NEES

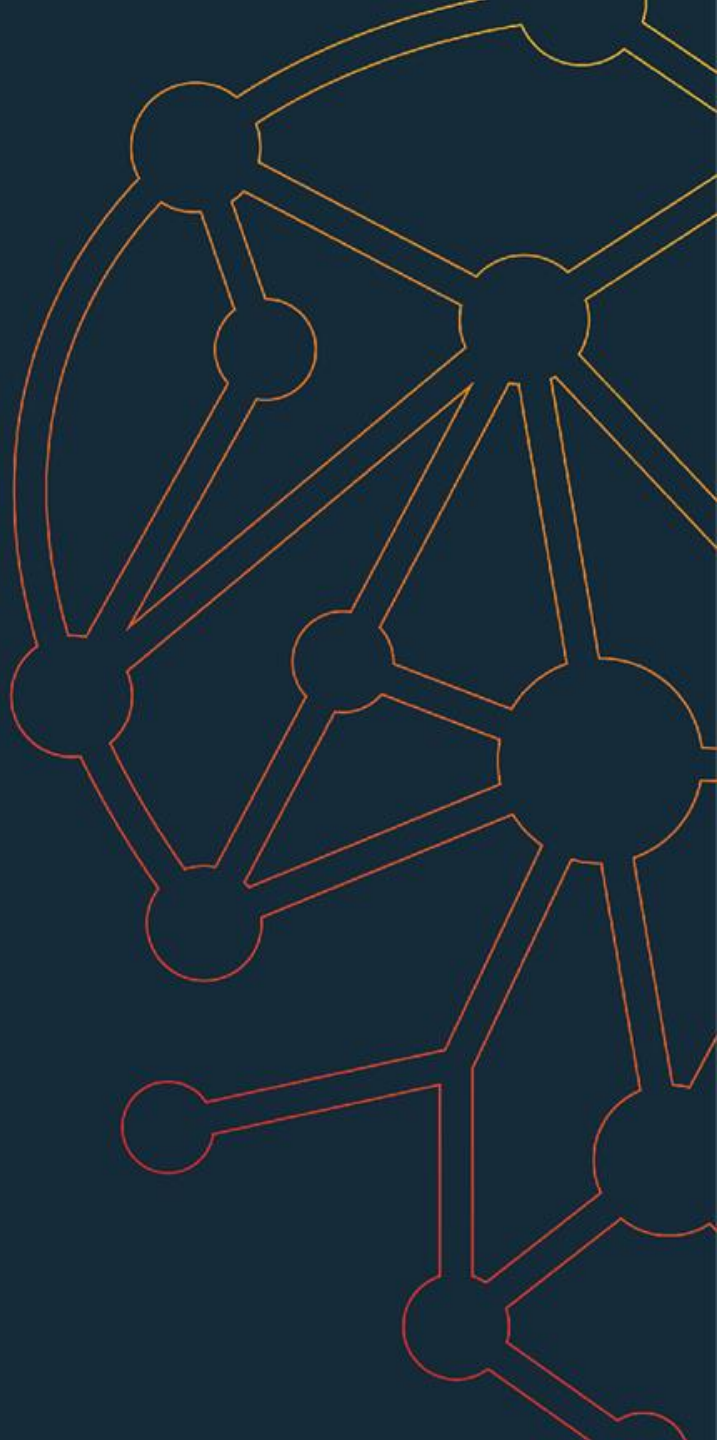
NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

NEES

NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

Segurança da Informação Conceitos e Práticas

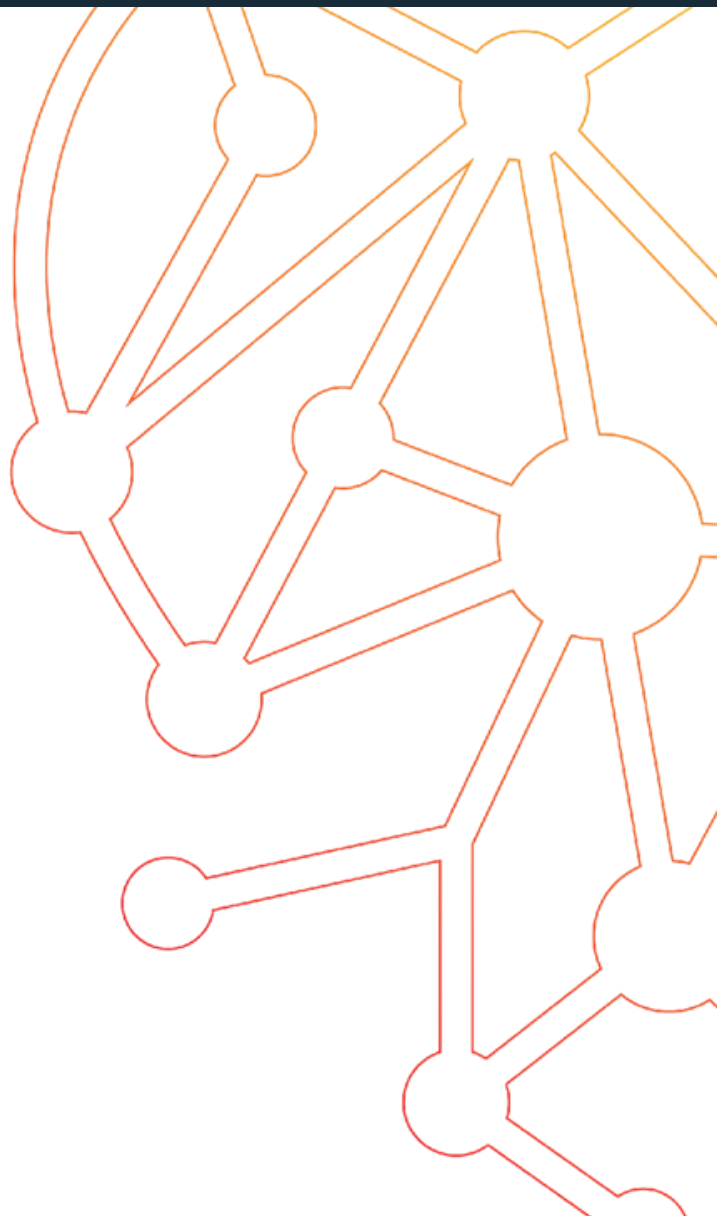
Entenda os fundamentos e como se proteger no mundo digital



NEES
NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

Por que a Segurança da Informação é importante?

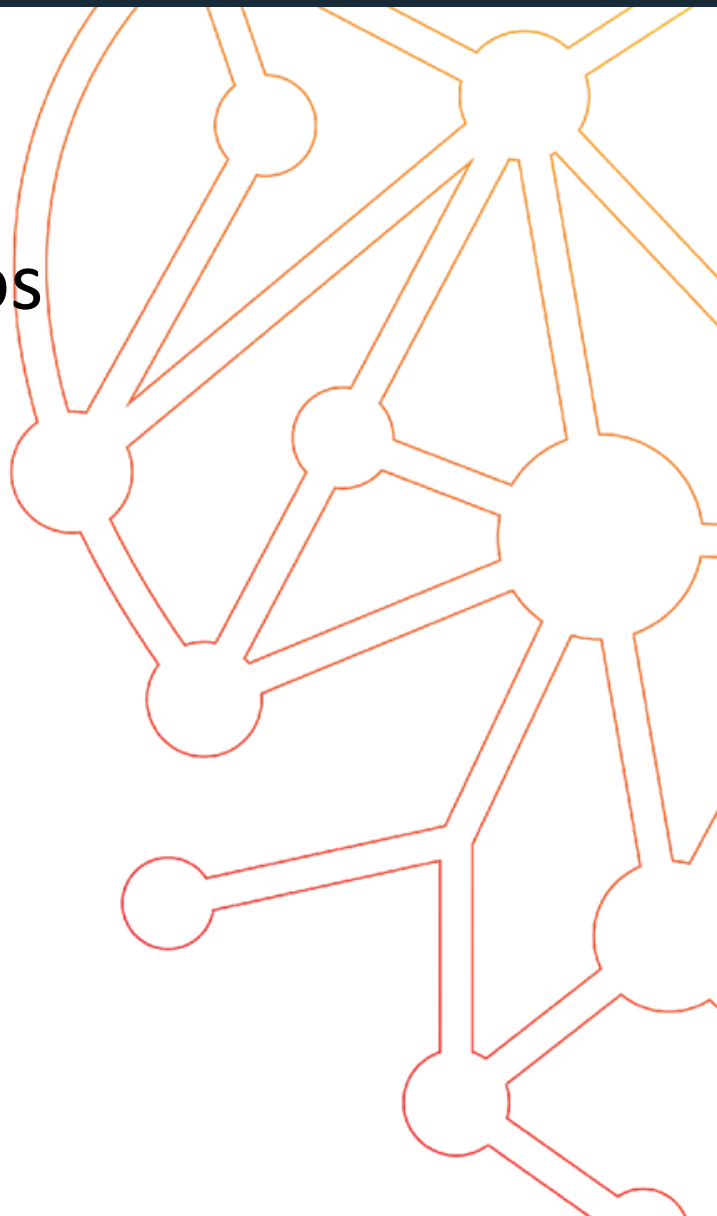
- Crescimento de ataques cibernéticos
- Exposição de dados pessoais e corporativos
- Impactos financeiros e reputacionais
- Compliance com leis (LGPD, GDPR, etc.)



NEES
NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

O que é Segurança da Informação?

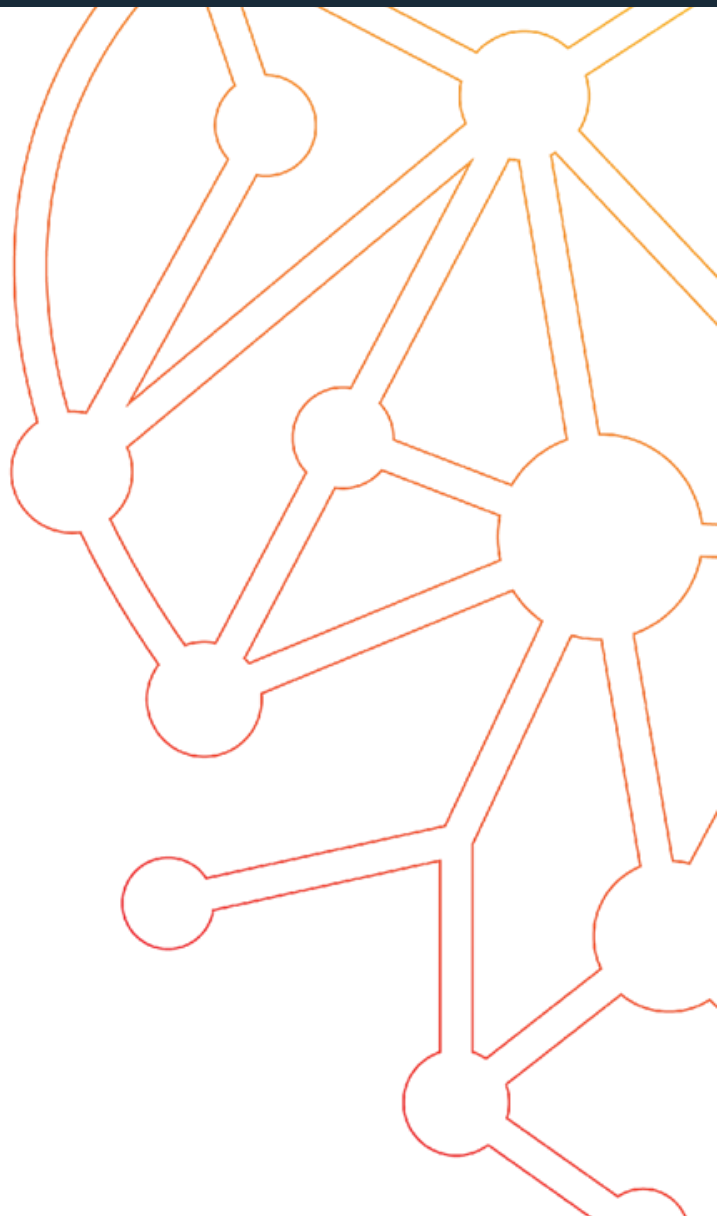
- Definição: proteção da informação contra acessos não autorizados, alterações e destruição
- Pilares da Segurança (CID):
  - Confidencialidade
  - Integridade
  - Disponibilidade



NEES NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

Tipos de ameaças

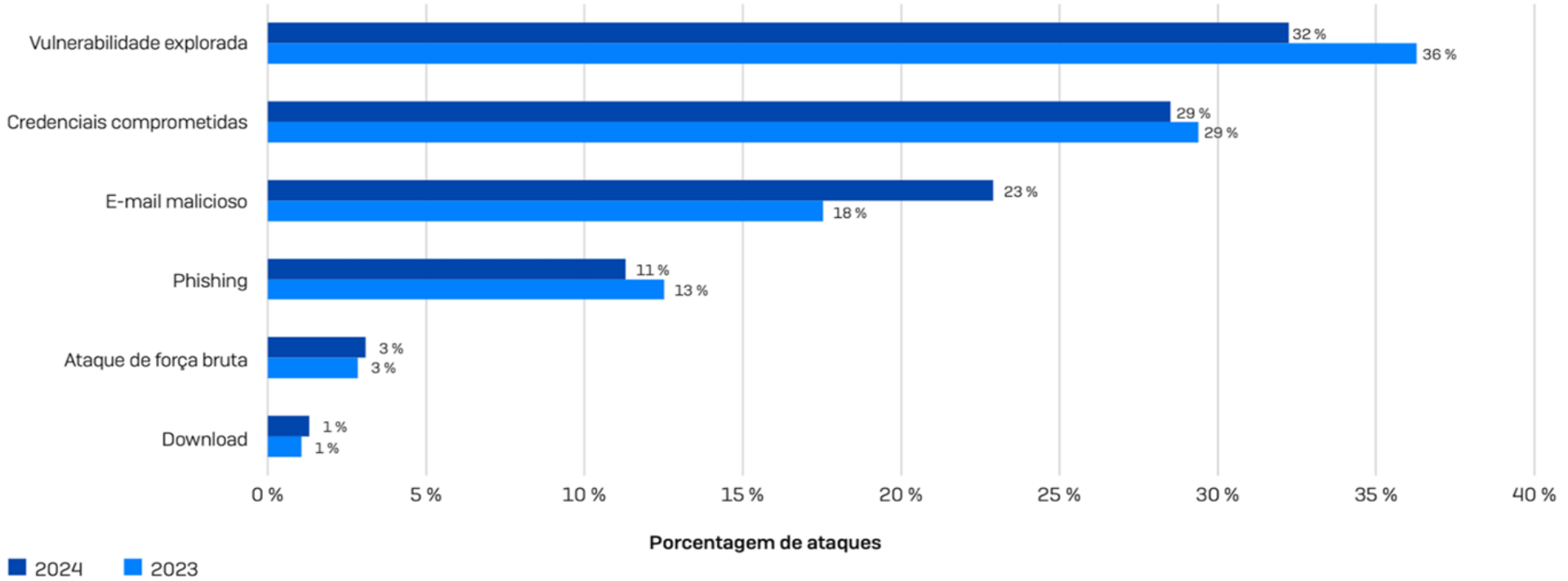
- Malware (vírus, ransomware, spyware)
- Phishing e engenharia social
- Ataques de negação de serviço (DDoS)
- Vazamento de dados
- Ameaças internas



NEES NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

TLP:CLEAR

Causas primárias dos ataques de *ransomware*



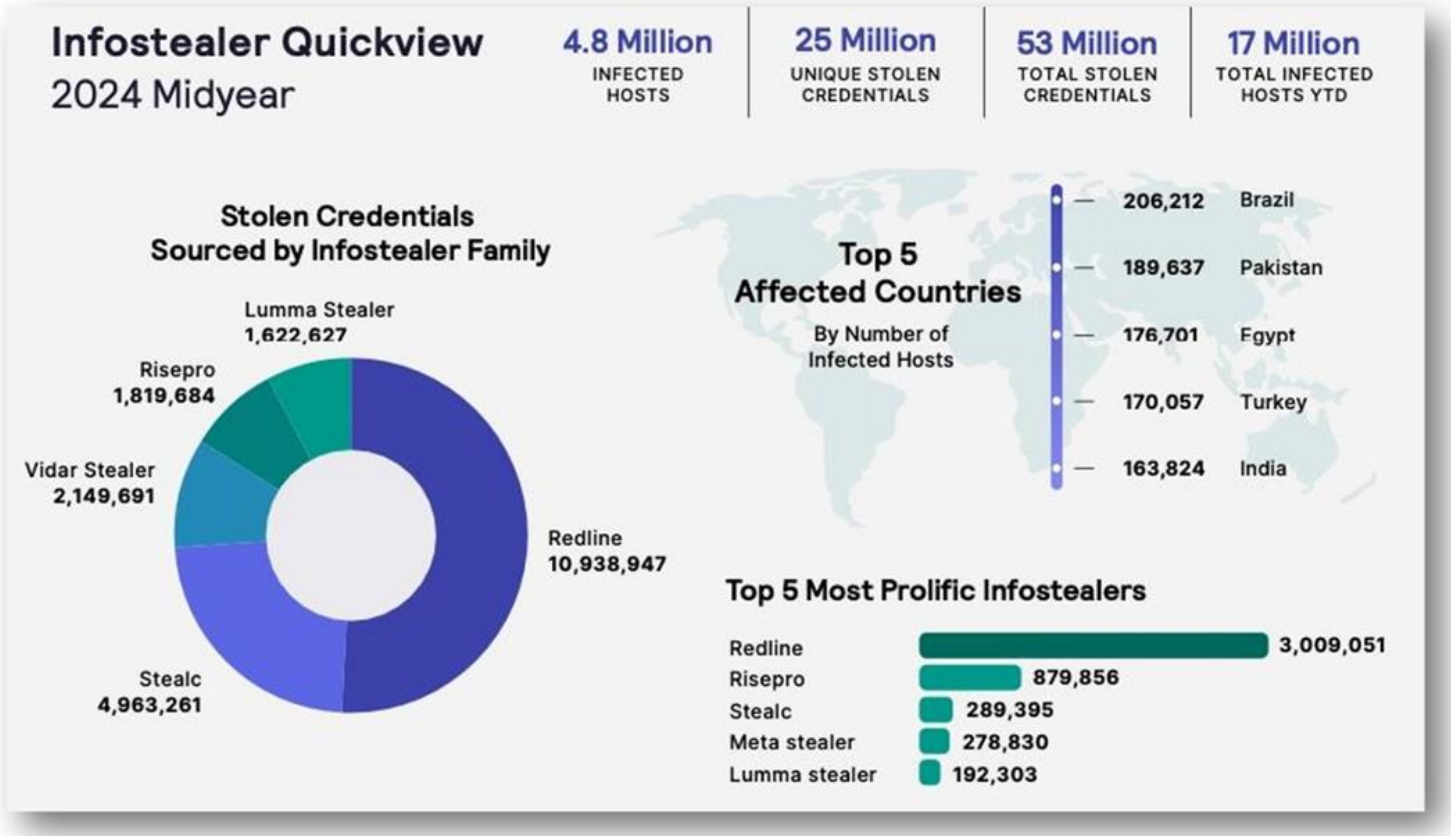
Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. n=2.974 organizações atingidas por ransomware.

Fonte: https://www.sophos.com/pt-br/content/state-of-ransomware

NEES NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

TLP:CLEAR

Causas primárias dos ataques de *ransomware*

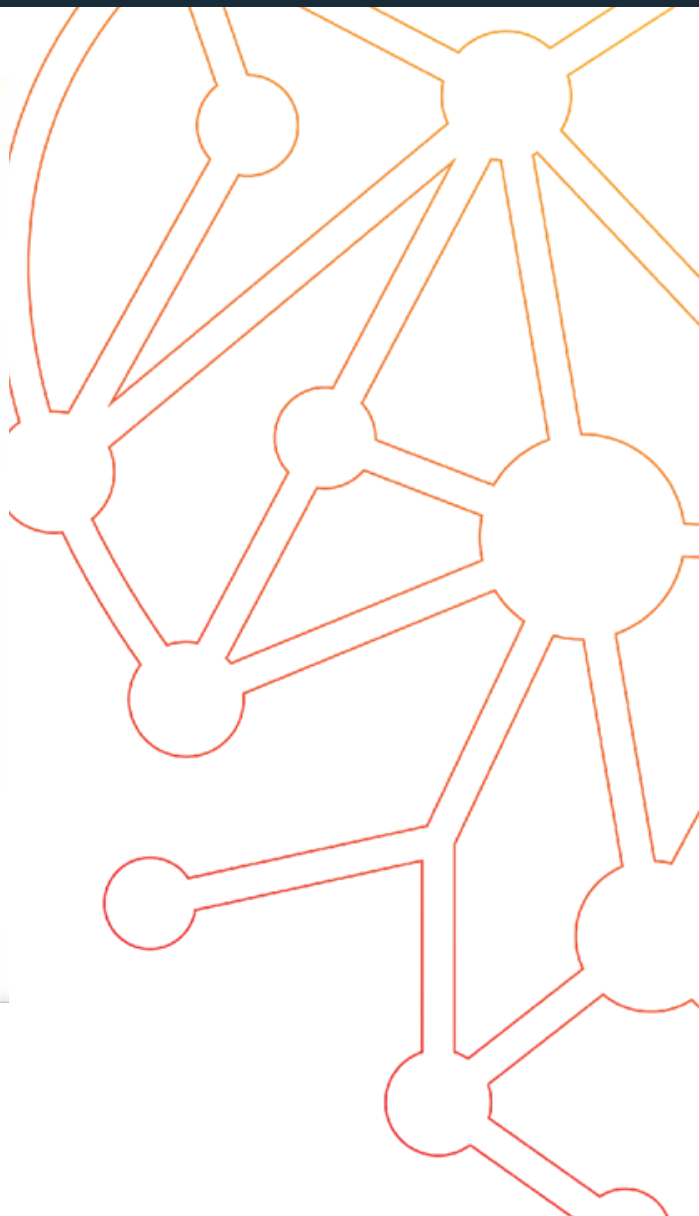


Fonte: https://go.flashpoint.io/ransomware_survival_guide

NEES NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

Boa práticas de Segurança

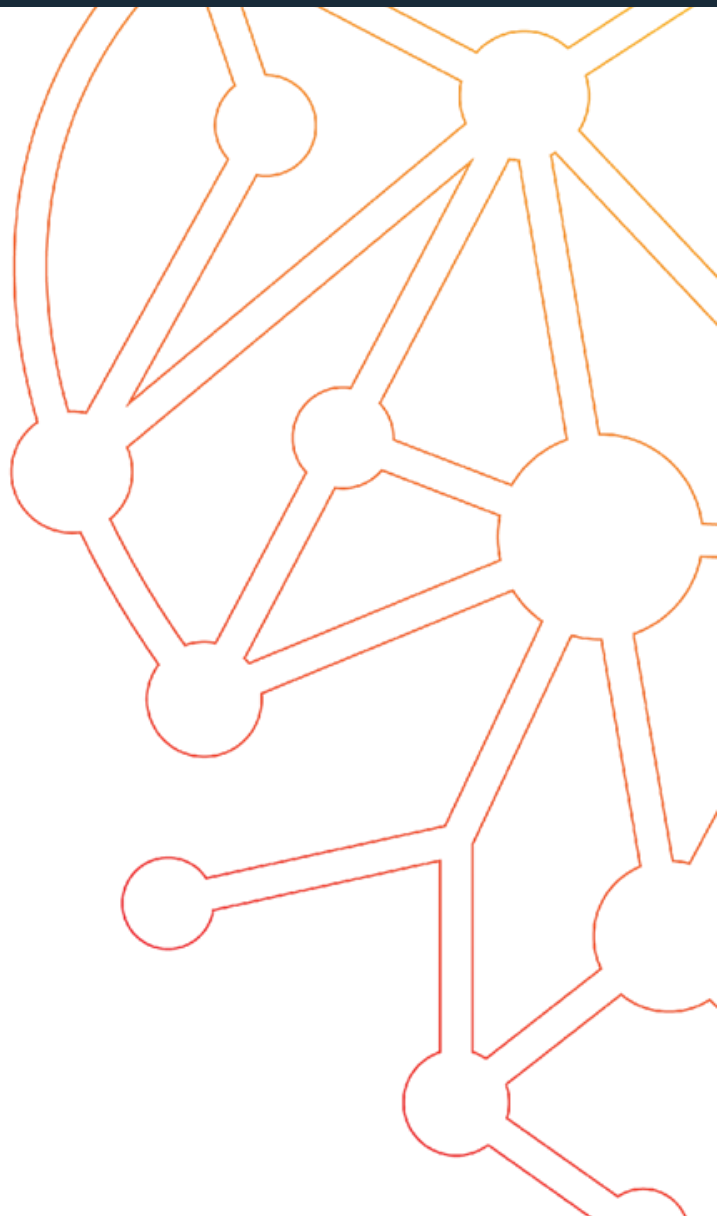
	Medida
Controle de Acesso e gestão de identidade	• **Implementar autenticação com múltiplos fatores** • Adequar permissões ao mínimo necessário (Privilégio Mínimo)
Gestão de Vulnerabilidades	• **Manter equipamentos e sistemas atualizados** - priorizar sistemas expostos e vulnerabilidades ativamente exploradas
Reduzir superfície de ataque	• **Segmentar** a rede • **Desativar** serviços que **não são usados** • **Não expor** serviços e dados desnecessariamente na Internet
Backup	• **Fazer e testar *backups* periodicamente** • **Proteger** contra acesso e modificação não autorizada
Conhecer e monitorar o ambiente	• **Conhecer o que é padrão no ambiente e monitorar:** - *logins* em contas de acesso remoto - *logins* em contas com privilégios de administração - criação de contas de usuário - tráfego de saída - grandes quantidade de dados ou conexões muito longas
Pessoas – Treinamento e conscientização	• **Treinar colaboradores para que saibam reconhecer e reportem:** - *phishing* e outros potenciais ataques de engenharia social - infecção por *malware*
Processos e procedimentos	• **Ter um plano de resposta a incidentes**



NEES
NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

Cultura de Segurança

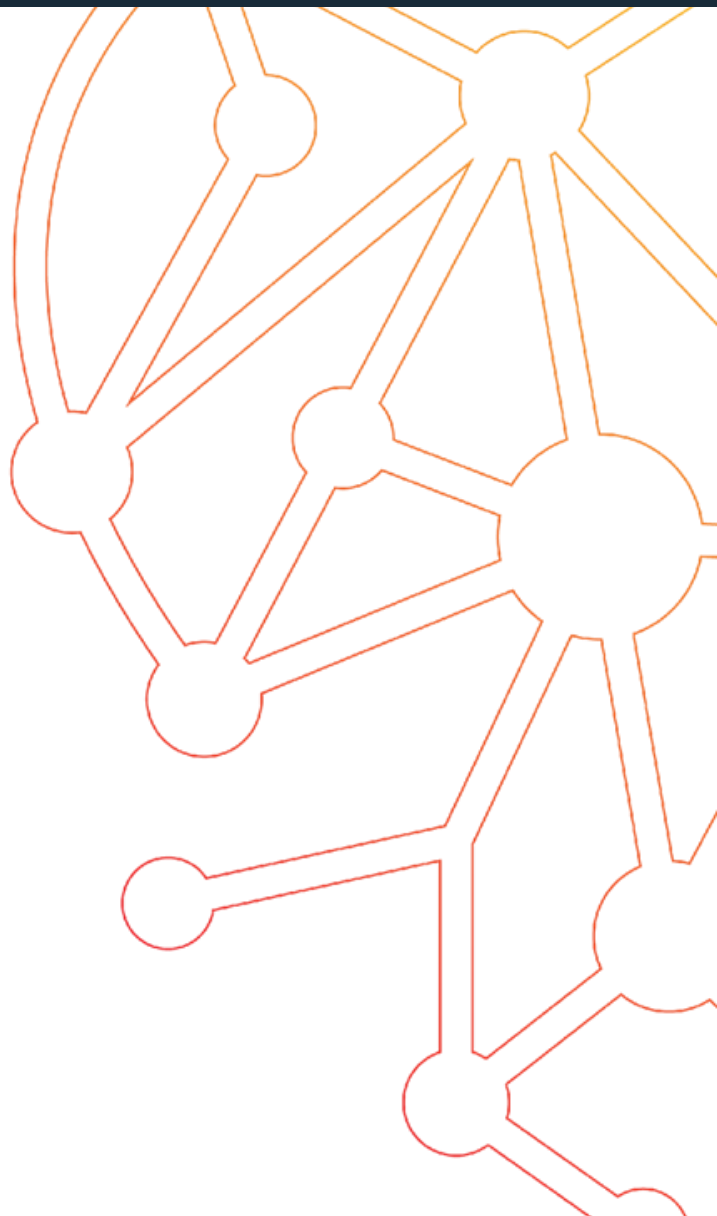
- Treinamento e conscientização de colaboradores
- Simulações de phishing
- Comunicação interna efetiva
- Segurança no dia a dia



NEES
NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

Segurança da nuvem e dispositivos móveis

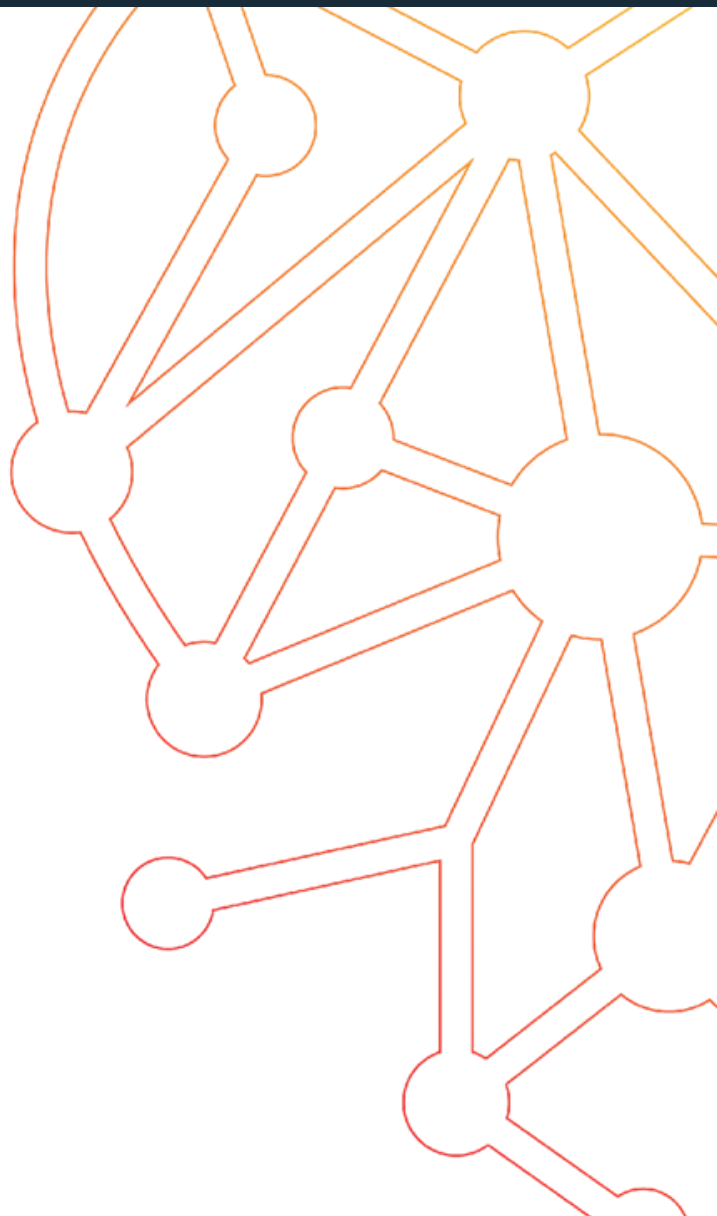
- Uso seguro de serviços em nuvem (autenticação, criptografia)
- Proteção de dispositivos móveis e BYOD
- Cuidados com redes públicas (shopping, aeroporto etc)



NEES NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

Conformidade e regulamentações

- **LGPD (Brasil)**
- GDPR (Europa)
- **ISO 27001**
- **Governança de TI**



NEES NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

NEES

NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

NEES

NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

NEES
NÚCLEO DE EXCELÊNCIA EM TECNOLOGIAS SOCIAIS

Obrigado!