Segurança de Dados, Armazenamento e Manutenção

Luiz Machado

Head de Eng. & IT Services - Cilia Tecnologia
AWS Community Builder - Security & Identity (3Y)
Líder de comunidade - @GYNSec
Criar, desenvolver e contribuir com ferramentas OpenSource

Por que a segurança de dados é tão importante ?

Se hoje você perdesse o acesso ao seu celular ou notebook, quanto da sua vida estaria comprometido?

Você já usou a mesma senha, ou uma variação dela, em mais de um serviço?

Por que a segurança de dados é tão importante ?

Dados são valiosos

Suas fotos, documentos e informações pessoais têm valor incalculável para você.

Criminosos estão atentos

Atacantes procuram constantemente formas de roubar informações pessoais.

Falhas acontecem

Dispositivos quebram. Arquivos corrompem. Backups previnem perdas permanentes.

Cumprimento de normas e regulações

Medidas básicas de segurança reduzem drasticamente os riscos.

Como armazenar dados com segurança?

Nuvem

Acesso em qualquer lugar.

Sincronização automática.

- Google Drive (15GB grátis)
- OneDrive (5GB grátis)
- iCloud (5GB grátis)

Use autenticação em dois fatores sempre!

Dispositivos Físicos

Sem dependência de internet. Controle total.

- HD Externo (ideal para backups grandes)
- SSD Externo (mais rápido, durável)
- Pen Drive (portátil, limitado)

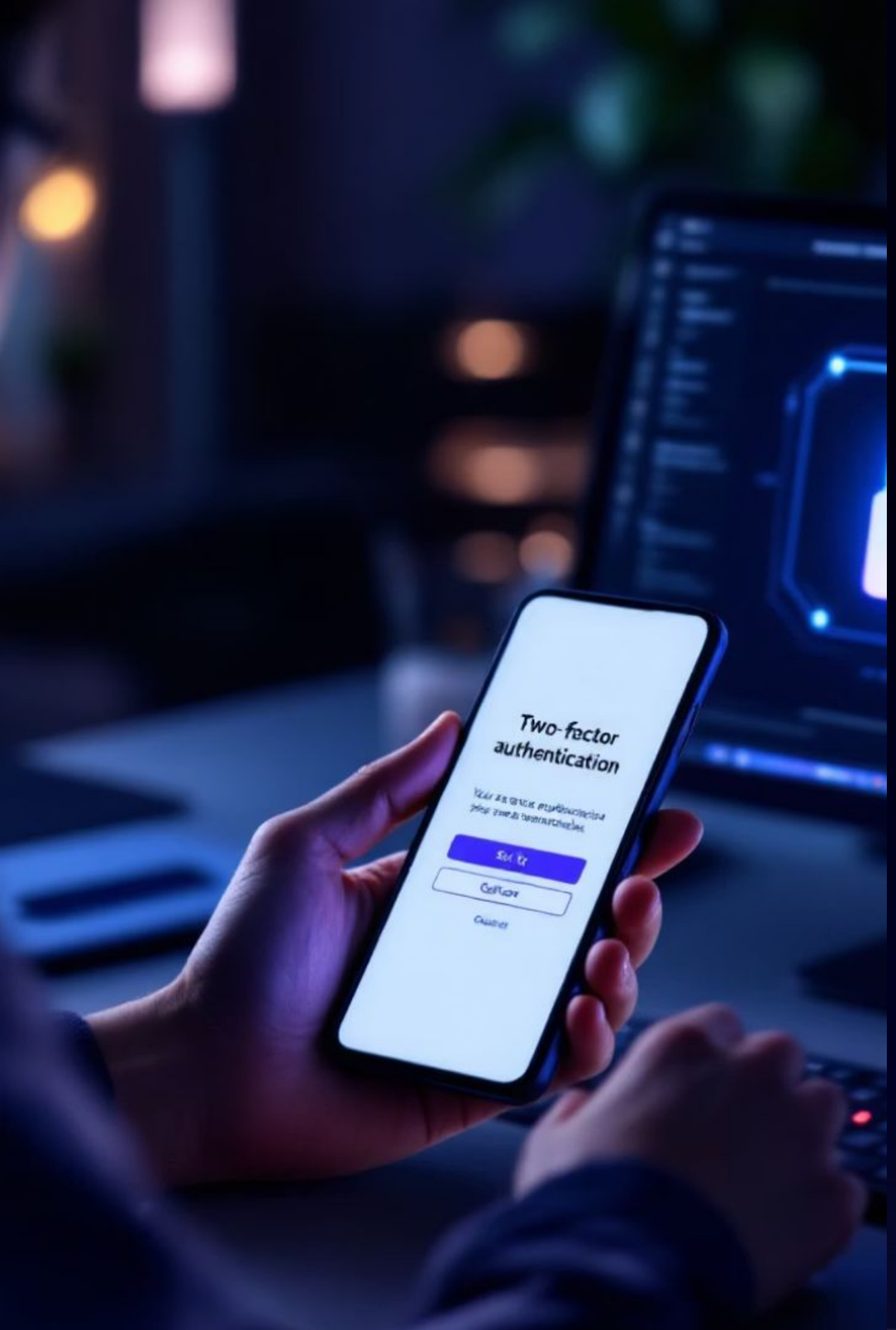
Guarde em local seguro, longe de líquidos e calor.

Dispositivos Móveis

Conveniência com riscos.

- Ative sincronização automática
- Use bloqueio de tela seguro
- Criptografe seu dispositivo

Nunca guarde dados sensíveis apenas no celular.



Boas Práticas de Segurança

Senhas Fortes

Use senhas longas com letras, números e símbolos.

Nunca repita senhas entre serviços diferentes.

Considere frases-senha: "GatoAzulCorre@Rápido22!"

Autenticação em Dois Fatores

Adiciona camada extra de segurança.

Mesmo com senha vazada, conta permanece protegida.

Use apps como Google Authenticator ou Microsoft Authenticator.

Atualizações de Sistema

Corrigem falhas de segurança conhecidas.

Configure atualizações automáticas quando possível.

Nunca ignore alertas de atualização.

Criptografia

Protege arquivos mesmo se dispositivo for roubado.

Windows: BitLocker. Mac: FileVault.

Para arquivos específicos: VeraCrypt ou AxCrypt.

Evitando Vazamentos e Acessos Indevidos

Reconheça Ameaças

Identifique emails suspeitos. Desconfie de ofertas muito boas.

Proteja Dispositivos

Ative bloqueio automático. Use senhas fortes em todos aparelhos.

Configure Privacidade

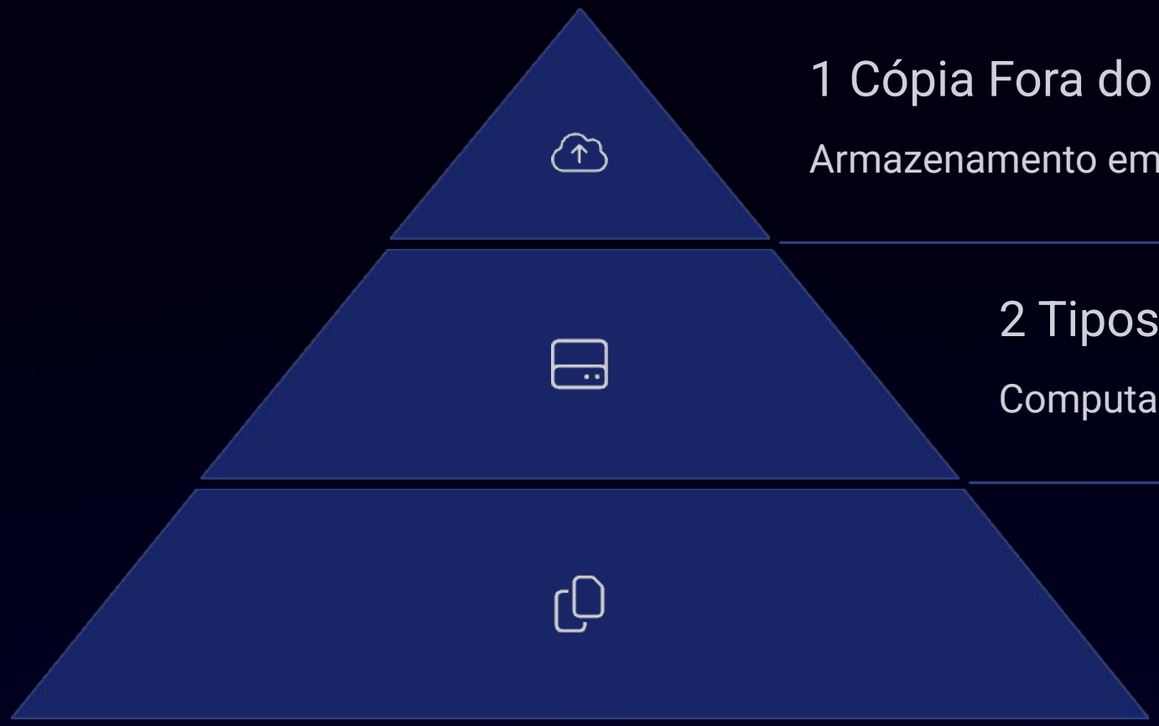
Revise permissões de compartilhamento. Limite acesso de terceiros.

Proteja Conexões

Evite Wi-Fi públicos. Use VPN para conexões sensíveis.

Lembre-se: Nunca compartilhe senhas por email ou mensagens.

A Regra 3-2-1 de Backup



1 Cópia Fora do Local

Armazenamento em nuvem ou dispositivo guardado em outro lugar

2 Tipos de Mídia

Computador + HD externo ou nuvem + dispositivo físico

3 Cópias Totais

Original + duas cópias de backup

Automatize seus backups. Configure para rodar semanalmente.

Verifique regularmente se seus backups estão funcionando corretamente.

Ferramentas Recomendadas

Tipo	Ferramenta	Custo	Facilidade
Backup	Google Drive	Gratuito (15GB)	Muito fácil
Backup	Syncthing	Gratuito	Moderado
Gerenciador de Senhas	Bitwarden	Gratuito/Premium	Fácil
Gerenciador de Senhas	KeePass	Gratuito	Moderado
Criptografia	VeraCrypt	Gratuito	Difícil

Escolha ferramentas adequadas ao seu nível técnico. Comece pelas mais simples.

Checklist de Segurança Digital

Use senhas fortes e diferentes

Adote um gerenciador de senhas como Bitwarden ou 1Password.

Ative autenticação em dois fatores

Em todas as contas importantes: email, banco, redes sociais.

Configure backups automáticos

Seguindo a regra 3-2-1, com verificação mensal.

Mantenha sistemas atualizados

Ative atualizações automáticas em todos seus dispositivos.

Fique atento a links e anexos

Nunca abra arquivos suspeitos ou clique em links duvidosos.

Proteja seu mundo digital com pequenas ações diárias. Sua segurança vale o esforço!

Obrigado