



# Introdução à Segurança da Informação

# Objetivo

- Compreender os conceitos fundamentais da segurança da informação.



# Segurança da Informação

Segurança da Informação é o conjunto de medidas e tecnologias que protegem as informações, sejam elas digitais ou físicas, de forma a evitar danos ou prejuízos a uma organização.



# Importância da SI

- 1 Proteção de Dados
- 2 Continuidade dos Negócios
- 3 Conformidade com Leis e Regulamentos
- 4 Reputação e Confiança

# Os 3 Pilares da SI

## Confidencialidade

Garantir que apenas pessoas autorizadas tenham acesso às informações.

## Integridade

Assegurar que as informações não sejam alteradas de forma não autorizada.

## Disponibilidade

Certificar que as informações estejam acessíveis aos usuários autorizados quando necessário.





# Confidencialidade



Criptografia

Senhas Robustas

# Integridade



Checksums



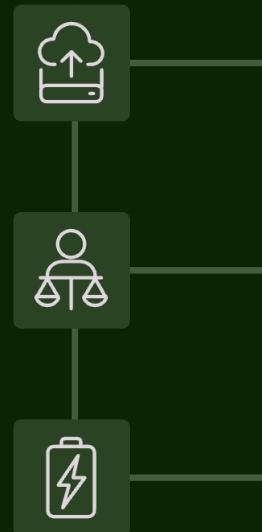
Logs de Auditoria





**24** / **7**

## Disponibilidade



Redundância

Balanceamento de Carga

Nobreaks, Geradores



# Autenticidade

- Biometria
- Certificado Digital
- Contas Verificadas



# Irretratabilidade



# O que são Ameaças?

- 1 Ação Intencional
- 2 Origem Diversa
- 3 Objetivos Variados



TLP:CLEAR



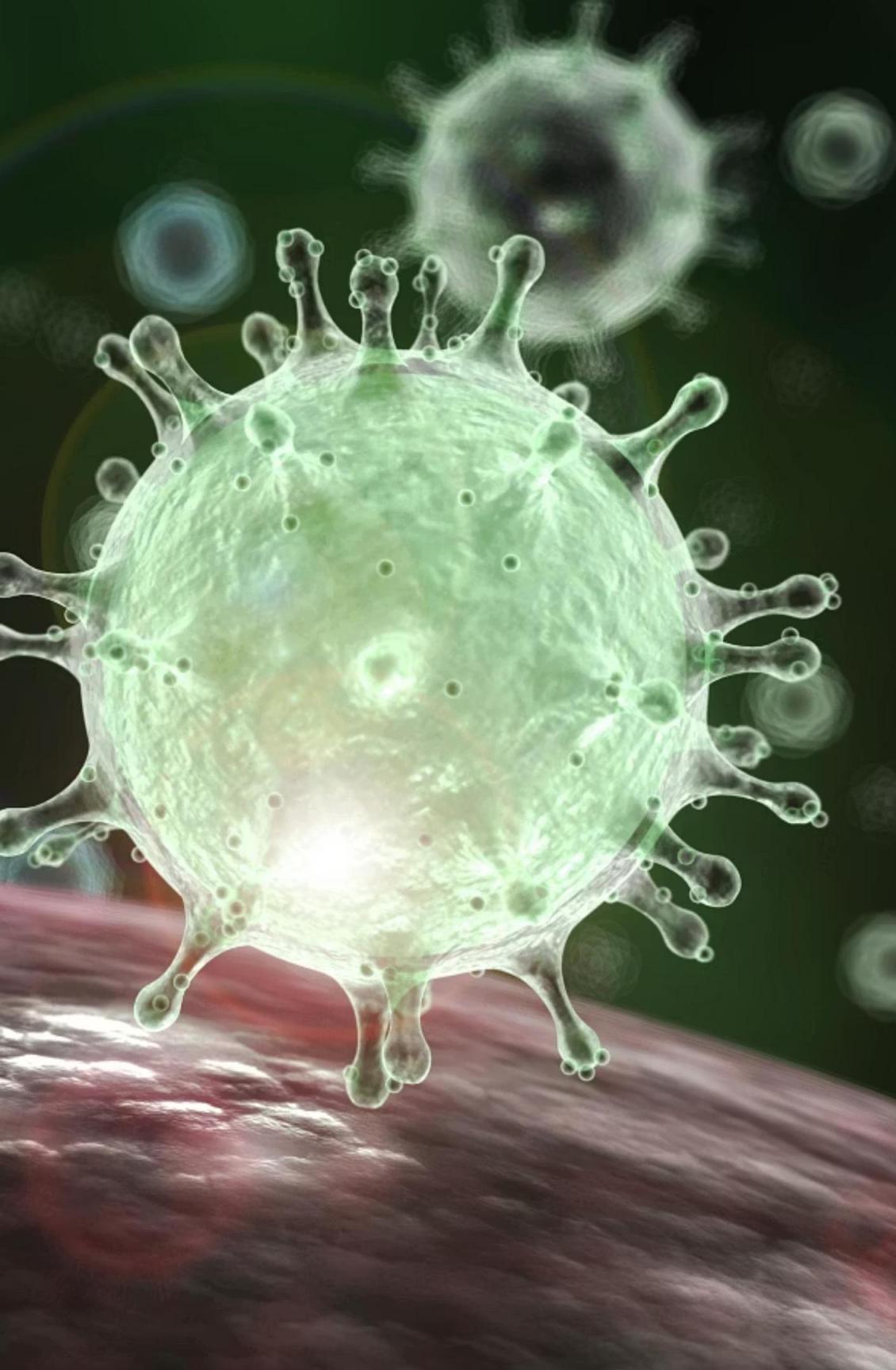
# Ameaças Comuns

Malware

Phishing

DDoS

Ameaça Interna



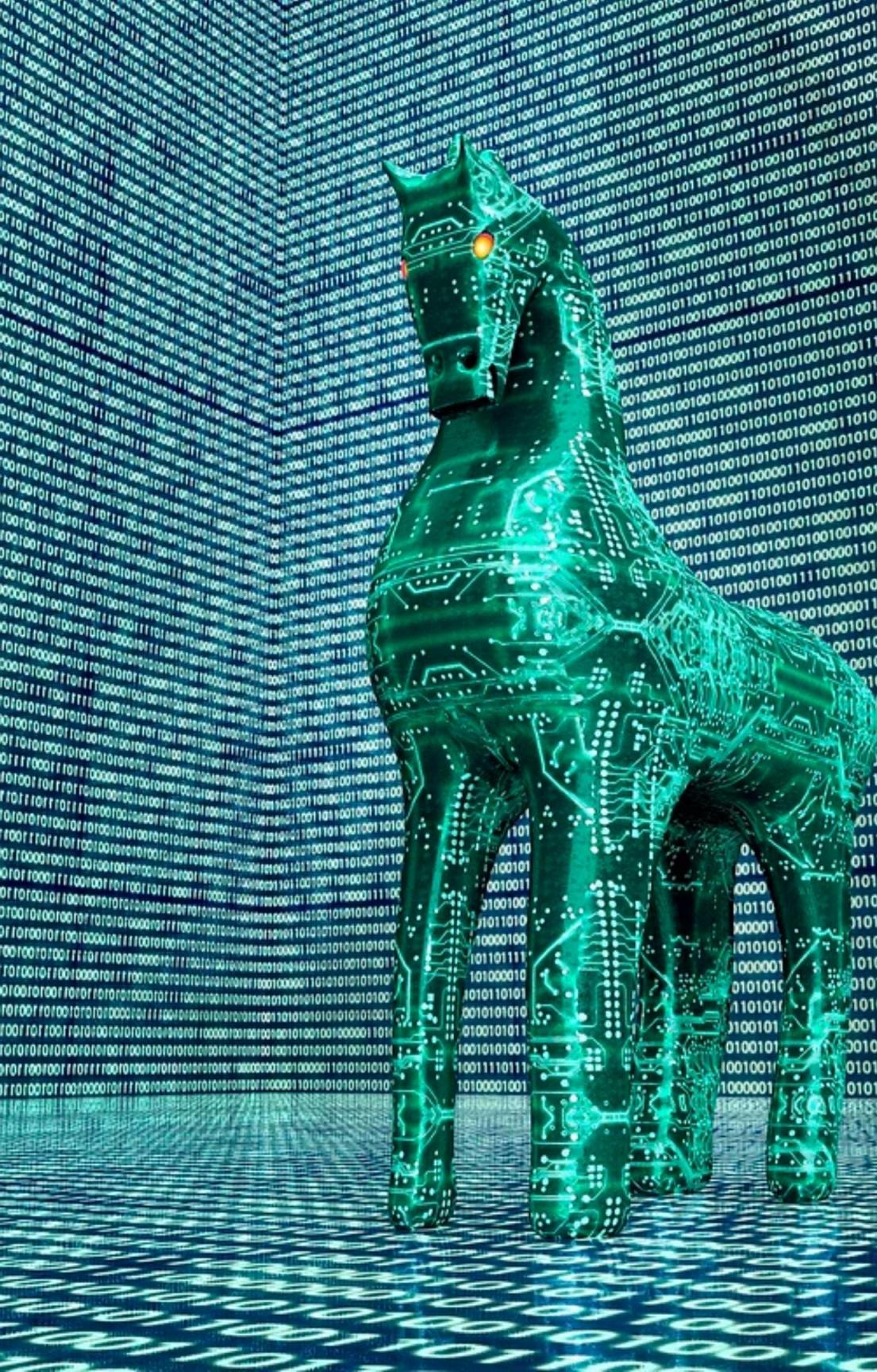
# Vírus

É um tipo de malware que se anexa a arquivos legítimos e precisa da interação do usuário para ser executado e se espalhar.



# Worms

É um tipo de malware capaz de se replicar e se espalhar automaticamente sem a necessidade de ação do usuário. Diferente de um vírus, ele não precisa infectar arquivos específicos para se propagar.



# Trojans

É um tipo de malware que se disfarça como um software legítimo ou útil para enganar o usuário e obter acesso ao sistema. Ele não se replica sozinho, mas pode abrir portas para outros ataques.



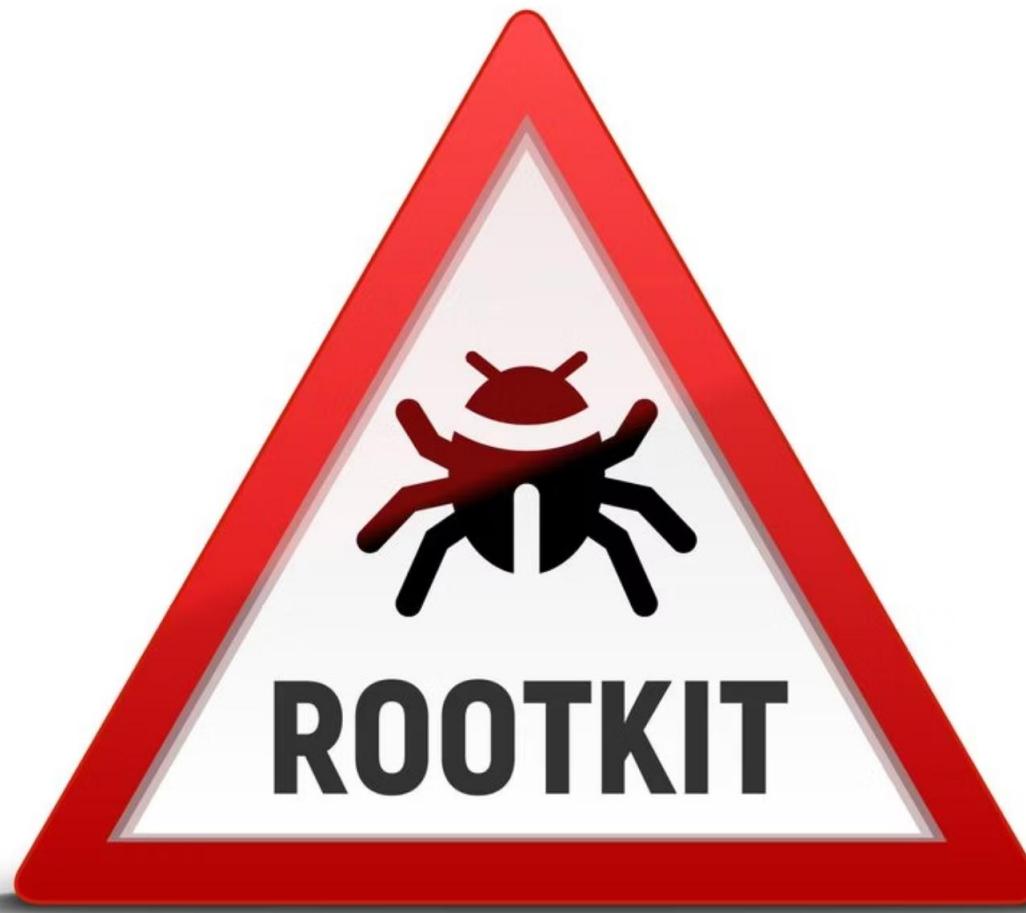
# Spywares

É um tipo de malware projetado para espionar a atividade do usuário sem seu consentimento. Ele coleta informações pessoais, como dados bancários, credenciais de login, histórico de navegação e até gravações de áudio e vídeo.



# Adware

É um tipo de software que exibe anúncios indesejados no computador ou dispositivo móvel. Embora alguns adwares sejam legítimos e usados para monetização de aplicativos gratuitos, muitos operam de forma maliciosa, exibindo propagandas intrusivas, coletando dados do usuário e redirecionando para sites perigosos.



## Rootkit

É um tipo de malware projetado para obter acesso privilegiado ao sistema operacional e, ao mesmo tempo, permanecer oculto, impedindo sua detecção. O termo vem da junção de root (superusuário com privilégios administrativos) e kit (conjunto de ferramentas que permite controle remoto e ocultação de presença).



# Ransomware

É um tipo de malware que sequestra os dados de um sistema através de criptografia e exige um pagamento para restaurar o acesso. Seu nome vem da junção de ransom (resgate) + ware (software). É uma das ameaças mais perigosas atualmente, afetando usuários comuns, empresas e governos.



# O que são Vulnerabilidades?

- 1 Pontos Fracos
- 2 Diversos Tipos
- 3 Riscos Associados



# Vulnerabilidades Comuns

Falhas de Software

Configurações  
Incorretas

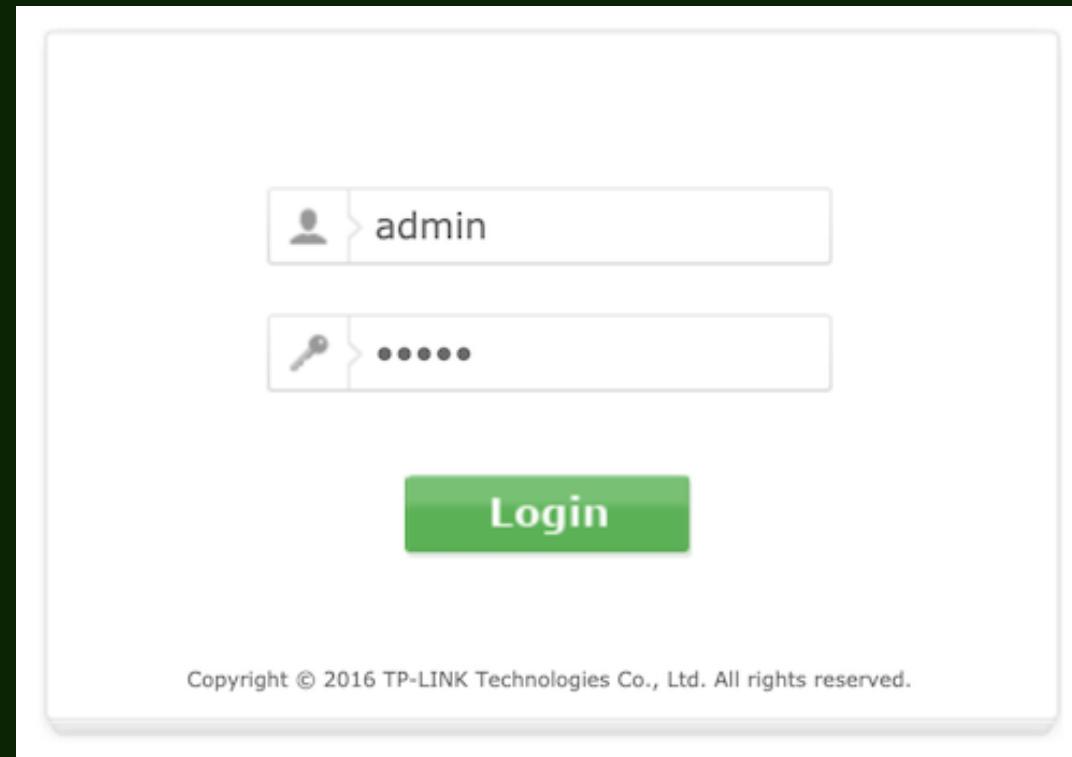
Falta de  
Atualização

Erro Humano



# Falhas de Software

- Buffer Overflow
- SQL Injection
- Cross-Site Scripting

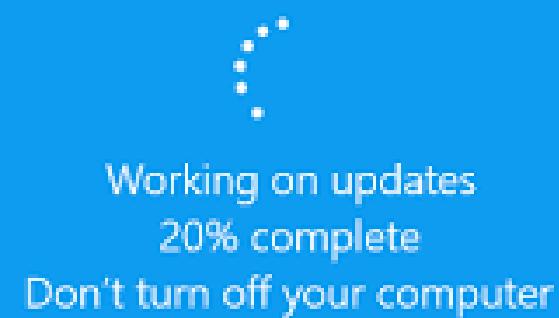


## Configurações Incorretas

- Padrão
- Excesso de Permissões
- Exposição desnecessária

# Falta de Atualização

- Negligência





# Erro Humano

- Falta de treinamento
- Senhas fracas



- Vulnerabilidades e Exposições Comuns
  - Lista Pública
  - Ano + ID
- [MITRE](#)  
[NVD \(NIST\)](#)



# Gestão de Riscos

Identificar, avaliar e mitigar os riscos que  
ameaçam a Segurança da Informação

A photograph showing a row of people's hands and arms resting on a long wooden conference table. They are all holding pens and writing in small, open notebooks. The scene is well-lit from the side, creating strong shadows and highlights on the hands and the table surface.

# Identificação e Avaliação de Riscos

- 1 Levantamento de Ativos
- 2 Identificação de Ameaças
- 3 Identificação de Vulnerabilidades
- 4 Classificação dos Riscos

# Mitigação de Riscos

## Controles Preventivos

Implementar controles preventivos, como firewalls, sistemas de detecção e prevenção de intrusão (IPS/IDS) e atualizações de segurança, pode ajudar a reduzir a probabilidade de um incidente ocorrer.

## Planos de Contingência

Ter planos de contingência, como backups regulares e procedimentos de recuperação de desastres, pode minimizar o impacto caso um incidente ocorra. Isso garante a continuidade das operações.

## Monitoramento Contínuo

O monitoramento contínuo de atividades suspeitas e a análise de registros (logs) ajudam a detectar e responder rapidamente a incidentes, limitando os danos.

# O Risco pode ser:

 Evitado

 Reduzido

 Transferido

 Aceito

# A Gestão de Riscos proporciona:

1 Proteção de Ativos

2 Redução de Impactos

3 Melhoria a Conformidade

4 Aumento da Resiliência

5 Auxílio na Tomada de Decisões



# Medidas de Segurança

As principais medidas de segurança incluem controles preventivos, detectivos e corretivos.

# Controles Preventivos

- 1 Políticas de Acesso
- 2 Autenticação Forte
- 3 Criptografia
- 4 Firewall

# Controles Detectivos

- 1 Monitoramento de Atividades
- 2 Análise de Logs
- 3 Sistemas de Detecção de Intrusão

# Controles Corretivos

- 1 Planos de Resposta a Incidentes
- 2 Restauração de Backups
- 3 Atualização de Softwares

# Criptografia

## Confidencialidade

A criptografia garante que apenas pessoas autorizadas possam acessar os dados.

## Integridade

Assegura que as informações não sejam alteradas durante o armazenamento ou transmissão.

## Autenticidade

Permite a verificação da origem e a autenticidade dos dados criptografados.

# Firewalls e Antivírus

## Firewalls

Sistemas que controlam e monitoram o tráfego de rede, bloqueando acessos não autorizados.

## Antivírus

Programas que detectam, previnem e removem malware, protegendo os sistemas contra ameaças.

## Complementares

Firewalls e antivírus trabalham em conjunto para fornecer uma defesa abrangente.

# Políticas de Segurança

- 1 Definição
- 2 Implementação
- 3 Revisão

## Examples of cyber-security policies

-  Acceptable Use Policy
-  Password Requirements Policy
-  Access Control Policy
-  Remote Access Policy
-  Data Management Policy
-  Breach Response Policy
-  Disaster Recovery Policy

TLP:CLEAR

# Papéis e Responsabilidades



## Usuários

Cumprir as políticas de segurança e denunciar atividades suspeitas.



## Administradores

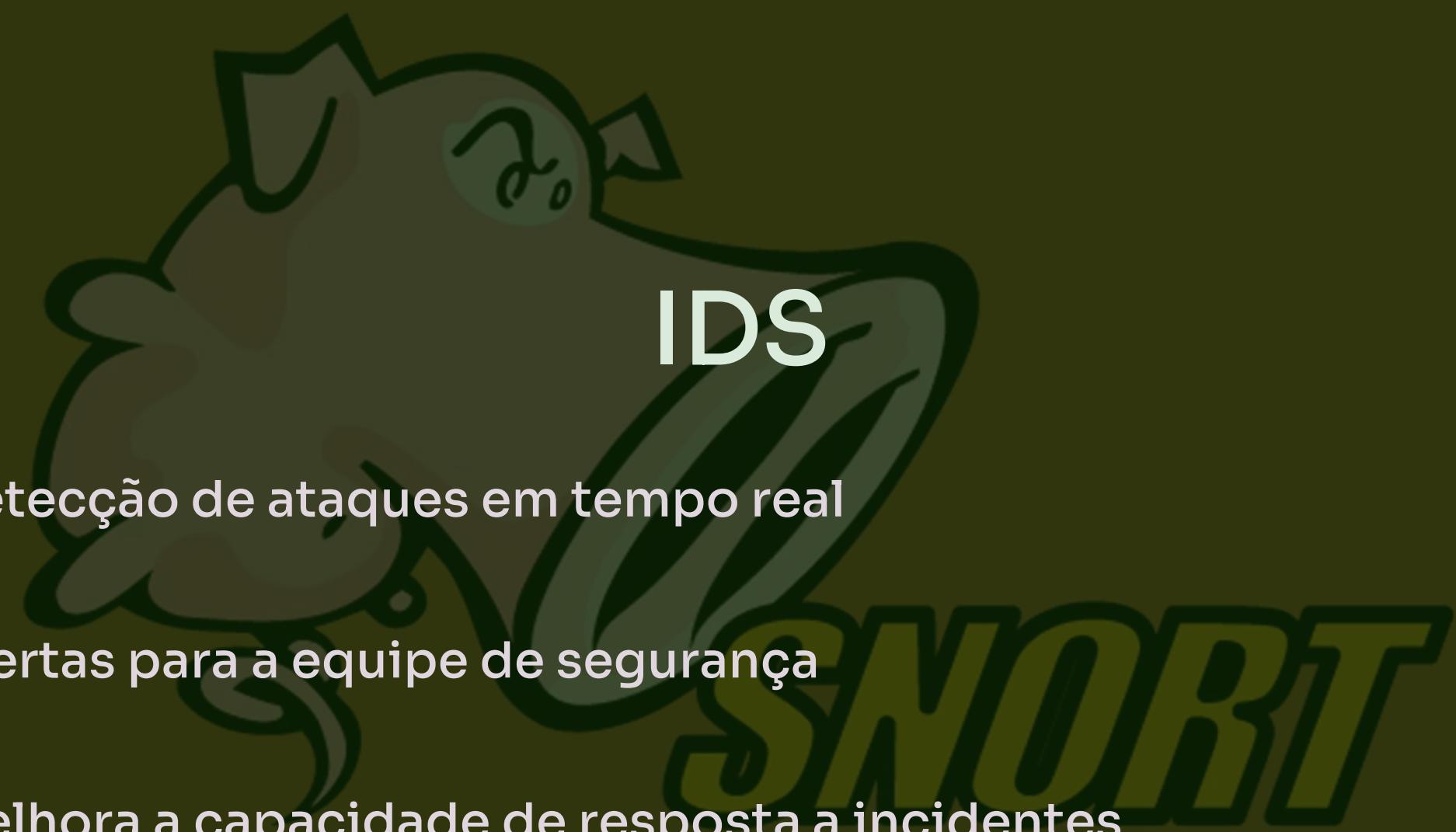
Implementar e manter os controles de segurança nos sistemas.



## Gestores

Definir e revisar as políticas, investir em segurança e supervisionar a equipe.





# IDS

- Detecção de ataques em tempo real

- Alertas para a equipe de segurança

- Melhora a capacidade de resposta a incidentes

OPENSOURCE NETWORK INTRUSION DETECTION TOOL

# Backup

Garantir a restauração da informações e sistemas

Evitar perda permanente dos dados

3-2-1

# Princípios Fundamentais de SI

Três princípios fundamentais: Segurança por Design, Defesa em Profundidade e Mínimo Privilégio.



# Segurança por Design

- 1 Planejamento Antecipado
- 2 Segurança em todas as camadas
- 3 Testes e validação contínuos
- 4 Automação de Segurança

# BY DESIGN

## Benefícios

1

Redução de Vulnerabilidades

2

Eficiência

3

Conformidade



ManageEngine  
EventLog Ana



security  
union

FireEye

Google Cloud IDS



# Defesa em Profundidade

- 1 Múltiplas Camadas de Segurança
- 2 Diversificação de Controles
- 3 Isolamento de Sistemas
- 4 Monitoramento e Respostas Contínuos



# Benefícios

- 1 Redundância de Segurança
- 2 Cobertura Abrangente
- 3 Flexibilidade



**DO NOT ENTER**  
Authorized Person Only

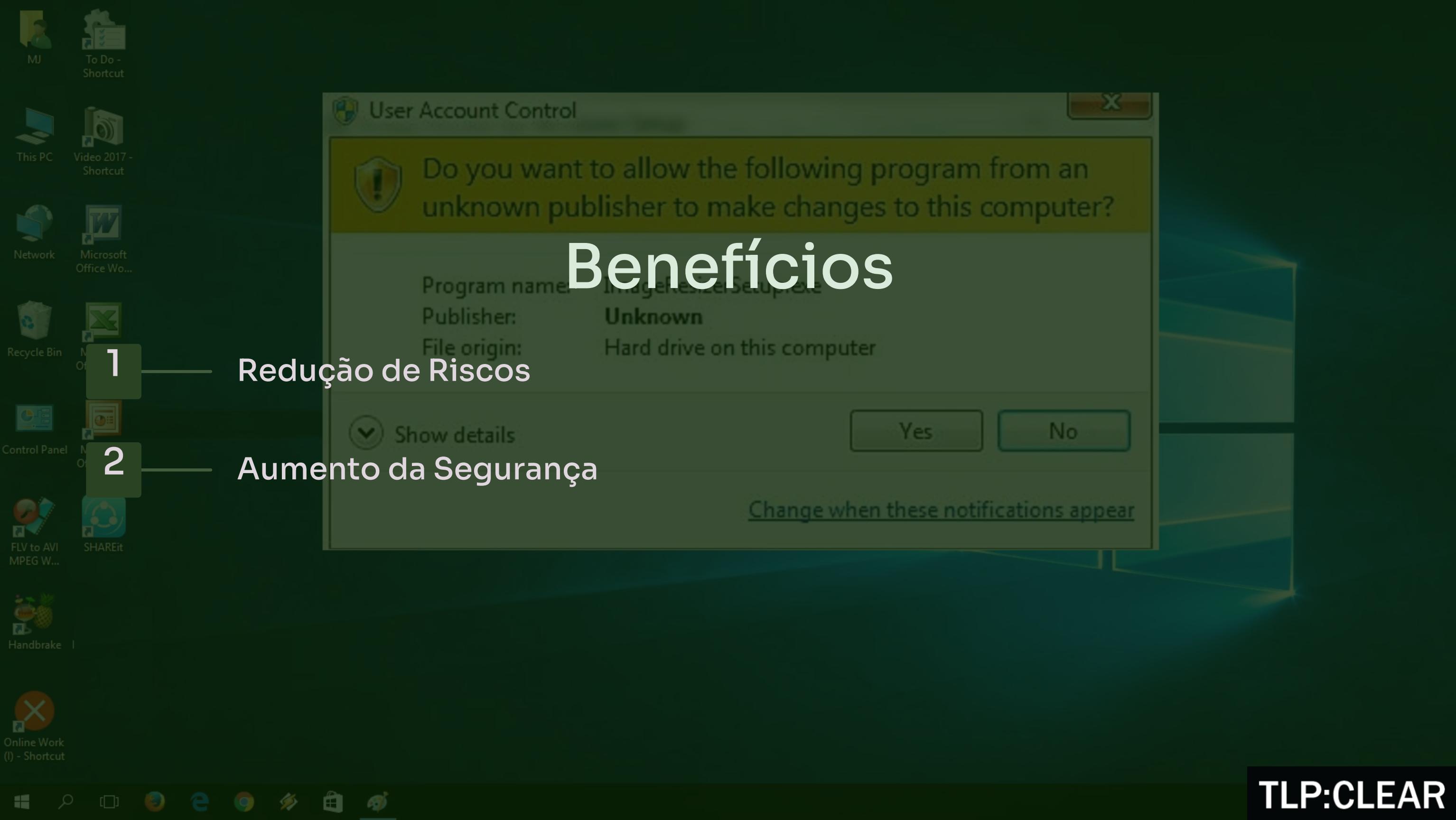
my

Image ID: 2  
www.alan

# Princípio do Menor Privilégio

- 1 Controle de Acesso Rigoroso
- 2 Revisão Regular de Privilégios
- 3 Segregação de Funções

TLP:CLEAR



# Benefícios

Redução de Riscos

Aumento da Segurança

TLP:CLEAR

# Resumindo...



## Segurança por Design

Garante que a segurança seja uma consideração fundamental desde o início.



## Defesa em Profundidade

Cria múltiplas barreiras contra ameaças potenciais.



## Mínimo Privilégio

Limita o acesso para reduzir a superfície de ataque.

A integração destes princípios cria uma estratégia de segurança robusta e abrangente.

Juntos, eles fornecem uma base sólida para proteger sistemas e dados críticos.

A photograph of a silver padlock mounted on a metal surface. The padlock's shackle has been modified to contain a green printed circuit board (PCB) with various electronic components and wires, representing the intersection of physical security and digital technology.

# Normas e Padrões de SI

Diversas normas e padrões internacionais foram desenvolvidos para ajudar organizações a proteger suas informações críticas.

# ISO/IEC 27001

## 1 Gestão de Riscos

A ISO/IEC 27001 fornece uma estrutura abrangente para identificar, avaliar e tratar os riscos de segurança da informação de uma organização.

## 2 Melhoria Contínua

O padrão incentiva a implementação de um sistema de gestão de segurança da informação (SGSI) que promove a melhoria contínua dos controles e processos.

## 3 Certificação Internacional

A certificação ISO/IEC 27001 é reconhecida globalmente e demonstra o compromisso da organização com a segurança da informação.

## 4 Abordagem Abrangente

O padrão abrange uma ampla gama de controles de segurança, desde a gestão de riscos até a conscientização dos funcionários.



TLP:CLEAR



# LGPD

Proteção de Dados Pessoais

Conformidade Obrigatória

Direitos dos Titulares

Governança de Dados

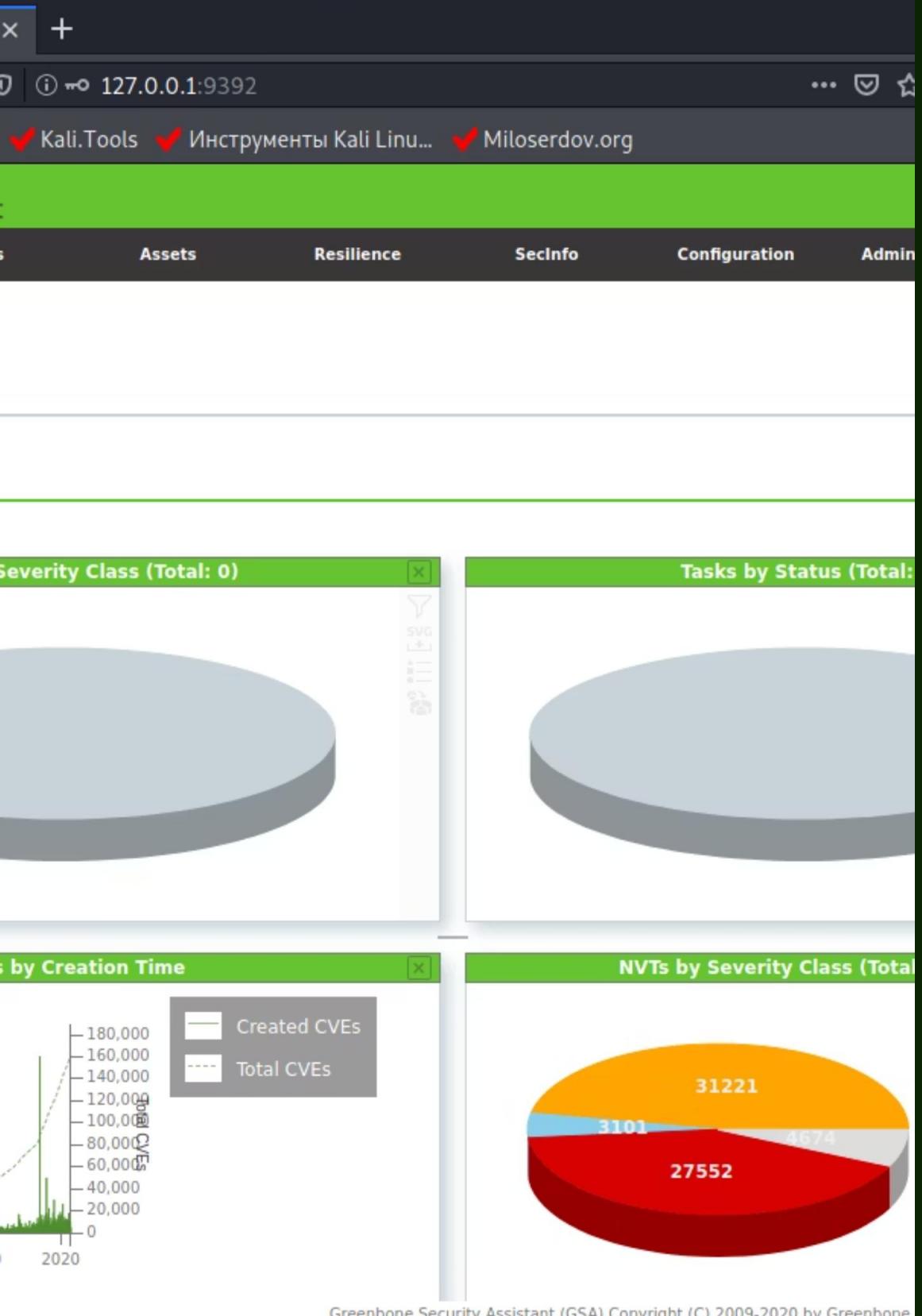
A segurança da informação é um desafio constante, mas fundamental para proteger dados e sistemas. A **conscientização**, o **conhecimento** e a **implementação de medidas de proteção** são essenciais para navegar com segurança no mundo digital.

A segurança da informação é uma **responsabilidade de todos**. Mantenha-se informado, pratique boas práticas e contribua para um ambiente digital mais seguro.



# Hands-on!

TLP:CLEAR



# Identificar e Gerenciar Vulnerabilidades

## VM-Kali com o GVM (Greenbone Vulnerability Management)

- Iniciar as VMs do Kali e do Metasploitable (C:\VMs)
- Adicionar a VM do Metasploitable como **alvo** e fazer um **scan** de Vulnerabilidades
- Analisar as Vulnerabilidades encontradas

TLP:CLEAR

# CTFs

## Security Principles

<https://tryhackme.com/room/securityprinciples>

## Vulnerabilities 101

<https://tryhackme.com/room/vulnerabilities101>

## OpenVAS

<https://tryhackme.com/room/openvas>

## Roundcube CVE-2025-49113

<https://tryhackme.com/room/roundcubecve202549113>