CEARÁ
GOVERNO DO ESTADO
VICE-GOVERNADORIA

CTIGI

CARTILHA

Dicas de Segurança da Informação

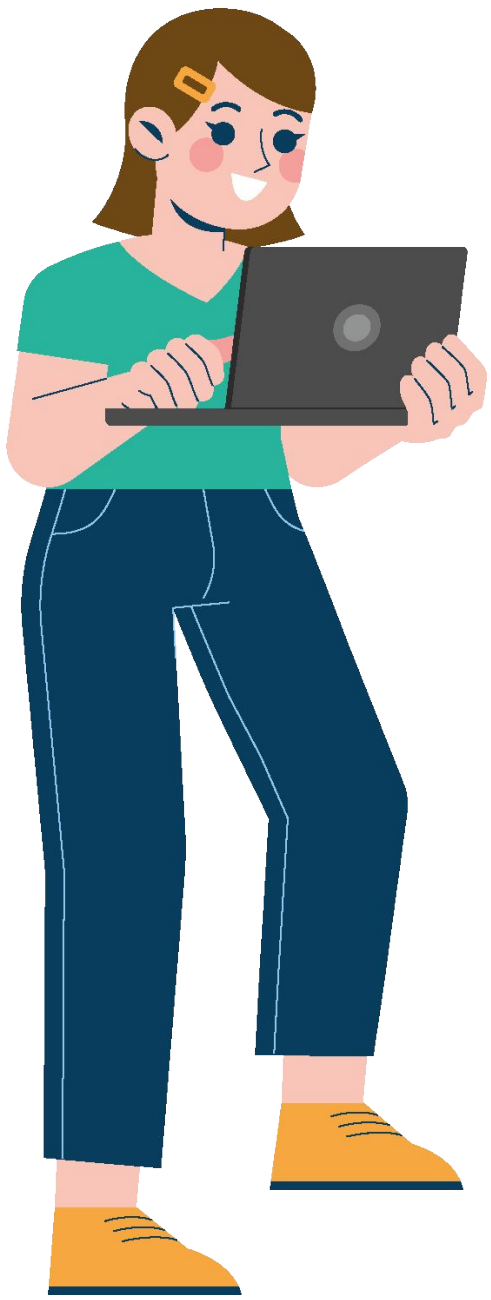
Conceitos importantes e boas práticas

Edição 1
08/01/2026

Antes de prosseguirmos, vamos entender alguns pontos essenciais:

O que são informações?

Na área de Cibersegurança, **Informações** nada mais são do que **Dados que possuem um certo valor, seja ele estratégico, financeiro ou pessoal para uma organização ou indivíduo.**



Qual ativo mais valioso de uma organização?

Quando entramos no âmbito corporativo, muitas vezes podemos achar que os ativos mais importantes para uma empresa são suas fábricas, escritórios, máquinas ou até mesmo seus funcionários, entretanto, a grosso modo, tudo isso pode ser substituído, mesmo que com muito esforço.

Ao longo dos últimos anos, assim como descreve Kevin Mitnik, considerado um dos maiores especialistas em cibersegurança nos EUA, com o avanço das tecnologias e de ataques cibernéticos, **as informações passaram a ser considerada como o maior ativo para uma organização**, pois dados como lista e dados de clientes, planos de novos produtos e projetos, dados de P&D, dentre outros, **estão ligados diretamente aos processos organizacionais e as tomadas de decisões no nível mais alto de uma empresa**, logo sua perda ou roubo, pode levá-la a falência de fato, portanto **devem ser protegidas a qualquer custo.**

O que é a Segurança da Informação (SI)?

Também pode ser considerada como Cibersegurança, é um conjunto de **práticas, políticas e tecnologias usadas para proteger dados e sistemas contra acessos não autorizados, alterações ou destruições.**

A Segurança da Informação gira em torno de que?

A SI tem como objetivo garantir 3 principais pilares:

- **Confidencialidade** – garante que apenas pessoas autorizadas tenham acesso às informações;
- **Integridade** – assegura que os dados permaneçam sem alterações indevidas até o final da sua vida útil;
- **Disponibilidade** – busca garantir que os sistemas e dados estejam disponíveis sempre que necessários, evitando interrupções.

Tais pilares buscam minimizar riscos que possam comprometer a continuidade das operações de uma organização.

Investimento em Cibersegurança

Dada a crescente relevância da segurança da informação, empresas que desejam se proteger investem de forma significativa nessa área.

Organizações que negligenciam essa necessidade enfrentam riscos elevados de ataques cibernéticos.

Estima-se que os investimentos globais em cibersegurança alcancem cerca de **US$ 212 bilhões até o final de 2025**, refletindo a urgência e importância de proteger dados em um mundo cada vez digital.

Papel do Usuário na Cibersegurança

Mesmo com avanço das tecnologias de proteção, uso de firewalls, equipes especializadas de Cibersegurança e treinamentos constantes, **o elo mais fraco ainda é o fator humano, pois é a partir de um "ação humana" que muitos ataques/ vazamentos ocorrem.**

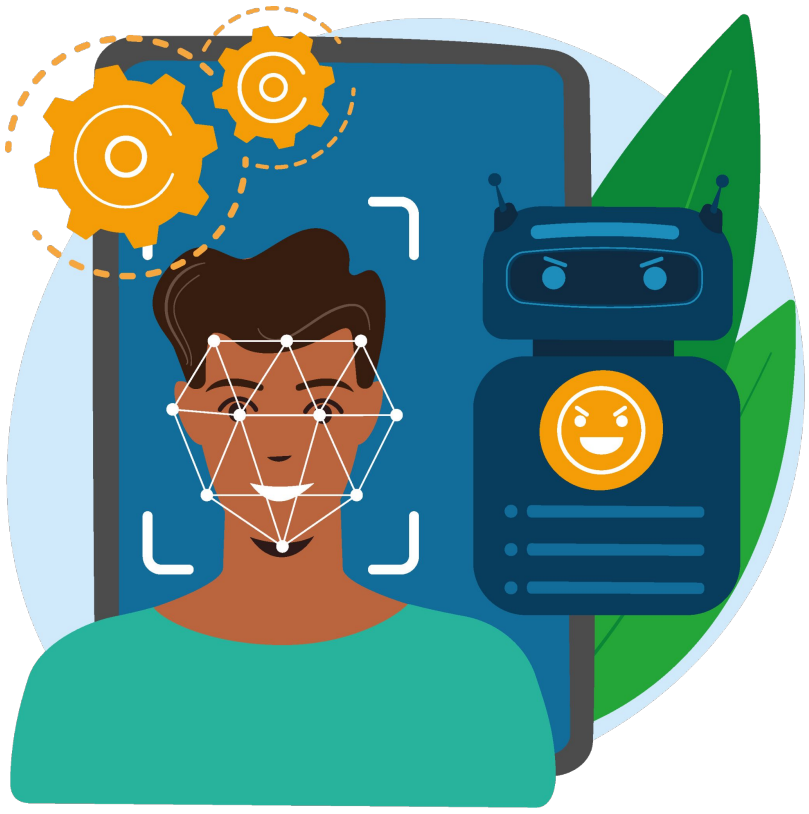
Logo, é **extremamente fundamental que o usuário adote uma postura ativa**, seguindo boas práticas e hábitos seguros no dia a dia pessoal ou corporativo.

Inteligência Artificial e Segurança de Dados

IA x Cibersegurança:

A Inteligência Artificial tem transformado positivamente o nosso dia a dia. Ela já está presente em ferramentas que agilizam diagnósticos médicos, automatizam tarefas repetitivas, otimizam processos empresariais e até ajudam a identificar fraudes em tempo real.

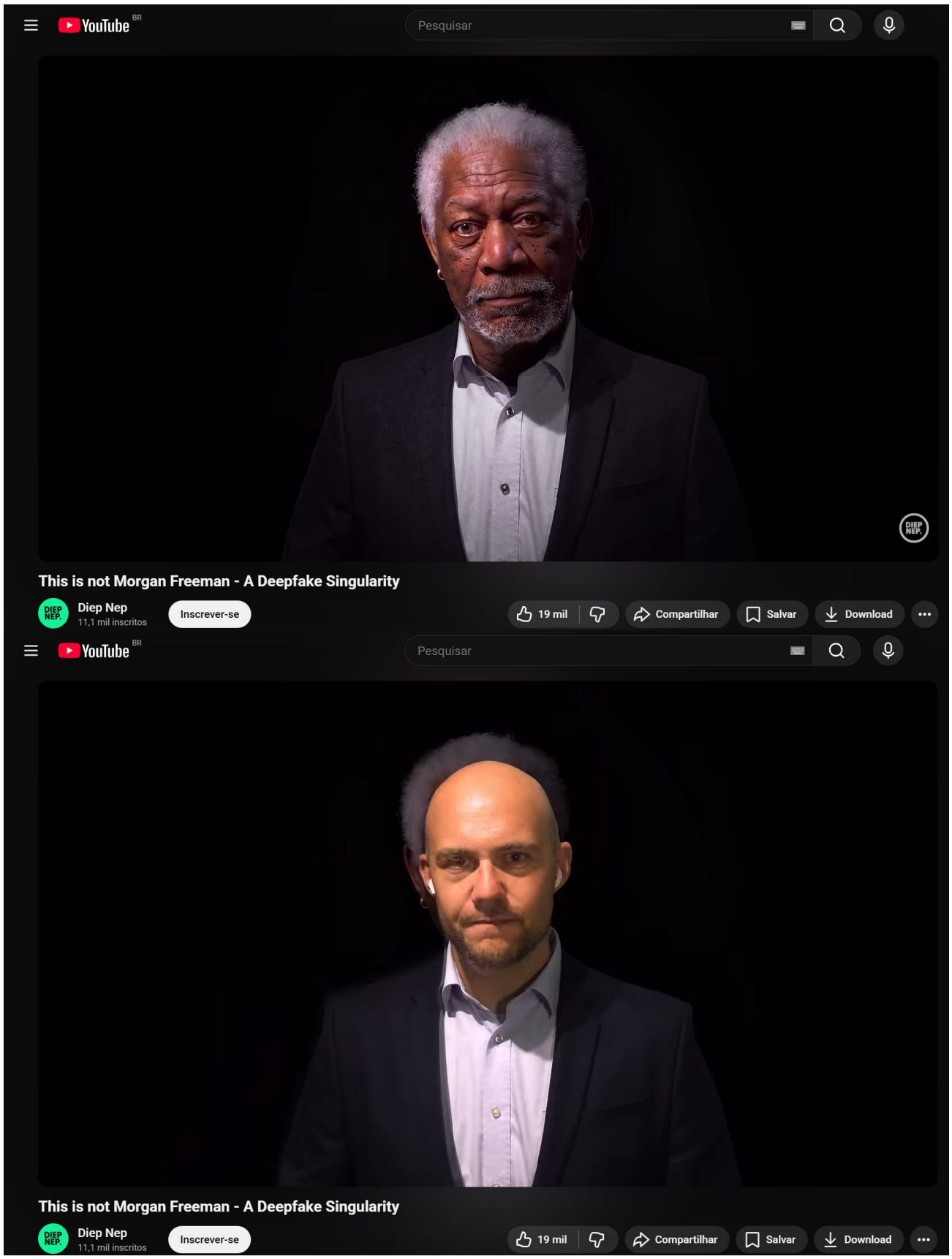
No campo da cibersegurança, a IA também atua de forma poderosa: **detectando comportamentos suspeitos, fortalecendo sistemas de defesa e ajudando a responder mais rápido a ameaças.**



Com os benefícios, vêm os desafios...

Infelizmente, assim como qualquer tecnologia, **a IA também pode ser usada de forma maliciosa.** Hackers têm explorado seus recursos para **automatizar ataques, criar conteúdos falsos hiper-realistas, clonando faces, gestos e até vozes**, essas são as famosas **DeepFakes**.

Exemplo de DeepFake



Este não é Morgan Freeman

Verificar sempre fontes de vídeos e áudios recebidos por e-mail ou redes sociais.

Legislação no Brasil e estaduais

LGPD (Lei nº 13.709/2018)

- Proteção de Dados Pessoais.

- Regras para tratamento de Dados Pessoais, visando proteger a privacidade e segurança dos indivíduos

- Implicações em Cibersegurança

Marco Civil (Lei nº 12.965/2014)

- Princípios, Garantias, Direitos e Deveres para o uso da internet

- Aspectos relacionados à proteção de dados e segurança das informações na rede

Carolina Dieckmann (Lei nº 12.737/2012)

- Também conhecida como Lei de Crimes Cibernéticos

- Tipificação de crimes digitais

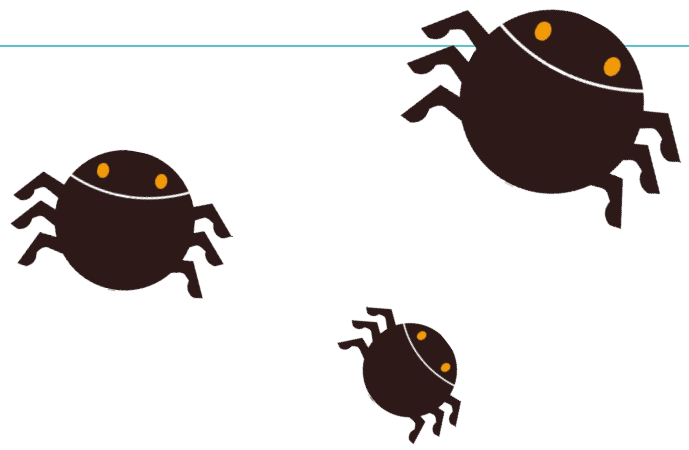
- Prevê Penalidades para tais crimes

O que são Hackers?

Embora o termo “hacker” seja frequentemente mal interpretado, **hackers nada mais são que indivíduos com alto conhecimento em computadores, redes e desenvolvimento de softwares**, não necessariamente criminosos. **Aqueles que utilizam tais conhecimento para realizar crimes virtuais, podemos classificá-los como Cibercriminosos ou ainda, Hackers Black Hat.**

Principais Ataques Hackers Atualmente

- **Engenharia Social:** Manipulação das vítimas para obter informações confidenciais;
- **Phishing:** Roubo de credenciais via e-mails enganosos. Ex: Mensagens suspeitas, solicitando informações e/ou com links clicáveis.
- **Ransonware:** Software malicioso que rouba e criptografa os dados, exigindo pagamento para resgate;
- **DoS DDoS:** Ataque para sobrecarregar servidores e derrubar sites ou sistemas;
- **Exploração de Vulnerabilidades:** Acessos não autorizados por falta de segurança;



Exemplos Reais

Engenharia Social

Situação (Exemplo comum no dia a dia)

Você recebe uma ligação ou mensagem no WhatsApp de alguém dizendo:

> *"Oi mãe/pai, troquei de número. Salva esse contato. Preciso que você me faça um PIX urgente para essa chave abaixo, depois explico!"*

Onde está o golpe?

- O golpista sempre busca se passar por alguém conhecido. (pai/mãe, responsável do banco...)
- Usa pressão emocional ("Urgente", "Explico depois")
- Solicita transferências imediatas.

Como não cair nesses golpes?

- Nunca faça transferências imediatas sem confirmar identidade.
- Ligue para números antigos para confirmar.
- Desconfie de pedidos urgentes.
- Golpistas evitam chamadas por vídeo.

Exemplos Reais

Phishing

Situação (Exemplo comum no dia a dia)

Você recebe um e-mail com a seguinte mensagem:

"Correios informa : Sua encomenda está retida. Clique no link para regularizar o pagamento."

Onde está o golpe?

- Uso de nomes de empresas conhecidas. (Correios, Mercado Livre, Bradesco...)
- Links falsos que imitam sites oficiais.
- Solicitação de dados pessoais ou pagamentos de taxas no link enviado.

Como não cair nesses golpes?

- Verifique sempre o remetente da mensagem, golpistas usam contas com nomes enganosos. (br4desco-financeiro@..., m3rc4ado_livre@.....)
- Evite clicar em links recebidos por e-mail ou SMS.
- Desconfie de erros de escrita.
- Empresas legítimas não cobram taxas enviadas por links de e-mail aleatoriamente.

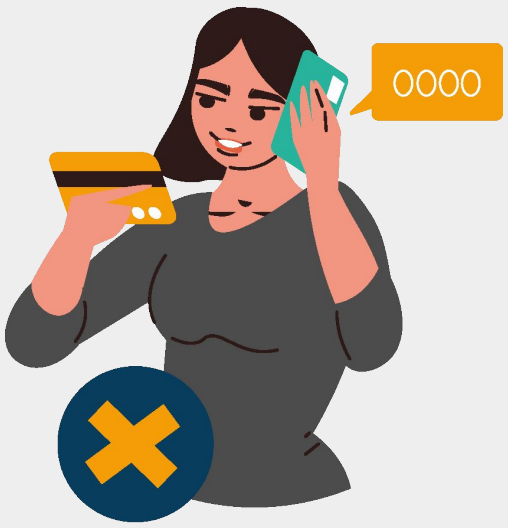
Exemplos Reais

Exploração de Vulnerabilidade *(Rede Social Invadida)*

Situação (Exemplo comum no dia a dia)

O perfil de uma pessoa conhecida no Instagram é Hackeado e o logo após começam a aparecer Stories contendo:

> *"Pessoal, estou vendendo esse iPhone/Notebook por um preço imperdível via PIX, só hoje."*

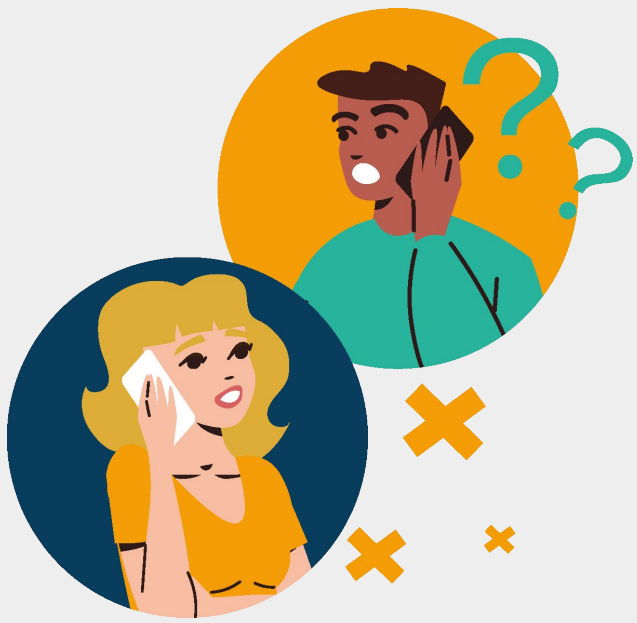


Onde está o golpe?

- O perfil é real, com fotos, seguidores, então traz uma veracidade maior para o golpista.
- Preços muito abaixo do mercado.
- Pressão para compra imediata (Só hoje)
- Pagamentos apenas por PIX, sem nota ou garantia.

Como não cair nesses golpes?

- Confirme com a pessoa em outros canais, como ligação ou WhatsApp.
- Desconfie de uma grande quantidade de Stories aleatoriamente de um perfil que não tem esse histórico.
- Preços muito abaixo são sinais clássicos de golpe.
- Perfis hackeados costumam desativar comentários.



Casos Reais de Ataques no Brasil

Supremo Tribunal de Justiça – STJ
(2020)

- Ataque Ransonware
- Sistema fora do ar durante dias
- Hackers pediram pagamento em Criptomoedas para liberar os dados

Americanas
(2022)

- Ataque cibernético de Negação de Serviço
- Site fora do ar durante 5 dias
- Prejuízo estimado em quase R$ 1 Bilhão

Unimed
(2025)

- Interceptação do sistema de comunicações Kafka e chatbot Sara
- Possível vazamento de 140 mil mensagens contendo dados de mais de 14 milhões de clientes

Algumas Estatísticas Importantes

24% **dos brasileiros**

já sofreram de golpes digitais nos últimos

12 meses.

Fonte: *DataSenado, 2024*

O Brasil registra

4.600

tentativas de golpes

por hora.

Fonte: *Poder360, Datafolha e Fórum Brasileiro de Segurança Pública, 2024*

4 **em cada** **10**

brasileiros já foram vítimas de golpes virtuais, e a preocupação das empresas

cresceu **58%**

em apenas um ano.

Fonte: *Serasa Experian, 2024*

A seguir, 8 boas práticas de Cibersegurança para você tornar seus dados e dispositivos mais seguros

1. Senhas Fortes e Seguras

- Utilize senhas fortes, com combinações de letras maiúsculas/minúsculas, números e caracteres.
- Evite a reutilização de senhas para vários sites/apps diferentes e, principalmente, o compartilhamento de senhas com outros.
- Outra forma interessante é utilizar um gerenciador de senhas para armazenar e organizar todas as suas credenciais, como KeeWeb ou KeePass.

2. Autenticação Two-Factor (2FA ou Dois-Fatores)

- Utilize a autenticação de Dois Fatores para adicionar mais uma camada de segurança para os acessos às suas contas.
- Através deste recurso, seus logins se tornam mais seguros, visto que não basta ter apenas as credenciais de acesso para logar, existem ainda outra etapa de verificação.
- Grande maioria dos sites/softwares hoje em dia já possuem integração com 2FA. É interessante que usemos um software próprio para isso, como o Google Authenticator, ao invés de códigos via SMS.

3. Atualizações do Sistema Operacional e Softwares

- Mantenha sempre seus sistemas e aplicativos atualizados, pois atualizações trazem não só novidades e correções de bugs, mas também corrigem falhas de segurança, o que é crucial para manter seus dados mais seguros.
- Ative as atualizações automáticas sempre que está configuração estiver disponível.

4. Backup Regular de Dados

- Realizar frequentemente o backup dos seus principais documentos e arquivos é algo extremamente importante e recomendável, uma vez que, em caso de perdas por alguma situação inesperada, você terá uma cópia guardada.
- O mais recomendado é utilizar o backup em nuvem por aplicações como Google Drive ou One Drive, mas também é possível utilizar um HD Externo ou Pen Drive. Os usuários também devem utilizar as Pastas Compartilhadas na Rede para realizar backups e evitar de salvar arquivos críticos localmente.

5. Proteção contra Malwares

- Malwares são considerados quaisquer softwares maliciosos criados para causar danos a dispositivos ou redes, como roubar informações, interromper sistemas ou usar recursos de forma indevida. Eles podem se apresentar de diferentes formas, como Vírus e Trojans, e geralmente se espalham pela internet disfarçados de aplicações legítimas.
- Portanto, busque sempre utilizar softwares de antivírus/antimalwares em seus dispositivos, realizando verificações regulares para detectar possíveis ameaças presentes no sistema.

6. Downloads Seguros

- Evite realizar downloads de sites/lojas desconhecidos, buscando sempre priorizar fontes confiáveis como as lojas padrões dos dispositivos (App Store, Google Play Store, Microsoft Store).
- Na internet existem diversos sites que funcionam como repositórios para downloads de outras aplicações, como o famoso “Baixaki”, entretanto muitos desses sites colocam aplicações indesejadas dentro dos instaladores dos programas. Portanto, buscar o download no site oficial da aplicação é a solução mais segura.

7. Segurança nos E-mails

- Verifique sempre o cabeçalho dos e-mails que você recebe, especialmente o campo de remetente, é muito comum que criminosos coloquem nomes similares a empresas com o objetivo de enganar.
- Evite clicar em links e baixar anexos de e-mails de remetentes desconhecidos, você pode estar acessando ou baixando um malware para seu sistema.
- Desconfie de propagandas muito exageradas e principalmente de solicitações de informações pessoais ou financeiras.

8. Segurança em Redes

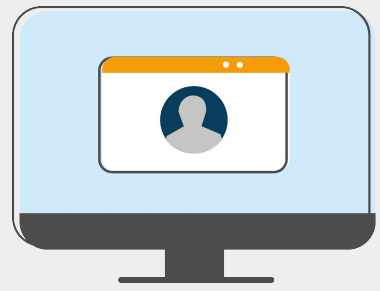
- Evite se conectar a redes Wi-Fi públicas, especialmente de locais como Shoppings e Eventos grandes. Essas redes costumam a ter baixa segurança e são alvos fáceis para atacantes interceptarem informações pessoais.
- Priorize redes protegidas por senha, e sempre possível, prefira utilizar a internet móvel do seu dispositivo quando estiver em locais públicos.

Bônus

Além disso, aqui estão alguns hábitos importantes para você adotar no dia a dia dentro do nosso órgão:

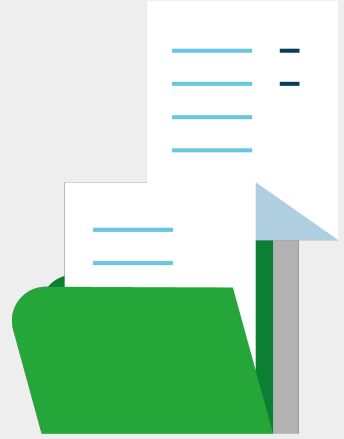
Busque sempre desligar sua máquina ao final de todo expediente;

Mantenha sua máquina bloqueada toda vez que se retirar da sua estação de trabalho;

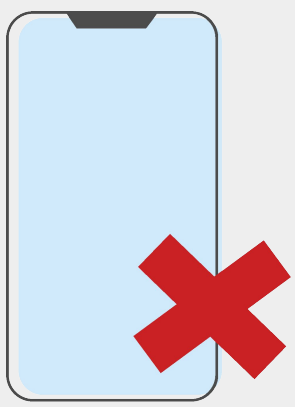


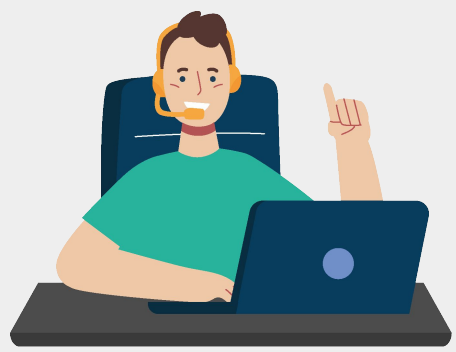
Evite compartilhar suas senhas com outros colaboradores;

Não salve arquivos pessoais, como fotos/vídeos, dentro do computador institucional;



Evite utilizar dispositivos pessoais para acessar os sistemas e dados institucionais, priorize os dispositivos fornecidos pelo órgão.





Priorize a abertura de chamados pelo E-mail ou Plataforma do Suporte
suporteti@vicegov.ce.gov.br

Educação contínua

Manter-se atualizado sobre as boas práticas de segurança da informação é fundamental para assegurar a proteção dos dados e sistemas do nosso órgão.

Com a evolução constante das ameaças cibernéticas, os usuários se tornam alvos cada vez mais frequentes de ataques sofisticados, como phishing, ransomware e malware.

Nesse contexto, **é vital que todos os colaboradores participem de treinamentos regulares e se mantenham informados sobre as últimas tendências e vulnerabilidades em segurança digital.**

Essa postura preventiva é essencial para fortalecer a defesa contra ameaças emergentes e minimizar riscos operacionais.

A segurança da informação não é responsabilidade só do setor de TI.

É de todos nós!

CTIGI AGRADECE A SUA ATENÇÃO!

CEARÁ
GOVERNO DO ESTADO
VICE-GOVERNADORIA

CTIGI
Coordenadoria de Tecnologia da Informação, Governança e Inovação

2026