

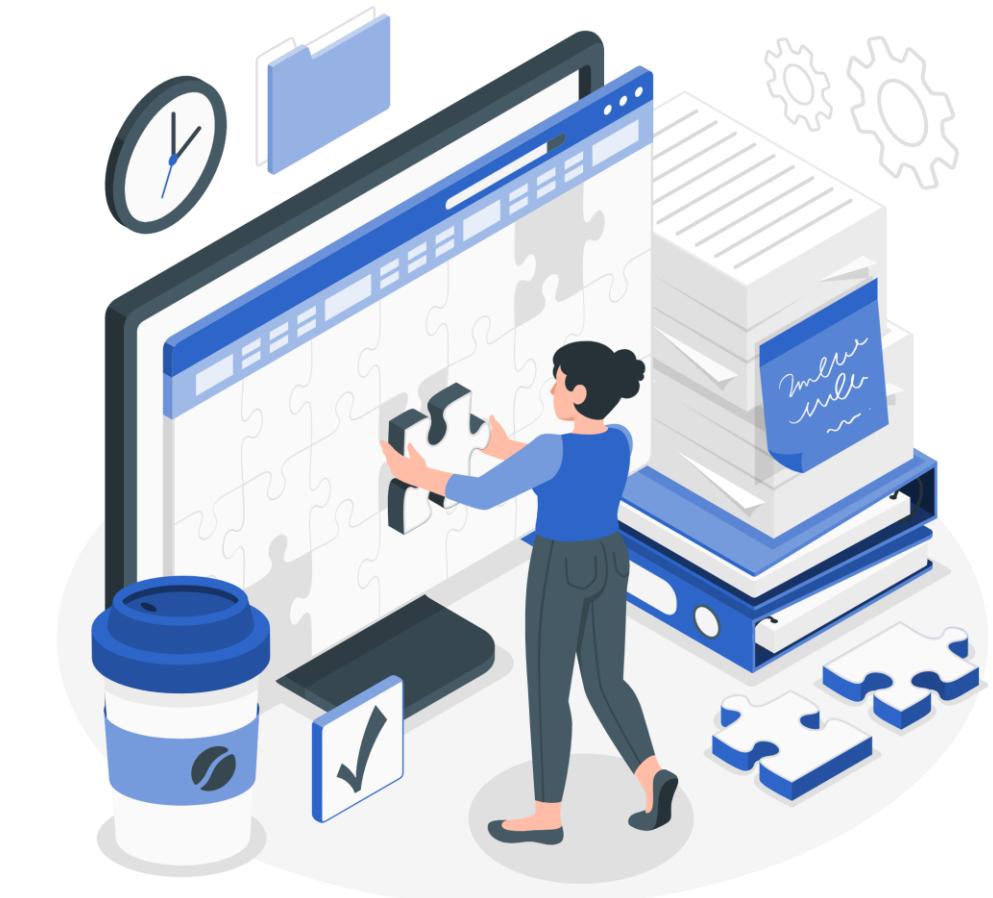
# Segurança da empresa ao software

Será que eu tranquei a porta?



# Agenda

Por onde começar  
Análise de ameaças e risco  
Segurança de ativos  
Segurança de pessoas



# Quem somos



*Daniel Paiva Fernandes*

Formado em Direito pela FDSM (2004) e em Sistemas de Informação pela UNIFEI (2017) com graduação-sanduíche em Stockton University – EUA (2016), é aluno de Mestrado em Computação Aplicada (UNIFEI) e atualmente trabalha no Inatel Competence Center no projeto P&D de BSS da Ericsson, onde atua como Test Lead e Security Master.

[in/paivafernandes](#)



*Frederico Augusto Laranjo Silva*  
Formado em Sistemas de Informação pela FAI (2013), Pós-graduado em Desenvolvimento de Aplicações para Dispositivos Móveis e Cloud Computing pelo Inatel (2018), atualmente trabalha no Inatel Competence Center no projeto P&D de BSS da Ericsson, onde atua como Product Owner e Team Leader.

[in/fredllaranjo](#) A circular portrait of a man with dark hair, a beard, and glasses, wearing a blue shirt. He is looking directly at the camera.

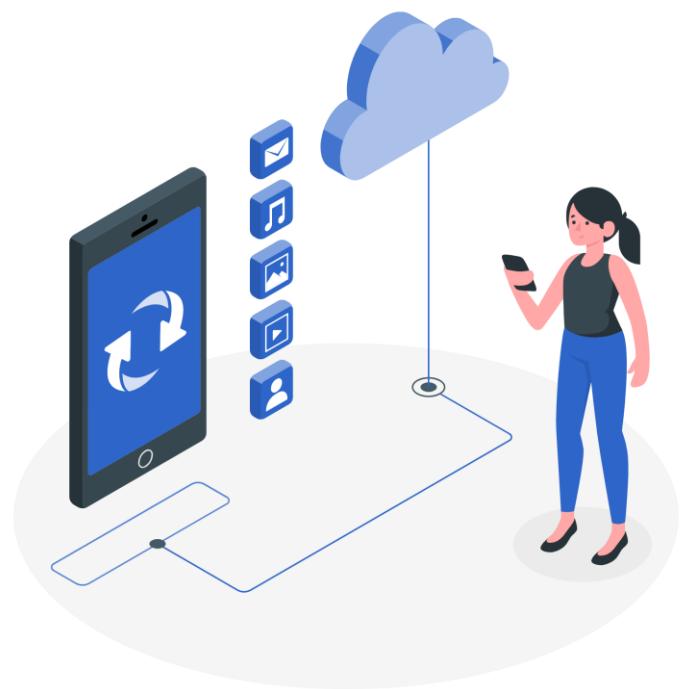
# Uma breve introdução

# Qual cenário nos encontramos



+ 300% crimes  
cibernéticos  
(FBI)

+ 630% ataques em  
serviços cloud  
(FinTech News)

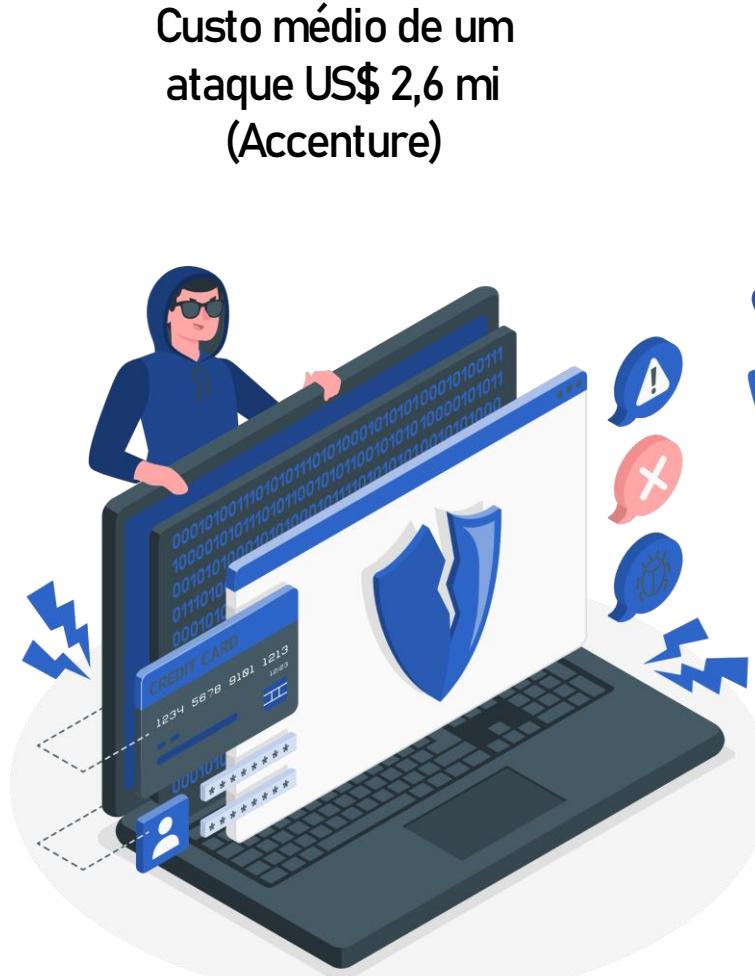


Trabalho remoto =  
falha de segurança  
em 20% das  
empresas  
(MalwareBytes)

# Qual cenário nos encontramos



Mercado de  
US\$ 170,4 bi  
até 2022  
(Gartner)



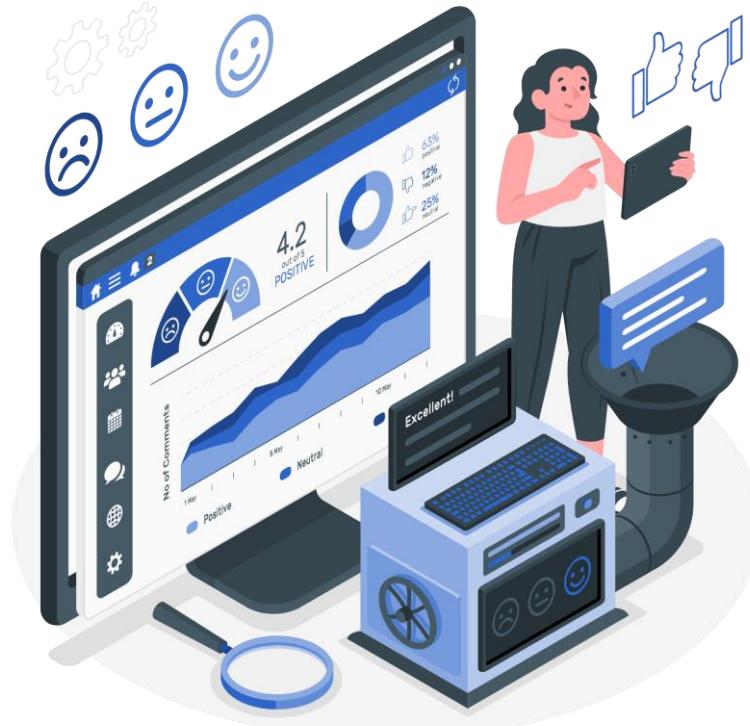
Custo médio de um  
ataque US\$ 2,6 mi  
(Accenture)



Ransomware + de  
US\$ 20bi em 2021  
com 1 ataque a cada  
11 segundos

# Sobre o retorno de investimento

A credibilidade de qualquer empresa está em jogo quando há violação de segurança



Uma empresa sem equipe preparada arca com US\$ 5,29 milhões em custos, contra US\$ 2 milhões quando as empresas estão preparadas (IBM)

# LGPD e GDPR - Fique de olho



No primeiro ano a GDPR entrou em vigor, o valor total de multas foi de U\$63 milhões

...e você, deixou sua porta aberta?



# 01

## Por onde começar?

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

Descrição

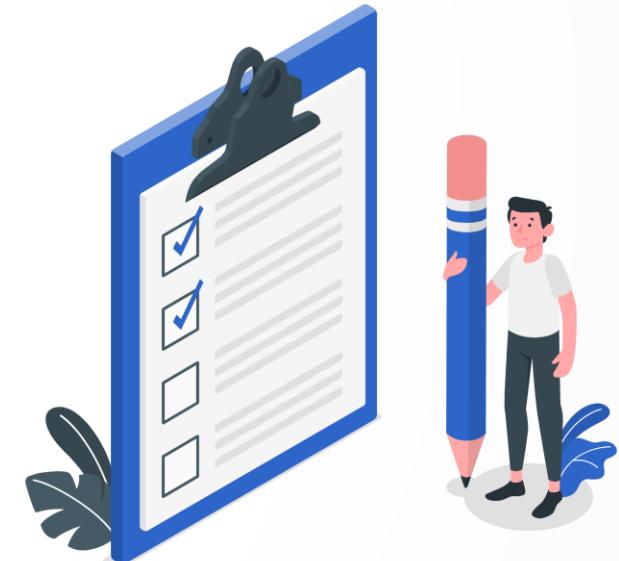
Qual estado a empresa se encontra?

Estabelecimento de Governança e Políticas de Segurança

# Qual estado a empresa se encontra?

Fazer um diagnóstico de sua empresa:

1. Qual é o tamanho da organização?
2. Quais os ativos que devem ser protegidos?
3. Quantos projetos existem?
4. Nossos projetos trabalham com informações que extrapolam o campo da segurança e também envolvem a gestão de dados privados?
5. Existe planos de expansão de projetos ou de ativos?
6. Quais são as políticas e estratégias existentes para garantir segurança e privacidade?



Por onde começar?

Análise de ameaças e risco

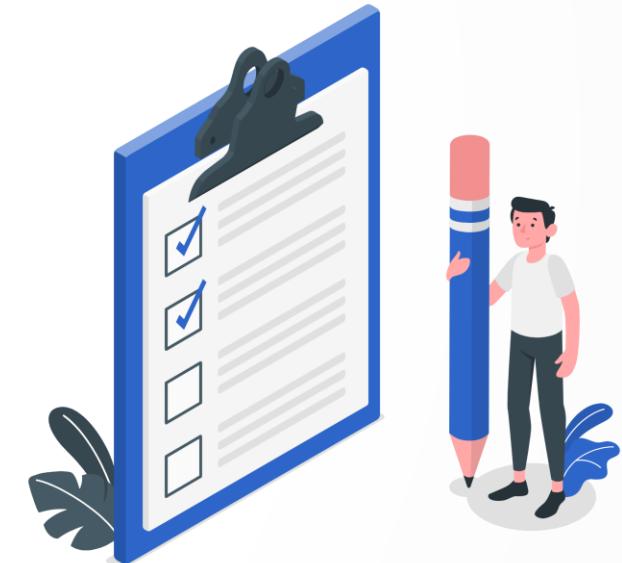
Segurança de ativos

Segurança de pessoas

# Qual estado a empresa se encontra?

Um modelo de maturidade tem 2 componentes:

- i) o meio de medir e descrever o desenvolvimento de um objeto, mostrando a progressão hierárquica;
- ii) os critérios para medir os processos



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Qual estado a empresa se encontra?

Por onde começar?  
Análise de ameaças e risco  
Segurança de ativos  
Segurança de pessoas

Microsoft Security Assessment Tool (MSAT 4.0)

**Perfil de risco da empresa (PRE):** Medição dos riscos a que uma organização está exposta, com base no ambiente do negócio e no setor em que ela compete.

**Índice de defesa em profundidade (IDP):** Medida das defesas de segurança usadas por pessoas, processos e tecnologias para ajudar a atenuar os riscos identificados para uma empresa.



# Qual estado a empresa se encontra?

The screenshot shows the Microsoft Security Assessment Tool (SAT) interface. The title bar reads "Microsoft® Security Assessment Tool". The left sidebar menu lists several categories: Infra-estrutura, Aplicativos, Operações, and Pessoal. Under "Infra-estrutura", there are four items: Defesa do perímetro, Autenticação, Gerenciamento e monitoramento, and Implantação e uso. The main content area is titled "Infra-estrutura" and contains a detailed description of the section's focus on network operations and security. A "Avançar >" button is located in the bottom right corner of the main content area.

Microsoft® Security Assessment Tool

SAT ▶ Avaliação modelo ▶

- Infra-estrutura
  - Defesa do perímetro
  - Autenticação
  - Gerenciamento e monitoramento
  - Implantação e uso
  - Projeto de aplicativos
  - Armazenamento de dados e comunicações
- Operações
  - Ambiente
  - Política de segurança
  - Gerenciamento de patches e atualizações
  - Backup e restauração
- Pessoal
  - Requisitos e avaliações

**Infra-estrutura**

Esta seção se concentra no funcionamento correto da rede, quais os processos de negócios (internos ou externos) que deve suportar, como os hosts são instalados e implantados e como a rede será efetivamente gerenciada e mantida. Com o estabelecimento de um projeto sólido de infra-estrutura que seja compreendido e seguido, a organização pode identificar facilmente as áreas de risco e elaborar métodos para reduzir as ameaças. Você deve levar aproximadamente 10 minutos para preencher esta seção.

Avançar >

Envie-nos seus comentários.

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Qual estado a empresa se encontra?

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

The screenshot shows the Microsoft Security Assessment Tool (SAT) interface. The title bar reads "Microsoft® Security Assessment Tool". The left sidebar menu includes "SAT", "Avaliação modelo", and several sections: "Infra-estrutura" (checked), "Defesa do perímetro", "Autenticação", "Gerenciamento e monitoramento", "Aplicativos" (selected), "Operações", "Pessoal", and "Requisitos e avaliações". Under "Aplicativos", there are three items: "Implantação e uso", "Projeto de aplicativos", and "Armazenamento de dados e comunicações". The main content area is titled "Aplicativos" and contains the following text: "Esta seção trata dos aplicativos do seu ambiente que são críticos para os negócios e os avalia do ponto de vista da segurança e da disponibilidade. Esta seção examinará as tecnologias usadas no ambiente para aumentar a defesa em profundidade. Você levará aproximadamente 10 minutos para preencher esta seção." At the bottom right of the content area is a button labeled "Envie-nos seus comentários.". Navigation buttons "<> Voltar" and "Avançar >" are located at the bottom center.

# Qual estado a empresa se encontra?

The screenshot shows the Microsoft Security Assessment Tool (SAT) interface. The title bar reads "Microsoft® Security Assessment Tool". The left sidebar menu is titled "SAT > Avaliação modelo >" and lists three main categories: "Aplicativos" (with items "Implantação e uso", "Projeto de aplicativos", and "Armazenamento de dados e comunicações" marked with green checkmarks), "Operações" (with items "Ambiente", "Política de segurança", "Gerenciamento de patches e atualizações", and "Backup e restauração" marked with yellow warning icons), and "Pessoal" (with items "Requisitos e avaliações", "Política e procedimentos", and "Treinamento e conscientização" marked with yellow warning icons). The main content area is titled "Operações" and contains the following text: "Esta seção avalia as práticas, procedimentos e diretrizes operacionais que a organização segue para melhorar as estratégias de defesa em profundidade e incluir mais do que apenas tecnologias de defesa. Examina as áreas que controlam os builds (compilações) dos sistemas, a documentação de rede, backup e restauração no ambiente. Você deve levar aproximadamente 10 minutos para preencher esta seção." At the bottom right of the content area, there are "Voltar" (Back) and "Avançar >" (Next >) buttons. A small "Envie-nos seus comentários." (Send us your comments) button is located at the very bottom right.

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Qual estado a empresa se encontra?

Por onde começar?

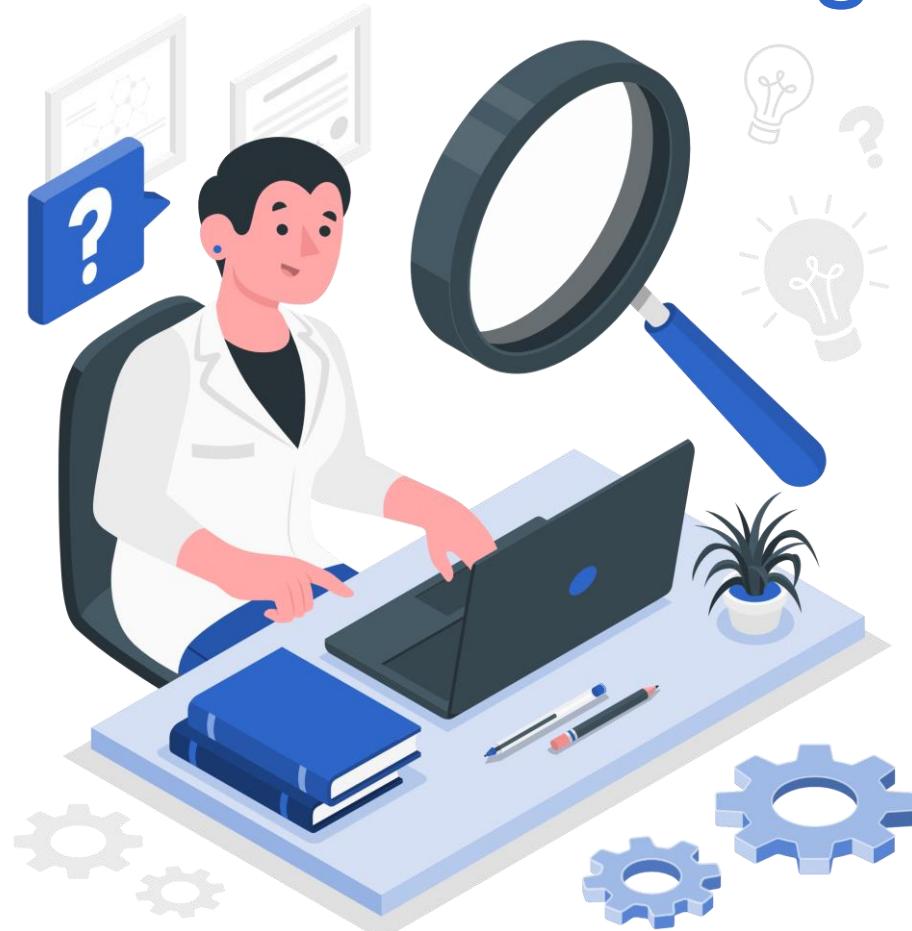
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

The screenshot shows the Microsoft Security Assessment Tool (SAT) interface. The title bar reads "Microsoft® Security Assessment Tool". The main navigation menu on the left shows "SAT > Avaliação modelo". The left sidebar contains a tree view with categories: "Aplicativos" (Applications) with "Implantação e uso", "Projeto de aplicativos", and "Armazenamento de dados e comunicações"; "Operações" (Operations) with "Ambiente", "Política de segurança", "Gerenciamento de patches e atualizações", and "Backup e restauração". A section titled "Pessoal" (Personal) is currently selected, indicated by a blue background. The content area for "Pessoal" includes the following text: "Esta seção examina os processos da empresa que controlam as políticas corporativas de segurança, os processos de RH e o treinamento e a conscientização de segurança dos funcionários. Também se concentra em lidar com a segurança na medida em que esta se relaciona com as operações do dia-a-dia. Esta seção ajuda a avaliar como são atenuados os riscos na área de pessoal. Você deve levar aproximadamente 10 minutos para preencher esta seção." Below this text are three warning icons: "Requisitos e avaliações", "Política e procedimentos", and "Treinamento e conscientização". At the bottom right of the content area is a "Envie-nos seus comentários." (Send us your comments) button. Navigation buttons "< Voltar" (Back) and "Avançar >" (Next) are located at the bottom of the sidebar.

# Estabelecimento de Governança e Políticas de Segurança



**Se tratando de incidentes, como a organização lida com incidentes no momento?**

- analisar casos reais, incidentes registrados pela organização,
- estender o campo de observação para empresas no mesmo ramo de mercado.

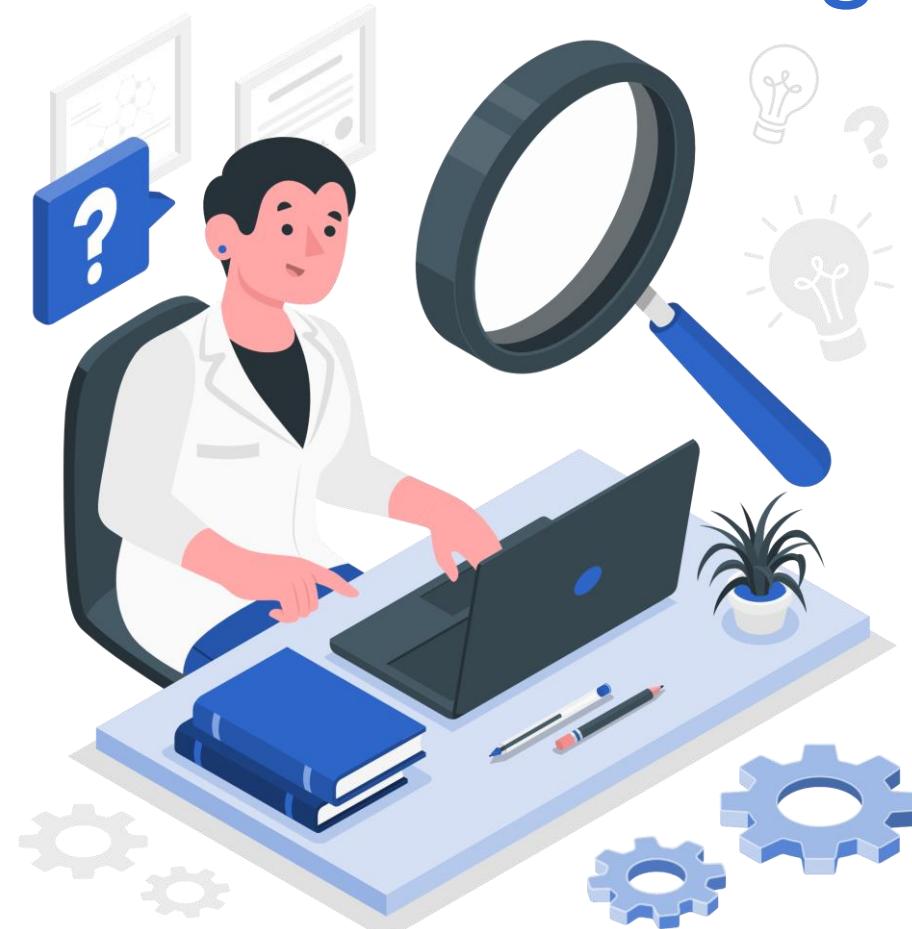
Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Estabelecimento de Governança e Políticas de Segurança



O seu plano de gestão seria capaz de mitigar os incidentes?

O que faltou para que o incidente recebesse o devido tratamento?

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Estabelecimento de Governança e Políticas de Segurança

Por onde começar?

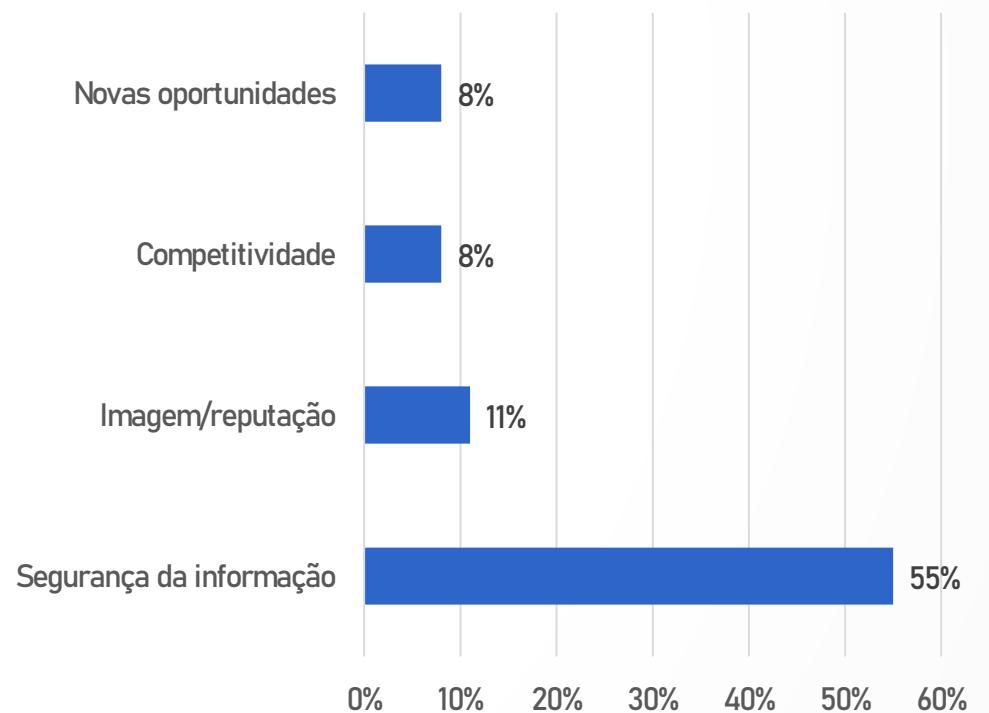
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas



Melhorias após adoção da ISO27001  
(Help Net Security, 2016)



# Estabelecimento de Governança e Políticas de Segurança

Por onde começar?  
Análise de ameaças e risco  
Segurança de ativos  
Segurança de pessoas

## Definição de requisitos de segurança

**Exemplo, RFC3871 define requisitos de seguranças operacional para infraestrutura de redes de ISP IP networks (roteadores e switches):**

### 2.2.4. Permitir a seleção de parâmetros criptográficos

#### Requisito.

O dispositivo DEVE permitir que o operador selecione parâmetros criptográficos. Isso deve incluir comprimentos-chave e algoritmos.

#### Justificativa.

A criptografia usando certos algoritmos e comprimentos-chave pode ser considerada "forte" em um ponto no tempo, mas "fraca" em outro.

O aumento constante do poder computacional reduz continuamente o tempo necessário para quebrar a criptografia de uma certa força.

Fraquezas podem ser descobertas em algoritmos. A capacidade de selecionar um algoritmo diferente é uma ferramenta útil para manter a segurança diante de tais descobertas.

#### Exemplos.

Des de 56 bits já foi considerado seguro. Em 1998 foi quebrado por uma máquina construída sob medida em menos de 3 dias. A capacidade de selecionar algoritmos e comprimentos-chave daria ao operador opções (diferentes algoritmos, chaves mais longas) em face de tais desenvolvimentos.

#### Avisos.

Nenhum

# Estabelecimento de Governança e Políticas de Segurança

## OWASP Proactive Controls – C1:

Quatro etapas para implementar requisites de segurança:

- Descoberta e Seleção
- Investigação e documentação
- Implementação
- Teste

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

02

# Análise de ameaças e risco

Descrição

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

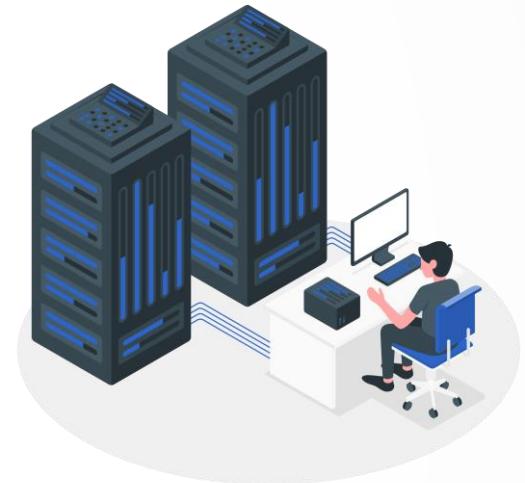
Definição de ativos e classificação de segurança

Data flow diagram

Classificação de ameaças com STRIDE

# Definição de ativos e classificação de segurança

Os ativos da empresa são tudo aquilo que pode estar sujeito a ameaças cuja perda da confidencialidade, integridade ou disponibilidade podem implicar em prejuízo.



**dispositivos físicos:** Roteadores, servidores, câmeras, equipamentos

**software:** Sistemas operacionais, firewall, máquinas virtuais

**serviços de rede:** VPN, protocolos wireless, redes óticas

Por onde começar?

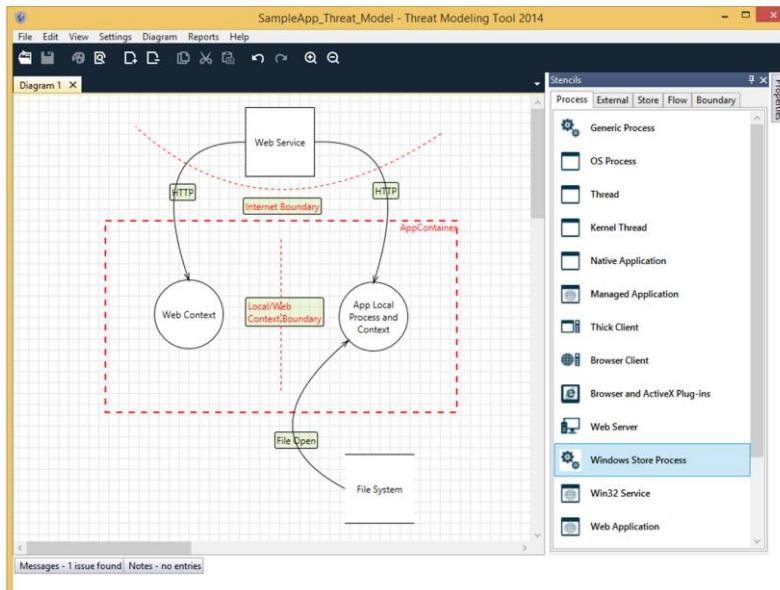
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

Por onde começar?  
Análise de ameaças e risco  
Segurança de ativos  
Segurança de pessoas

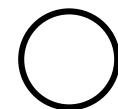
- O data flow diagram (DFD) deve:
- Complementar a compreensão da instituição sobre o fluxo de informações
- Identificar conjuntos de dados e subconjuntos compartilhados entre sistemas
- Identificar aplicativos compartilhando dados
- Destacar a classificação dos dados que estão sendo transmitidos



# Data flow diagram

Tem por objetivo capturar os principais componentes de um Sistema de Informações, como os dados se movem dentro do sistema, pontos de interação do usuário e os limites de confiança.

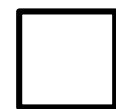
# Data flow diagram



**Processo:** atividades que podem modificar ou redirecionar a entrada recebida para suas saídas adequadas



data store: dados armazenados de forma temporária ou permanente.



**Entidade externa:** pode ser um processo, armazenamento de dados ou até mesmo um sistema completo fora do seu controle direto.



**Fluxo de dados:** A movimentação de dados entre a fonte de dados e o destino.



**Limites de confiança:** são usados para descrever o fluxo de dados à medida que cruza diferentes níveis de zona de confiança.

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Classificação de ameaças com STRIDE

**Spoofing:** ou falsificação, consiste em passar por alguém.

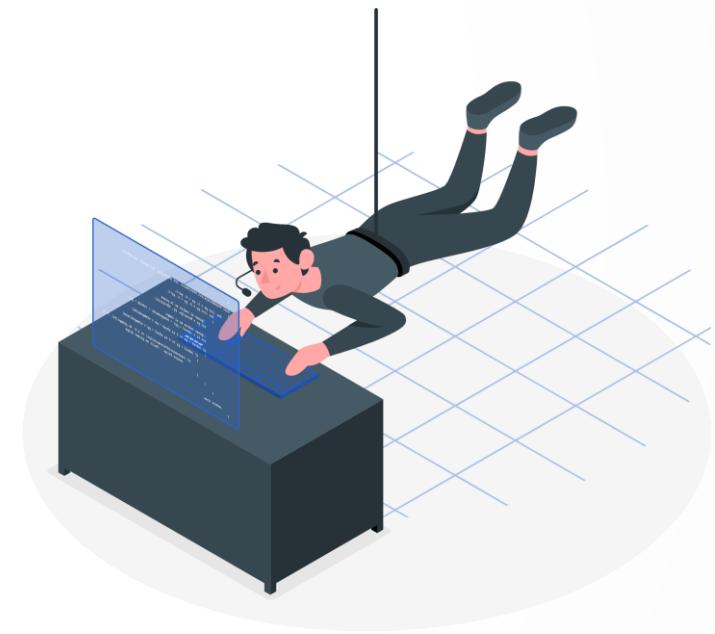
**Tampering:** ou adulteração de dados sem autorização.

**Repudiation:** evitar ser responsabilizado por uma ação.

**Information disclosure:** acessar dados sem permissão.

**Denial of service:** sobrecarregar o sistema para torná-lo indisponível.

**Elevation of privilege:** conseguir mais privilégios do que o devido no sistema.



Por onde começar?

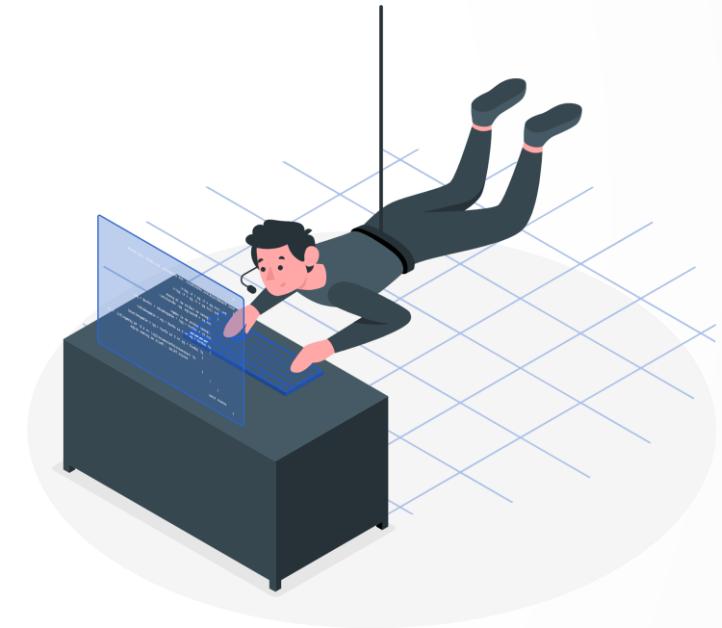
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Classificação de ameaças com STRIDE

Ameaça	CS	DFD
Spoofing	autenticação	Processo, entidade externa
Tampering	integridade	Processo, data store e fluxo de dados
Repudiation	Não-repúdio	Processo, entidade externa e data store
Information disclosure	Confidencialidade	Processo, data store e fluxo de dados
Denial of service	Disponibilidade	Processo, data store e fluxo de dados
Elevation of privilege	Autorização	Processo



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

Por onde começar?  
Análise de ameaças e risco  
Segurança de ativos  
Segurança de pessoas

Evento	Ação	Plano
Não cumprir obrigações de conformidade	EVITAR	Implementar processo formal de monitoramento de conformidade
Perda de Praticante	REDUZIR	Implementar plano de sucessão
Falha na coleta de recebíveis em tempo hábil	REDUZIR	Implementar o rastreamento de recebíveis e o processo de acompanhamento de devedores
	TRANSFERIR	

# Identificação e avaliação de riscos e planos de mitigação

Evitar

Reducir

Compartilhar ou Transferir

Aceitar

03

Por onde começar?  
Análise de ameaças e risco  
Segurança de ativos  
Segurança de pessoas

# Segurança de ativos

Hardening  
Infraestrutura  
Segurança em Cloud  
Segurança no ambiente de desenvolvimento

Descrição

# Hardening

Também conhecido por blindagem de sistemas, trata-se de técnicas para prover mais segurança em servidores e serviços, sejam esses externos (web) ou internos como bancos de dados, arquivos e outros ativos acessíveis através da rede.

Sair do "*default*"



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Hardening

**Segurança física**

**Sistemas Operacionais**

**Aplicações**

**Ferramentas de segurança**

**Redes e serviços**

**Auditoria e monitoramento de sistemas**

**Controle de acesso**

**Encriptação de dados**

**Correções e atualizações**

**Backup do sistema**

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Hardening

CIS® – Center for Internet Security, Inc.

CIS-CAT

CIS Hardened Images

The image shows a screenshot of the CIS (Center for Internet Security) website. It features two main sections: 'Secure Your Organization' and 'Secure Specific Platforms'. Under 'Secure Your Organization', there are links to 'CIS Controls®' (prioritized & simplified best practices), 'CIS RAM' (information security risk assessment method), and 'CIS Controls Community' (help develop and maintain the Controls). Under 'Secure Specific Platforms', there are links to 'CIS Benchmarks™' (100+ vendor-neutral configuration guides), 'CIS-CAT®' (assess system conformance to CIS Benchmarks), and 'CIS Benchmarks Community' (develop & update secure configuration guides). Additionally, there is a link to 'CIS Hardened Images®' (virtual images hardened to CIS Benchmarks).

Secure Your Organization	Secure Specific Platforms
<b>CIS Controls®</b> Prioritized & simplified best practices	<b>CIS Benchmarks™</b> 100+ vendor-neutral configuration guides
<b>CIS RAM</b> Information security risk assessment method	<b>CIS-CAT®</b> Assess system conformance to CIS Benchmarks
<b>CIS Controls Community</b> Help develop and maintain the Controls	<b>CIS Benchmarks Community</b> Develop & update secure configuration guides
	<b>CIS Hardened Images®</b> Virtual images hardened to CIS Benchmarks

# Hardening

**Itens no plano de segurança de informação:**

- Particionamento de discos
- Serviços desnecessários e inseguros
- Política de força e renovação de senhas
- Usuários inválidos
- Desconexão de usuários não autorizados
- GRUB (senha criptografada)

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Hardening

- Políticas de rede / utilização
- Gerenciamento de privilégios (root/admin)
- Segurança no Terminal (logout)
- SSH
- Portas abertas
- Permissões de execução

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Hardening

## Hardening - Artigo Revista Infra Magazine 1

<https://www.devmedia.com.br/hardening-artigo-revista-infra-magazine-1/20818>

## Security Hardening Standards: Why do you need one?

<https://www.packetlabs.net/security-hardening-standards/>

## The Center for Internet Security, Inc. (CIS®)

<https://www.cisecurity.org/about-us/>



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Infraestrutura

Cada camada a ser protegida é importante.

Identificação do valor do bem protegido e dos impactos diretos e indiretos no acesso indevido.

- Assim como casas tem portões, portas e ainda assim guardamos o que temos de valor dentro de cofres.



# Infraestrutura

A grande disponibilidade de ferramentas facilita o uso, mas antes um levantamento das vulnerabilidades e riscos precisa ser feito para identificar onde são necessárias.

Prevenção, combate e auditoria.

Oportunidade para prestadores de serviço

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Infraestrutura

Onde atuar:

- Backup
- Inventário
- Antivírus
- Monitoramento
- Firewall
- Navegação

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Infraestrutura

- Patch
- Wireless
- AD
- E-mail e SPAM
- Padronização SO
- Rede

Por onde começar?

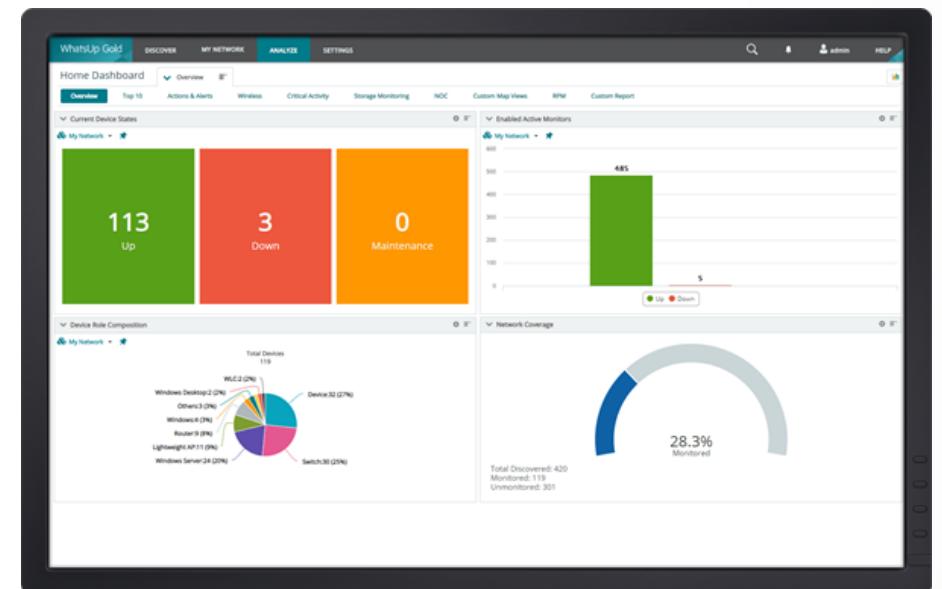
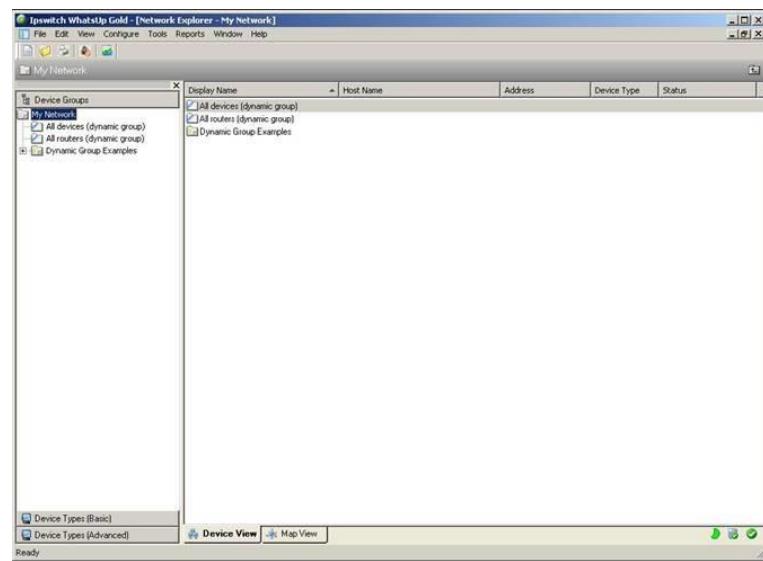
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Infraestrutura

## WhatsUp



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

Por onde começar?

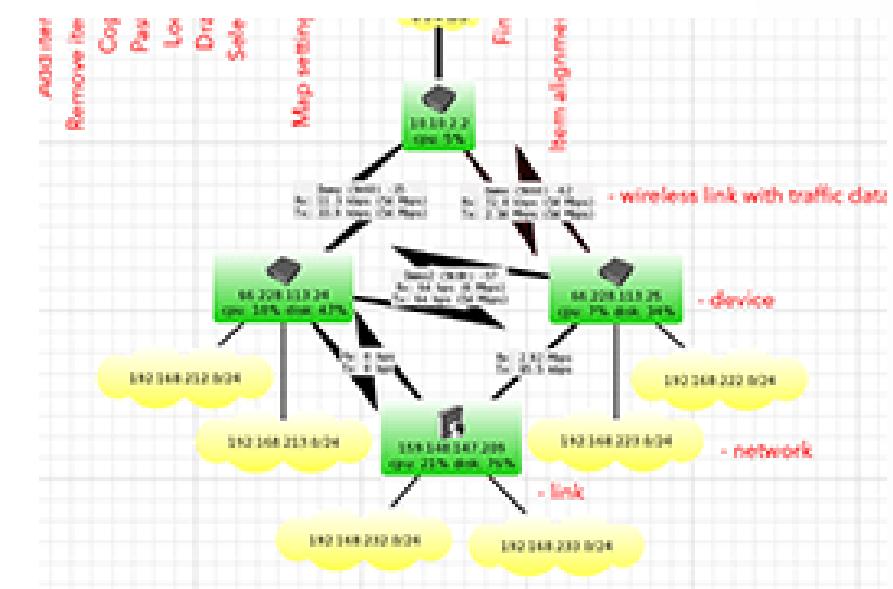
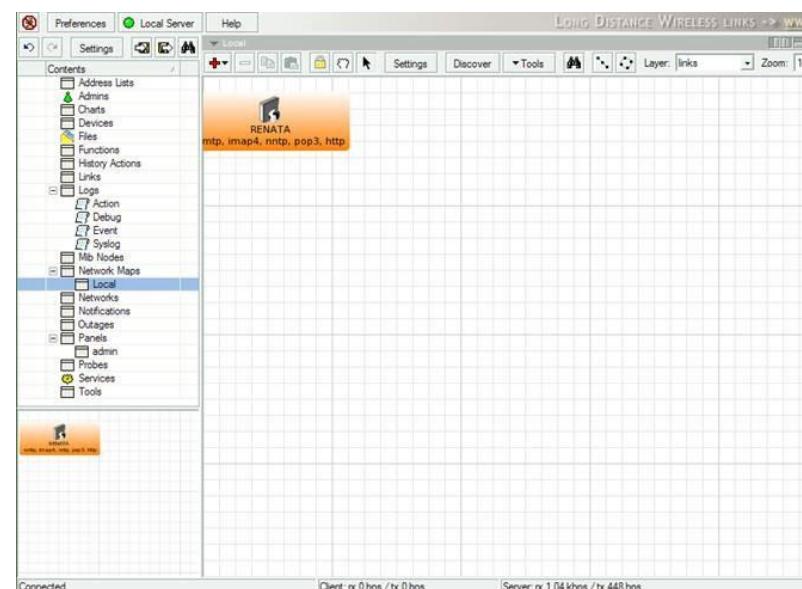
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Infraestrutura

## TheDude (Mikrotik)



Por onde começar?

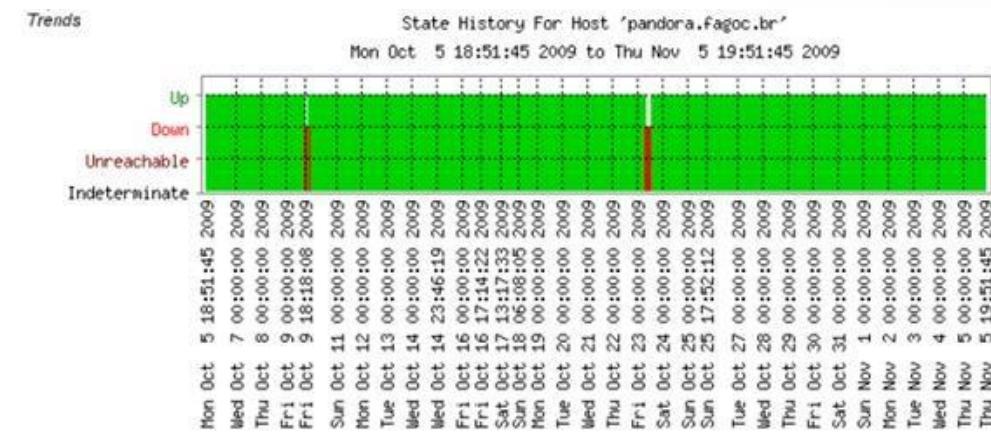
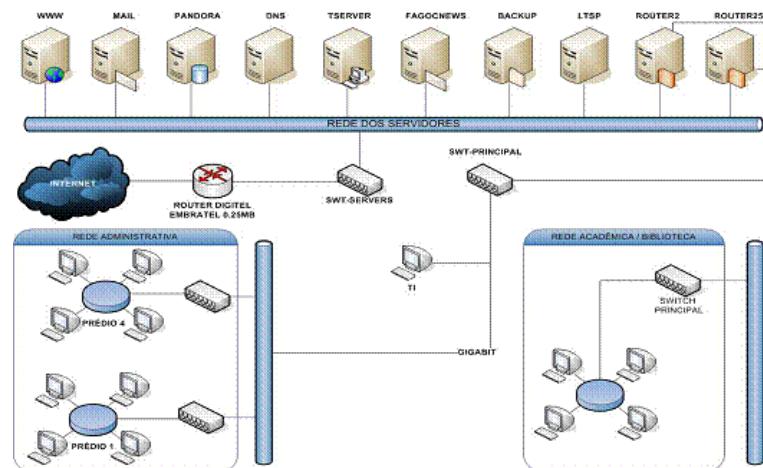
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Infraestrutura

## Nagios



### State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
HTTP	98.270% (98.270%)	0.000% (0.000%)	0.000% (0.000%)	1.730% (1.730%)	0.000%
MySQL	95.389% (95.389%)	0.000% (0.000%)	0.000% (0.000%)	4.611% (4.611%)	0.000%
PING	95.609% (95.609%)	0.503% (0.503%)	0.000% (0.000%)	3.889% (3.889%)	0.000%
Average	96.423% (96.423%)	0.168% (0.168%)	0.000% (0.000%)	3.410% (3.410%)	0.000%

Por onde começar?

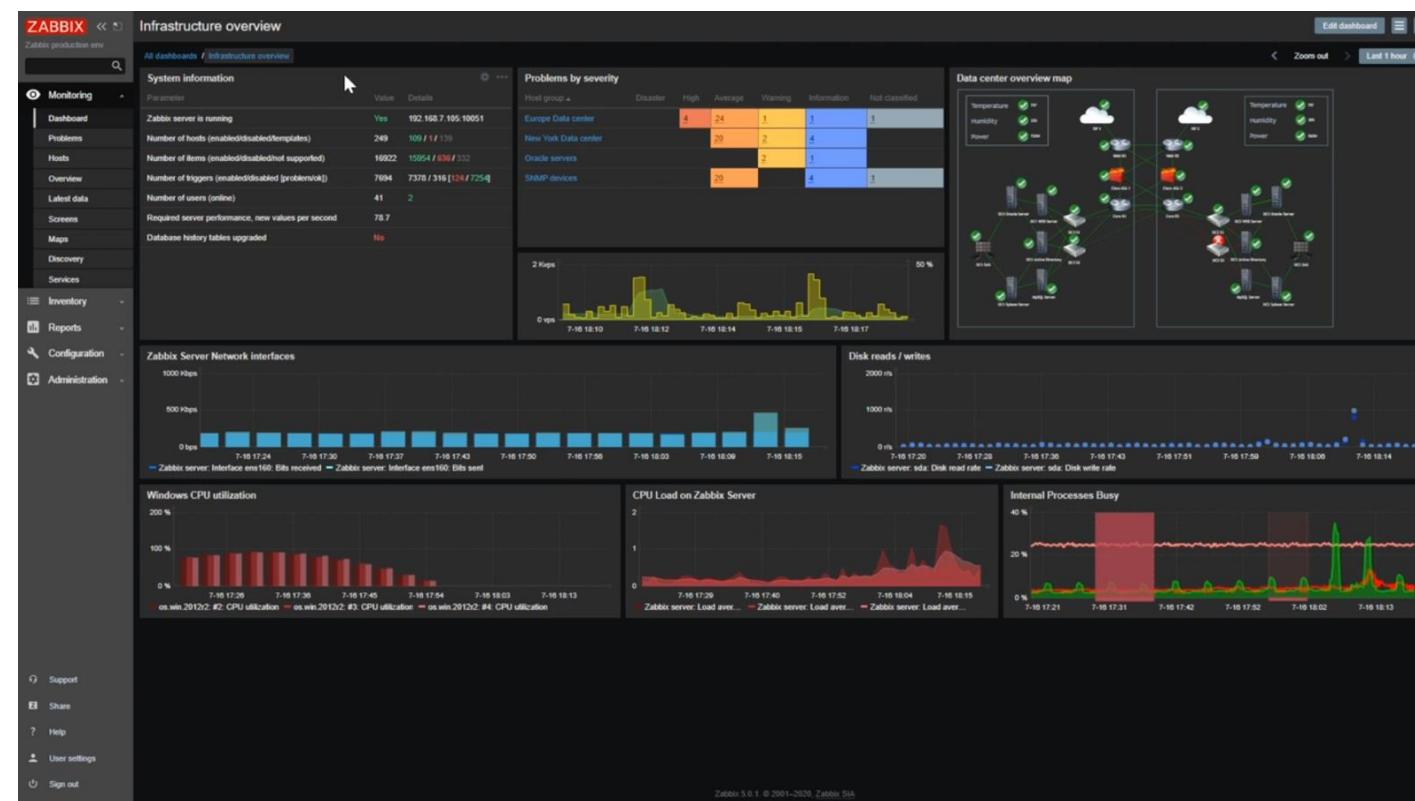
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Infraestrutura

## Zabbix (Open Source)



Por onde começar?

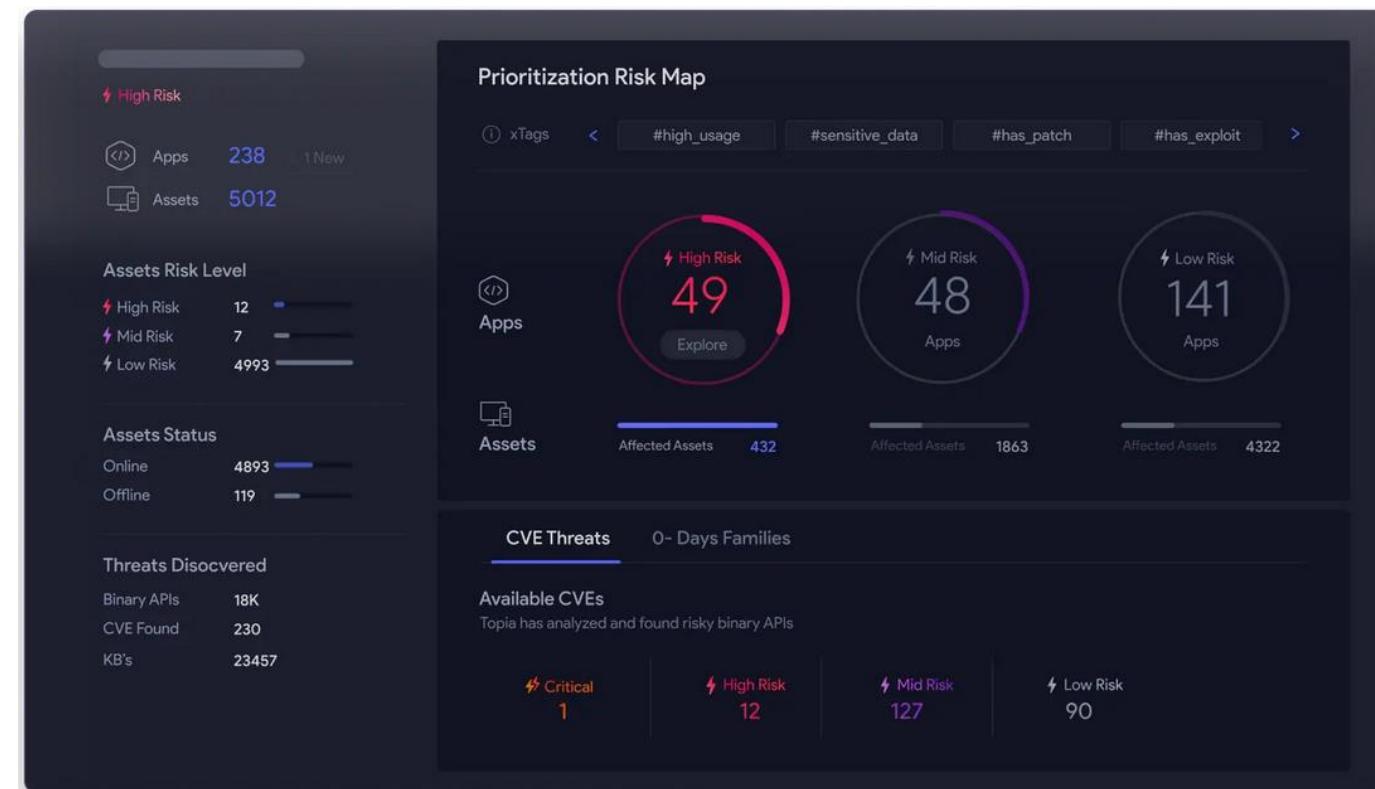
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Infraestrutura

Vicarius



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Infraestrutura

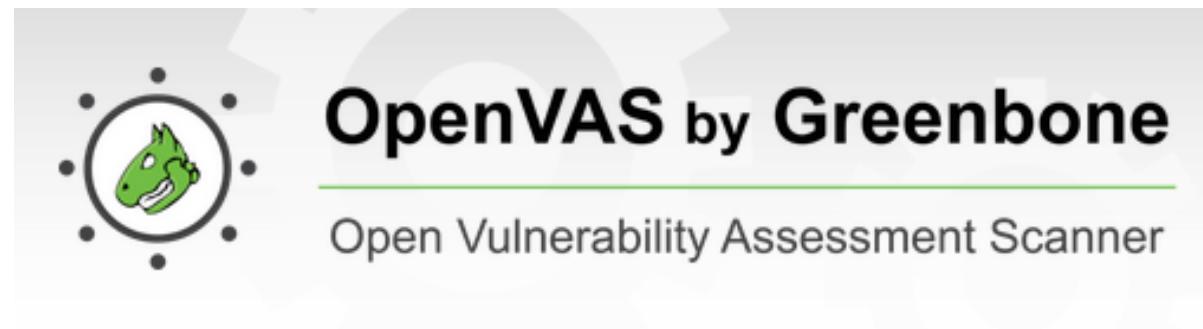
## NESSUS

The screenshot shows the Nessus web interface with the following sections:

- Left Sidebar:**
  - FOLDERS: My Scans, All Scans, Trash.
  - RESOURCES: Policies, Plugin Rules.
  - TENABLE: Community, Research, Plugin Release Notes.
- Header:** nessus, Scans, Settings, fredlaranç@inatel.br, profile icon.
- Discovery:** Host Discovery (A simple way to discover live hosts and open ports).
- Vulnerabilities:**
  - Basic Network Scan, Advanced Scan, Advanced Dynamic Scan, Malware Scan, Mobile Device Scan, Web Application Tests, Credentialed Patch Audit.
  - Intel AMT Security Bypass, Spectre and Meltdown, WannaCry Ransomware, Ripple20 Remote Scan, Zeroloon Remote Scan, Solarisate, 2020 Threat Landscape Retrospective (TLR).
  - ProxyLogon : MS Exchange, PrintNightmare, Active Directory Starter Scan.
- Compliance:**
  - Audit Cloud Infrastructure, Internal PCI Network Scan, MDM Config Audit, Offline Config Audit, PCI Quarterly External Scan, Policy Compliance Auditing, SCAP and OVAL Auditing.
- Tenable News:** Focus on the Fundamentals: 6 Steps to Defend Again... (Read More)
- Bottom Footer:** 66

# Infraestrutura

OpenVAS



Por onde começar?

Análise de ameaças e risco

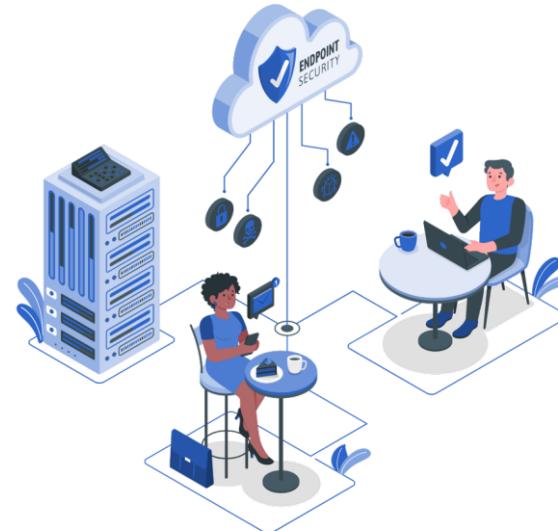
Segurança de ativos

Segurança de pessoas

# Segurança em Cloud

Maior exposição e suscetibilidade a ataques.

- Assegure que os dados e sistemas estejam seguros
- Acompanhe o estado dos dados e das configurações de segurança
- Monitoramento constante de parâmetros (notificação)



# Segurança em Cloud

- Recursos hospedados
- Perímetros
- Ameaças sofisticadas

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Segurança em Cloud

## Responsabilidade

- Conformidade (GDPR / LGPD)
- Softwares confiáveis
- Ciclos de vida
- Portabilidade
- Monitoramento
- Pessoal qualificado

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Segurança em Cloud

Nuvem pública

Nuvem privada

Nuvem híbrida

Multicloud

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Segurança em Cloud

Infraestrutura, plataforma, software como serviço

- Autenticação
- Backup e restauração

Infraestrutura (IaaS)	Plataforma (PaaS)	Software (SaaS)
Sistema Operacional e Rede	Desenvolvimento, Servidor de aplicação, Banco de Dados	Controle de acesso das aplicações
Máquinas provisionadas com atualizações e correções	Atualizações e correções para os sistemas providos na plataforma	Áreas da aplicação com controle de permissão
Responsabilidade em impedir usuários de desabilitarem a segurança do sistema	Medidas de segurança no compartilhamento de Servidor de aplicação ou Banco de Dados	Criptografia na comunicação
Isolamento de rede	Criptografia do banco de dados	Prevenção de perda de dados (DLP)

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Segurança no ambiente de desenvolvimento

Nenhuma falha conhecida deve ser levada pra produção



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Segurança no ambiente de desenvolvimento

## Boas práticas:

- Gerenciamento de código fonte
- Realização de testes
- Correção de bugs
- Integração contínua
- Documentação
- Padrões de código seguro

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Segurança no ambiente de desenvolvimento

## As ameaças dentro de casa

- 3PP
- FOSS
- Docker images

## Proteções:

- Análise de versões específicas
- Repositório de versões estáveis / checksum
- Testes de Integração

Por onde começar?

Análise de ameaças e risco

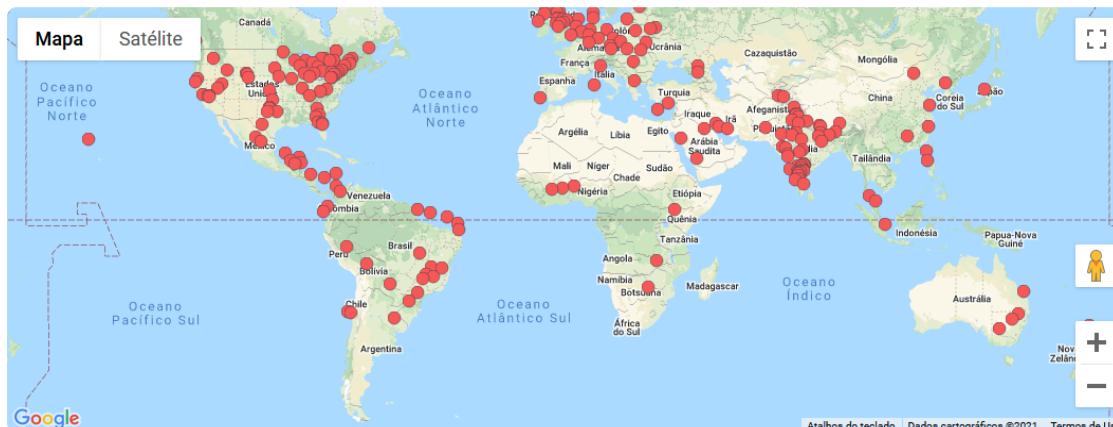
Segurança de ativos

Segurança de pessoas

# Segurança no ambiente de desenvolvimento

OWASP – Open Web Application Security Project

- Top 10 (<https://www.owasptopten.org/>)
- Guias de teste (Mobile)
- Comunidade



OWASP® Foundation

Membros

93.516

Grupos

232

Países

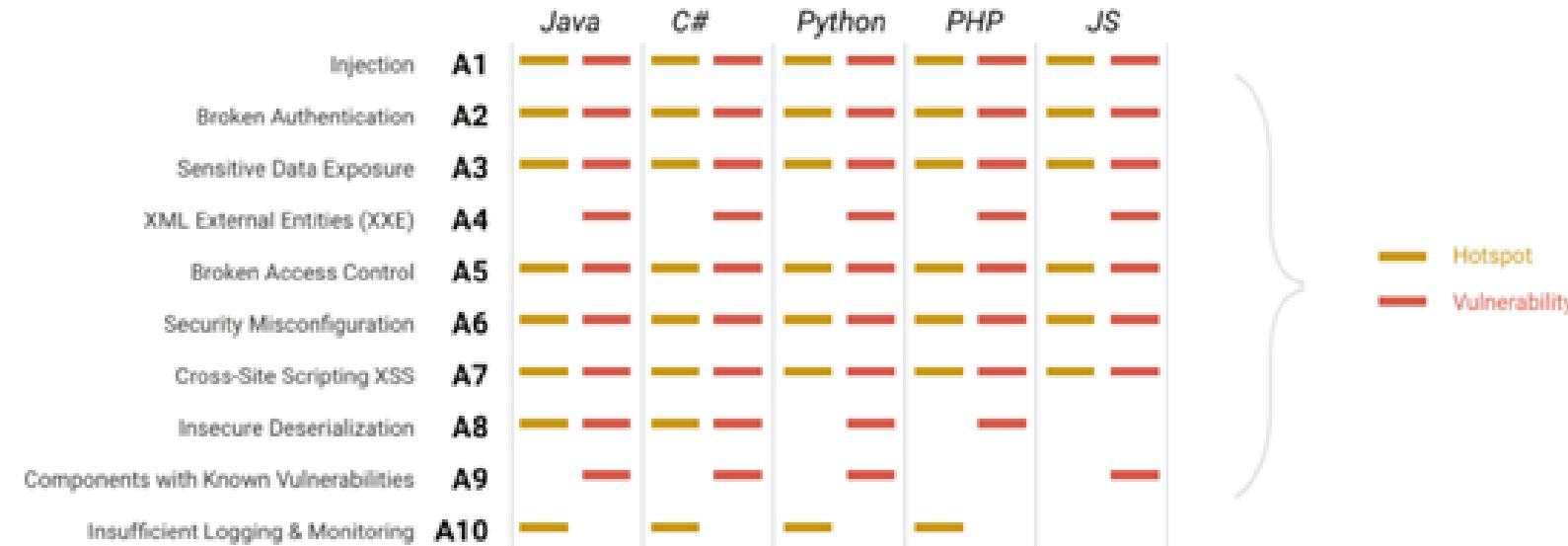
72

## South America

- OWASP Asuncion, Paraguay
- OWASP Belem
- OWASP Belo Horizonte
- OWASP Bogota
- OWASP Bolivia
- OWASP Brasilia
- OWASP Cartagena
- OWASP Chile
- OWASP Cusco
- OWASP Fortaleza
- OWASP Guayaquil
- OWASP Lima
- OWASP Medellin
- OWASP Monterrey
- OWASP Natal
- OWASP Patagonia
- OWASP Porto Alegre
- OWASP Queretaro City
- OWASP Quito
- OWASP Recife
- OWASP Rio De Janeiro
- OWASP Santa Rita do Sapucai
- OWASP Sao Paulo
- OWASP Uruguay
- OWASP Vina Del Mar
- OWASP Vitoria

# Segurança no ambiente de desenvolvimento

- CI/CD
- SAST – SonarQube [SonarQube](#)



# Segurança no ambiente de desenvolvimento

OWASP ZAP

Aplicações e websites vulneráveis

| <https://sectigostore.com/blog/13-vulnerable-websites-web-apps-for-pen-testing-and-research/>

Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

04

Por onde começar?  
Análise de ameaças e risco  
Segurança de ativos  
Segurança de pessoas

# Segurança de pessoas

Descrição

Segurança de pessoas  
Treinamento  
Conscientização e avaliação

# Segurança de pessoas



Toyota, 2019: Prejuízo de **US\$ 37 mi**

Condado de Cabarrus, EUA, 2018: Prejuízo de **US\$ 1,7 mi**

Pesquisa LastPass (2017):  
**59%** compreendem importância de senhas seguras  
**91%** entendem os riscos do reuso de senhas  
**41%** usavam senhas fáceis de lembrar  
**61%** usavam senhas iguais ou semelhantes



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Treinamento

- Survey para coleta e dados
- Modelagem de programas de treinamentos e focados em papéis
- Ensinar sobre os principais vetores de ameaça:
  - Identificar Phishing
  - Engenharia social
  - Criação de senhas válidas (utilização de gerenciadores e autenticação multifatores)
  - Cuidados na rede wi-fi doméstica
  - Utilização adequada do equipamento da empresa
  - Responsividade a eventos



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

Por onde começar?  
Análise de ameaças e risco  
Segurança de ativos  
Segurança de pessoas

# Treinamento

## Cursos gratuitos:

[Information Security: Context and Introduction | Coursera](#)

[Cybersecurity for Everyone | Coursera](#)

[NSE Institute: Library \(fortinet.com\)](#)

### Aprendizado gratuito na Udemy



Segurança da Informação para Iniciantes na Prática  
Emerson Patron, Marcus Oliveira  
4.6 ★★★★★ (107)  
42 horas no total • 11 aulas • Iniciante  
Gratuito



Cyber Security Course for Beginners - Level 01  
FourTrails Technologies  
4.1 ★★★★★ (11.3K)  
1 hora 46 min • 12 aulas • Iniciante  
Gratuito



Security Awareness Campaigns (Lite)  
Michael Goedeker  
4.2 ★★★★★ (5.3K)  
31 minutos no total • 8 aulas • Iniciante  
Gratuito



Build Your Own Cyber Lab at Home  
Kyle Stoen  
4.4 ★★★★★ (2.0K)  
1,3 horas no total • 22 aulas • Técnico avançado  
Gratuito

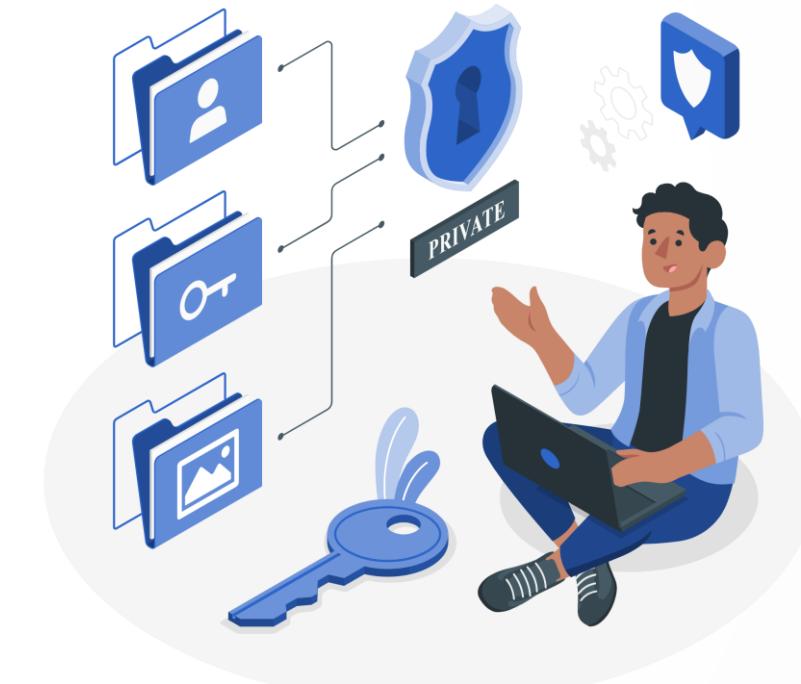


Cybersecurity Awareness Training  
Eric Schertzman  
4.5 ★★★★★ (2.3K)  
38 minutos no total • 12 aulas • Técnico avançado  
Gratuito

# Conscientização e avaliação

Mecanismos de incentivo e/ou recompensa:

- sistema de pontuação por desempenho nos treinamentos
- scoreboard
- programas de recompensa ou vouchers para concessão de descontos
- Seleção de “embaixadores da segurança”



Por onde começar?

Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

# Conscientização e avaliação

Por onde começar?

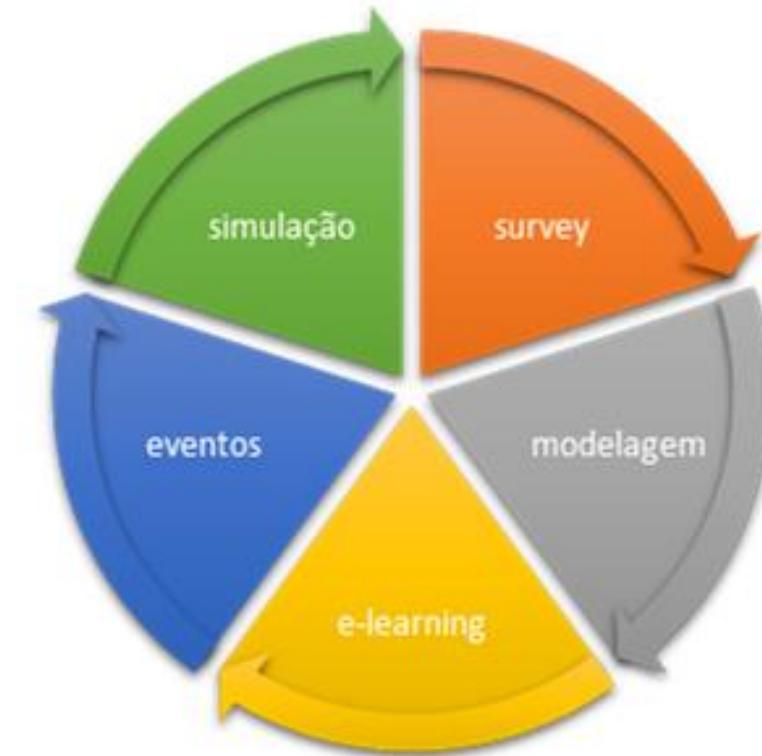
Análise de ameaças e risco

Segurança de ativos

Segurança de pessoas

Com os resultados, será possível definir novas políticas para reforçar o engajamento

Definição de um processo cílico de melhoria contínua.



## Centro de Segurança Cibernética do Inatel:

<https://inatel.br/cxsc/>



## Maiores informações, referências, links:



[github.com/danielpfernandes/tdc\\_transformations\\_sec\\_inatel](https://github.com/danielpfernandes/tdc_transformations_sec_inatel)

**Obrigado!**

Todas as imagens foram desenvolvidas por Freepik, disponíveis em <https://storyset.com>