Fundamentos de Cybersegurança

Agenda

- Introdução a Cybersegurança
- Conceitos básicos e tipos de ameaças
- Boas práticas de segurança digital e proteção de dados
- Riscos em redes e dispositivos
- Comportamentos seguros e cultura de segurança
- Revisão e encerramento

Objetivos do Curso

Objetivo Geral

Introduzir os participantes ao universo da cibersegurança, desenvolvendo uma consciência crítica e preventiva sobre o uso seguro de tecnologias.

Público-Alvo

- Pessoas interessadas em segurança digital
- Estudantes iniciantes na área de tecnologia
- Profissionais de áreas afins
- Faixa etária: a partir de 16 anos

Objetivos Específicos

- Compreender os conceitos básicos da segurança da informação
- Identificar os principais tipos de ameaças e ataques cibernéticos
- Apresentar boas práticas de segurança digital para usuários comuns
- Reconhecer a importância da proteção de dados pessoais e corporativos
- Estimular comportamentos seguros no ambiente virtual

Metodologia

Exposição teórica com apoio de slides
Discussão de casos reais
Diálogos guiados sobre situações do dia a dia

Conceitos Básicos de Segurança

O que é Cybersegurança?

Conjunto de práticas, tecnologias e processos destinados a proteger sistemas, redes, dispositivos e dados contra ataques digitais, danos ou acessos não autorizados.

Princípios Fundamentais (CID)

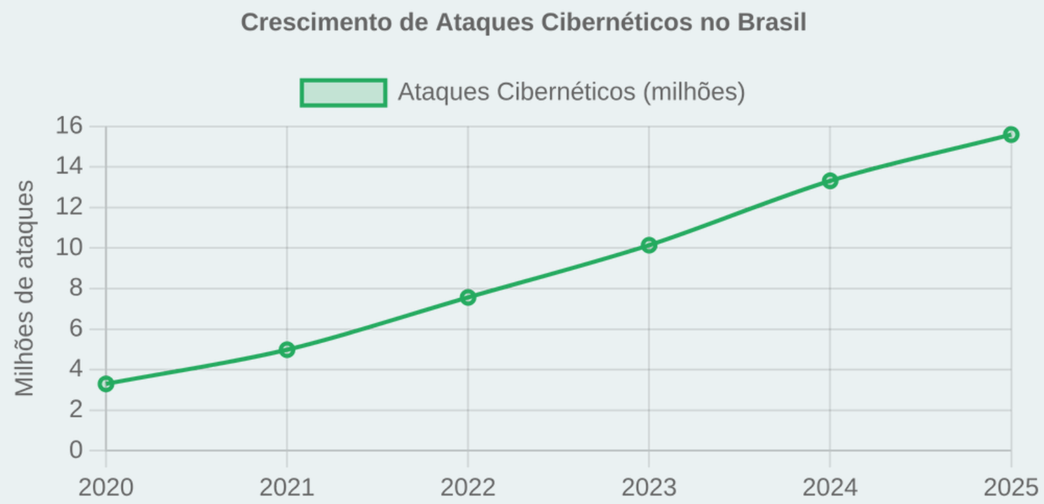
Confidencialidade
Garantir queinformaçõessensíveis sejam acessadas apenas por pessoas autorizadas.

Integridade
Assegurarqueos dados não sejam alterados de forma indevida ou não autorizada.

Disponibilidade
Garantirquesistemase dados estejam acessíveis quando necessário.

Conceitos Básicos de Segurança

Importância da Cybersegurança



Áreas da Cybersegurança

Segurança de Rede

Segurança de Dispositivos

Segurança de Dados

Segurança em Nuvem

Segurança de Aplicações

Segurança Humana

Ameaças Cibernéticas

Principais Tipos de Ameaças

Malware

Software malicioso projetado para danificar, invadir ou comprometer sistemas. Inclui vírus, worms, trojans e ransomware.

Phishing

Tentativas de obter informações sensíveis (senhas, dados de cartão) através de comunicações fraudulentas que se passam por fontes confiáveis.



Ameaças Cibernéticas

Principais Tipos de Ameaças

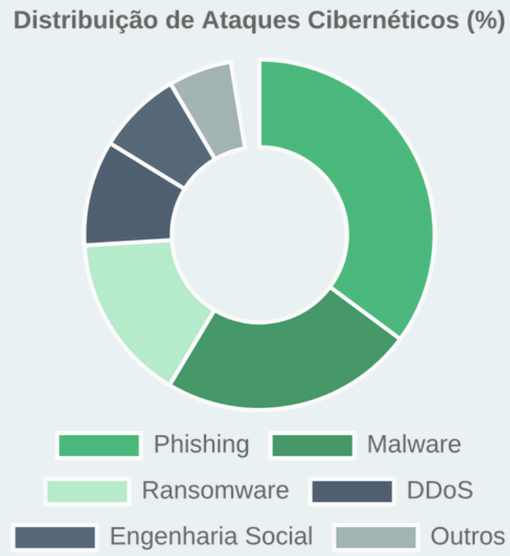
Ransomware

Tipo de malware que criptografa dados e exige pagamento de resgate para restaurar o acesso.

Engenharia Social

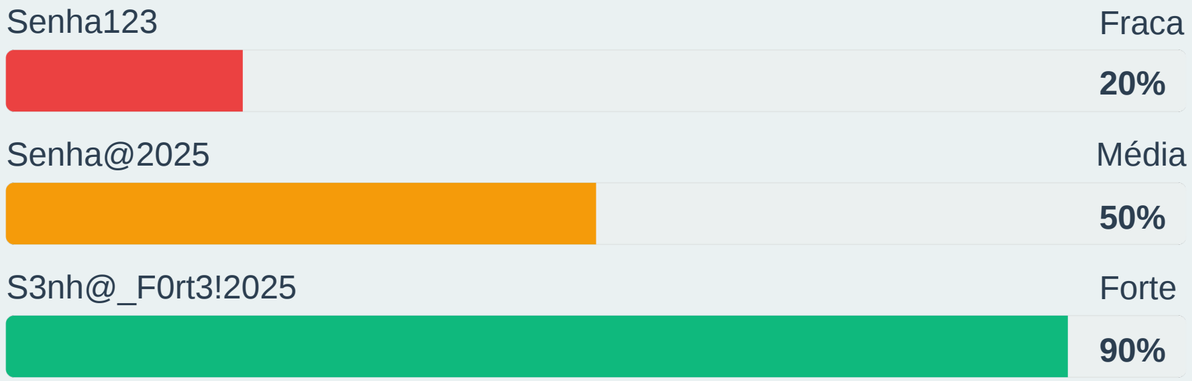
Manipulação psicológica para induzir pessoas a realizar ações ou divulgar informações confidenciais.

Distribuição de Ataques



Boas Práticas de Segurança

Senhas Seguras



Use senhas fortes e únicas
Combine letras maiúsculas, minúsculas, números e símbolos. Mínimo de 12 caracteres.

Ative autenticação de dois fatores (2FA)
Adicione uma camada extra de segurança além da senha.

Use um gerenciador de senhas
Facilita o uso de senhas diferentes para cada serviço.

Troque senhas regularmente
Especialmente para contas sensíveis como e-mail e bancos.

Boas Práticas de Segurança

Navegação Segura

Verifique conexões HTTPS
Procure pelo cadeado na barra de endereços antes de inserir dados sensíveis.

Mantenha software atualizado
Atualizações frequentemente corrigem vulnerabilidades de segurança.

Use antivírus e firewall
Mantenha-os ativos e atualizados em todos os dispositivos.

Cuidado com downloads
Baixe arquivos apenas de fontes confiáveis.

Faça backup regularmente
Mantenha cópias de segurança de dados importantes em locais diferentes.



Proteção de Dados

Dados Sensíveis

Dados Pessoais
Nome, endereço, CPF, RG, data de nascimento, e-mail, telefone.

Dados Financeiros
Números de cartão de crédito, senhas bancárias, histórico de transações.

Dados de Saúde
Histórico médico, resultados de exames, informações sobre tratamentos.

Dados Profissionais
Informações de trabalho, salário, avaliações de desempenho.

LGPD - Lei Geral de Proteção de Dados

Lei brasileira que regula as atividades de tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e privacidade.



Proteção de Dados

Estratégias de Proteção

Criptografia
Utilize serviços e aplicativos que ofereçam criptografia de ponta a ponta.

Controle de acesso
Compartilhe informações apenas com pessoas e serviços confiáveis.

Configurações de privacidade
Revise e ajuste as configurações de privacidade em redes sociais e aplicativos.



Exclusão segura
Apague dados sensíveis de forma segura quando não forem mais necessários.

Termos de uso e políticas de privacidade
Leia atentamente antes de concordar com o compartilhamento de dados.

Segurança em Redes e Dispositivos

Segurança em Redes - Redes Wi-Fi

Use senhas fortes e WPA3 quando disponível. Evite redes públicas para acessar dados sensíveis.

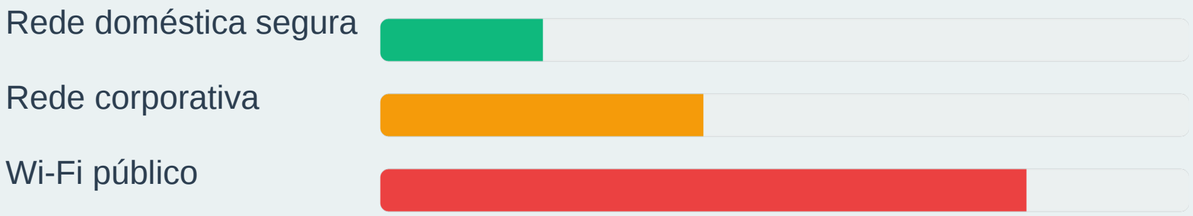
VPN (Rede Privada Virtual)

Use VPN para criptografar sua conexão, especialmente em redes públicas ou não confiáveis.

Segmentação de rede

Separe dispositivos IoT e convidados da sua rede principal para limitar riscos.

Níveis de Risco em Redes



Configuração de roteadores

Altere senhas padrão, mantenha o firmware atualizado e desative acesso remoto desnecessário.

Segurança em Redes e Dispositivos

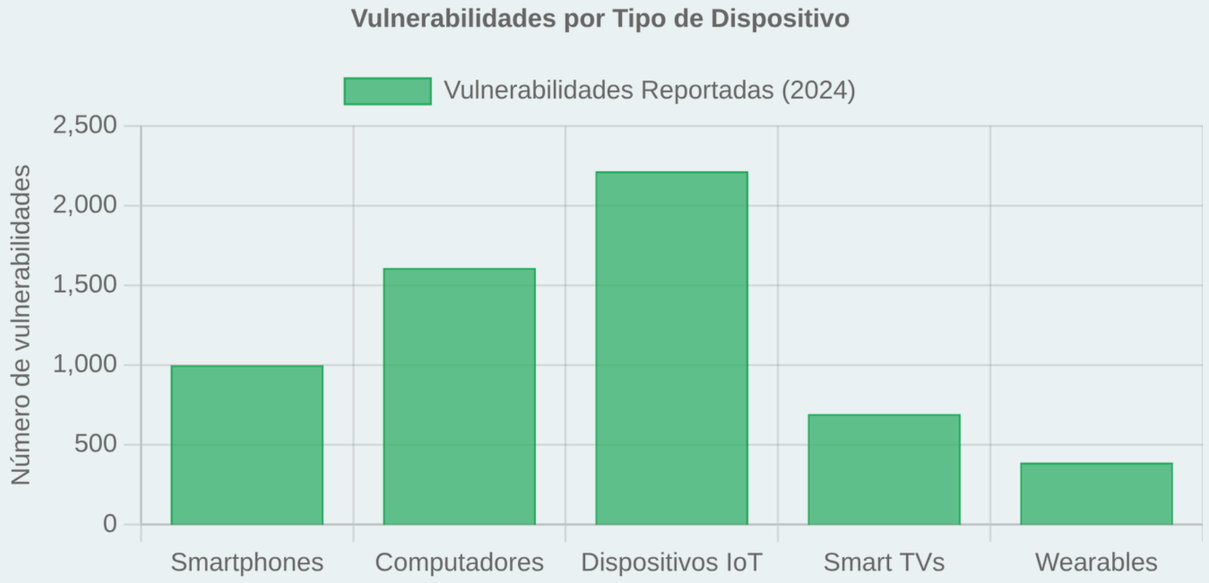
Segurança em Dispositivos

Smartphones e tablets
Mantenha o sistema operacional e aplicativos atualizados.
Use bloqueio de tela e criptografia de dispositivo.

Computadores
Instale atualizações de segurança regularmente.
Use software antivírus e firewall.

Dispositivos IoT
Altere senhas padrão, atualize firmware e
desative recursos desnecessários.

Armazenamento externo
Criptografe dispositivos de armazenamento externo que
contenham dados sensíveis.



Cultura de Segurança

O que é Cultura de Segurança?

Conjunto de valores, conhecimentos, atitudes e comportamentos compartilhados que priorizam a segurança da informação em todos os níveis.



Pilares da Cultura de Segurança

Educação contínua
Manter-se informado sobre novas ameaças e práticas de segurança.

Consciência de riscos
Reconhecer potenciais ameaças e vulnerabilidades no dia a dia.

Responsabilidade compartilhada
Entender que a segurança é responsabilidade de todos, não apenas de especialistas.

Melhoria contínua
Adaptar-se constantemente às novas tecnologias e ameaças.

Cultura de Segurança

Comportamentos Seguros

Verificar antes de clicar

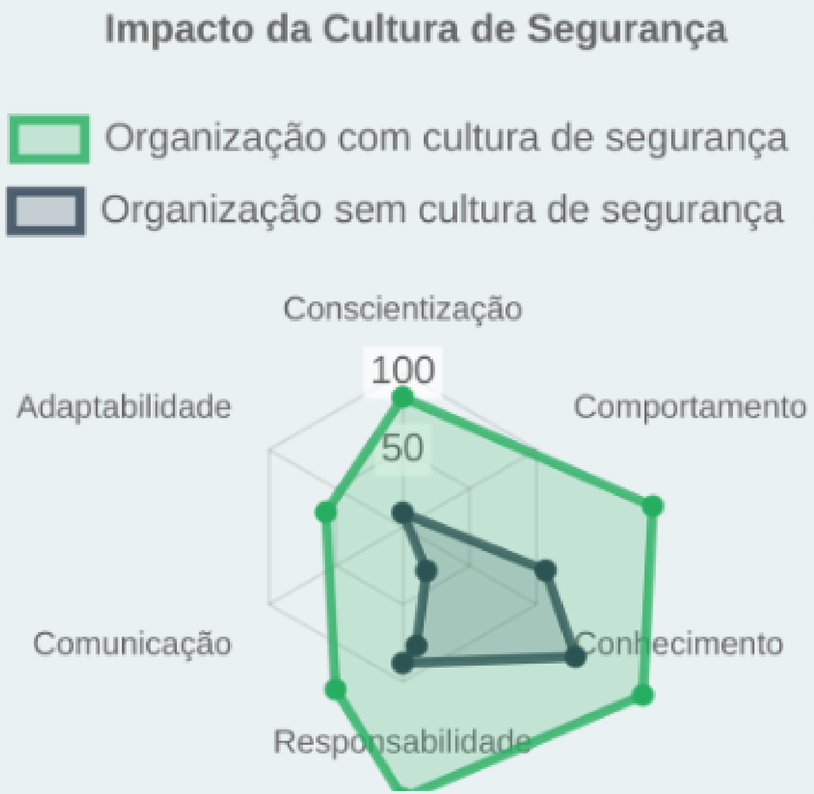
Analise links e anexos antes de abri-los, mesmo que pareçam vir de fontes confiáveis.

Questionar solicitações incomuns

Desconfie de pedidos urgentes de informações sensíveis, mesmo que pareçam legítimos.

Reportar incidentes

Comunique imediatamente qualquer atividade suspeita ou violação de segurança.



Principais Pontos

Segurança é um processo contínuo
Não é uma solução única, mas um conjunto de práticas constantes.

Equilíbrio é essencial
Segurança deve ser balanceada com usabilidade e praticidade.

Fator humano é crucial
A maioria das violações de segurança envolve erro humano ou engenharia social.

Adaptação constante
As ameaças evoluem rapidamente, exigindo atualização contínua.

Conclusão e Recursos

Conclusão e Recursos

Próximos Passos

1. Faça uma auditoria de segurança pessoal
2. Atualize senhas e ative autenticação de dois fatores
3. Verifique configurações de privacidade em suas contas
4. Mantenha-se informado sobre novas ameaças
5. Compartilhe conhecimentos com amigos e familiares

Recursos para Aprendizado

Continue seu aprendizado sobre cybersegurança com estes recursos confiáveis:

STALLINGS, William. Segurança em redes de computadores.

CERT.br - Cartilhas e guias de segurança na internet

KASPERSKY Academy - Materiais educativos online

Canal "Segurança Legal" (YouTube e podcast)

OWASP Foundation (https://owasp.org)