

# Cibersegurança

TechGuide - Alura, FIAP e PM3

---

## Nível 1

### Linha de comando - Fundamentos:

- CLI é um programa de linha de comando que aceita entradas de texto para executar funções do sistema operacional.
- Conhecer os principais comandos

### Conteúdos

- **Site** Microsoft Docs: Como usar argumentos de linha de comando para terminal do Windows (<https://docs.microsoft.com/pt-br/windows/terminal/command-line-arguments?tabs=windows>)
- **YouTube** Estevan Maito: Linha de comando básica - 8 comandos mais frequentes - WINDOWS e LINUX (<https://www.youtube.com/watch?v=rKBqXJZocYk>)
- **YouTube** Ninja do Linux: Comandos básicos da linha de comando do Linux ([https://www.youtube.com/watch?v=rs\\_yshFGu8E](https://www.youtube.com/watch?v=rs_yshFGu8E))

### Conteúdos Alura:

- **Artigo** CMD: dicas para trabalhar no prompt do Windows (<https://www.alura.com.br/artigos/cmd-dicas-para-trabalhar-no-prompt-do-windows>)
- **Artigo** Como configurar variáveis de ambiente no Windows, Linux e macOS (<https://www.alura.com.br/artigos/configurar-variaveis-ambiente-windows-linux-macos>)

- **Site** Primeiras aulas do Curso Windows Prompt: Trabalhando na linha de comando (<https://www.alura.com.br/conteudo/windows-prompt-utilizando-cmd>)
- **Curso** Curso Windows Prompt: Trabalhando na linha de comando (<https://www.alura.com.br/curso-online-prompt>)
- **Curso** Curso Terminal: aprenda comandos para executar tarefas (<https://cursos.alura.com.br/course/terminal-comandos-executar-tarefas>)

## Python - Fundamentos:

- Python é uma linguagem de programação de alto nível, de uso geral, amplamente utilizada em aplicações web, desenvolvimento de software, ciência de dados e Machine Learning. Sua filosofia de projeto enfatiza a legibilidade do código com o uso de indentação significativa. Python é dinamicamente tipada e tem um garbage collector.
- Conhecer os tipos primitivos
- Declarar variáveis, considerando os diferentes tipos
- Usar estruturas condicionais ('if', 'else')
- Conhecer os operadores de atribuição e comparação
- Usar estruturas de repetição e laços ('while', 'for')
- Usar funções, passando parâmetros e argumentos
- Manipular métodos
- Manipular arrays e listas
- Obter dados de uma API
- Criar construtores
- Funções anônimas

## Conteúdos

- **Site** Documentação Python (<https://docs.python.org/pt-br/3/tutorial/>)
- **Artigo** Programação | Python — Parte 1 (<https://medium.com/turing-talks/turing-talks-4-python-parte-1-29b8d9efd0a5>)

- **Artigo** Introdução ao Python  
(<https://medium.com/@goularteduarda.a/introdu%C3%A7%C3%A3o-ao-python-d30c29eba0d6>)
- **YouTube** Eduardo Mendes: Curso introdutório de Python  
(<https://www.youtube.com/watch?v=yTQDbqmv8Ho>)

### Conteúdos Alura:

- **Artigo** O que é Python? História, Sintaxe e um Guia para iniciar na Linguagem (<https://www.alura.com.br/artigos/python>)
- **Podcast** Hipsters.tech: Python – Hipsters 122  
(<https://www.hipsters.tech/python-hipsters-122/>)
- **Podcast** Hipsters.tech: Python Fluente – Hipsters Ponto Tech 179  
(<https://www.hipsters.tech/python-fluente-hipsters-ponto-tech-179/>)
- **YouTube** Alura: A linguagem Python - Alura Live 94  
(<https://www.youtube.com/watch?v=Nbt0eQHChol>)
- **YouTube** Alura: O que é Python? (<https://www.youtube.com/watch?v=-LATVnPcvHI>)
- **Artigo** Python - Uma Introdução à Linguagem  
(<https://www.alura.com.br/artigos/python-uma-introducao-a-linguagem>)
- **Artigo** Python: Trabalhando com precisão em números decimais  
(<https://www.alura.com.br/artigos/precisao-numeros-decimais-python>)
- **Artigo** Listas em Python: operações básicas  
(<https://www.alura.com.br/artigos/listas-no-python>)
- **Artigo** Como comparar objetos no Python?  
(<https://www.alura.com.br/artigos/como-comparar-objetos-no-python>)
- **Artigo** Python datetime: Lidando com datas e horários  
(<https://www.alura.com.br/artigos/lidando-com-datas-e-horarios-no-python>)
- **Curso** Curso Python: crie a sua primeira aplicação  
(<https://cursos.alura.com.br/course/python-crie-sua-primeira-aplicacao>)
- **Curso** Formação Python e orientação a objetos  
(<https://cursos.alura.com.br/formacao-linguagem-python>)

## Criptografia - Fundamentos:

- Criptografia em segurança virtual é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

### Conteúdos

- **Artigo** Introdução a criptografia (<https://medium.com/@m0blabs/introdução-a-criptografia-820206eda5a9>)
- **Artigo** Conceitos básicos de criptografia (<https://medium.com/prognosys/conceitos-básicos-de-criptografia-624eb6ec3171>)
- **Artigo** Criptografia simétrica (<https://medium.com/prognosys/criptografia-simétrica-6b4271ff697c>)
- **Artigo** Criptografia Assimétrica RSA (<https://medium.com/@tarcisioma/algorithm-de-criptografia-assimétrica-rsa-c6254a3c7042>)
- **Artigo** Algoritmos de criptografia (<https://www.kaspersky.com.br/resource-center/definitions/encryption>)
- **YouTube** Criptografia Assimétrica (<https://www.youtube.com/watch?v=GeSnN8Tt04U>)
- **YouTube** Criptografia (Guia Básico para Entender Como Funciona) (<https://www.youtube.com/watch?v=qHFbuXpz7e4>)
- **Artigo** Uma introdução à criptografia de chave pública e PGP (<https://ssd.eff.org/pt-br/module/uma-introdu%C3%A7%C3%A3o-%C3%A0-criptografia-de-chave-p%C3%BAblica-e-pgp>)

### Conteúdos Alura:

- **Artigo** Criptografia: entendendo as diferenças entre simétrica, assimétrica e homomórfica (<https://www.alura.com.br/artigos/criptografia-diferencas-simetica-assimetrica-homomorfica>)
- **Curso** Curso de DevOps: trabalhando com tráfego seguro em comunicações web (<https://cursos.alura.com.br/course/devops-trafego-seguro->

[comunicacoes-web\)](#)

## Framework de Cibersegurança:

- O Framework de Cibersegurança são guias de orientação para as organizações - em qualquer setor ou comunidade - que buscam melhorar o gerenciamento de riscos de segurança cibernética por meio da utilização de Framework. Embora o Framework de Cibersegurança não seja uma abordagem única para gerenciar riscos de segurança cibernética para organizações, em última análise, visa reduzir e gerenciar melhor esses riscos. Como tal, este guia destina-se a toda e qualquer organização, independentemente do setor ou tamanho.

## Conteúdos

- **Site** NIST (<https://www.nist.gov/cyberframework>)
- **Site** SOC2 (<https://www.aicpa.org/home>)
- **Site** ISO 27001 (<https://www.27001.pt/index.html>)
- **Artigo** Cybersecurity Framework 101 (<https://medium.com/edureka/cybersecurity-framework-89bbab5aaf17>)
- **Artigo** Top 10 Cybersecurity Frameworks to Know (<https://medium.com/@niitwork0921/top-10-cybersecurity-frameworks-to-know-8ee51d4f5b3e>)
- **Artigo** Cyber Security Guide (<https://www.stanfieldit.com/cyber-security/>)
- **YouTube** NIST Cybersecurity Framework Overview (<https://www.youtube.com/watch?v=4NSQCmAw6Ck>)
- **YouTube** The Cybersecurity Framework (<https://www.youtube.com/watch?v=J9ToNuwmyF0>)

## Técnicas Hacker:

- Entender as metodologias e as técnicas que os invasores usam para realizar o reconhecimento como uma etapa de pré-ataque, incluindo como eles usam inteligência de código aberto, varredura de rede e ataques de enumeração de alvos para encontrar as lacunas na segurança de sua rede.

- Usar técnicas de invasores para avaliar a segurança de uma rede de destino, avaliando protocolos e endpoints populares para Windows, Linux e destinos de nuvem.

## Conteúdos

- **Site** PTES ([http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page))
- **Site** OWASP (<https://owasp.org>)
- **Site** OSSTMM (<https://www.isecom.org/OSSTMM.3.pdf>)
- **Artigo** As Etapas de um Pentest (<https://reddyyz.medium.com/as-etapas-de-um-pentest-31b72ed326ac>)
- **Artigo** Password Cracking (<https://medium.com/rangeforce/password-cracking-6d9612915f03>)
- **Artigo** My pentesting methodology (Enumeration) (<https://medium.com/@nclvnp/enumeration-1976c5d55b1b>)
- **YouTube** How To Become A Hacker In 2022 (<https://www.youtube.com/watch?v=W6vcd2gJw3Q>)
- **Site** Hack The Box: A Massive Hacking Playground (<https://www.hackthebox.com>)

## Análise de Vulnerabilidades:

- Técnicas e táticas de framework de vários serviços e ferramentas que oferece uma solução de varredura e gerenciamento de vulnerabilidade.

## Conteúdos

- **Artigo** Nessus Vulnerability Scanner (<https://medium.com/@justinwolbert/nessus-vulnerability-scanner-22719d3bd9f7>)
- **Artigo** Ethical Hacking — Nessus (<https://medium.com/@rafaelrenovaci/ethical-hacking-nessus-f68d418a052c>)
- **Artigo** Open source vulnerability assessment tool OpenVAS (<https://medium.com/purple-team/open-source-vulnerability-assessment->

[tool-openvas-e7036c1e48fd](#))

- **Artigo** OpenVAS Install (<https://www.geeksforgeeks.org/installing-openvas-on-kali-linux/>)
- **YouTube** Análise de Vulnerabilidades com Nessus e OpenVAS em Distribuição Kali Linux (<https://www.youtube.com/watch?v=m7VjkYQEiHE>)
- **YouTube** Scanning Best Practices (<https://www.youtube.com/watch?v=SlRyd3f57c0>)
- **Site** Nessus (<https://www.tenable.com/downloads/nessus?loginAttempted=true>)
- **Site** Qualys (<https://www.qualys.com>)

## Firewalls, IDS e IPS:

- Definições e diferenças entre dispositivos de segurança de rede, firewalls, sistemas de prevenção de intrusão (IPS) e sistemas de detecção de intrusão (IDS).
- Um firewall permite o tráfego dependendo de um conjunto de regras que foram configuradas. Ele é baseado nos endereços de origem, destino e porta. Um firewall pode negar qualquer tráfego que não satisfaça os critérios especificados.
- IDS são dispositivos de sistema de monitoramento passivo que monitoram o tráfego de rede à medida que viajam pela rede, comparam padrões de assinatura, e acionar um alarme se for detectada atividade suspeita ou ameaça de segurança conhecida.
- O IPS é um dispositivo ativo que impede ataques, bloqueando-os.

## Conteúdos

- **Site** pfSense (<https://www.pfsense.org>)
- **Artigo** UFW: Descomplicando o Firewall (<https://medium.com/permalink-univesp/ufw-descomplicando-o-firewall-83159d85b57a>)
- **Artigo** O que é e por que usar um firewall Pfsense pra sua rede? (<https://phbols.medium.com/o-que-é-e-por-que-usar-um-firewall-pfsense-pra-sua-rede-35813c7ef2e>)

- **Artigo** IPTABLES VS NFTABLES (<https://medium.com/@nayara.watanuki/iptables-vs-nftables-883e3afc8e83>)
- **Artigo** Sistemas de detecção de intrusos e sistemas de prevenção de intrusos (<https://medium.com/mobicareoficial/sistemas-de-detec%C3%A7%C3%A3o-e-de-preven%C3%A7%C3%A3o-de-intrusos-princ%C3%ADpios-e-aplica%C3%A7%C3%A3o-de-entropia-9a33680f3948>)
- **Artigo** Learning More about IPS and IDS (<https://gupta-bless.medium.com/learning-more-about-ips-and-ids-ef6d859c2ab3>)
- **YouTube** Firewall com Iptables: Teoria e Prática ([https://www.youtube.com/watch?v=\\_xluY\\_3EQ2o](https://www.youtube.com/watch?v=_xluY_3EQ2o))
- **YouTube** iptables Complete Guide (<https://www.youtube.com/watch?v=6Ra17Qpj68c>)

## Investigação Digital - Fundamentos:

- Investigação Digital é o uso da ciência para investigar crimes digitais e determinar fatos, que surgiu a partir do uso e disseminação de sistemas digitais, como computadores e smartphones.

## Conteúdos

- **YouTube** DFIRScience: Intro to Cybercrime and Networks (<https://www.youtube.com/watch?v=sKijlRCRiKU>)
- **YouTube** DFIRScience: Cybersecurity and Cybercrime (<https://www.youtube.com/watch?v=3kEkXunWKaU>)
- **YouTube** DFIRScience: Digital Investigation Methods ([https://www.youtube.com/watch?v=72lhrc\\_MZ6o](https://www.youtube.com/watch?v=72lhrc_MZ6o))
- **YouTube** My CS: Digital Forensics Tools (<https://www.youtube.com/watch?v=Hwbb7zAWamg>)
- **Artigo** What is Digital Forensics (<https://haniahshafi.medium.com/what-is-digital-forensics-and-how-it-is-used-in-investigations-4389fdce7549>)



- **Artigo** Digital Forensics Investigation Steps (<https://medium.com/cyversity/digital-forensics-investigation-steps-f06a82c2c4ac>)

## Quebra de senhas:

- Em criptoanálise e segurança, a quebra de senhas é o processo de recuperação de senhas de dados que foram armazenados ou transmitidos por um sistema de computador de forma codificada. Uma abordagem comum (ataque de força bruta) é tentar repetidamente suposições para a senha e compará-las com um hash criptográfico disponível da senha.

## Conteúdos

- **Artigo** Password Cracking (<https://medium.com/rangeforce/password-cracking-6d9612915f03>)
- **Artigo** Cyber Security: Password Attacks (<https://liu-111.medium.com/cyber-security-password-attacks-8ea7fbdf307a>)
- **Artigo** Brute force SSH e FTP (<https://medium.com/@murilothink/realizando-ataque-de-brute-force-ssh-e-ftp-com-a-ferramenta-medusa-f6bd44b5bf53>)
- **Artigo** Brute-force attacks with Kali Linux (<https://pentestit.medium.com/brute-force-attacks-using-kali-linux-49e57bb89259>)
- **Artigo** DVWA 1.9+: Ataque brute force (<https://medium.com/canivete-sui%C3%A7o-hacker/dvwa-1-9-ii-e201af3f8617>)
- **Artigo** Hashcat 101: Cracking Password Hashes (<https://medium.com/@cyberforensicator57/hashcat-101-cracking-password-hashes-bb524b115f71>)
- **YouTube** Demonstração de Ataque Brute Force (<https://www.youtube.com/watch?v=Un4DlpDvkXU>)
- **YouTube** Medusa Tutorial (<https://www.youtube.com/watch?v=hZQ3AumggaA>)

## Open-Source Intelligence:

- OSINT (do inglês Open Source Intelligence) trata-se de um recurso que pode ser traduzido de uma forma simplificada como "Inteligência de Fontes Abertas". Trata-se de um conjunto de atividades para coletar, armazenar e analisar as informações de fontes públicas, basicamente, qualquer dado sobre uma empresa ou pessoa que possa ser encontrado por meio de ferramentas da Internet ou OSINT framework, como os buscadores.

### Conteúdos

- **Artigo** What Is Open Source Intelligence? (<https://medium.com/codex/what-is-open-source-intelligence-osint-43e56eb113b4>)
- **Artigo** Open Source Intelligence (OSINT) 101 (<https://medium.datadriveninvestor.com/open-source-intelligence-osint-101-d96f47ff2ff1>)
- **Site** OSINT (<https://osintframework.com/>)
- **Site** haveibeenpwned (<https://haveibeenpwned.com/>)
- **Site** checkusername (<https://checkusernames.com/>)
- **Artigo** OSINT What is it (<https://medium.com/transparent-data-eng/osint-what-is-it-and-what-does-it-have-to-do-with-open-sources-of-information-ec35daeea1c0>)
- **YouTube** O que é Inteligência Cibernética? O que é OSINT? (<https://www.youtube.com/watch?v=4kQ9ocPPPvs>)
- **YouTube** Crowsec Edtech | Carlos Vieira: Conheça uma ferramenta poderosa - Maltego (<https://www.youtube.com/watch?v=3DoGnYDOT-4>)

## Centro de Operações de Segurança:

- O SOC (Security Operations Center) é o departamento que vem para planejar e respaldar toda a estratégia de segurança da T.I, monitorando, prevenindo e remediando brechas, falhas e possíveis ataques, tudo de maneira proativa.

## Conteúdos

- **Artigo** SECURITY OPERATIONS CENTER — SOC (<https://medium.com/predict/security-operations-center-soc-e5f47e277a35>)
- **Artigo** What is the Blue Team? (<https://medium.com/@BurakDamoglu/introduction-to-security-operations-center-73e2e50f3ba7>)
- **Artigo** Security Operations Center (<https://medium.com/fnplus/security-operations-center-93e67268180a>)
- **YouTube** joe blaney: What is a Security operations centre SOC (<https://www.youtube.com/watch?v=3S01vLlvubE>)
- **Artigo** Future Of The SOC (<https://medium.com/anton-on-security/new-paper-future-of-the-soc-process-consistency-and-creativity-a-delicate-balance-paper-3-of-f73fe653c04d>)
- **YouTube** Construindo um SOC (Security Operations Center) (<https://www.youtube.com/watch?v=GP0sUdWs3Yg>)
- **YouTube** Fujitsu: Inside the Security Operations Centre (<https://www.youtube.com/watch?v=6LwyTWPKDnQ>)
- **YouTube** Telstra Enterprise: Security Operations Centre (<https://www.youtube.com/watch?v=zadlfhI0XQc>)

## Penetration Testing - Fundamentos:

- Pentest (Penetration Testing) é a prática de testar um sistema de computador, rede ou aplicativo da Web para encontrar vulnerabilidades que um invasor possa explorar, simulando um ataque contra os ativos de TI de uma organização.

## Conteúdos

- **Artigo** What is Penetration Testing? (<https://medium.com/edureka/what-is-penetration-testing-f91668e2291a>)
- **Artigo** From Zero to your first Penetration Test (<https://medium.com/hootsuite-engineering/penetration-testing-d887d081c5c5>)

- **Artigo** Quick Guide to Web Penetration Testing (<https://corneacristian.medium.com/quick-guide-to-web-penetration-testing-546c6196c909>)
- **Artigo** Pentesting Fundamentals (<https://infosecwriteups.com/pentesting-fundamentals-tryhackme-717f51d6126b>)
- **YouTube** O que é um Pentest? ([https://www.youtube.com/watch?v=Gf\\_BYCCKPiM](https://www.youtube.com/watch?v=Gf_BYCCKPiM))
- **YouTube** Como fazer um Pentest Externo do zero (<https://www.youtube.com/watch?v=H1auWPjioeU>)
- **YouTube** Qual a diferença entre Pentest e Bug Bounty? (<https://www.youtube.com/watch?v=ee4Yw8SNvis>)

### Conteúdos Alura:

- **Curso** Curso Pentest: explorando vulnerabilidades em aplicações web (<https://cursos.alura.com.br/course/pentest-explorando-vulnerabilidades-aplicacoes-web>)
- **Curso** Curso Pentest: investigando vulnerabilidades em um servidor de aplicações web (<https://cursos.alura.com.br/course/pentest-vulnerabilidades-servidor-aplicacoes-web>)
- **Curso** Curso Pentest: combinando vulnerabilidades e acessando o Shell (<https://cursos.alura.com.br/course/pentest-combinando-vulnerabilidades-acessando-shell>)

## Nível 2

### Segurança de Endpoint:

- A segurança de endpoint, ou proteção de endpoint, é a abordagem de segurança cibernética para defender endpoints como desktops, laptops e dispositivos móveis contra atividades maliciosas.

### Conteúdos

- **Artigo** Endpoint Security: I (<https://medium.com/starting-up-security/endpoint-security-intuition-around-the-mudge-disclosures->

[dfbe014790f2](#))

- **Artigo** Introduction to FireEye Endpoint Security (<https://medium.com/@knoldus/introduction-to-fireeye-endpoint-security-3534c9bf60fe>)
- **Artigo** EPP vs EDR vs XDR: Endpoint Security Comparison (<https://altexsoft.medium.com/epp-vs-edr-vs-xdr-endpoint-security-comparison-57409987f65e>)
- **Artigo** Endpoint Security -Antivirus, EPP & EDR (<https://anandadip.medium.com/endpoint-security-antivirus-epp-edr-99496597b892>)
- **Artigo** What is Endpoint Detection and Response (EDR) (<https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/>)
- **Artigo** EDR vs. NGAV (<https://www.crowdstrike.com/cybersecurity-101/endpoint-security/edr-vs-ngav/>)
- **Artigo** Introduction to Advanced Endpoint Protection (AEP) (<https://www.crowdstrike.com/cybersecurity-101/endpoint-security/advanced-endpoint-protection-aep/>)
- **Artigo** Endpoint Security (<https://www.crowdstrike.com/cybersecurity-101/endpoint-security/>)
- **YouTube** Heimdal: Endpoint Security - Definition, Benefits, and Key Components ([https://www.youtube.com/watch?v=2CVP9-Qslcw&ab\\_channel=Heimdal%C2%AE](https://www.youtube.com/watch?v=2CVP9-Qslcw&ab_channel=Heimdal%C2%AE))

## Metasploit - Ataque e Análise:

- Metasploit é a estrutura de teste de penetração mais usada do mundo.

## Conteúdos

- **Site** Metasploit (<https://www.metasploit.com/>)
- **Artigo** Kali Linux & Metasploit: Getting Started with Pen Testing (<https://medium.com/cyberdefendersprogram/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b>)

- **Artigo** Criação de Backdoor com MSFVENOM  
(<https://medium.com/@rafaelrenovaci/analise-de-malwares-01-6ac62f849283>)
- **Artigo** Hack Windows 10 with Metasploit  
(<https://medium.com/@leandro.almeida/hack-windows-10-with-metasploit-329c283db99a>)
- **YouTube** HackerSploit: Metasploit For Beginners 1  
([https://www.youtube.com/watch?v=8lR27r8Y\\_ik](https://www.youtube.com/watch?v=8lR27r8Y_ik))
- **YouTube** HackerSploit: Metasploit For Beginners 2  
(<https://www.youtube.com/watch?v=6SNHuWaLuhU>)
- **YouTube** HackerSploit: Metasploit For Beginners 3  
(<https://www.youtube.com/watch?v=CyB6Uta9VTI>)
- **YouTube** Metasploit - Ferramenta para Pentest  
(<https://www.youtube.com/watch?v=NyHaQJix0Ho>)

## Web application - Segurança:

- A segurança de aplicativos da Web (também conhecida como Web AppSec) é a ideia de criar sites para funcionar conforme o esperado, mesmo quando estão sob ataque. O conceito envolve uma coleção de controles de segurança projetados em um aplicativo da Web para proteger seus ativos de agentes potencialmente maliciosos.

## Conteúdos

- **Artigo** How to Secure Web Apps — A Web App Security Checklist  
(<https://medium.com/quick-code/how-to-secure-web-apps-a-web-app-security-checklist-bb27cf049d1d>)
- **Artigo** Web Application Security Basics  
(<https://mtrdesign.medium.com/web-application-security-basics-9b7553f51e8a>)
- **Artigo** Web Application Security (<https://pub.towardsai.net/web-application-security-top-11-best-practices-for-2020-c3a485e40de8>)
- **Artigo** Web Application Security Best Practices  
(<https://javascript.plainenglish.io/web-application-security-best-practices->

[881e3cfde2a1](#))

- **YouTube** House Of Secure Network: Web Application Security - Best Practices (<https://www.youtube.com/watch?v=RedZvpyRd38>)
- **YouTube** OWASP e o novo Top 10 Web application Security Risks ([https://www.youtube.com/watch?v=3EdFeJO\\_mB0](https://www.youtube.com/watch?v=3EdFeJO_mB0))
- **YouTube** Fireship: 7 Security Risks (<https://www.youtube.com/watch?v=4YOpLi9Oxs>)
- **YouTube** SAST / DAST ([https://www.youtube.com/watch?v=5cOkNbH\\_jPU](https://www.youtube.com/watch?v=5cOkNbH_jPU))

## Web application - Vulnerabilidade:

- As vulnerabilidades de aplicativos da Web envolvem uma falha ou fraqueza do sistema em um aplicativo baseado na Web. Eles existem há anos, em grande parte devido à não validação ou limpeza de entradas de formulário, servidores web mal configurados e falhas de design de aplicativos, e podem ser explorados para comprometer a segurança do aplicativo. Essas vulnerabilidades não são iguais a outros tipos comuns de vulnerabilidades, como rede ou ativo. Eles surgem porque os aplicativos da Web precisam interagir com vários usuários em várias redes, e esse nível de acessibilidade é facilmente aproveitado pelos hackers.

## Conteúdos

- **Site** OWASP Top Ten (<https://owasp.org/www-project-top-ten/>)
- **Artigo** Web Application Security Basics 101 (<https://medium.com/nerd-for-tech/devsecops-basics-where-to-start-aa7babee4ac4>)
- **Artigo** Web Application Security: From Vulnerabilities to Monitoring (<https://medium.com/swlh/web-application-security-from-vulnerabilities-to-monitoring-7a3c2dfbfa23>)
- **Artigo** DVWA (<https://medium.com/@rafaelrenovaci/instala%C3%A7%C3%A3o-dvwa-f70705af9d3e>)
- **Artigo** SQL Injection (<https://medium.com/@rafaelrenovaci/dvwa-solution-sql-injection-3be3709caea4>)

- **Artigo** File Inclusion (<https://medium.com/@rafaelrenovaci/dvwa-solution-file-inclusion-2a7f1504242b>)
- **Artigo** Brute Force (<https://medium.com/@rafaelrenovaci/dvwa-solution-brute-force-ee44c29a25e0>)
- **YouTube** CryptoCat: Damn Vulnerable Web Application (DVWA) (Playlist) (<https://www.youtube.com/playlist?list=PLHUKi1UIEgOJLPSFZaFKMoexpM6qhOb4Q>)
- **YouTube** Cloud Security Training & Consulting: OWASP 2021 Top 10 Web Application Vulnerabilities (<https://www.youtube.com/watch?v=NATCMnghei0>)

## Gerenciamento de Dispositivos Móveis:

- O gerenciamento de dispositivos móveis refere-se a qualquer ferramenta ou software projetado para ajudar os administradores para controlar e proteger dispositivos móveis como smartphones e tablets em uma organização. O gerenciamento de dispositivos móveis é uma parte importante do gerenciamento de mobilidade empresarial e do gerenciamento de endpoints, especialmente à medida que mais empresas adotam políticas de BYOD (traga seu próprio dispositivo) que permitem que os funcionários acessem dados, arquivos e aplicativos da empresa em seus dispositivos pessoais.

## Conteúdos

- **Artigo** What is Mobile Device Management (<https://hexnode.medium.com/what-is-mobile-device-management-mdm-3fd7fb4755b6>)
- **Artigo** Mobile Device Management Guide (<https://medium.com/codex/mobile-device-management-guide-2022-aosp-for-custom-mdm-6b9758aee4a8>)
- **Artigo** How To Address Privacy Concerns (<https://dennisturpitka.medium.com/how-to-address-privacy-concerns-when-building-a-mobile-device-management-solution-9bda148234df>)
- **Artigo** Top 5 mobile device management (<https://hexnode.medium.com/top-5-apple-mobile-device-management-platforms-for-2020-e6d626e68da5>)



- **YouTube** Entenda o que é MDM e quais as principais funcionalidades (<https://www.youtube.com/watch?v=EF7-4iNfVfs>)
- **YouTube** MTG, Inc.: What is MDM (Mobile Device Management)? ([https://www.youtube.com/watch?v=ug5KUH\\_jdA4](https://www.youtube.com/watch?v=ug5KUH_jdA4))
- **YouTube** Nutto 1981: Managing Microsoft 365 Mobility and Security MS 101 Day1 ([https://www.youtube.com/watch?v=2WTuDawLTxA&ab\\_channel=Nutto1981](https://www.youtube.com/watch?v=2WTuDawLTxA&ab_channel=Nutto1981))
- **YouTube** Harry Lowton: What Is Microsoft Intune? (<https://www.youtube.com/watch?v=ildHLspps7M>)

## SIEM e SOAR:

- Security Information and Event Management (SIEM) são softwares que agregam e analisam informações de várias fontes diferentes em toda a infra-estrutura.
- Security Orchestration, Automation, and Response (SOAR) irá ajudar com o gerenciamento de ameaças e vulnerabilidades, resposta a incidentes de segurança e automação da operação de segurança.

## Conteúdos

- **Artigo** SIEM (<https://medium.com/sysadminas/elastic-siem-introdu%C3%A7%C3%A3o-e3486a0c995e>)
- **Artigo** Security Information & Event Management (<https://blog.gofix.com.br/security-information-event-management-siem-b7a9a2c70837>)
- **Artigo** SIEM e SOC para iniciantes (<https://medium.com/@mariliasroch/siem-e-soc-para-iniciantes-a36c9ad40b46>)
- **Artigo** Introdução ao OSSIM (<https://lucxs.medium.com/siem-introdu%C3%A7%C3%A3o-ao-ossim-98a45fffeb19>)
- **Artigo** Top Free Security Information and Event Management(SIEM) Software's (<https://kalhara-sampath.medium.com/top-free-security-information-and-event-management-siem-sofware-20c6d8f32a6f>)

- **Site** O que é o ELK Stack? (<https://www.elastic.co/pt/what-is/elk-stack>)
- **YouTube** BlackPerl: SOC Open Source (<https://www.youtube.com/watch?v=t6PqjLlVgdA>)
- **YouTube** Ebenezer Solution: Como configurar o SIEM Wazuh ([https://www.youtube.com/watch?v=wT\\_z5fRnoXc](https://www.youtube.com/watch?v=wT_z5fRnoXc))

## Hardening de Servidores:

- A proteção do servidor é um conjunto de disciplinas e técnicas que melhoram a segurança de um servidor 'em produção'. Hardening é um requisito de estruturas de segurança em diversos frameworks.

## Conteúdos

- **Artigo** Introdução a Hardening de Servidores (<https://medium.com/@gabub/introdu%C3%A7%C3%A3o-a-hardening-de-servidores-27570fc8597a>)
- **Artigo** Linux Server Hardening (<https://medium.com/@thefoursec/linux-server-hardening-e659db8ec689>)
- **Artigo** 5 Steps to (Secure)Hardening (<https://saeedrz.medium.com/5-steps-to-hardening-your-server-centos-7-25e1851c8204>)
- **Artigo** Como fazer o Hardening do seu servidor Linux (<https://phbols.medium.com/como-fazer-o-hardening-do-seu-servidor-linux-14b6f1b3499b>)
- **Artigo** Server Architecture Security (Windows) (<https://medium.com/@jbrendan86/server-architecture-security-windows-2da580d58e62>)
- **YouTube** Linode: Hardening Access to Your Server (<https://www.youtube.com/watch?v=eeaFoZISq6I>)
- **YouTube** Christian Lempa: How to protect Linux from Hackers ([https://www.youtube.com/watch?v=Bx\\_HkLVBz9M](https://www.youtube.com/watch?v=Bx_HkLVBz9M))
- **YouTube** INEtraining: Linux Security & Server Hardening - Linux PAM (<https://www.youtube.com/watch?v=N4DP68TK0AQ>)

- **YouTube** IT Ops Talk: How to Harden Windows Server ([https://www.youtube.com/watch?v=HG\\_z\\_Q7LMIM&ab\\_channel=ITOpsTalk](https://www.youtube.com/watch?v=HG_z_Q7LMIM&ab_channel=ITOpsTalk))

## Análise Forense na Nuvem:

- A investigação de dados armazenados na nuvem pode ser uma variedade de abordagens, desde investigações de inteligência de código aberto (OSINT) até investigações de contas na nuvem de indivíduos participantes que divulgam suas credenciais de login (mais frequentemente de vítimas e testemunhas do que de suspeitos), para obter e análise de devoluções de garantias de provedores de serviços em nuvem para obter acesso às contas de suspeitos.

## Conteúdos

- **Artigo** Cloud Forensics Tools ([https://medium.com/@cloud\\_tips/cloud-forensics-788f0c8fe69c](https://medium.com/@cloud_tips/cloud-forensics-788f0c8fe69c))
- **Artigo** Cloud forensics (<https://kumarshivam-66534.medium.com/cloud-forensics-be18e14230de>)
- **Artigo** Digital Forensic Challenges In Cloud Computing (<https://medium.com/@frosky/digital-forensic-challenges-in-cloud-computing-part-1-c06301cbe174>)
- **Artigo** Overview of Cloud Forensics (<https://medium.com/sigma-xi-vit/overview-of-cloud-forensics-b928537791e6>)
- **Artigo** How to Think about Threat Detection (<https://medium.com/anton-on-security/how-to-think-about-threat-detection-in-the-cloud-1baff902afe5>)
- **YouTube** Forensic Focus: Forensics In The Cloud - How To Conduct An Office 365 Investigation (<https://www.youtube.com/watch?v=wFjFjemaxml>)
- **YouTube** SANS Digital Forensics and Incident Response: Cloud Forensics & Incident Response Course (<https://www.youtube.com/watch?v=XoeuAVJwkQ8>)

## Recuperação de Dados:

- A recuperação de dados é um processo orientado por software que permite recuperar e restaurar arquivos perdidos, excluídos, inacessíveis,

corrompidos ou danificados para que você possa voltar ao trabalho rapidamente. À medida que o cenário de negócios e nossas vidas em geral se tornam mais dependentes de dados, cresce a necessidade de proteger os sistemas de dados.

## Conteúdos

- **Artigo** Data Recovery (<https://medium.com/@rohitpatil97/data-recovery-c9818f19441d>)
- **Artigo** Data Loss Restoration (<https://medium.com/@danielmop/survey-research-paper-data-loss-restoration-4fae9fa38685>)
- **Artigo** Data Recovery and AI (<https://medium.com/@joanna.riley/data-recovery-and-ai-what-you-need-to-know-75a44c79385d>)
- **Artigo** Upcoming Future Of Data Backup & Recovery (<https://kunalranjane.medium.com/upcoming-future-of-data-backup-recovery-509d7fc1690f>)
- **Artigo** How to Recover Deleted Files (<https://medium.com/android-news/how-to-recover-deleted-files-from-hard-drive-a-step-by-step-recovery-solution-14355745239a>)
- **YouTube** Techquickie: Data Recovery As Fast As Possible (<https://www.youtube.com/watch?v=PWuWOSOCGxE>)
- **YouTube** Techquickie: Data Recovery Services (<https://www.youtube.com/watch?v=v0QkafslNrM>)
- **YouTube** IBM Technology: Disaster Recovery vs. Backup (<https://www.youtube.com/watch?v=07EHsPuKXc0>)

## Segurança de Contêineres:

- A segurança de contêineres é o processo de combinar políticas de segurança para assegurar que a integridade do contêiner esteja protegida. A segurança do contêiner é importante porque a imagem do contêiner contém todos os componentes que, eventualmente, executarão seu aplicativo. Se houver vulnerabilidades à espreita na imagem do contêiner, o risco e a gravidade potencial dos problemas de segurança durante a produção aumentam.

## Conteúdos

- **Artigo** Container Security Solutions (<https://medium.com/xenonstack-security/container-security-solutions-framework-mechanism-and-strategy-24de3891a12b>)
- **Artigo** Container Security Threats (<https://medium.com/oreillymedia/container-security-threats-38649261fb4f>)
- **Artigo** Top 20 Docker Security Tips (<https://towardsdatascience.com/top-20-docker-security-tips-81c41dd06f57>)
- **Artigo** Container Security (<https://blog.pentesteracademy.com/learning-path-container-security-9a9c47760250>)
- **YouTube** IBM Technology: Container Security Explained ([https://www.youtube.com/watch?v=b\\_euX\\_M82uI](https://www.youtube.com/watch?v=b_euX_M82uI))
- **YouTube** The Linux Foundation: Container Security 101 (<https://www.youtube.com/watch?v=PDDiOI7ckzQ>)
- **YouTube** HackerSploit: Docker Security Essentials (<https://www.youtube.com/watch?v=KINjl1tlo2w>)
- **YouTube** HackerSploit: Auditing Docker Security (<https://www.youtube.com/watch?v=mQkVB6KMHCg>)
- **YouTube** Roadsec: Segurança em Docker - Mais que containers ([https://www.youtube.com/watch?v=5ya\\_t0YWfyE](https://www.youtube.com/watch?v=5ya_t0YWfyE))

## Análise Forense de Memória:

- A análise forense de memória (às vezes chamada de análise de memória) refere-se à análise de dados voláteis no despejo de memória de um computador. Os profissionais de segurança da informação realizam análises forenses de memória para investigar e identificar ataques ou comportamentos maliciosos que não deixam rastros facilmente detectáveis nos dados do disco rígido.

## Conteúdos

- **Artigo** Memory Analysis For Beginners (<https://infosecwriteups.com/memory-analysis-for-beginners-with-volatility->

[coreflood-trojan-part-1-89981433eeb6\)](#)

- **Artigo** First steps to volatile memory analysis (<https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1>)
- **Artigo** Analyzing Memory Dump with Volatility (<https://blog.pentesteracademy.com/analyzing-memory-dump-with-volatility-302f30917713>)
- **Artigo** Memory Analysis For Beginners With Volatility (<https://infosecwriteups.com/memory-analysis-for-beginners-with-volatility-coreflood-trojan-part-2-42bdb46683f2>)
- **YouTube** 13Cubed: Introduction to Memory Forensics (<https://www.youtube.com/watch?v=1PAGcPJFwbE>)
- **YouTube** DFIRScience: Introduction to Memory Forensics with Volatility 3 ([https://www.youtube.com/watch?v=Uk3DEgY5Ue8&ab\\_channel=DFIRScience](https://www.youtube.com/watch?v=Uk3DEgY5Ue8&ab_channel=DFIRScience))
- **YouTube** SANS Digital Forensics and Incident Response: Using Memory Analysis for Faster Response to User Investigations (<https://www.youtube.com/watch?v=QzPk1oyzMzc>)
- **YouTube** 13Cubed: Introduction to Windows Forensics (<https://www.youtube.com/watch?v=VYROU-ZwZX8>)

## Análise Forense de Rede:

- A análise forense de rede diz respeito à coleta, monitoramento e análise de atividades de rede para descobrir a origem de ataques, vírus, intrusões ou violações de segurança que ocorrem em uma rede ou no tráfego de rede. Como tal, a análise forense de rede é considerada juntamente com a análise forense móvel ou a análise forense de imagem digital, como residindo sob o guarda-chuva da análise forense digital.

## Conteúdos

- **Artigo** Network Analysis (<https://medium.com/@wenhaowu92/network-analysis-travel-time-and-accessibility-5848b4ae5f65>)

- **Artigo** What is Network Analysis?  
(<https://towardsdatascience.com/network-analysis-d734cd7270f8>)
- **Artigo** Using Wireshark to show you, how unsecure a public network can be  
(<https://bernardosr1.medium.com/using-wireshark-to-show-you-how-unsecure-a-public-network-can-be-f93e373767a8>)
- **Artigo** Analyzing a bot-infected host with Wireshark  
(<https://medium.com/geekculture/analyzing-a-bot-infected-host-with-wireshark-c707068fffa2>)
- **YouTube** Semi Yulianto: Digital Forensics - Analyzing Network Traffic  
(<https://www.youtube.com/watch?v=jPQCHZIN88g>)
- **YouTube** FreeEduHub: Network Forensics (<https://www.youtube.com/watch?v=VklrX2lfCNk>)
- **YouTube** edureka!: Cybersecurity & Digital Forensics Tutorial  
(<https://www.youtube.com/watch?v=cg1p3SRZHNY>)
- **YouTube** Netsec Explained: Advanced Wireshark Network  
([https://www.youtube.com/watch?v=e\\_dsGhvg9CU](https://www.youtube.com/watch?v=e_dsGhvg9CU))

## Scripts PowerShell para segurança:

- Um script ofuscado pode ser malicioso e difícil de detectar com inspeção visual durante o processo de aprovação do script. Revise visualmente os scripts do PowerShell e use ferramentas de inspeção para ajudar a detectar problemas de script suspeitos. Essas ferramentas nem sempre podem determinar a intenção do autor do PowerShell, portanto, podem chamar a atenção para um script suspeito.

## Conteúdos

- **Artigo** Using PowerShell for Password Security Checks  
(<https://medium.com/@jeffreypinkstaff/using-powershell-for-password-security-checks-3e229c39303>)
- **Artigo** PowerShell — Testing your workstation security posture  
(<https://medium.com/@smurf3r5/powershell-testing-your-workstation-security-posture-add06d4061eb>)

- **Artigo** Malicious PowerShell Usage Detection (<https://0xneel.medium.com/malicious-powershell-usage-detection-f0ce9b6cca81>)
- **Artigo** Encrypt & Decrypt Data with PowerShell (<https://medium.com/@sumindaniro/encrypt-decrypt-data-with-powershell-4a1316a0834b>)
- **Artigo** Run PowerShell without Powershell.exe (<https://bank-security.medium.com/how-to-running-powershell-commands-without-powershell-exe-a6a19595f628>)
- **YouTube** QuickStart: Using PowerShell for Cyber Security (<https://www.youtube.com/watch?v=K9zVwjJ4nk>)
- **YouTube** Michael Ferrie: Scripting for Security 1 - Introduction to PowerShell ([https://www.youtube.com/watch?v=XQIVi\\_OJ2ZA](https://www.youtube.com/watch?v=XQIVi_OJ2ZA))
- **YouTube** SecurityFWD: Beginner's Guide to Building AD Security Tools with PowerShell (<https://www.youtube.com/watch?v=Kk7nJe1T-ik>)

## Nível 3

### Arquitetura de Segurança de Rede:

- A segurança de rede prepara você para tarefas como proteger os dados da empresa contra roubo, danos, interrupções e outros. Um profissional da área irá projetar e implementar uma arquitetura segura para dispositivos de rede, bem como oferecer suporte de segurança e garantir a integridade deles.

### Conteúdos

- **Artigo** Network Architecture and How to Design a Secure Network (<https://nirasha.medium.com/network-architecture-and-how-to-design-a-secure-network-669848bff76c>)
- **Artigo** Cybersecurity Architecture (<https://medium.com/cloud-security/cybersecurity-architecture-66714e39bd91>)



- **Artigo** Security Architecture is Not A Checklist (<https://medium.com/cloud-security/security-architecture-is-not-a-checklist-b86f1dc0aa0c>)
- **Artigo** CCNA security (<https://hamzamhirsi.medium.com/ccna-security-part-1-networking-security-concepts-aeaab60b506e>)
- **YouTube** edureka!: Network Security Tutorial (<https://www.youtube.com/watch?v=6JubI1UnJTE>)
- **YouTube** Cássio Batista Pereira: Network Security, a carreira pouco falada (<https://www.youtube.com/watch?v=z5W8krdHkqA>)
- **YouTube** Snap One: Networking Design (<https://www.youtube.com/watch?v=sckuGYiHYRA>)

## Threat Hunting:

- A busca de ameaças (Threat Hunting) é a prática de procurar proativamente por ameaças cibernéticas que estão à espreita sem serem detectadas em uma rede. A caça a ameaças cibernéticas se aprofunda para encontrar agentes mal-intencionados em seu ambiente que passaram pelas defesas de segurança de endpoint iniciais.

## Conteúdos

- **Artigo** Threat Hunting: The Basics (<https://kostas-ts.medium.com/threat-hunting-series-the-basics-cccadac830c6>)
- **Artigo** The Threat Hunting Process (<https://kostas-ts.medium.com/threat-hunting-series-the-threat-hunting-process-f76583f2475b>)
- **Artigo** What Makes a Good Threat Hunter (<https://kostas-ts.medium.com/threat-hunting-series-what-makes-a-good-threat-hunter-e2b1d0d07e8c>)
- **Artigo** Threat Hunting Guide (<https://medium.com/@joshuaspushock/threat-hunting-guide-5cd1444d8d95>)
- **YouTube** Threat Hunting Process e o Método Investigativo (<https://www.youtube.com/watch?v=Z4EbWPYt6vE>)
- **YouTube** O próximo nível de defesa (<https://www.youtube.com/watch?v=DmOkdVCdft4>)

- **YouTube** Threat Hunting com esteróides (<https://www.youtube.com/watch?v=THntxi5PYDg>)
- **YouTube** The PC Security Channel: Threat Hunting Tutorial - Introduction ([https://www.youtube.com/watch?v=qrZsc5lkchl&ab\\_channel=ThePCSecurityChannel](https://www.youtube.com/watch?v=qrZsc5lkchl&ab_channel=ThePCSecurityChannel))
- **YouTube** SANS EMEA: Effective (Threat) Hunting Techniques ([https://www.youtube.com/watch?v=JmKSnRMW\\_6w&ab\\_channel=SANSEMEA](https://www.youtube.com/watch?v=JmKSnRMW_6w&ab_channel=SANSEMEA))
- **YouTube** SANS Institute: Hunting for Post-Exploitation Stage Attacks with Elastic Stack (<https://www.youtube.com/watch?v=PdCQChYrxXg>)

## Segurança física:

- A segurança física é a proteção de pessoas, propriedades e ativos físicos de ações e eventos que podem causar danos ou perdas. Embora muitas vezes negligenciada em favor da segurança cibernética, a segurança física é igualmente importante.

## Conteúdos

- **Artigo** What Is Physical Security (<https://www.sine.co/blog/what-is-physical-security-understanding-workplace-safety/>)
- **Artigo** Cyber Security and Physical Security (<https://rchen8.medium.com/cyber-security-and-physical-security-are-very-different-22e31a933907>)
- **Artigo** What is a Physical Security Architect? (<https://jay-pang.medium.com/what-is-a-physical-security-architect-2e8bd8b4b130>)
- **YouTube** Tom Olzak: Physical Security Part 1 - Intro and Site Barriers (<https://www.youtube.com/watch?v=j9MQMVn3FV4>)
- **YouTube** Tom Olzak: Physical Security Part 2 - Walls, Doors, and Locks (<https://www.youtube.com/watch?v=EAeVUDMDSn4>)
- **YouTube** Tom Olzak: Physical Security Part 3 - Lights, Sensors, and Alarms (<https://www.youtube.com/watch?v=tyFkj5UrPJQ>)

- **YouTube** Tom Olzak: Physical Security Part 4 - Environmental Controls ([https://www.youtube.com/watch?v=o\\_ENagQ60nY](https://www.youtube.com/watch?v=o_ENagQ60nY))

## Gerenciamento de Resposta a Incidentes:

- A resposta a incidentes é um processo estruturado que as organizações usam para identificar e lidar com incidentes de segurança cibernética. A resposta inclui vários estágios, incluindo preparação para incidentes, detecção e análise de um incidente de segurança, contenção, erradicação e recuperação total e análise e aprendizado pós-incidente.

## Conteúdos

- **Artigo** Incident Management (<https://hugoodias.medium.com/incident-management-8defb3812352>)
- **Artigo** An Incident Response Plan for Startups (<https://medium.com/starting-up-security/an-incident-response-plan-for-startups-26549596b914>)
- **Artigo** Incident Response Management (<https://fergusmacdermot.medium.com/incident-management-methods-cb9274c264fe>)
- **Artigo** Cybersecurity incident response plan (<https://strategicoutlook.medium.com/why-organizations-need-to-have-a-formal-cyber-security-incident-response-plan-2c13f2e4082>)
- **YouTube** Ascend Technologies: The Six Phases of Incident Response (<https://www.youtube.com/watch?v=X4IPEpATNxg>)
- **YouTube** Skillset: Incident Response Plan (<https://www.youtube.com/watch?v=PhROeWMPBqU>)
- **YouTube** WissenX Akademie: Incident Response Process, Lifecycle & Methodology (<https://www.youtube.com/watch?v=Sr8tfoZJa3M>)

## Análise de Malware:

- A análise de malware é o processo de compreensão do comportamento e da finalidade de um arquivo ou URL suspeito. A saída da análise ajuda na detecção e mitigação da ameaça potencial.

## Conteúdos

- **Artigo** Malware Analysis- The art of understanding malware  
(<https://medium.com/techiepedia/malware-analysis-the-art-of-understanding-malware-ffc5e69feb3e>)
- **Artigo** Malware Analysis 101 - Basic Static Analysis  
(<https://infosecwriteups.com/malware-analysis-101-basic-static-analysis-db59119bc00a>)
- **Artigo** Malware Analysis — Tools And Resources  
(<https://nasbench.medium.com/malware-analysis-tools-and-resources-16eb17666886>)
- **Artigo** Malware Analysis 101 - Sandboxing  
(<https://infosecwriteups.com/malware-analysis-101-sandboxing-746a06432334>)
- **Artigo** Malware Analysis: Introduction to YARA  
(<https://medium.com/@ammadb/malware-analysis-introduction-to-yara-e11b89e02ba6>)
- **YouTube** Papo Binário: AMO - Análise de Malware Online (Playlist)  
(<https://www.youtube.com/playlist?list=PLIfZMtpPYFP7281QqcwivCTuKeelXxg7G>)
- **YouTube** Papo Binário: CERO - Curso de Engenharia Reversa Online (Playlist)  
(<https://www.youtube.com/playlist?list=PLIfZMtpPYFP6zLKlNyAeWY1I85VpyshAA>)
- **YouTube** Papo Binário: CEB - Curso de Exploração de Binários (Playlist)  
([https://www.youtube.com/playlist?list=PLIfZMtpPYFP4MaQhy\\_iR8uM0mJEs7P7s3](https://www.youtube.com/playlist?list=PLIfZMtpPYFP4MaQhy_iR8uM0mJEs7P7s3))

## Segurança de Aplicações de Software:

- A segurança de aplicações descreve as medidas de segurança no nível do aplicativo que visam impedir que dados ou códigos dentro da aplicação sejam roubados ou invadidos. Ele abrange as considerações de segurança que ocorrem durante o desenvolvimento e o design de aplicativos, mas

também envolve sistemas e abordagens para proteger os aplicativos depois que eles são implantados.

## Conteúdos

- **Artigo** Application security vs. software security ([https://medium.com/@SW\\_Integrity/application-security-vs-software-security-whats-the-difference-3d345413927c](https://medium.com/@SW_Integrity/application-security-vs-software-security-whats-the-difference-3d345413927c))
- **Artigo** A Comprehensive Guide To Application Security (<https://medium.com/edureka/application-security-tutorial-e6a0dda25f5c>)
- **Artigo** Application Security Best Practices ([https://medium.com/@cloud\\_tips/application-security-best-practices-c63b79f29a99](https://medium.com/@cloud_tips/application-security-best-practices-c63b79f29a99))
- **Artigo** Importance of Software Security (<https://medium.com/nerd-for-tech/importance-of-software-security-application-security-non-technical-hacking-encryption-and-365c93def04e>)
- **YouTube** Application Security 101 - What you need to know in 8 minutes ([https://www.youtube.com/watch?v=Dp019cWu1cg&t=1s&ab\\_channel=Snyk](https://www.youtube.com/watch?v=Dp019cWu1cg&t=1s&ab_channel=Snyk))
- **YouTube** edureka!: Application Security (<https://www.youtube.com/watch?v=gfFKuiZ9Y7s>)
- **YouTube** GOTO Conferences: Secure by Design – the Architect's Guide to Security Design Principles (<https://www.youtube.com/watch?v=4qN3JBGd1g8>)
- **YouTube** Cybr: Introduction to Application Security - Course ([https://www.youtube.com/watch?v=3QOlo2pEpvc&ab\\_channel=Cybr](https://www.youtube.com/watch?v=3QOlo2pEpvc&ab_channel=Cybr))

## Conteúdos Alura:

- **Curso** Formação Cibersegurança (<https://cursos.alura.com.br/formacao-ciberseguranca>)

## Arquitetura Zero Trust:

- Zero Trust é um modelo de segurança de rede baseado na filosofia de que nenhuma pessoa ou dispositivo dentro ou fora da rede de uma organização

deve ter acesso para se conectar a sistemas ou serviços de TI até que seja autenticado e verificado continuamente.

## Conteúdos

- **YouTube** Zero Trust - E o Fatídico Fim da VPN ([https://www.youtube.com/watch?v=T\\_J3\\_R7tz1Q](https://www.youtube.com/watch?v=T_J3_R7tz1Q))
- **Artigo** NIST - Zero Trust Architecture (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>)
- **Artigo** What does Zero Trust Architecture stand for? (<https://medium.com/databulls/what-does-zero-trust-architecture-stand-for-3facb50226b4>)
- **Artigo** Zero Trust Architecture (<https://medium.com/geekculture/to-the-letter-zero-trust-architecture-zta-according-to-nist-800-207-1-3cf2b23d383b>)
- **Artigo** What Is Zero Trust Architecture (<https://medium.com/magalix/what-is-zero-trust-architecture-and-how-does-it-work-23067912335c>)
- **YouTube** Zero trust model (<https://www.youtube.com/watch?v=S6tobeRPr2U>)
- **YouTube** What is Zero Trust Network Access (<https://www.youtube.com/watch?v=DLQAbJm4gFM>)
- **YouTube** Descomplicando Zero Trust ([https://www.youtube.com/watch?v=Pjz\\_4U7lrLo](https://www.youtube.com/watch?v=Pjz_4U7lrLo))
- **YouTube** John Savill's Technical Training: Understanding and Getting Started with Zero Trust ([https://www.youtube.com/watch?v=hhS8VdGnfOU&ab\\_channel=JohnSavill%27sTechnicalTraining](https://www.youtube.com/watch?v=hhS8VdGnfOU&ab_channel=JohnSavill%27sTechnicalTraining))

## Conteúdos Alura:

- **Artigo** Modelo de Segurança Zero Trust: entenda como funciona e sua importância (<https://www.alura.com.br/artigos/modelo-seguranca-zero-trust-como-funciona>)

## Segurança na Nuvem:

- A segurança na nuvem, também conhecida como segurança da computação em nuvem, é um conjunto de medidas de segurança projetadas para proteger a infraestrutura, os aplicativos e os dados baseados em nuvem. Essas medidas garantem a autenticação de usuários e dispositivos, controle de acesso a dados e recursos e proteção de privacidade de dados. Eles também suportam a conformidade de dados regulatórios.

### Conteúdos

- **Artigo** Security in Cloud Computing (<https://medium.com/cyversity/security-in-cloud-computing-8d77b20e7a2d>)
- **Artigo** What Is Cloud Security Posture Management? (<https://blog.cloudboost.io/what-is-cloud-security-posture-management-7ca9650d18e6>)
- **Artigo** Cloud Applications Concept (<https://medium.com/databulls/new-era-cloud-applications-concept-and-security-4ccfe29db9d7>)
- **Artigo** Security IN the Cloud vs Security OF the Cloud (<https://medium.com/nerd-for-tech/security-in-the-cloud-vs-security-of-the-cloud-114dbcf962a9>)
- **YouTube** IBM Technology: What is Cloud Security? (<https://www.youtube.com/watch?v=jl8IKpjiCSM>)
- **YouTube** edureka!: Cloud Security Tutorial (<https://www.youtube.com/watch?v=0lw4KU5wHsk>)
- **YouTube** Simplilearn: Cloud Security Fundamentals ([https://www.youtube.com/watch?v=M\\_9hRPVH5SA](https://www.youtube.com/watch?v=M_9hRPVH5SA))

## Segurança Contínua - Automação e Monitoramento:

- O monitoramento contínuo de segurança é uma abordagem de segurança que envolve a automatização de uma parte significativa do gerenciamento de segurança. Isso inclui detecção de vulnerabilidades, monitoramento de configurações de nuvem, identidades e seus direitos e segurança de dados.

## Conteúdos

- **Artigo** Continuous Security (<https://medium.com/digital-transformation-and-platform-engineering/devsecops-automation-and-continuous-security-4b720d0082f0>)
- **Artigo** Continuous Security: A Necessity on Cloud (<https://nutanix.medium.com/continuous-security-a-necessity-on-cloud-848e6ef9cace>)
- **Artigo** DevOps Tools: Automation, Monitoring, CI/CD, and More (<https://altexsoft.medium.com/devops-tools-automation-monitoring-ci-cd-and-more-ac7c4ca31879>)
- **Artigo** Log Analysis for Digital Forensic Investigation (<https://medium.com/mii-cybersec/log-analysis-for-digital-forensic-investigation-e4a00f5a5c09>)
- **YouTube** Information Security Continuous Monitoring (<https://www.youtube.com/watch?v=1V5FyasVMaM>)
- **YouTube** Cloud Security Automation ([https://www.youtube.com/watch?v=2epVP58kn\\_Q](https://www.youtube.com/watch?v=2epVP58kn_Q))
- **YouTube** SOAR - Security Orchestration Automation and Response (<https://www.youtube.com/watch?v=i7H7VYkfUEw>)
- **YouTube** Continuous Cloud Security Monitoring (<https://www.youtube.com/watch?v=ePCK8quTP2o>)

## Habilidade Auxiliar: Sistemas e tecnologias

### Redes de Computadores - Fundamentos:

- Rede de computadores é uma malha que interliga milhares de sistemas computacionais para a transmissão de dados. Também conhecidos como nós, esses dispositivos interconectados enviam, recebem e trocam tráfego de dados, voz e vídeo, graças ao hardware e software que compõe o ambiente.
- Configurações de redes são essenciais para que seja possível acessar uma aplicação, principalmente se ela estiver na nuvem.



- Entenda melhor os componentes de rede e a suas atribuições
- Diferenciar os serviços disponibilizados a nível de rede
- Saber as diferenças entre as camadas de rede
- Saber o que é servidor web, proxy reverso e load balancer

## Conteúdos

- **Site** IBM: Conceitos de rede e comunicação (<https://www.ibm.com/docs/pt-br/aix/7.3?topic=management-network-communication-concepts>)
- **Site** AWS: O que são redes de computadores? (<https://aws.amazon.com/pt/what-is/computer-networking/>)
- **Site** Red Hat: O que é gerenciamento de rede? (<https://www.redhat.com/pt-br/topics/management/what-is-network-management>)
- **Artigo** Redes de Computadores — Sabendo o básico — Intro (<https://medium.com/code-breaker/redes-de-computadores-sabendo-o-b%C3%AAsico-intro-1a7d5653e118>)
- **Artigo** O protocolo TCP/IP (<https://joaomarcuraa.medium.com/o-protocolo-tcp-ip-1dc2cdb88b07>)
- **YouTube** Código Fonte TV: IP (Entenda finalmente como funciona o IPv4 e o IPv6) | Dicionário do Programador (<https://www.youtube.com/watch?v=O8DmpmBMUSw>)
- **YouTube** Rede de Computadores - Animação em 3D (<https://www.youtube.com/watch?v=lqcp3k8DgGw>)
- **Curso** Enterprise Networking, Security, and Automation (<https://www.netacad.com/pt-br/courses/networking/ccna-enterprise-networking-security-automation>)
- **Curso** Switching, Routing, and Wireless Essentials (<https://www.netacad.com/pt-br/courses/networking/ccna-switching-routing-wireless-essentials>)
- **Curso** Introduction to Networks (<https://www.netacad.com/pt-br/courses/networking/ccna-introduction-networks>)

## Conteúdos Alura:

- **Artigo** Rede de computadores: um guia completo sobre o que são, como funcionam e quais cursos fazer na área  
(<https://www.alura.com.br/artigos/rede-de-computadores>)
- **Artigo** Conhecendo algumas topologias de rede  
(<https://www.alura.com.br/artigos/conhecendo-algumas-topologias-de-rede>)
- **Artigo** Como calcular máscaras de sub-rede de forma simples  
(<https://www.alura.com.br/artigos/como-calcular-mascaras-de-sub-rede>)
- **Artigo** Entendendo os padrões de Wi-Fi  
(<https://www.alura.com.br/artigos/entendendo-os-padroes-de-wi-fi>)
- **Artigo** Diferenças entre Hubs e Switches  
(<https://www.alura.com.br/artigos/diferencas-entre-hubs-e-switches>)
- **Artigo** Entendendo os cabos de rede  
(<https://www.alura.com.br/artigos/entendendo-os-cabos-de-rede>)
- **Artigo** SSH, Telnet e as diferenças para conectar em um servidor  
(<https://www.alura.com.br/artigos/entendendo-as-diferencas-entre-telnet-e-ssh>)
- **Curso** Formação Redes de Computadores  
(<https://cursos.alura.com.br/formacao-redes>)

## HTTP - Fundamentos:

- HTTP significa Hyper Text Transfer Protocol. A comunicação entre computadores cliente e servidores web é feita enviando solicitações HTTP e recebendo respostas HTTP.
- Entender a diferença dos verbos HTTP
- Testar os requests e ver os status codes no navegador
- Saber fazer uma requisição HTTP na linha de comando com WGET
- Baixar uma imagem com WGET
- Fazer um post

## Conteúdos

- **Site** MDN Web Docs: Uma visão geral do HTTP (<https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Overview>)
- **Site** MDN Web Docs: Métodos de requisição HTTP (<https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Methods>)
- **Site** HTTP Cats (<https://http.cat/>)
- **Site** HTTP Dogs (<https://http.dog/>)
- **YouTube** Fabiano Gabardo Lemos: Requisições HTTP - GET, POST, PUT, PATCH DELETE (<https://www.youtube.com/watch?v=kncOJZrnkTg>)
- **YouTube** Programador a Bordo: Protocolo HTTP e TCP/IP - Introdução (<https://www.youtube.com/watch?v=V4XZ81vRGtM>)

## Conteúdos Alura:

- **Artigo** HTTP: Desmistificando o protocolo da Web (<https://www.alura.com.br/artigos/desmistificando-o-protocolo-http-parte-1>)
- **Artigo** Métodos de requisição do HTTP (<https://www.alura.com.br/artigos/metodos-de-requisicao-do-http>)
- **Artigo** Qual é a diferença entre HTTP e HTTPS? (<https://www.alura.com.br/artigos/qual-e-diferenca-entre-http-e-https>)
- **Podcast** Hipsters.tech: HTTP/2: magia com o novo protocolo - Hipsters 13 (<https://www.alura.com.br/podcast/http-2-magia-com-o-novo-protocolo-hipsters-13-a573>)
- **Curso** Curso HTTP: Entendendo a web por baixo dos panos (<https://www.alura.com.br/curso-online-http-entendendo-web-por-baixo-dos-panos>)

## Cloud - Fundamentos:

- Cloud, ou computação em nuvem é a distribuição de serviços de computação pela Internet usando um modelo de preço pago conforme o uso. Uma nuvem é composta de vários recursos de computação, que abrangem desde os próprios computadores (ou instâncias, na terminologia

de nuvem) até redes, armazenamento, bancos de dados e o que estiver em torno deles. Ou seja, tudo o que normalmente é necessário para montar o equivalente a uma sala de servidores, ou mesmo um data center completo, estará pronto para ser utilizado, configurado e executado.

- Conhecer a diferença entre IaaS, PaaS e SaaS
- Conhecer os maiores provedores de cloud
- Especializar-se em algum provedor

## Conteúdos

- **Artigo** Computação em nuvem (<https://medium.com/sysadminas/computa%C3%A7%C3%A3o-em-nuvem-515930304cf9>)
- **Artigo** O que é cloud? (<https://gabriel-faraday.medium.com/o-que-%C3%A9-cloud-991109e708c6>)
- **YouTube** Gabs Ferreira: Por que investir e estudar cloud? (<https://www.youtube.com/watch?v=Z45BTNeZ1I0>)
- **YouTube** Andre Iacono: O que é MICROSOFT AZURE? Qual Certificação começar em 2022? (<https://www.youtube.com/watch?v=f-oVzkvMwnE>)
- **YouTube** AWS: O que é a AWS? (<https://www.youtube.com/watch?v=8JI9wQ8sUdQ>)
- **YouTube** O que é Google Cloud e por que aprender? (<https://www.youtube.com/shorts/Lzq3f1DHWcl>)
- **Artigo** AWS vs Google Cloud vs Azure: o que cada um tem de melhor? (<https://medium.com/data-hackers/aws-vs-google-cloud-vs-azure-o-que-cada-um-tem-de-melhor-52107174f7b7>)
- **YouTube** Código Fonte TV: Azure (A plataforma Cloud da Microsoft) (<https://www.youtube.com/watch?v=YgE-sZaCuJ0>)
- **YouTube** Mundo da Cloud: AWS do Zero ao Expert (<https://www.youtube.com/watch?v=HiBCv9DolxI&list=PLtL97Owd1gkQ0dfqGW8OtJ-155Gs67Ecz>)

## Conteúdos Alura:

- **Podcast** Hipsters.tech: TechGuide - Fundamentos Cloud – Hipsters Ponto Tech #348 (<https://www.hipsters.tech/techguide-fundamentos-cloud-hipsters-ponto-tech-348/>)
- **Artigo** Cloud: o que é, História e Guia da computação em nuvem (<https://www.alura.com.br/artigos/cloud>)
- **Podcast** Hipsters.tech: Uma jornada Para o Cloud - Hipsters Deep Dive 005 (<https://www.alura.com.br/podcast/uma-jornada-para-o-cloud-hipsters-deep-dive-005-a1100>)
- **Podcast** Hipsters.tech: Histórias do Cloud - Hipsters 04 (<https://www.alura.com.br/podcast/historias-do-cloud-hipsters-04-a582>)
- **Artigo** Heroku, Vercel e outras opções de cloud como plataforma (<https://www.alura.com.br/artigos/heroku-vercel-outras-opcoes-cloud-plataforma>)
- **Artigo** AWS: Guia sobre o que é Amazon Web Services, seus Serviços e Certificações (<https://www.alura.com.br/artigos/aws>)
- **Artigo** Terraform: criando máquinas na Azure (<https://www.alura.com.br/artigos/terraform-maquinas-na-azure>)
- **YouTube** Alura: O que é cloud? (<https://www.YOUTUBE.com/watch?v=wev9fMrg-TU>)
- **YouTube** Alura: AWS, Google Cloud e Azure: Por onde começar? | Hipsters.Talks (<https://www.YOUTUBE.com/watch?v=z9k6rsdmWc0&t=300s>)
- **YouTube** Alura: Certificação em Cloud: Azure, AWS, Google | Hipsters.Talks ([https://www.YOUTUBE.com/watch?v=W4K82n\\_WK5g&t=290s](https://www.YOUTUBE.com/watch?v=W4K82n_WK5g&t=290s))
- **Curso** Formação Começando em Cloud Computing (<https://cursos.alura.com.br/formacao-cloud-computing>)
- **Curso** Formação Amazon Web Services (<https://cursos.alura.com.br/formacao-amazon-web-services>)
- **Curso** Formação Google Certified Associate Cloud Engineer (<https://cursos.alura.com.br/formacao-google-certified-associate-cloud->

[engineer\)](#)

- **Curso** Formação Certificação AWS Certified Cloud Practitioner (<https://cursos.alura.com.br/formacao-aws-certified-cloud-practitioner>)
- **Curso** Formação Containers com AWS ECS e EKS (<https://cursos.alura.com.br/formacao-containers-aws>)
- **Curso** Formação Google Cloud Platform (<https://cursos.alura.com.br/formacao-google-cloud>)
- **Curso** Formação Certificação Google Certified Associate Cloud Engineer (<https://cursos.alura.com.br/formacao-google-certified-associate-cloud-engineer>)
- **Curso** Formação Azure (<https://cursos.alura.com.br/formacao-conhecendo-azure>)
- **Curso** Formação Certificação AZ-900: Microsoft Azure Fundamentals (<https://cursos.alura.com.br/formacao-certificacao-az-900-microsoft-azure-fundamentals>)

## Linux - Fundamentos:

- Linux é um termo popularmente empregado para se referir a sistemas operacionais que utilizam o Kernel Linux. As distribuições incluem o Kernel Linux, além de softwares de sistema e bibliotecas.
- Conhecer o sistema de diretórios do Linux
- Compactar e descompactar arquivos
- Editar arquivos no console com o VI
- Gerenciar os processos rodando na máquina
- Conhecer as variáveis de ambiente e o PATH
- Gerenciar pacotes
- Realizar comunicação remota com o SSH e SCP

## Conteúdos

- **Artigo** Comandos linux (<https://pllara.medium.com/comandos-linux-4db7307c17b7>)

- **Artigo** Comandos básicos no Linux (<https://medium.com/linkapi-solutions/comandos-b%C3%A1sicos-no-linux-95079363ab0e>)
- **YouTube** Ninja do Linux: Comandos básicos da linha de comando do Linux ([https://www.youtube.com/watch?v=rs\\_yshFGu8E](https://www.youtube.com/watch?v=rs_yshFGu8E))
- **Curso** MIT - The Missing Semester of Your CS Education (inglês) (<https://missing.csail.mit.edu/>)

### Conteúdos Alura:

- **Artigo** Linux: download, instalação, distribuições e principais comandos (<https://www.alura.com.br/artigos/linux-download-instalacao-distribuicoes-e-principais-comandos>)
- **Artigo** Procurando arquivos no Linux (<https://www.alura.com.br/artigos/procurando-arquivos-no-linux>)
- **Artigo** Criando comandos no Linux com Bash (<https://www.alura.com.br/artigos/criando-comandos-no-linux-com-bash>)
- **Artigo** Linux - Visualizando tamanhos de Diretórios (<https://www.alura.com.br/artigos/como-visualizar-o-tamanho-de-diretorios-no-linux>)
- **Artigo** Entendendo as permissões no Linux (<https://www.alura.com.br/artigos/entendendo-as-permissoes-no-linux>)
- **Artigo** Linux: compactando e descompactando arquivos com o tar (<https://www.alura.com.br/artigos/linux-compactando-e-descompactando-arquivos-com-o-tar>)
- **Artigo** SSH: o acesso remoto aos servidores (<https://www.alura.com.br/artigos/como-acessar-servidores-remotamente-com-ssh>)
- **Curso** Linux Onboarding: usando a CLI de uma forma rápida e prática (<https://cursos.alura.com.br/course/linux-onboarding-utilizar-cli-forma-rapida-pratica>)
- **Curso** Linux Onboarding: localizando arquivos e conteúdos (<https://cursos.alura.com.br/course/linux-onboarding-arquivos-conteudos>)

- **Curso** Linux Onboarding: obtendo e tratando informações do sistema (<https://cursos.alura.com.br/course/linux-onboarding-informacoes-sistema>)
- **Curso** Linux Onboarding: trabalhe com usuários, permissões e dispositivos (<https://cursos.alura.com.br/course/linux-onboarding-usuarios-permissoes-dispositivos>)
- **Curso** DevOps: explorando conceitos, comandos e scripts no Linux CLI (<https://www.alura.com.br/curso-online-devops-conceitos-comandos-scripts-linux-cli>)

## Habilidade Auxiliar: Segurança da Informação

### Gestão de risco, ameaças e vulnerabilidades:

- Gerenciar riscos é o processo de planejar, organizar e controlar recursos e pessoas para minimizar danos ou fazer com que os riscos virem oportunidades. Prever os riscos é uma prática importante, afinal, dessa forma é possível reverter o que pode dar errado e alcançar resultados positivos ao longo do processo.

### Conteúdos

- **Site** ISO 27001 (<https://www.27001.pt/index.html>)
- **Site** CVSS (<https://nvd.nist.gov/vuln-metrics/cvss>)
- **Artigo** Gestão de vulnerabilidades como estratégia de negócios (<https://phbols.medium.com/voc%C3%AA-conhece-esses-perigos-3b6758997ae3>)
- **Site** O que é gerenciamento de vulnerabilidades? (<https://www.ibm.com/br-pt/topics/vulnerability-management>)
- **Site** Common Vulnerability Scoring System (<https://www.first.org/cvss/user-guide>)
- **YouTube** Gestão de risco e vulnerabilidade (<https://www.youtube.com/watch?v=k2uMAQh1AaE>)
- **YouTube** Ameaças, Vulnerabilidades e Riscos (<https://www.youtube.com/watch?v=AWUhXq4FDNo>)



- **YouTube** Gestão de Vulnerabilidades com Base em Risco  
(<https://www.youtube.com/watch?v=J23tKyQuoTQ>)
- **YouTube** Riscos, Ameaças e Vulnerabilidades em Segurança da Informação  
([https://www.youtube.com/watch?v=zD3M\\_EqkVFg](https://www.youtube.com/watch?v=zD3M_EqkVFg))

## Confidencialidade, Integridade e Disponibilidade:

- Os 3 princípios fundamentais da segurança da informação. Qualquer bom programa de gerenciamento de segurança da informação deve ser projetado para alcançar os três princípios de segurança da informação são comumente conhecidos como CIA (em inglês, a sigla CIA significa "Confidentiality", "Integrity" e "Availability", o que corresponde à sigla CID em português — Confidencialidade, Integridade e Disponibilidade).

## Conteúdos

- **Artigo** Um guia sobre normas de segurança da informação  
(<https://medium.com/sysadminas/um-guia-sobre-normas-de-seguran%C3%A7a-da-informa%C3%A7%C3%A3o-500400d349ee>)
- **Artigo** Segurança da Informação  
(<https://medium.com/sysadminas/seguran%C3%A7a-c65dd9f825c0>)
- **Artigo** O que é segurança da informação? (<https://medium.com/crypt0-women/o-que-%C3%A9-seguran%C3%A7a-da-informa%C3%A7%C3%A3o-9185d18dcd9f>)
- **Artigo** Confiabilidade nos Aspectos da Segurança da Informação  
(<https://medium.com/@fertorresfs/confiabilidade-nos-aspectos-da-seguran%C3%A7a-da-informa%C3%A7%C3%A3o-99359a01abee>)
- **Artigo** Segurança da Informação, uma abordagem básica porém necessária  
(<https://medium.com/eusouelliot/seguran%C3%A7a-da-informa%C3%A7%C3%A3o-uma-abordagem-b%C3%A1sica-por%C3%A9m-necess%C3%A1ria-9b37c716aad9>)
- **YouTube** ISO 27002 | Uma visão geral no contexto da LGPD  
(<https://www.youtube.com/watch?v=Gp8WjPv0kj8>)
- **YouTube** Segurança da Informação - ISO 27002 - Parte 1  
(<https://www.youtube.com/watch?v=8p9KBcuvwQI>)

- **YouTube** 5 PASSOS PARA IMPLEMENTAR A ISO 27001  
(<https://www.youtube.com/watch?v=P1Oi-gBuMmo>)

## Gerenciamento de identidade e acesso (IAM):

- Gestão de identidades, também conhecida como gestão de identidades e acessos (GIA) ou pelo seu termo em inglês, identity and access management (IAM) está entre as disciplinas de segurança da informação que habilita os indivíduos corretos à acessar os recursos corretos no momento correto e pelos motivos corretos.

## Conteúdos

- **Artigo** What is Identity and Access Management  
(<https://medium.com/identity-beyond-borders/identity-and-access-management-10166c309f11>)
- **Artigo** Introduction to Identity and Access Management  
(<https://medium.com/identity-beyond-borders/introduction-to-identity-and-access-management-2f3b80862647>)
- **Artigo** What is IAM? (<https://bojithapiyathilake.medium.com/identity-and-access-management-components-c501d786db4c>)
- **Artigo** What is IAM as a service (<https://medium.com/hypto/identity-and-access-management-iam-e04d2354a57>)
- **Artigo** Open-source Identity and Access Management System  
(<https://medium.com/@devops.ent/top-identity-and-access-management-systems-iam-open-source-enterprise-92cf66560a55>)
- **YouTube** IBM Technology: Identity & Access Management (IAM)  
([https://www.youtube.com/watch?v=aNj36g7fSsU&ab\\_channel=IBMTechology](https://www.youtube.com/watch?v=aNj36g7fSsU&ab_channel=IBMTechology))
- **YouTube** VMware End-User Computing: Identity and Access Management - Technical Overview ([https://www.youtube.com/watch?v=Tcvsefz5DmA&ab\\_channel=VMwareEnd-UserComputing](https://www.youtube.com/watch?v=Tcvsefz5DmA&ab_channel=VMwareEnd-UserComputing))

## Conteúdos Alura:

- **Artigo** O que é gerenciamento de identidade e acesso (IAM)?  
(<https://www.alura.com.br/artigos/gerenciamento-identidade-acesso-iam>)

## Conscientização de Segurança:

- À medida que os ataques cibernéticos se tornam mais prevalentes e sofisticados, as empresas devem confiar mais em seus funcionários para garantir que eles não coloquem os dados em risco ou sejam vítimas de ransomware. Mas os funcionários estão mais ocupados do que nunca. E, criar uma cultura de cibersegurança no trabalho torna-se mais importante e mais desafiador quando os funcionários trabalham em casa.

## Conteúdos

- **Artigo** A mudança de cultura com a conscientização de segurança da informação (<https://medium.com/@rogosantos/a-mudan%C3%A7a-de-cultura-com-a-conscientiza%C3%A7%C3%A3o-de-seguran%C3%A7a-da-informa%C3%A7%C3%A3o-b6f701f0f6f4>)
- **Artigo** Segurança da informação: focando no fator humano (<https://medium.com/@boschtechbr/seguran%C3%A7a-da-informa%C3%A7%C3%A3o-focando-no-fator-humano-e67fe163c341>)
- **Artigo** A importância de conscientizar (<https://medium.com/@rogosantos/a-import%C3%A2ncia-de-conscientizar-funcion%C3%A1rios-sobre-ciberseguran%C3%A7a-desde-o-primeiro-dia-83efcadd8ec9>)
- **YouTube** Métricas para programas de conscientização em segurança da informação (<https://www.youtube.com/watch?v=vkBxVu7k7Q8>)
- **YouTube** Conscientização de usuários em segurança da informação (<https://www.youtube.com/watch?v=vkBxVu7k7Q8>)
- **YouTube** 7 ações que, isoladas, não são um programa de conscientização em SI ([https://www.youtube.com/watch?v=96mC\\_EJN0jg](https://www.youtube.com/watch?v=96mC_EJN0jg))
- **YouTube** Política de Segurança da Informação (<https://www.youtube.com/watch?v=nQ2ptWBr-Rw>)

## Proteção de dados:

- A proteção de dados é o processo de proteger informações importantes de forma que garanta a confidencialidade, integridade e a disponibilidade destes dados.

## Conteúdos

- **YouTube** ENTENDA O QUE É LGPD (<https://www.youtube.com/watch?v=dPipsp5arAc>)
- **YouTube** Tudo que você precisa saber sobre a LGPD (<https://www.youtube.com/watch?v=hu6Xlc7QVnE>)
- **YouTube** O que você precisa saber sobre o GDPR (<https://www.youtube.com/watch?v=egGvTgk3HH8>)
- **YouTube** DLP – Data Loss Prevention (<https://www.youtube.com/watch?v=VHeX3D2WOUc>)
- **Artigo** Como estudei para certificação Privacy and Data Protection Foundation (PDPF) (<https://caiovicentinni.medium.com/como-estudei-para-certifica%C3%A7%C3%A3o-privacy-and-data-protection-foundation-pdpf-81a824aa9f5e>)
- **Artigo** Com a Lei em vigor, quais as diferenças entre a LGPD e GDPR? (<https://medium.com/@rogosantos/com-a-lei-em-vigor-quais-as-diferen%C3%A7as-entre-a-lgpd-e-gdpr-8e6d008c898d>)
- **Artigo** Como a LGPD pode impactar na Experiência do Usuário (UX) (<https://brasil.uxdesign.cc/como-a-lei-geral-de-prote%C3%A7%C3%A3o-de-dados-pode-afetar-a-experi%C3%Aancia-do-usu%C3%A1rio-e514270bf59c>)

## Segurança em autenticação e senhas:

- Uma senha forte faz toda diferença quando o assunto é proteção de dados. Afinal, ela é construída de maneira a dificultar e muito que seja quebrada por um hacker ou ataque de massa. A senha, você sabe, é um mecanismo que permite o acesso de uma pessoa a um determinado serviço.

## Conteúdos

- **Site** How Secure is Your Password? (<https://www.passwordmonster.com/>)
- **Artigo** Como criar senhas realmente seguras (<https://medium.com/the-autistic-nikkei/como-criar-senhas-realmente-seguras-d39b4442db1c>)
- **Artigo** Password Security: THM Writeup (<https://medium.com/bug-bounty-hunting/password-security-thm-writeup-cc9088207af3>)
- **Artigo** What Is a Secure Password? (<https://medium.com/geekculture/what-is-a-secure-password-97263aeedea9>)
- **YouTube** Bit Oxygen: Authentication in Computer Security (<https://www.youtube.com/watch?v=7oTkgG1v-rU>)
- **YouTube** Linus Tech Tips: Password Security Best Practices (<https://www.youtube.com/watch?v=t8SQo3R7qeU>)

---

TechGuide - Alura  
Alura, PM3 e FIAP  
O Techguide.sh é um projeto open source