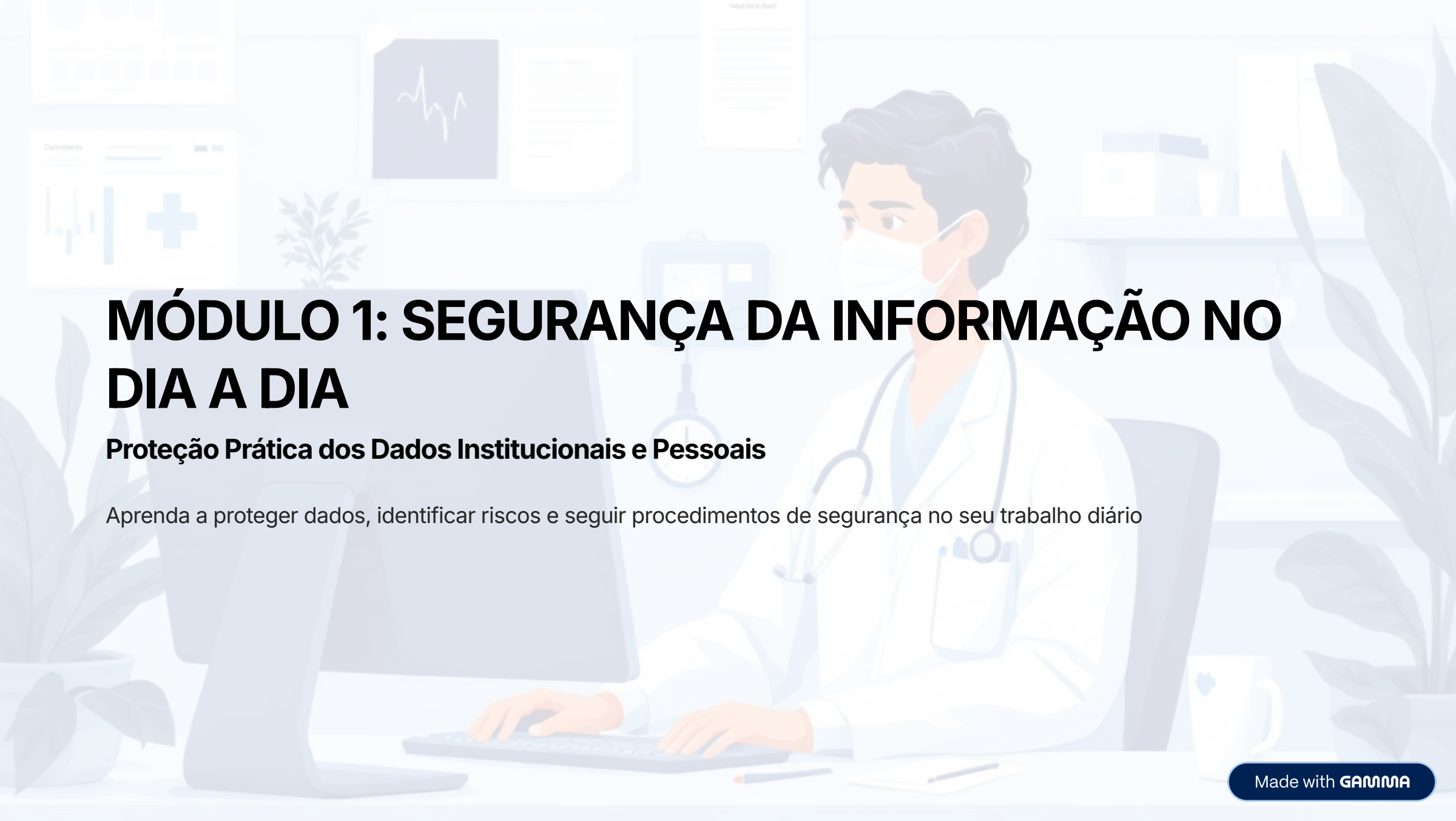


MÓDULO 1: SEGURANÇA DA INFORMAÇÃO NO DIA A DIA

Proteção Prática dos Dados Institucionais e Pessoais

Aprenda a proteger dados, identificar riscos e seguir procedimentos de segurança no seu trabalho diário

Por Que Segurança da Informação É Tão Importante?

No serviço público de saúde, você trabalha com informações muito sensíveis. Dados de pacientes, diagnósticos, históricos médicos — tudo isso é valioso e precisa ser protegido.

Riscos Reais:

- Vazamento de dados: Informações de pacientes expostas na internet
- Fraude: Criminosos usam dados para abrir contas ou fazer compras
- Prejuízo institucional: Perda de confiança dos cidadãos
- Consequências legais: Multas e processos por não proteger dados

Histórias Reais:

Em 2023, um hospital brasileiro teve dados de 50 mil pacientes vazados por falta de segurança básica. Resultado: multa de R$ 2 milhões e perda de confiança pública.

Sua Responsabilidade:

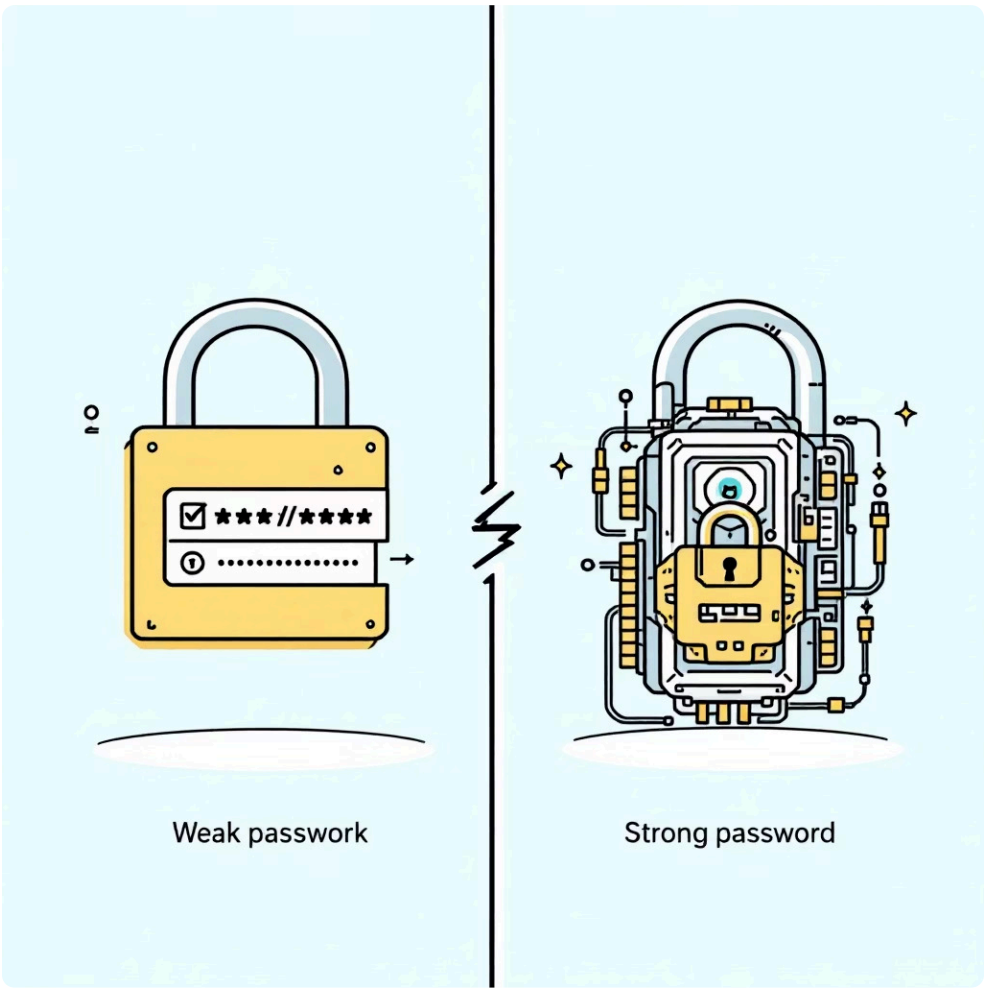
Você é a primeira linha de defesa. Senhas fracas, e-mails abertos, dispositivos desprotegidos — tudo isso pode levar a vazamentos.

Lembre-se:

Proteger dados não é apenas obrigação legal, é ética profissional.

Criando Senhas Realmente Fortes

Uma senha fraca é como deixar a porta de sua casa aberta. Criminosos conseguem entrar facilmente. Uma senha forte é como uma fechadura de segurança.



❌ SENHAS FRACAS:

- 123456
- senha123
- admin
- seu nome ou data de nascimento
- mesma senha em vários lugares

✅ SENHAS FORTES:

- Mínimo 12 caracteres
- Misture: MAIÚSCULAS, minúsculas, números, símbolos
- Exemplo: Br@sil2024#Saúde!
- Única para cada sistema
- Sem informações pessoais

- ☐ Tem pelo menos 12 caracteres?
- ☐ Tem letras maiúsculas E minúsculas?
- ☐ Tem números?
- ☐ Tem símbolos (@, #, !, $)?
- ☐ Não contém seu nome ou data de nascimento?
- ☐ É diferente de outras senhas suas?

Use um gerenciador de senhas (como Bitwarden ou 1Password) para guardar senhas fortes com segurança.

Identificando E-mails Suspeitos e Phishing

Phishing é quando criminosos enviam e-mails falsos fingindo ser do banco, do chefe ou de empresas conhecidas para roubar suas senhas e dados. É uma das ameaças mais comuns no ambiente digital.

🚩 SINAIS DE ALERTA:

- Remetente estranho ou parecido com alguém conhecido
- Pedido urgente para clicar em link ou abrir anexo
- Erros de digitação ou português ruim
- Ameaças ('sua conta será bloqueada')
- Ofertas muito boas para ser verdade

❌ NUNCA FAÇA:

- Clique em links de e-mails suspeitos
- Abra anexos de remetentes desconhecidos
- Responda com suas senhas ou dados pessoais
- Baixe arquivos de e-mails não confiáveis

✅ SEMPRE FAÇA:

- Verifique o endereço de e-mail completo
- Passe o mouse sobre links para ver o URL real
- Quando em dúvida, ligue para a pessoa
- Reporte e-mails suspeitos ao TI

📞 SE RECEBER UM E-MAIL SUSPEITO:

- Não clique em nada
- Reporte ao setor de TI
- Delete o e-mail
- Avise seus colegas

Exemplo de phishing: E-mail que parece do seu chefe pedindo para transferir dinheiro urgentemente. Solução: Ligue para o chefe para confirmar.

Segurança em Dispositivos Móveis

Seu Celular Também Precisa de Proteção

Muitos servidores acessam sistemas de saúde pelo celular ou tablet. Se o aparelho cair em mãos erradas sem proteção adequada, dados sensíveis podem ser expostos.

01

Use Senha ou Biometria:

Desbloqueie com PIN, padrão ou impressão digital

02

Atualize o Sistema:

Instale atualizações de segurança regularmente

03

Cuidado com Apps:

Baixe apenas de lojas oficiais (Google Play, App Store)

04

Não Use Wi-Fi Público:

Evite acessar sistemas sensíveis em redes abertas

05

Ative Localização Remota:

Se perder o celular, você consegue rastreá-lo

- Celular tem senha ou biometria?
- Sistema operacional está atualizado?
- Você só baixa apps de lojas oficiais?
- Não acessa dados sensíveis em Wi-Fi público?
- Sabe como rastrear seu celular se perder?

Se perder seu celular com dados de trabalho, avise o TI imediatamente!

Onde Salvar Arquivos com Segurança

Nem todo lugar é seguro para guardar arquivos. Você precisa saber onde salvar cada tipo de informação.

Nuvem Institucional (OneDrive, Google Drive corporativo)

✅ MELHOR OPÇÃO: Criptografada, com backup automático, acesso controlado

Computador da Instituição

✅ BOM: Protegido por antivírus e firewall, mas faça backup

Celular Pessoal

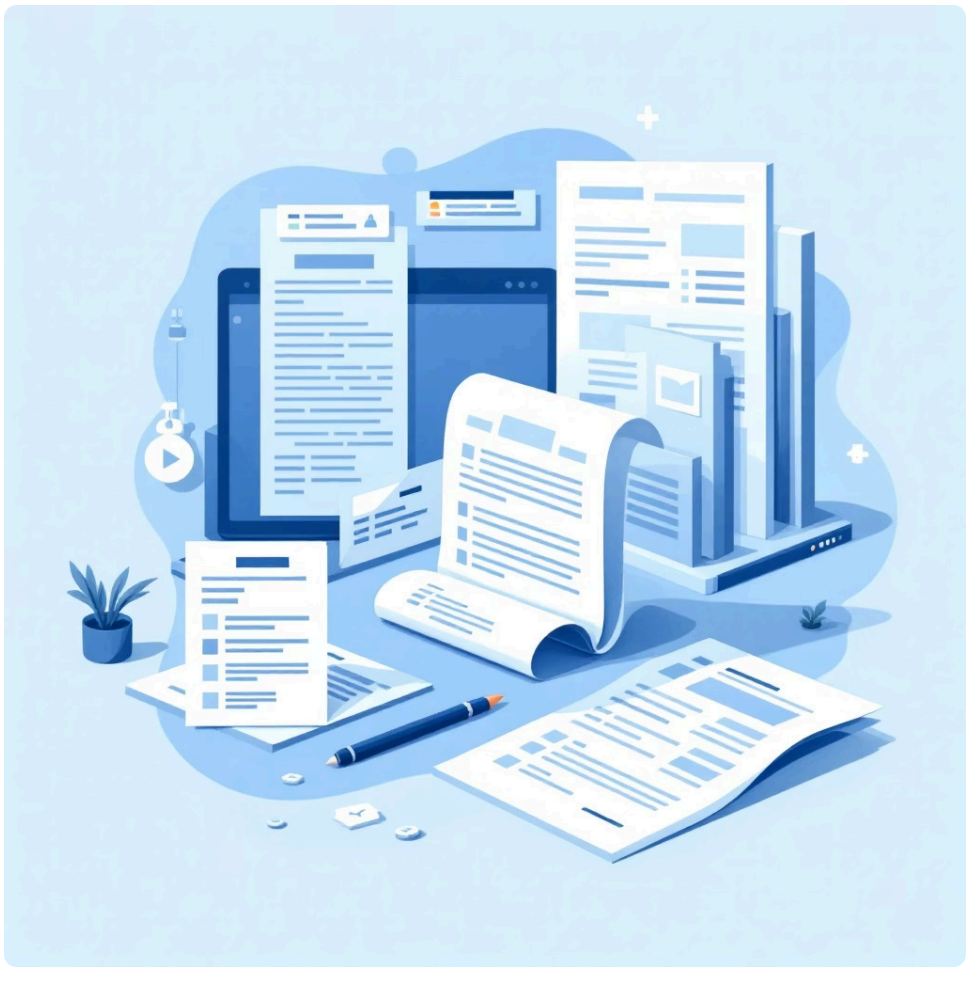
❌ EVITE : Dados de trabalho não devem estar em dispositivos pessoais

Pen Drive ou HD Externo

❌ RISCO: Fácil de perder ou roubar. Se usar, criptografe!

Regra de Ouro: Dados de trabalho SEMPRE na nuvem institucional ou computador da instituição. Nunca em dispositivos pessoais ou pen drives desprotegidos.

Classificação de Documentos: Público, Restrito, Sigiloso



Nem todo documento é igual. A lei exige que você classifique informações corretamente para protegê-las adequadamente.

🟢 PÚBLICO

Pode ser compartilhado com qualquer pessoa

Exemplos: Horários de funcionamento, protocolos gerais, informações sobre serviços

Proteção: Nenhuma especial

🟡 RESTRITO

Pode ser compartilhado apenas com pessoas autorizadas

Exemplos: Dados de pacientes, informações financeiras, relatórios internos

Proteção: Acesso controlado, senha, criptografia

🔴 SIGILOSO

Acesso muito limitado, apenas pessoas específicas

Exemplos: Investigações, informações de segurança, dados de autoridades

Proteção: Máxima segurança, acesso rastreado

- ☐ Você sabe classificar cada documento?
- ☐ Você guarda documentos restritos com segurança?
- ☐ Você nunca compartilha documentos sigilosos?
- ☐ Você sabe quem pode acessar cada tipo?

Dica: Quando em dúvida, classifique como RESTRITO. É melhor ser cauteloso.

Backup: Por Que e Como Fazer

Backup é uma cópia de segurança de seus arquivos. Se algo der errado (vírus, falha do computador, acidente), você não perde tudo.

Por Que Fazer Backup?

- Proteção contra vírus e ransomware
- Recuperação de arquivos deletados por acidente
- Proteção contra falhas de hardware
- Conformidade com leis de proteção de dados

Como Fazer Backup:

1. Use a nuvem institucional (automático)
2. Faça backup semanal em HD externo criptografado
3. Teste o backup: Verifique se consegue restaurar

Frequência Recomendada:

- Dados críticos: Diariamente
- Dados importantes: Semanalmente
- Dados gerais: Mensalmente

Checklist de Backup:

- ☐ Você faz backup regularmente?
- ☐ Seu backup está criptografado?
- ☐ Você testou restaurar um arquivo?
- ☐ Você guarda o backup em local seguro?

Lembre-se: Um backup que você não testou é um backup que não funciona!

Principais Aprendizados do Módulo 1

Senhas Fortes: Mínimo 12 caracteres, misture tipos

E-mail Seguro: Identifique phishing, nunca clique em links suspeitos

Dispositivos Móveis: Sempre protegidos com senha ou biometria

Armazenamento: Nuvem institucional é o melhor lugar

Classificação: Público, Restrito, Sigiloso

Emergências: Avise o TI imediatamente

Você Completou o Módulo 1!

Segurança da Informação no Dia a Dia

Parabéns! Você agora entende os princípios fundamentais de segurança da informação e como aplicá-los no seu trabalho diário.

Lembre-se dos Princípios Fundamentais:

Você é a primeira linha de defesa contra ameaças digitais. Sua vigilância protege não apenas seus dados, mas os de todos os pacientes que confiamos em nosso cuidado.

Nos vemos no próximo módulo!

SENHAS E ACESSO

- Senhas fortes com 12+ caracteres
- Nunca compartilhe suas credenciais
- Mude senha regularmente
- Use autenticação de dois fatores

E-MAIL E COMUNICAÇÃO

- Identifique phishing e golpes
- Nunca clique em links suspeitos
- Verifique o remetente
- Reporte e-mails suspeitos

DISPOSITIVOS E ARMAZENAMENTO

- Celular sempre protegido
- Nuvem institucional para dados
- Backup regular e testado
- Nunca use pen drives desprotegidos

DOCUMENTOS E DESCARTE

- Classifique corretamente
- Guarde com segurança
- Destrua fisicamente quando necessário
- Delete permanentemente arquivos digitais

EMERGÊNCIAS

- Avise o TI imediatamente
- Não tente resolver sozinho
- Documente o incidente
- Aprenda com o ocorrido

Situações de Emergência: O Que Fazer

Às vezes, algo dá errado. Você suspeita de uma invasão, seu computador está lento, recebeu um e-mail estranho. O que fazer?

🚨 SUSPEITA DE INVASÃO:

- Desligue o computador imediatamente
- Não tente 'investigar' sozinho
- Avise o setor de TI
- Mude sua senha em outro computador

🚨 COMPUTADOR LENTO OU TRAVANDO:

- Pode ser vírus ou malware
- Avise o TI para verificar
- Não instale programas para 'limpar'
- Não clique em pop-ups de 'limpeza'

🚨 RECEBEU E-MAIL SUSPEITO:

- Não clique em links
- Não abra anexos
- Reporte ao TI
- Delete o e-mail

🚨 PERDEU DADOS OU ARQUIVO FOI DELETADO:

- Avise o TI imediatamente
- Não tente recuperar sozinho
- Quanto antes avisar, melhor a chance de recuperação
- Tenha um backup atualizado

Contato de Emergência TI: [número/e-mail]. Disponível 24/7 para emergências de segurança.