ferramentas em um fluxo de trabalho contínuo e colaborativo. Terceiro, porque exige uma habilidade de se adaptar às mudanças constantes nas demandas dos clientes e nas ameaças cibernéticas.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# DevSecOps – desafios e benefícios



Por outro lado, o trabalho do DevSecOps também traz muitos benefícios. Primeiro, porque contribui para o desenvolvimento de softwares mais seguros e mais rápidos, que podem atender às necessidades e às expectativas dos clientes com mais qualidade e eficiência. Segundo, porque contribui para a redução dos riscos de ataques cibernéticos ou falhas na entrega, que podem causar danos à reputação, à operação e ao resultado da empresa. Terceiro, porque contribui para o aumento da produtividade e da satisfação das equipes de desenvolvimento, segurança e operações.



Fonte: Imagem criada por Inteligência Artificial no Bing.

# Conclusão

## Conclusão

Red Team: são os profissionais que simulam ataques cibernéticos contra os sistemas e as redes da empresa, com o objetivo de identificar e explorar as vulnerabilidades existentes. Eles usam as mesmas ferramentas e técnicas que os hackers maliciosos usariam, e reportam os resultados e as recomendações para a equipe de defesa. O papel do Red Team é testar e avaliar a segurança da informação da empresa, e ajudar a prevenir ataques reais.

# Conclusão

Blue Team: são os profissionais que se dedicam a defender os sistemas e as redes da empresa contra os ataques cibernéticos, sejam eles simulados ou reais. Eles usam ferramentas e técnicas de segurança defensiva, como firewall, antivírus, criptografia, backup, entre outras. Eles monitoram, detectam, respondem e mitigam as ameaças virtuais, e fortalecem os mecanismos de proteção da empresa. O papel do BlueTeam é manter e melhorar a segurança da informação da empresa, e garantir a confiança e a reputação do negócio.

# Conclusão

DevSecOps: são os profissionais que integram as práticas de segurança da informação no processo de desenvolvimento de software. Eles usam ferramentas e técnicas de automação, integração contínua, entrega contínua, monitoramento e feedback. Eles colaboram com as equipes de desenvolvimento (Dev), operações (Ops) e segurança (Sec) para garantir que o software seja seguro desde o início até o fim do ciclo de vida. O papel do DevSecOps é acelerar e otimizar o desenvolvimento de software seguro, e reduzir os riscos de falhas e vulnerabilidades.

# Conclusão

Forense Digital: são os profissionais que coletam, preservam, analisam e apresentam evidências digitais relacionadas a crimes cibernéticos ou incidentes de segurança. Eles usam ferramentas e técnicas de análise forense, engenharia reversa, análise de malware, entre outras. Eles podem atuar em diferentes contextos, como investigações policiais, judiciais ou corporativas. O papel do Forense Digital é identificar e rastrear os autores e as vítimas dos crimes cibernéticos ou incidentes de segurança, e auxiliar na aplicação da lei e da justiça.

# Conclusão



GRG: são os profissionais que gerenciam os processos de governança, risco e conformidade (GRG) relacionados à cibersegurança nas empresas. Eles usam ferramentas e técnicas de gestão de projetos, auditoria interna, análise de risco, controle interno, entre outras. Eles alinham as estratégias de cibersegurança com os objetivos do negócio, as normas regulatórias e as boas práticas do mercado. O papel do GRG digital é garantir que a empresa esteja em conformidade com as leis e os padrões de cibersegurança, e gerenciar os riscos associados à cibersegurança.

# Aula 4 – Conceitos Iniciais



# Vírus

# Vírus – o que é?

Um vírus de computador é um tipo de **software malicioso** (malware) que consegue se **autorreplicar** dentro do computador, em unidades conectadas a ele, via internet e também através de rede local, podendo **prejudicar a segurança de dados** de uma empresa ou de uma pessoa. Um vírus de computador se liga a outros programas ou arquivos e **modifica** o seu funcionamento, podendo **causar danos ou alterações indesejadas**.



Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/05/99/20/77/1000\\_F\\_599207792\\_23Wc3Af1jcF6cF2hIRmk85oHwiGmwivP.jpg](https://as2.ftcdn.net/v2/jpg/05/99/20/77/1000_F_599207792_23Wc3Af1jcF6cF2hIRmk85oHwiGmwivP.jpg).  
Acesso em 24 Maio. 2023

# Vírus – o que é?

Eles são projetados para se **esconder** e se **infiltrar** em nossos dispositivos sem o nosso conhecimento, agindo como **parasitas digitais**. Assim como os vírus biológicos, os vírus de computador precisam de um **hospedeiro** para se **propagar** e podem ter diferentes graus de severidade.

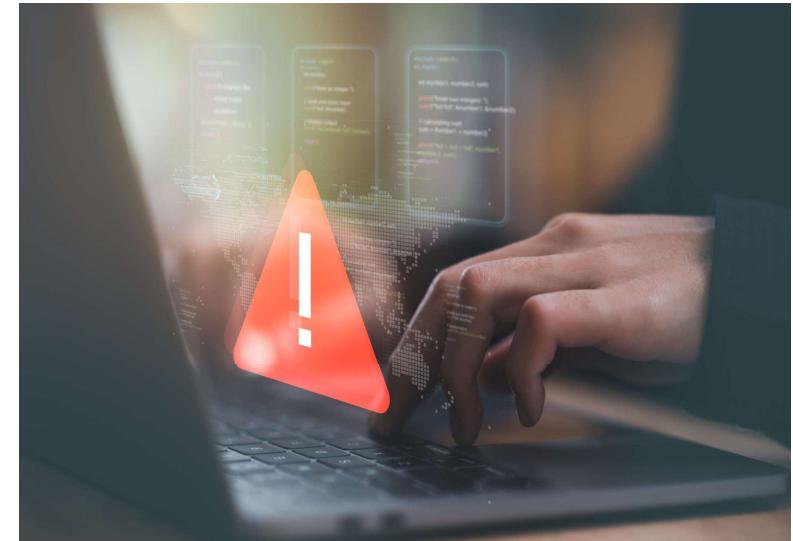


Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/05/99/20/77/1000\\_F\\_599207792\\_23Wc3Af1jcF6cF2hIRmk85oHwiGmwivP.jpg](https://as2.ftcdn.net/v2/jpg/05/99/20/77/1000_F_599207792_23Wc3Af1jcF6cF2hIRmk85oHwiGmwivP.jpg).  
Acesso em 24 Maio. 2023

# Vírus - Exemplos

Existem muitos tipos e exemplos de vírus de computador, cada um com características e objetivos diferentes. Alguns dos mais conhecidos são:

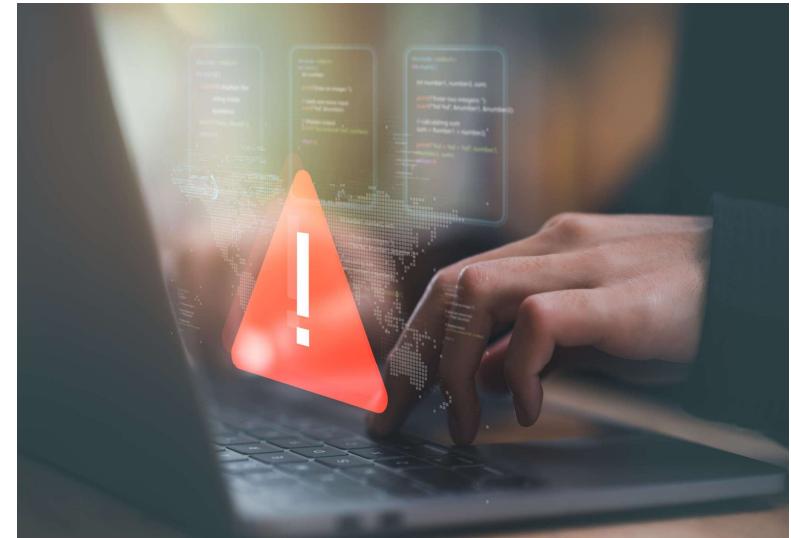
**Vírus de boot:** infectam a parte do **disco rígido** responsável pelo início do sistema operacional (o setor de inicialização ou boot). Eles impedem que o computador seja **iniciado corretamente** ou exibem mensagens falsas ou maliciosas na tela.



Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000\\_F\\_572860987\\_fhiuQM4q8SMgbJj9tKOST9hwYqgdmqh9.jpg](https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000_F_572860987_fhiuQM4q8SMgbJj9tKOST9hwYqgdmqh9.jpg).  
Acesso em 24 Maio. 2023

# Vírus - Exemplos

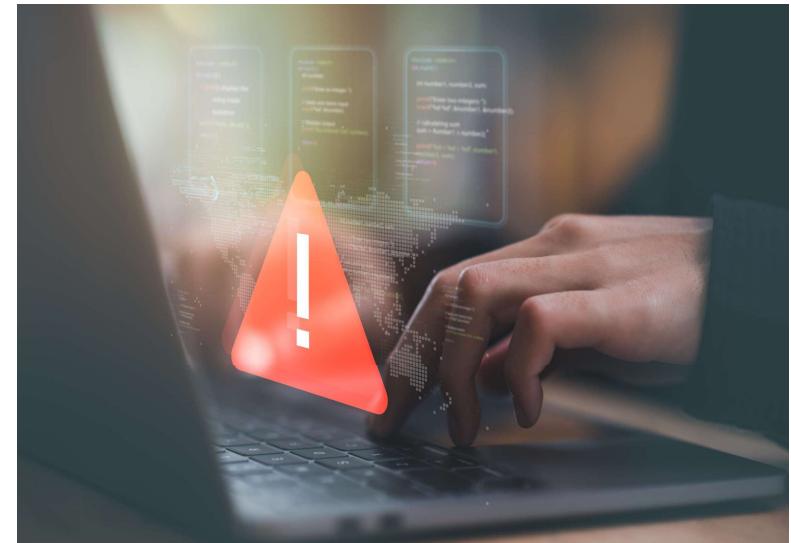
**Vírus de macro:** infectam arquivos que contêm macros, que são sequências de comandos usados para automatizar tarefas em programas como o Microsoft Word ou o Excel. Eles podem **alterar ou apagar dados, formatar o disco rígido ou enviar e-mails sem autorização.**



Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000\\_F\\_572860987\\_fhiuQM4q8SMgbJ9tKOST9hwYqgdmqh9.jpg](https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000_F_572860987_fhiuQM4q8SMgbJ9tKOST9hwYqgdmqh9.jpg).  
Acesso em 24 Maio. 2023

# Vírus - Exemplos

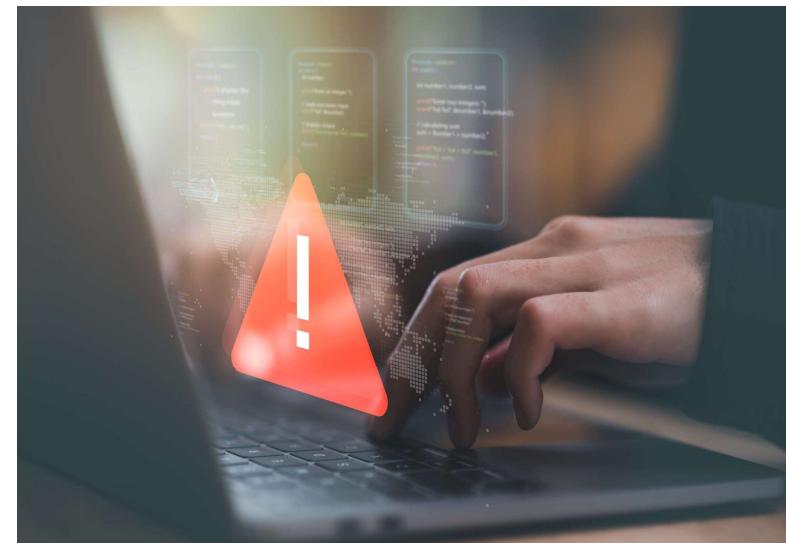
**Vírus residentes:** ficam **armazenados** na memória do computador e **infectam** outros **programas** ou **arquivos** quando eles **são executados**. Eles podem afetar o desempenho do sistema, corromper ou apagar dados ou abrir portas para outros malwares. Um exemplo famoso é o Stoned.Angelina, que foi descoberto em 1994 e exibia a mensagem "Your PC is now Stoned!" na tela ao iniciar o computador.



Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000\\_F\\_572860987\\_fhiuQM4q8SMgbJj9tKOST9hwYqgdmqh9.jpg](https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000_F_572860987_fhiuQM4q8SMgbJj9tKOST9hwYqgdmqh9.jpg).  
Acesso em 24 Maio. 2023

# Vírus - Exemplos

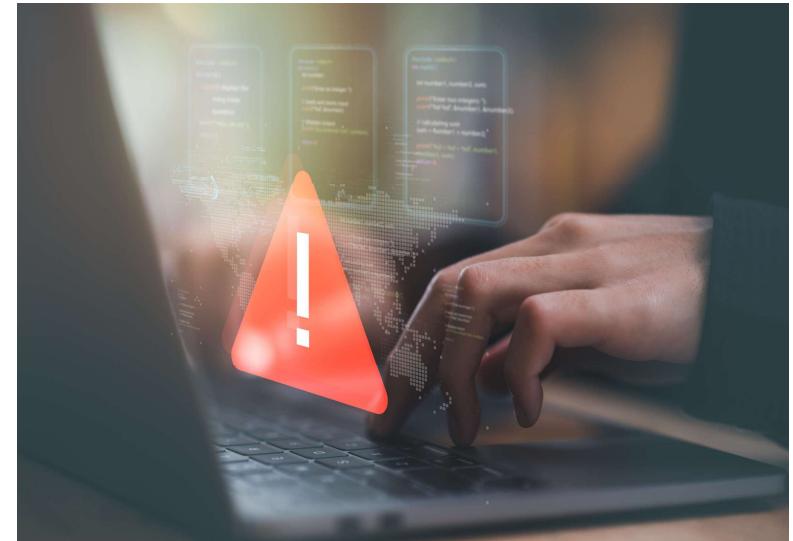
**Vírus polimórficos:** mudam o seu código a cada vez que se **replicam**, dificultando a sua **detecção** pelos **antivírus**. Eles podem ter diferentes formas de infecção e diferentes efeitos nos sistemas e nos dispositivos. Um exemplo famoso é o Elk Cloner, que foi descoberto em 1982 e é **considerado o primeiro vírus de computador da história**. Ele infectava disquetes do sistema operacional **Apple DOS** e exibia um poema na tela a cada 50 vezes que o disquete era inserido.



Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000\\_F\\_572860987\\_fhiuQM4q8SMgbJj9tKOST9hwYqgdmqh9.jpg](https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000_F_572860987_fhiuQM4q8SMgbJj9tKOST9hwYqgdmqh9.jpg).  
Acesso em 24 Maio, 2023

## Vírus - Exemplos

**WannaCry:** Lançado em 2017, esse vírus ransomware se espalhou rapidamente por meio de uma vulnerabilidade no sistema operacional Windows. Ele **criptografava** os **arquivos** do computador e **exigia** um **pagamento** em **criptomoedas** para **liberar o acesso** aos dados.



Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000\\_F\\_572860987\\_fhiuQM4q8SMgbJ9tKOST9hwYqgdmqh9.jpg](https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000_F_572860987_fhiuQM4q8SMgbJ9tKOST9hwYqgdmqh9.jpg).  
Acesso em 24 Maio. 2023

# Vírus - Exemplos

**ILOVEYOU:** Esse vírus, que apareceu em 2000, se propagava por meio de e-mails com um arquivo anexado chamado "**LOVE-LETTER-FOR-YOU.txt.vbs**". Ao ser aberto, ele se replicava para todos os contatos da vítima, causando **grandes danos**.



Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000\\_F\\_572860987\\_fhiuQM4q8SMgbJj9tKOST9hwYqgdmqh9.jpg](https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000_F_572860987_fhiuQM4q8SMgbJj9tKOST9hwYqgdmqh9.jpg).  
Acesso em 24 Maio. 2023.

## Vírus - Exemplos

**Stuxnet:** Esse vírus foi descoberto em 2010 e tinha como alvo sistemas de controle industrial, especialmente as usinas nucleares do Irã. Ele se infiltrava por meio de dispositivos USB infectados, causando danos físicos reais às máquinas controladas.



Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000\\_F\\_572860987\\_fhiuQM4q8SMgbJ9tKOST9hwYqgdmqh9.jpg](https://as2.ftcdn.net/v2/jpg/05/72/86/09/1000_F_572860987_fhiuQM4q8SMgbJ9tKOST9hwYqgdmqh9.jpg).  
Acesso em 24 Maio, 2023

## Vírus – transmissão

Os vírus de computador podem ser transmitidos de diversas formas, dependendo do tipo e da forma de infecção.

Algumas das formas mais comuns são:

Por meio de **arquivos** ou **links suspeitos** enviados por e-mail, redes sociais, mensageiros instantâneos ou outros meios de comunicação online. Ao **abrir** o arquivo ou **clicar** no **link**, o usuário pode **baixar** e **executar** o vírus sem perceber.



Fonte: Ameaça Cibernética.

Disponível em:

[https://as1.ftcdn.net/v2/jpg/05/85/87/48/1000\\_F\\_585874803\\_xUnh3QVJkclDPk28jD1Zt2nMqJtJjqMq.jpg](https://as1.ftcdn.net/v2/jpg/05/85/87/48/1000_F_585874803_xUnh3QVJkclDPk28jD1Zt2nMqJtJjqMq.jpg). Acesso em 24 Maio. 2023

## Vírus – transmissão

Por meio de dispositivos removíveis, como pen drives, cartões de memória, CDs ou DVDs, que podem estar **infectados** por vírus e **transferi-los** para o computador ao serem **conectados ou inseridos**.

Por meio de **downloads** de programas ou arquivos de fontes **não confiáveis**, como sites piratas, redes P2P ou torrents, que podem **conter vírus disfarçados** de conteúdos legítimos ou úteis.



Fonte: Ameaça Cibernética.

Disponível em:

[https://as1.ftcdn.net/v2/jpg/05/85/87/48/1000\\_F\\_585874803\\_xUNh3QVJkclDPk28jD1Zt2nMqJtJjqMq.jpg](https://as1.ftcdn.net/v2/jpg/05/85/87/48/1000_F_585874803_xUNh3QVJkclDPk28jD1Zt2nMqJtJjqMq.jpg).Acesso em 24 Maio, 2023

## Vírus – transmissão

Por meio de **brechas de segurança** nos sistemas operacionais, nos navegadores, nos aplicativos ou nos plugins, que podem **permitir a entrada** de vírus sem o **consentimento** ou o **conhecimento** do usuário.



Fonte: Ameaça Cibernética.

Disponível em:

[https://as1.ftcdn.net/v2/jpg/05/85/87/48/1000\\_F\\_585874803\\_xUNh3QVJkcIDPk28jD1Zt2nMqJtJjqMq.jpg](https://as1.ftcdn.net/v2/jpg/05/85/87/48/1000_F_585874803_xUNh3QVJkcIDPk28jD1Zt2nMqJtJjqMq.jpg). Acesso em 24 Maio. 2023

## Vírus – medidas preventivas

Para evitar a infecção por vírus de computador, os usuários devem adotar algumas medidas preventivas, como:

Usar um **antivírus atualizado e confiável**, que possa **detectar e remover** os vírus antes que eles causem danos. Ele ajudará a **identificar e eliminar** vírus em potencial.



Fonte: Ameaça Cibernética.

Disponível em:

[https://as2.ftcdn.net/v2/jpg/05/99/39/77/1000\\_F\\_599397789\\_eSSXQCcRtz1yUVbKqK5NTVxpHI9ccv13.jpg](https://as2.ftcdn.net/v2/jpg/05/99/39/77/1000_F_599397789_eSSXQCcRtz1yUVbKqK5NTVxpHI9ccv13.jpg). Acesso em 24 Maio. 2023

## Vírus – medidas preventivas

Evitar **abrir arquivos** ou **links suspeitos** enviados por e-mail, redes sociais, mensageiros instantâneos ou outros meios de comunicação online. Verificar sempre a **origem** e a **veracidade** das mensagens e dos **remetentes** antes de **clicar** ou **baixar** qualquer coisa.

Escanear os **dispositivos removíveis**, como pen drives, cartões de memória, CDs ou DVDs, antes de usá-los no computador. Não **conectar** ou **inserir** dispositivos **desconhecidos** ou **duvidosos**.



Fonte: Ameaça Cibernética.

Disponível em:

[https://as2.ftcdn.net/v2/jpg/05/99/39/77/1000\\_F\\_599397789\\_eSSXQCcRtz1yUVbKqK5NTVxpHI9ccv13.jpg](https://as2.ftcdn.net/v2/jpg/05/99/39/77/1000_F_599397789_eSSXQCcRtz1yUVbKqK5NTVxpHI9ccv13.jpg). Acesso em 24 Maio. 2023

## Vírus – medidas preventivas

Fazer **downloads de programas ou arquivos** apenas de fontes **confiáveis e verificadas**. Não baixar ou instalar **conteúdos piratas, ilegais ou duvidosos**.

Manter os sistemas operacionais, os navegadores, os aplicativos e os plugins **atualizados com as últimas versões e correções de segurança**. Não usar versões **desatualizadas ou obsoletas** que possam conter vulnerabilidades.



Fonte: Ameaça Cibernética.

Disponível em:

[https://as2.ftcdn.net/v2/jpg/05/99/39/77/1000\\_F\\_599397789\\_eSSXQCcRtz1yUVbKqK5NTVxpHI9ccv13.jpg](https://as2.ftcdn.net/v2/jpg/05/99/39/77/1000_F_599397789_eSSXQCcRtz1yUVbKqK5NTVxpHI9ccv13.jpg). Acesso em 24 Maio. 2023

## Vírus – medidas preventivas

Fazer **backup** dos dados **importantes** em um dispositivo **externo** ou em um serviço de **nuvem**. Assim, em caso de **infecção** por **vírus**, é possível **recuperar** os dados sem **perdas** ou **danos**.

Desconfie de e-mails **suspeitos**: evite abrir e-mails de **remetentes** desconhecidos ou **suspeitos**. Não clique em **links** ou faça **download** de **anexos** que pareçam suspeitos, mesmo que **pareçam vir de fontes conhecidas**.



Fonte: Ameaça Cibernética.

Disponível em:

[https://as2.ftcdn.net/v2/jpg/05/99/39/77/1000\\_F\\_599397789\\_eSSXQCcRtz1yUVbKqK5NTVxpHI9ccv13.jpg](https://as2.ftcdn.net/v2/jpg/05/99/39/77/1000_F_599397789_eSSXQCcRtz1yUVbKqK5NTVxpHI9ccv13.jpg). Acesso em 24 Maio, 2023

# Conclusão

Os vírus de computador são uma ameaça real e constante no mundo digital. Conhecendo o que são, como eles se propagam e as medidas preventivas que podemos adotar, podemos fortalecer a segurança online das pessoas e organizações. Lembre-se de manter-se atualizado sobre as últimas ameaças e práticas de segurança digital. Proteja-se e mantenha seus dispositivos e informações seguros.

# Termos e conceitos sobre ameaças cibernéticas

# Ameaças cibernéticas

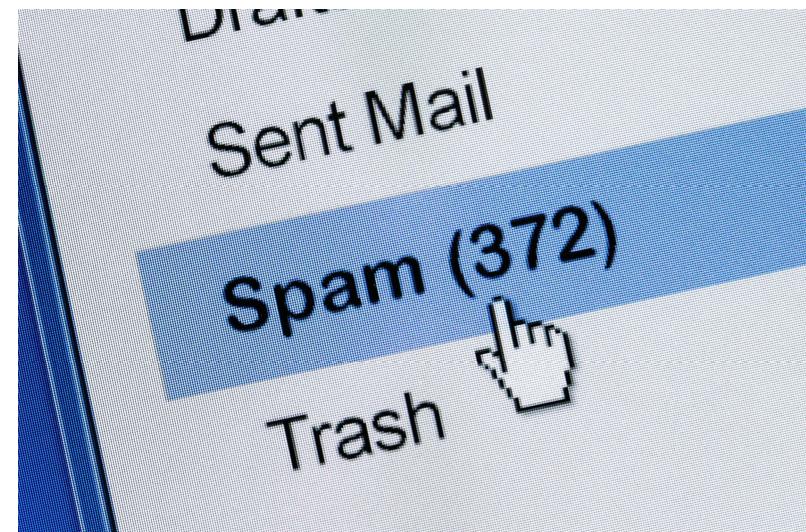
No mundo digital, estamos constantemente expostos a diversas ameaças que visam comprometer nossa **segurança e privacidade**. Nesta aula, vamos explorar algumas dessas ameaças, incluindo **SPAM, Spyware, Worms, Phishing, Botnets, Rootkits, Cavalo de troia, Ransomware e Engenharia Social**. Vamos entender o que são, como funcionam e ver exemplos reais de sua utilização.



Fonte: Ameaça Cibernética.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/06/10/79/07/1000\\_F\\_610790792\\_qBhrE9YCvJ7fmwA63bynqnt3vuNNzFml.jpg](https://as2.ftcdn.net/v2/jpg/06/10/79/07/1000_F_610790792_qBhrE9YCvJ7fmwA63bynqnt3vuNNzFml.jpg).  
Acesso em 1 Jun. 2023

# SPAM – o que é?

SPAM é uma mensagem eletrônica não-solicitada **enviada em massa**, para um **grande número** de pessoas. Na sua forma mais popular, um **SPAM** consiste em uma mensagem de **correio eletrônico** com fins **publicitários**, que promove produtos ou serviços **duvidosos ou fraudulentos**.



Fonte: SPAM.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/00/91/52/87/1000\\_F\\_91528736\\_kAGfrIkiESSps2x6JDnDvbJhgqdVdUME.jpg](https://as2.ftcdn.net/v2/jpg/00/91/52/87/1000_F_91528736_kAGfrIkiESSps2x6JDnDvbJhgqdVdUME.jpg).  
Acesso em 1 Jun. 2023

# SPAM – o que é?

O SPAM pode ser considerado uma forma de poluição digital, pois ocupa espaço nos servidores de e-mail, **consome recursos** da rede e do computador e atrapalha a comunicação **legítima** entre os usuários. Além disso, o SPAM pode ser usado como um meio para **disseminar vírus, spywares ou outras formas de malware**.



Fonte: SPAM.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/00/91/52/87/1000\\_F\\_91528736\\_kAGfrIkiESSps2x6JDnDvbJhqqdVdUME.jpg](https://as2.ftcdn.net/v2/jpg/00/91/52/87/1000_F_91528736_kAGfrIkiESSps2x6JDnDvbJhqqdVdUME.jpg).  
Acesso em 1 Jun. 2023

## SPAM – Exemplo

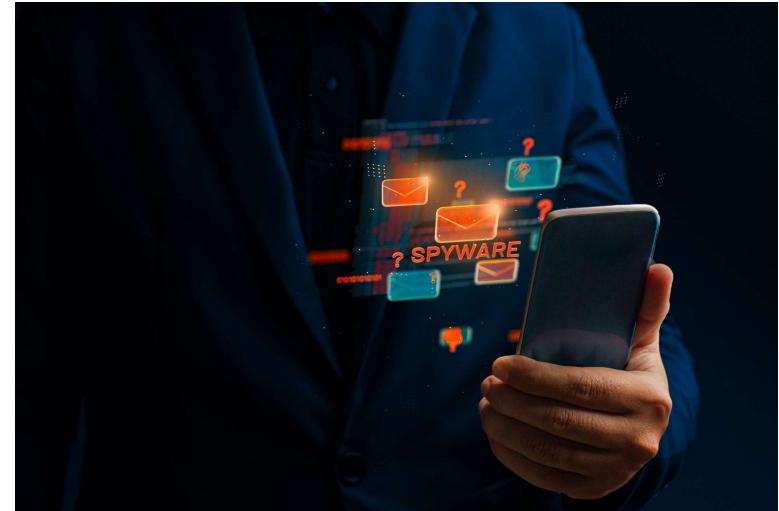
Um exemplo de SPAM, é quando recebemos uma mensagem eletrônica que oferece remédios para emagrecer ou de produtos digitais prometendo ganhos financeiros imediatos e altos. Essas mensagens costumam usar títulos **chamativos** e **falsos testemunhos** para atrair a **atenção** dos **destinatários**. Ao clicar no link da mensagem, o usuário pode ser direcionado para um **site falso** que solicita dados **pessoais** ou **financeiros** ou que instala um programa malicioso no seu computador.



Fonte: SPAM.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/00/91/52/87/1000\\_F\\_91528736\\_kAGfrIkESSps2x6JDnDvbJhgqdVdUME.jpg](https://as2.ftcdn.net/v2/jpg/00/91/52/87/1000_F_91528736_kAGfrIkESSps2x6JDnDvbJhgqdVdUME.jpg).  
Acesso em 1 Jun. 2023

# Spyware – o que é?

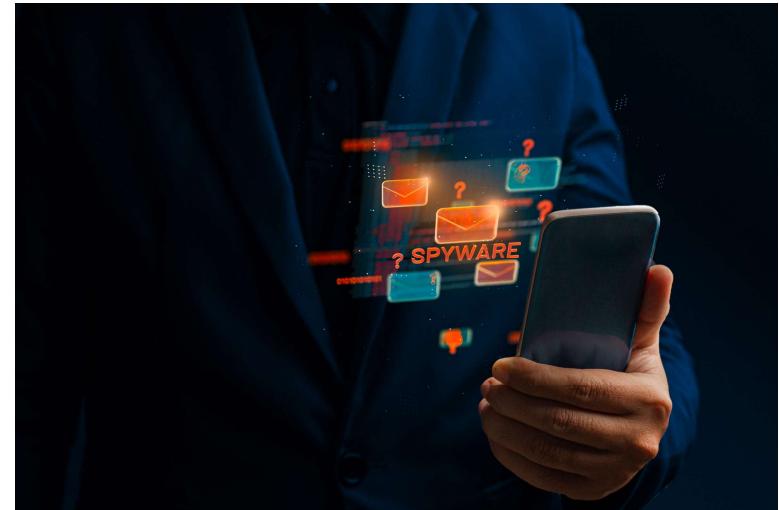
O termo Spyware, combinação em inglês de “spy” (espião) e “software” (programa), é um tipo de programa malicioso que **monitora as atividades do usuário no computador ou na internet** sem conhecimento e consentimento do usuário. O objetivo do Spyware é **coletar informações pessoais ou comerciais do usuário**, como hábitos de navegação, histórico de sites visitados, senhas, números de cartão de crédito e dados bancários, por exemplo.



Fonte: Spyware.  
Disponível em: [https://as1.ftcdn.net/v2/jpg/04/47/39/62/1000\\_F\\_447396293\\_cBhQ55C6DltfhAHOoylJdjt91x3bnfq.jpg](https://as1.ftcdn.net/v2/jpg/04/47/39/62/1000_F_447396293_cBhQ55C6DltfhAHOoylJdjt91x3bnfq.jpg).  
Acesso em 1 Jun. 2023

# Spyware – o que é?

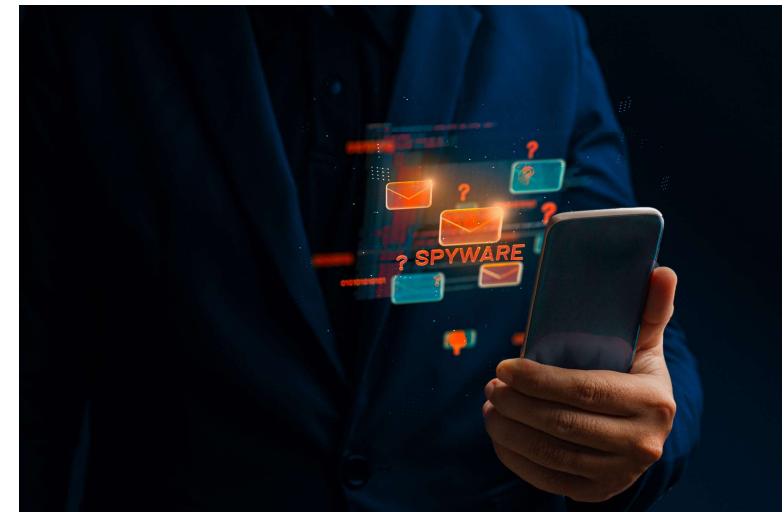
O Spyware pode ser instalado no computador de diversas formas, como por meio de **downloads de programas** ou **arquivos infectados**, por meio de **anexos** ou **links de e-mails suspeitos** ou por meio de **brechas de segurança** nos sistemas operacionais ou nos navegadores. Uma vez instalado, o Spyware pode enviar as informações coletadas para terceiros **sem autorização** do usuário.



Fonte: Spyware.  
Disponível em: [https://as1.ftcdn.net/v2/jpg/04/47/39/62/1000\\_F\\_447396293\\_cBhQ55C6DHTlhAHOoyIJdjt91x3bnfq.jpg](https://as1.ftcdn.net/v2/jpg/04/47/39/62/1000_F_447396293_cBhQ55C6DHTlhAHOoyIJdjt91x3bnfq.jpg).  
Acesso em 1 Jun. 2023

## Spyware – Exemplo

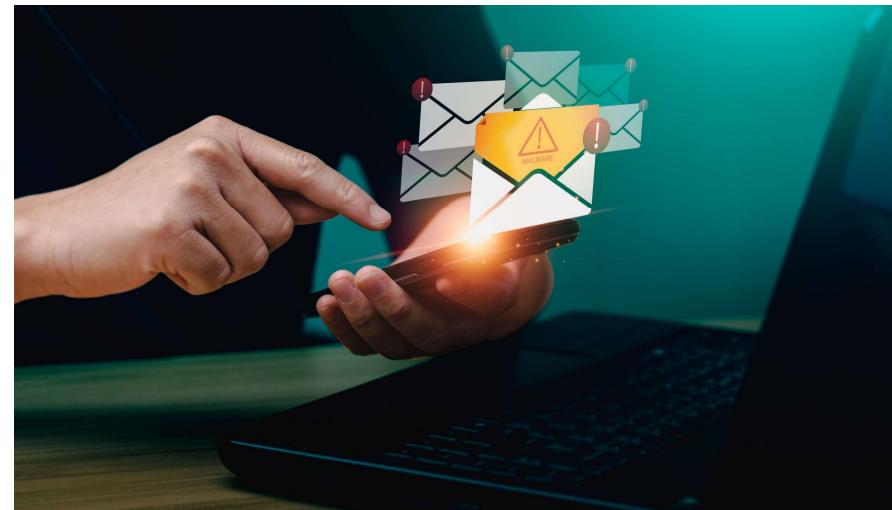
Um exemplo de Spyware é o Keylogger, que registra tudo o que o usuário **digita no teclado do computador**. Esse tipo de Spyware pode **capturar** senhas, números de cartão de crédito e outras informações confidenciais. Essas informações podem ser usadas para **roubar a identidade do usuário**, realizar compras online **indevidas** ou **acessar** contas **bancárias**.



Fonte: Spyware.  
Disponível em: [https://as1.ftcdn.net/v2/jpg/04/47/39/62/1000\\_F\\_447396293\\_cBhQ55C6DHtlfhAHOoyIjdjt91x3bnfq.jpg](https://as1.ftcdn.net/v2/jpg/04/47/39/62/1000_F_447396293_cBhQ55C6DHtlfhAHOoyIjdjt91x3bnfq.jpg).  
Acesso em 1 Jun. 2023

# Worms – o que é?

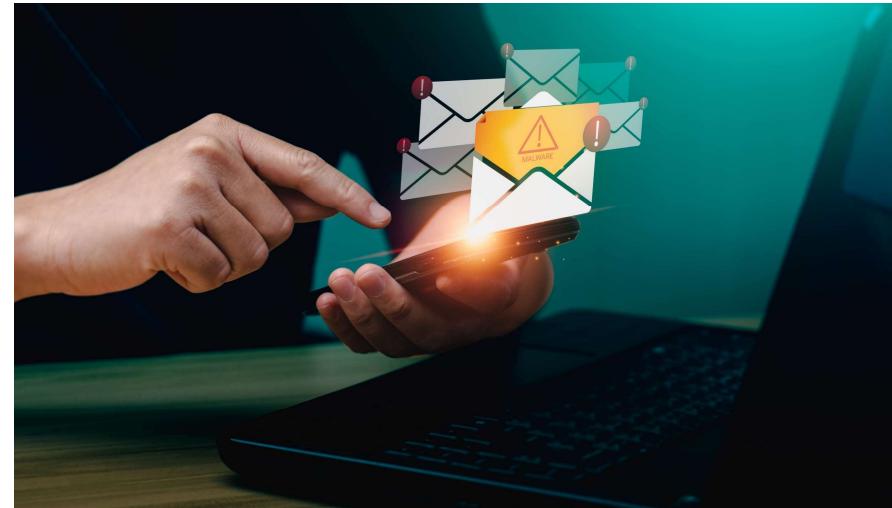
O termo **Worms** (vermes, em português), na área da informática, é semelhante a um vírus, porém com um diferencial: **é um programa autorreplicante**. Enquanto um vírus infecta um programa e necessita deste programa hospedeiro para se propagar, o Worms é um programa completo e **não precisa de outro** para se **propagar**.



Fonte: Worms Cibernético.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/06/10/83/21/1000\\_F\\_610832172\\_IB4D0NWUhilRERhQzp5pESByvHleNCu.jpg](https://as2.ftcdn.net/v2/jpg/06/10/83/21/1000_F_610832172_IB4D0NWUhilRERhQzp5pESByvHleNCu.jpg).  
Acesso em 1 Jun. 2023.

## Worms – o que é?

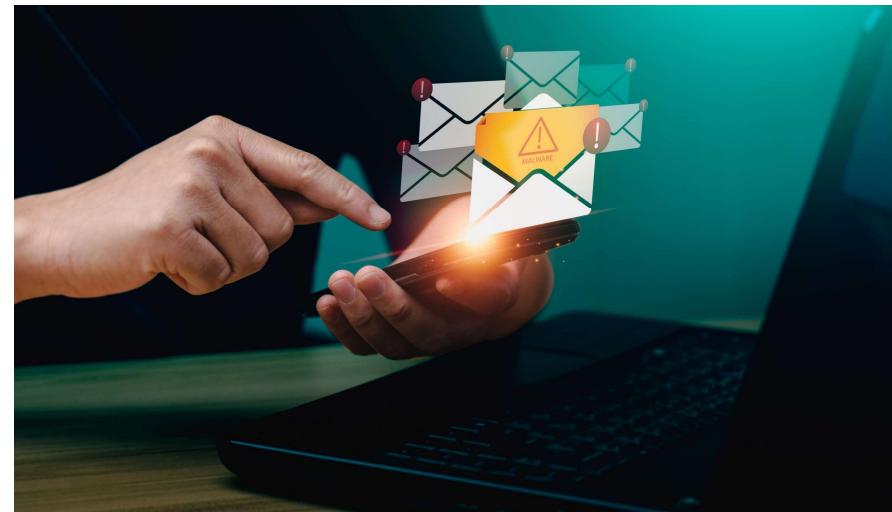
Worms pode ser projetado para tomar **ações maliciosas** após infectar um sistema, além de se **autorreplicar**. Ele pode **deletar** arquivos em um sistema, **enviar** documentos por e-mail, **consumir** a banda larga da rede ou **abrir portas** para outros malwares entarem.



Fonte: Worms Cibernético.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/06/10/83/21/1000\\_F\\_610832172\\_IB4D0NWUhilRERhQzp5pESByvHleNCu.jpg](https://as2.ftcdn.net/v2/jpg/06/10/83/21/1000_F_610832172_IB4D0NWUhilRERhQzp5pESByvHleNCu.jpg).  
Acesso em 1 Jun. 2023

## Worms – Exemplo

Um exemplo de Worms é o Conficker, que foi descoberto em 2008 e infectou milhões de computadores em todo o mundo. Esse Worms explorava uma **vulnerabilidade** no sistema operacional Windows e se espalhava pela rede local ou pela internet. Ele criava uma rede de computadores zumbis (botnet) que podia ser **controlada remotamente por hackers** para realizar **ataques distribuídos de negação de serviço (DDoS)** ou enviar SPAM.



Fonte: Worms Cibernético.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/06/10/83/21/1000\\_F\\_610832172\\_IB4D0NWUhilRERhQzp5pESByvHleNCu.jpg](https://as2.ftcdn.net/v2/jpg/06/10/83/21/1000_F_610832172_IB4D0NWUhilRERhQzp5pESByvHleNCu.jpg).  
Acesso em 1 Jun. 2023

# Phishing – o que é?

O termo **Phishing**, derivação em inglês de “fishing” (pescaria), é uma técnica de **fraude eletrônica** que usa a **engenharia social** para enganar os usuários e obter informações **confidenciais** ou **vantagens financeiras**. O objetivo do Phishing é se passar por uma **pessoa ou instituição confiável** e induzir o usuário a fornecer dados pessoais ou financeiros, como senhas, números de cartão de crédito, dados bancários etc.



Fonte: Phishing.  
Disponível em:  
[https://as2.ftcdn.net/v2/jpg/03/13/57/33/1000\\_F\\_313573379\\_oBerNuQKDWFPPQAiDNQrTg31mFuHO8p2.jpg](https://as2.ftcdn.net/v2/jpg/03/13/57/33/1000_F_313573379_oBerNuQKDWFPPQAiDNQrTg31mFuHO8p2.jpg). Acesso em 1 Jun. 2023

# Phishing – o que é?

O **Phishing** costuma usar **e-mails, mensagens instantâneas ou sites falsos** como **iscas** para atrair as vítimas. Esses meios de comunicação costumam usar **nomes, logotipos ou layouts semelhantes** aos das entidades verdadeiras para parecerem **legítimos**. Eles também costumam usar argumentos persuasivos, como ofertas imperdíveis, prêmios, cobranças ou atualizações cadastrais.



Fonte: Phishing.  
Disponível em:  
[https://as2.ftcdn.net/v2/jpg/03/13/57/33/1000\\_F\\_313573379\\_oBerNuQKDWFPPQAiDNQRtg31mFuHO8p2.jpg](https://as2.ftcdn.net/v2/jpg/03/13/57/33/1000_F_313573379_oBerNuQKDWFPPQAiDNQRtg31mFuHO8p2.jpg). Acesso em 1 Jun. 2023

## Phishing – Exemplo

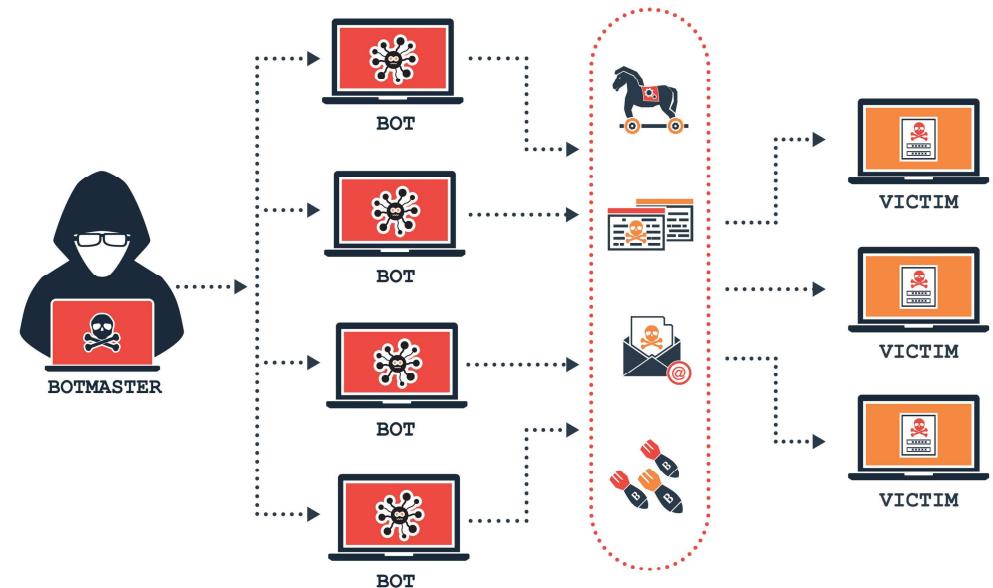
Um exemplo de **Phishing** é o e-mail que se passa por um banco e solicita ao usuário que atualize os seus dados cadastrais ou que **confirme** uma transação **suspeita**. Ao **clicar** no **link** do e-mail, o usuário é direcionado para um **site falso** que imita o site do banco e pede que ele **digite** os seus **dados bancários**. Esses dados são enviados para os **criminosos** que podem usá-los para acessar a **conta bancária** do usuário e realizar saques ou transferências **indevidas**.



Fonte: Phishing.  
Disponível em:  
[https://as2.ftcdn.net/v2/jpg/03/13/57/33/1000\\_F\\_313573379\\_oBerNuQKDWFPPQAiDNQrTg31mFuHO8p2.jpg](https://as2.ftcdn.net/v2/jpg/03/13/57/33/1000_F_313573379_oBerNuQKDWFPPQAiDNQrTg31mFuHO8p2.jpg). Acesso em 1 Jun. 2023

# Botnet – o que é?

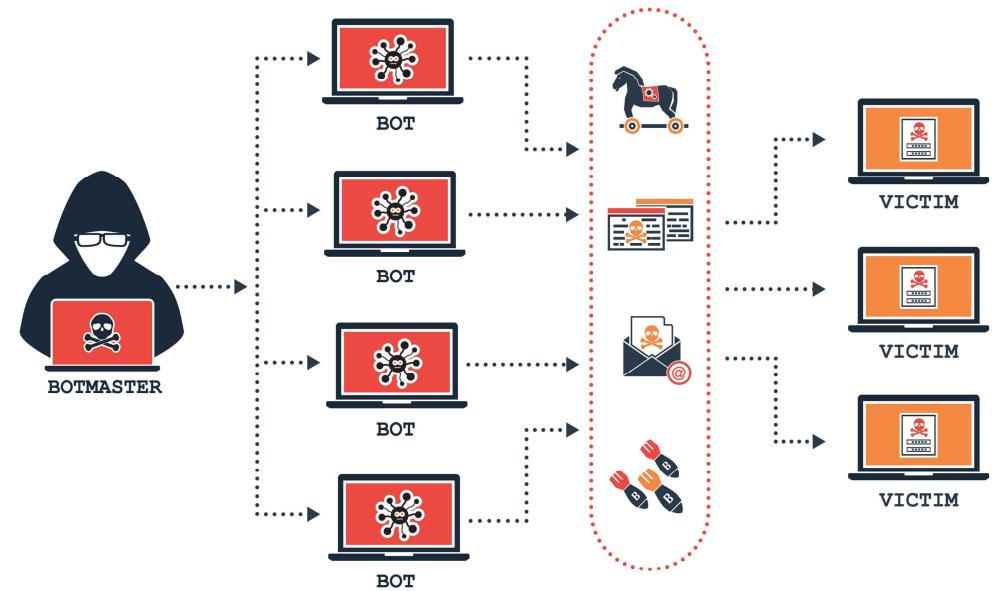
O termo botnet, combinação em inglês de “bot” (robô) e “net” (rede), é uma rede de computadores infectados por um malware que permite que um cibercriminoso controle-os remotamente. O objetivo de uma botnet é usar os recursos dos computadores infectados para realizar atividades maliciosas, como ataques de negação de serviço, propagação de códigos maliciosos, coleta de informações, envio de spam ou camuflagem da identidade do atacante.



Fonte: Botnet.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/01/82/01/75/1000\\_F\\_182017566\\_x4mkLJztU9Dvbqz1XmEKsDaMTG5s91hw.jpg](https://as2.ftcdn.net/v2/jpg/01/82/01/75/1000_F_182017566_x4mkLJztU9Dvbqz1XmEKsDaMTG5s91hw.jpg)  
Acesso em 1 Jun, 2023

## Botnet – o que é?

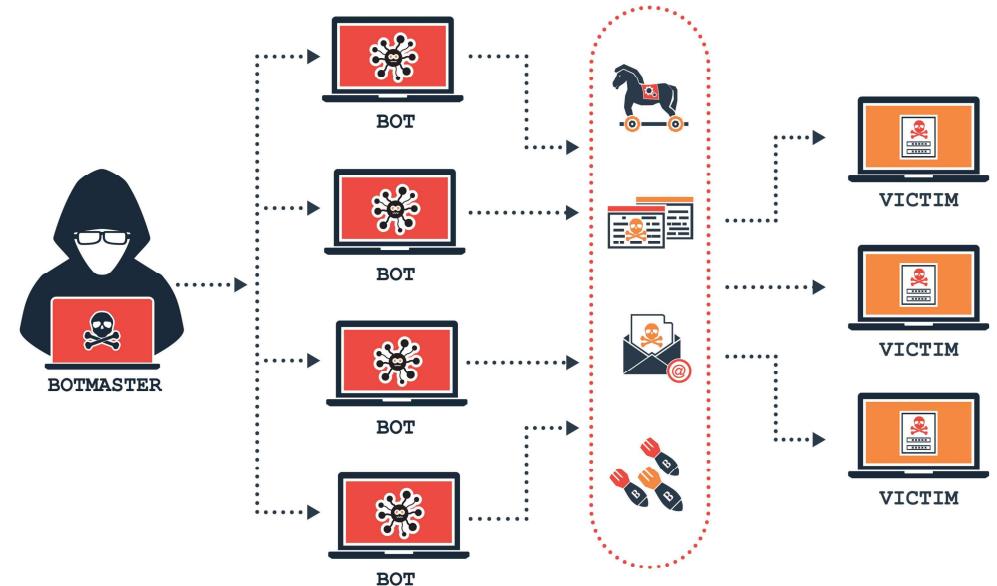
Uma botnet é formada quando um malware infecta um computador e o transforma em um “zumbi” ou “bot”, que passa a receber comandos de um servidor central controlado por um cibercriminoso. Esse servidor pode enviar instruções para os bots realizarem ações individuais ou coordenadas com outros bots da mesma rede. Os usuários dos computadores infectados geralmente não percebem que fazem parte de uma botnet, pois o malware costuma se esconder e consumir poucos recursos.



Fonte: Botnet.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/01/82/01/75/1000\\_F\\_182017566\\_x4mkLJztU9Dvbqz1XmEKsDaMTG5s91hw.jpg](https://as2.ftcdn.net/v2/jpg/01/82/01/75/1000_F_182017566_x4mkLJztU9Dvbqz1XmEKsDaMTG5s91hw.jpg)  
Acesso em 1 Jun, 2023

## Botnet – Exemplo

Um exemplo de botnet é o Mirai, que foi descoberto em 2016 e infectou milhares de dispositivos conectados à internet, como câmeras de segurança, roteadores e gravadores digitais. Esse botnet foi usado para realizar um dos maiores ataques de negação de serviço da história, que afetou sites como Twitter, Netflix, Spotify e Amazon.



Fonte: Botnet.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/01/82/01/75/1000\\_F\\_182017566\\_x4mkLJZtU9Dvbqz1XmEKsDaMTG5s91hw.jpg](https://as2.ftcdn.net/v2/jpg/01/82/01/75/1000_F_182017566_x4mkLJZtU9Dvbqz1XmEKsDaMTG5s91hw.jpg)  
Acesso em 1 Jun, 2023

# Rootkit – o que é?

O termo rootkit, combinação em inglês de “root” (raiz) e “kit” (conjunto), é um tipo de malware furtivo e perigoso que permite que cibercriminosos acessem o seu computador sem você saber. O objetivo de um rootkit é obter acesso privilegiado ao sistema operacional e modificar os seus arquivos e processos para ocultar a sua presença e a de outros malwares.



Fonte: Rootkit.  
Disponível em: [https://as1.ftcdn.net/v2/jpg/04/66/76/76/1000\\_F\\_466767607\\_WPssfzv5jMVd03cC4H4orECbQaYN6rR9.jpg](https://as1.ftcdn.net/v2/jpg/04/66/76/76/1000_F_466767607_WPssfzv5jMVd03cC4H4orECbQaYN6rR9.jpg).  
Acesso em 2 Jun. 2023.

# Rootkit – o que é?

Um rootkit pode ser instalado no computador por meio de downloads de programas ou arquivos infectados, por meio de anexos ou links de e-mails suspeitos ou por meio da exploração de vulnerabilidades nos sistemas operacionais ou nos aplicativos. Uma vez instalado, o rootkit pode enviar as informações coletadas para terceiros sem autorização do usuário, abrir portas para outros malwares entrarem ou criar um “backdoor” permanente para que o cibercriminoso possa retornar posteriormente.



Fonte: Rootkit.  
Disponível em: [https://as1.ftcdn.net/v2/jpg/04/66/76/76/1000\\_F\\_466767607\\_WPssfzv5jMVd03cC4H4orECbQaYN6rR9.jpg](https://as1.ftcdn.net/v2/jpg/04/66/76/76/1000_F_466767607_WPssfzv5jMVd03cC4H4orECbQaYN6rR9.jpg).  
Acesso em 2 Jun. 2023.

## Rootkit – Exemplo

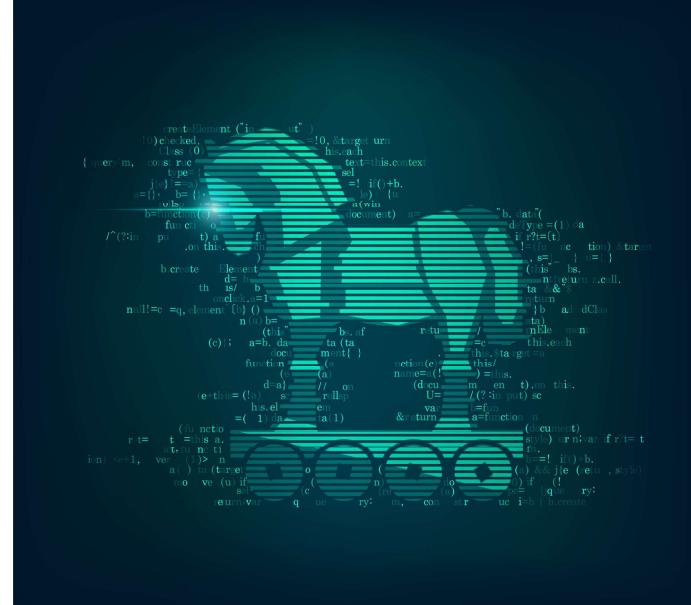
Um exemplo de rootkit é o Stuxnet, que foi descoberto em 2010 e infectou centenas de computadores em instalações nucleares no Irã. Esse rootkit foi projetado para sabotar o funcionamento das centrífugas usadas para enriquecer urânio, alterando a velocidade de rotação e causando danos físicos. Esse rootkit era tão sofisticado que conseguiu se espalhar por dispositivos removíveis e se adaptar a diferentes sistemas operacionais.



Fonte: Rootkit.  
Disponível em: [https://as1.ftcdn.net/v2/jpg/04/66/76/76/1000\\_F\\_466767607\\_WPssfzv5jMVd03cC4H4orECbQaYN6rR9.jpg](https://as1.ftcdn.net/v2/jpg/04/66/76/76/1000_F_466767607_WPssfzv5jMVd03cC4H4orECbQaYN6rR9.jpg).  
Acesso em 2 Jun. 2023.

# Cavalo de troia – o que é?

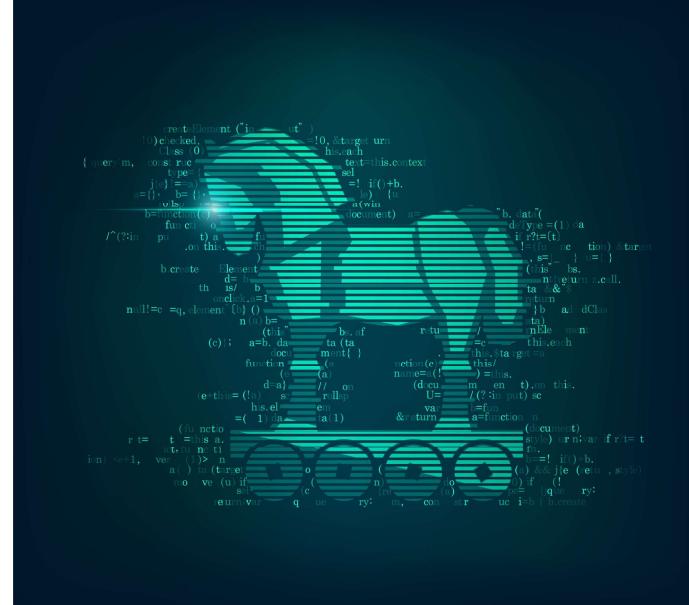
Um cavalo de troia (do inglês, Trojan horse, ou simplesmente, trojan) é um programa malicioso que se disfarça de algo legítimo ou desejável para enganar os usuários e induzi-los a instalá-lo no seu computador. O nome vem da lenda grega antiga do cavalo de madeira que os gregos usaram para invadir a cidade de Troia.



Fonte: Cavalo de troia.  
Disponível em: <https://as2.ftcdn.net/v2/jpg/02/92/47/81/mVdkzNn6Am9kuB1GY13eMkoPN3EvFiDs.jpg>.  
Acesso em 2 Jun. 2023

# Cavalo de troia – o que é?

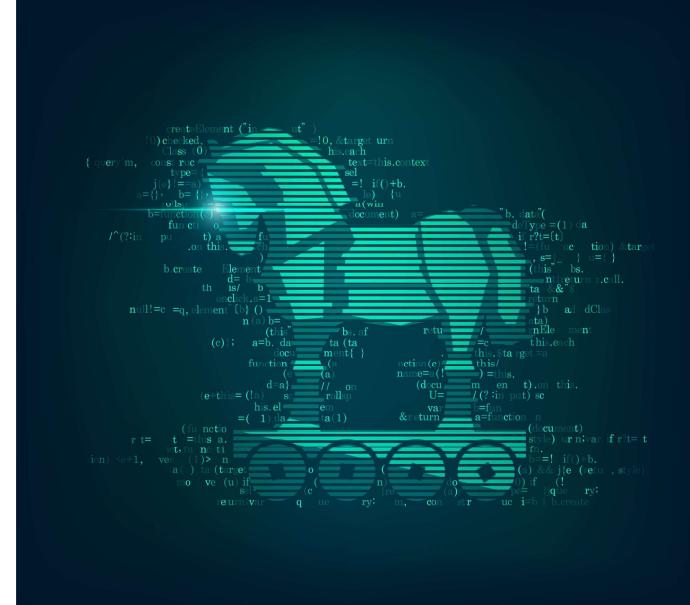
Um cavalo de troia pode ter diferentes formas e funções, mas geralmente ele serve como uma porta de entrada para outros malwares ou para cibercriminosos que querem acessar o seu computador sem o seu conhecimento ou consentimento. Um cavalo de troia pode roubar as suas informações pessoais ou financeiras, danificar ou apagar os seus arquivos, alterar as configurações do seu sistema, monitorar as suas atividades online ou usar os recursos do seu computador para fins maliciosos.



Fonte: Cavalo de troia.  
Disponível em: <https://as2.ftcdn.net/v2/jpg/02/92/47/81/mVdkzNn6Am9kuB1GY13eMkoPN3EvFiDs.jpg>.  
Acesso em 2 Jun. 2023

# Cavalo de troia – Exemplo

Um exemplo de Cavalo de Troia, é o famoso Zeus, que foi descoberto em 2007 e infectou milhões de computadores em todo o mundo. Que tinha como objetivo roubar as credenciais bancárias dos usuários, como senhas, números de cartão de crédito ou dados de contas. Ele utilizava técnicas como: keyloggers (que registram tudo o que o usuário digita no teclado), screenloggers (que capturam imagens da tela do usuário) ou web injects (que modificam as páginas web dos bancos para inserir campos falsos).



Fonte: Cavalo de troia.  
 Disponível em: <https://as2.ftcdn.net/v2/jpg/02/92/47/81/mVdkzNn6Am9kuB1GY13eMkoPN3EvFiDs.jpg>.  
 Acesso em 2 Jun. 2023

## Conclusão

Esses são alguns dos tipos mais comuns de ataques cibernéticos que podem afetar o seu computador ou a sua segurança online. Eles podem ter diferentes objetivos e formas de infecção, mas todos eles podem causar danos ou prejuízos para pessoas e organizações. É essencial estarmos cientes dessas ameaças e adotarmos medidas preventivas, como manter sistemas e programas atualizados, utilizar antivírus confiáveis, evitar clicar em links suspeitos e nunca fornecer informações pessoais ou financeiras em sites não confiáveis. Proteger-se é fundamental para garantir a segurança e privacidade no mundo digital em constante evolução.

# Aula 5 – Como se proteger

# Ameaças digitais

As ameaças digitais são os **riscos e perigos** que existem no **ambiente online**, como ataques de hackers, vírus, malware, phishing, ransomware, roubo de dados e fraudes. Essas ameaças podem afetar a **segurança**, a **privacidade** e a **integridade** das informações pessoais e profissionais, bem como causar danos financeiros, operacionais e reputacionais.



Fonte: Ameaças digitais.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/01/33/87/03/1000\\_F\\_133870380\\_I3cEUzFJLVG6eYsZo8VUO7UQ5xIFRbA2.jpg](https://as2.ftcdn.net/v2/jpg/01/33/87/03/1000_F_133870380_I3cEUzFJLVG6eYsZo8VUO7UQ5xIFRbA2.jpg)  
Acesso em 1 Jun. 2023

# Ameaças digitais

Para se **proteger** das ameaças digitais, é preciso ter **consciência** dos riscos e das **boas práticas** de cibersegurança. A conscientização é o processo de **educação** e sensibilização das pessoas sobre os conceitos, as normas e as medidas de proteção no **ambiente digital**. A **conscientização é fundamental** para criar uma cultura de segurança cibernética nas organizações e na sociedade.



Fonte: Ameaças digitais.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/01/33/87/03/1000\\_F\\_133870380\\_I3cEUzFJLVG6eYsZo8VUO7UQ5xIFRbA2.jpg](https://as2.ftcdn.net/v2/jpg/01/33/87/03/1000_F_133870380_I3cEUzFJLVG6eYsZo8VUO7UQ5xIFRbA2.jpg)  
Acesso em 1 Jun. 2023

# Boas práticas

As boas práticas de cibersegurança são as ações e os comportamentos que visam **prevenir, detectar e responder** às ameaças digitais. Algumas das boas práticas são:

**Usar senhas fortes e únicas.** As senhas devem ser compostas por letras maiúsculas e minúsculas, números e símbolos, e ter no mínimo oito caracteres. Além disso, devem ser diferentes para cada conta ou serviço online, e **trocadas periodicamente**. Para facilitar o gerenciamento das senhas, pode-se usar um gerenciador de senhas confiável.



Fonte: Boas práticas.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000\\_F\\_472245346\\_DJHbYCP RylyKvk6nv3iRITGn7LAWvVTt.jpg](https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000_F_472245346_DJHbYCP RylyKvk6nv3iRITGn7LAWvVTt.jpg)  
Acesso em 1 Jun. 2023

# Boas práticas



**Ativar a autenticação de dois fatores.** A autenticação de dois fatores é uma **camada extra de segurança** que exige um código ou um dispositivo adicional para **confirmar a identidade do usuário** ao acessar uma conta ou serviço online. Essa medida dificulta o acesso indevido por terceiros, mesmo que a senha seja comprometida.



Fonte: Boas práticas.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000\\_F\\_472245346\\_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg](https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000_F_472245346_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg)  
Acesso em 1 Jun. 2023

# Boas práticas

**Atualizar os sistemas e os aplicativos.** As atualizações dos sistemas operacionais e dos aplicativos contêm **correções** de bugs e **vulnerabilidades** que podem ser exploradas por hackers. Por isso, é importante manter os dispositivos e os programas sempre **atualizados** com as **versões mais recentes**.



Fonte: Boas práticas.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000\\_F\\_472245346\\_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg](https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000_F_472245346_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg)  
Acesso em 1 Jun. 2023

# Boas práticas

**Instalar um antivírus.** Um antivírus é um software que **detecta** e **elimina** programas maliciosos que podem **infectar** os dispositivos e **comprometer** os dados. É importante instalar um **antivírus** confiável em todos os dispositivos que se conectam à internet, como computadores, notebooks, smartphones e tablets.



Fonte: Boas práticas.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000\\_F\\_472245346\\_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg](https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000_F_472245346_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg)  
Acesso em 1 Jun. 2023

# Boas práticas

**Não clicar em links ou anexos suspeitos.** Os links ou anexos suspeitos podem conter vírus, malware ou phishing, que são tentativas de **enganar o usuário** para obter informações pessoais ou financeiras. Antes de clicar em um link ou abrir um anexo, é preciso **verificar a origem, o conteúdo e a veracidade** da mensagem.



Fonte: Boas práticas.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000\\_F\\_472245346\\_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg](https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000_F_472245346_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg)  
Acesso em 1 Jun. 2023

## Boas práticas

**Usar redes Wi-Fi seguras.** As redes Wi-Fi públicas ou abertas podem ser interceptadas por hackers que podem **roubar** ou **alterar** os dados transmitidos. Por isso, é recomendável usar redes Wi-Fi seguras, com **criptografia** e **senha**, ou usar uma **VPN** (rede privada virtual) para **proteger** a conexão.



Fonte: Boas práticas.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000\\_F\\_472245346\\_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg](https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000_F_472245346_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg)  
Acesso em 1 Jun. 2023

# Boas práticas

**Fazer backup dos dados.** O backup dos dados é a **cópia de segurança** das informações armazenadas nos **dispositivos físicos** ou na **nuvem**. O backup permite **recuperar** os dados em caso de **perda, roubo ou dano** dos dispositivos, ou em caso de ataque cibernético. O backup deve ser feito **regularmente e armazenado** em um **local seguro**.



Fonte: Boas práticas.  
Disponível em: [https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000\\_F\\_472245346\\_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg](https://as2.ftcdn.net/v2/jpg/04/72/24/53/1000_F_472245346_DJHbYCPRLyKvk6nv3jRITGn7LAWvVTt.jpg)  
Acesso em 1 Jun. 2023



# Boas práticas de Cibersegurança

# Como implementar

Para implementar as boas práticas de cibersegurança, é preciso seguir algumas etapas básicas:

Avaliar o nível de exposição às ameaças digitais. É preciso **identificar** quais são os dados mais **sensíveis e valiosos** que se possui ou se acessa online, quais são os dispositivos que se usa para se **conectar à internet**, quais são os serviços ou aplicativos que se utiliza **online** e quais são os **riscos** mais prováveis e mais **graves** que se pode **enfrentar**.



Fonte: Implementação.  
Disponível em: [https://as1.ftcdn.net/v2/jpg/05/98/29/80/1000\\_F\\_598298028\\_dIZVHJ5KYxfGjGYfADxb76xzxFJY2Z7.jpg](https://as1.ftcdn.net/v2/jpg/05/98/29/80/1000_F_598298028_dIZVHJ5KYxfGjGYfADxb76xzxFJY2Z7.jpg)  
Acesso em 1 Jun. 2023

# Como implementar

Escolher as medidas de proteção adequadas. É preciso **selecionar** as medidas de proteção que **atendam** às **necessidades** e aos **objetivos** de cada **pessoa** ou **organização**, considerando fatores como o tipo de atividade online, o orçamento disponível, o nível de complexidade da rede, o grau de confiança nos provedores e o tipo de resultado esperado.



Fonte: Implementação.  
Disponível em: [https://as1.ftcdn.net/v2/jpg/05/98/29/80/1000\\_F\\_598298028\\_dIZVHJ5KYxfGgjGYfADxb76xzxFJY2Z7.jpg](https://as1.ftcdn.net/v2/jpg/05/98/29/80/1000_F_598298028_dIZVHJ5KYxfGgjGYfADxb76xzxFJY2Z7.jpg)  
Acesso em 1 Jun. 2023

## Como implementar

**Implementar** e **monitorar** as medidas de proteção escolhidas. É preciso **instalar** e **configurar** as medidas de proteção nos dispositivos e nas contas online, seguindo as **melhores práticas** recomendadas pelos fornecedores ou pelos especialistas. Além disso, é preciso **monitorar** e revisar **continuamente** as **medidas de proteção**, verificando se elas estão funcionando corretamente, **atualizando-as** regularmente e resolvendo quaisquer problemas que possam surgir.



Fonte: Implementação.  
Disponível em: [https://as1.ftcdn.net/v2/jpg/05/98/29/80/1000\\_F\\_598298028\\_dIZVHJ5KYxfGjGYfADxb76xzxFJY2Z7.jpg](https://as1.ftcdn.net/v2/jpg/05/98/29/80/1000_F_598298028_dIZVHJ5KYxfGjGYfADxb76xzxFJY2Z7.jpg)  
Acesso em 1 Jun. 2023

## Conclusão

As ameaças digitais são os riscos e perigos que existem no ambiente online, como ataques de hackers, vírus, malware, phishing, ransomware, roubo de dados, fraudes e outros. Para se proteger das ameaças digitais, é preciso ter consciência dos riscos e das boas práticas de cibersegurança. A conscientização é o processo de educação e sensibilização das pessoas sobre os conceitos, as normas e as medidas de proteção no ambiente digital. A conscientização é fundamental para criar uma cultura de segurança cibernética nas organizações e na sociedade.

