

# CYBER NEWS

O Boletim Informativo Oficial de Gestão de Riscos em Terceiros



## NESTA EDIÇÃO

### GERENCIAMENTO CONTÍNUO DE VUNERABILIDADES

- Por que é importante?
- Boas Práticas

### DEFESA CONTRA MALWARE

- O que é Malware?
- Exemplos comuns de Malware
- Como Malware se Espalha
- Sinais de Infecção
- O que fazer se for Infectado?
- Boas Práticas de Defesa

## CONCLUSÃO

## Você sabia que pequenas falhas podem colocar todo o seu ambiente em risco?

Por isso, neste volume, vamos falar sobre como lidar com o gerenciamento de vulnerabilidades, o que é o malware e como proteger a sua empresa contra ele.

### Gerenciamento Contínuo de Vulnerabilidades

O gerenciamento contínuo de vulnerabilidades é um processo que identifica e corrige falhas de segurança em sistemas e redes o tempo todo. Diferente de verificações feitas de vez em quando, ele funciona de forma constante e automática, ajudando a evitar ataques e que brechas sejam exploradas por cibercriminosos.

#### 🔔 Por que é importante?

- 🌐 Redução do risco de ataques cibernéticos;
- ⚙️ Melhoria na postura de segurança da organização;
- 🛡️ Prevenção de falhas que impactam a continuidade dos negócios;
- 🔒 Conformidade com normas e regulamentações (LGPD, ISO 27001, etc.)

#### 📦 Boas práticas

- ✅ Mantenha os sistemas e softwares sempre atualizados.
- ✅ Utilize ferramentas de proteção.
- ✅ Integre o gerenciamento com os processos de ITSM
- ✅ Documente e acompanhe os indicadores de desempenho (tempo médio de correção, % de falhas críticas corrigidas).

## Defesa contra o Malware

### O que é o Malware?

Malware (abreviação de malicious software) é um tipo de programa criado para causar danos, roubar dados, interromper sistemas ou permitir acesso não autorizado a dispositivos. Ele pode se disfarçar de arquivos legítimos, e-mails, links ou até atualizações falsas.

#### Exemplos comuns de malware:

- 🦠 Vírus – Se espalham ao infectar arquivos e programas.
- 🔒 Ransomware – Bloqueia o acesso aos dados e exige pagamento para liberá-los.
- 🕵️ Spyware – Espiona o usuário e coleta informações.
- 🔄 Worms – Se replicam automaticamente e se espalham por redes.
- 🐎 Trojans (Cavalos de Troia) – Parecem inofensivos, mas escondem funções maliciosas.

#### Como o Malware se espalha:

- 📧 Anexos de e-mail falsos ou suspeitos.
- 🔗 Links maliciosos em mensagens ou redes sociais.
- 💻 Downloads de softwares piratas.
- 🔌 Dispositivos USB infectados.
- 🔧 Falhas não corrigidas no sistema.



#### Boas Práticas de Defesa

- ✅ Mantenha seu antivírus atualizado e ativo.
- 🔄 Atualize o sistema operacional e os softwares com frequência.
- ⚠️ Desconfie de e-mails com anexos ou links não esperados.
- 🌐 Evite acessar sites suspeitos ou baixar programas de fontes não oficiais.
- 🔒 Use senhas fortes e ative a autenticação em dois fatores (2FA).
- 🔌 Não conecte dispositivos externos desconhecidos.
- 👤 Nunca ignore alertas de segurança do sistema ou antivírus.

## Conclusão

Sigam as boas práticas, mantenham seus sistemas atualizados e ajudem a proteger os dados da empresa. Prevenir é sempre melhor do que remediar.

Se notarem algo estranho ou tiverem dúvidas, falem com a sua equipe de TI ou Segurança da Informação.

Fiquem atentos aos próximos boletins para mais dicas!



O malware está mais próximo do que você imagina.  
Proteja-se!

#### Sinais de infecção:

- 🌐 Lentidão incomum no computador.
- 🌐 Redirecionamento para sites estranhos.
- 🗨️ Pop-ups constantes e indesejados.
- 📁 Arquivos sumindo ou se corrompendo.

#### O que fazer se for infectado?

- 🔌 Desconecte o equipamento da internet
- 💻 Não tente "resolver sozinho" sem conhecimento técnico.
- 📞 Avise imediatamente o setor de TI ou Segurança da Informação.
- 📄 Anote o que aconteceu (mensagens, arquivos acessados, etc.).

