EMPRESA X

GUIA PRÁTICO DE SEGURANÇA DA INFORMAÇÃO

Proteja seus dados e evite ataques cibernéticos

SUMÁRIO

INTRODUÇÃO

A Segurança da Informação é essencial para qualquer organização, independentemente do seu porte ou setor. Com a crescente digitalização das operações, ameaças cibernéticas como ataques de hackers, vazamentos de dados e fraudes estão cada vez mais frequentes.

📢 Por que isso importa?

✓ Evita prejuízos financeiros causados por golpes e fraudes.

✓ Protege informações sigilosas de clientes e da empresa.

✓ Mantém a reputação da organização segura no mercado.

✓ Atende a normas e regulamentações (como LGPD, ISO/IEC 27001).

BOAS PRÁTICAS PARA SENHAS SEGURAS

As senhas são a primeira linha de defesa contra invasões. Senhas fracas facilitam o acesso de invasores a sistemas corporativos.

01 — Senhas fortes

Use pelo menos 12 caracteres misturando letras maiúsculas, minúsculas, números e símbolos.
Evite informações óbvias e não reutilize senhas em diferentes serviços. Ex: “Xj8@Tq!9bD3#P”

02 — Criptografia de frases

Em vez de usar uma senha curta e difícil de lembrar, opte por frases longas e fáceis de memorizar, em seguida é possível criptografar sua frase para uma maior segurança. Ex: “*ComiPizza3x#N0Cafe$” ou “da3c34013e5bf996cae321b42d04192a8a21a7cc” após criptografar no formato “sha1”

03 — Autenticação de dois Fatores

Mesmo uma senha forte pode ser comprometida. O 2FA (Two-Factor Authentication) adiciona uma camada extra de proteção, exigindo um segundo código de verificação. Você pode utilizar aplicativos autenticadores como o Google Authenticator e o Microsoft Authenticator. Ex: Digite sua senha -> Insira o código gerado no Google Authenticator -> Acesse sua conta de forma protegida

COMO IDENTIFICAR UM E-MAIL DE PHISHING?

Os ataques de phishing são uma das maiores ameaças corporativas. Criminosos enviam e-mails falsos tentando enganar funcionários para roubar dados ou infectar sistemas.

SINAL DE ALERTA	
Erro de ortografia e gramática	• Empresas legítimas revisam seus e-mails
Remetente estranho	• **Verifique sempre o domínio do e-mail.**
Links suspeitos	• Passe o mouse sobre o link para verificar o endereço real.
Pedido urgente de informações pessoais	• **Bancos e empresas nunca pedem senhas por e-mail**

COMO IDENTIFICAR UM E-MAIL DE PHISHING?

Exemplo:

A fatura falhou - conta bloqueada

NETFLLIX

Oi [redacted]

Estamos tendo problemas com suas informações de faturamento atuais. Tentaremos novamente, mas por enquanto você pode atualizar seu MASTERCARD em seus detalhes de pagamento.

ATUALIZAR CONTA AGORA

Estamos aqui para ajudar quando você precisar. Visite a Central de Ajuda para mais informações ou entre em contato conosco .

Seus amigos no Netflix

PROTEÇÃO DE DADOS CONFIDENCIAIS

A segurança dos dados é responsabilidade de todos os funcionários. O vazamento de informações pode trazer prejuízos enormes para a empresa e para os clientes.

Armazenamento

Fazer isso

Habilitar senhas para planilhas, PDFs e documentos sigilosos

Usar servidores seguros ou soluções em nuvem com criptografia

Manter o **Acesso Restrito** a dados sensíveis

Não fazer isso

Deixar arquivos sensíveis salvos em computadores pessoais

Compartilhamento

Fazer isso

Usar plataformas seguras: OneDrive e Google Drive

Compartilhar links com expiração automática

Utilizar criptografia ponta a ponta ao enviar informações críticas

Não fazer isso

Enviar dados sensíveis por e-mail sem criptografia

Usar pendrives ou HDs externos sem proteção

Compartilhar senhas ou credenciais

Descarte

Fazer isso

Utilizar ferramentas para apagar arquivos permanentemente

Utilizar trituradores de papel para destruir arquivos físicos

Nunca jogar documentos inteiros no lixo sem rasgá-los

Não fazer isso

Apagar arquivos apenas jogando na lixeira do computador. Eles ainda podem ser recuperados!

Proteja seus dados: armazene com segurança, compartilhe com cautela, descarte com responsabilidade!

POLÍTICAS DE SEGURANÇA DA EMPRESA

As políticas de segurança da informação são um conjunto de diretrizes que definem regras e boas práticas para garantir a proteção dos dados da empresa e de seus colaboradores. Elas estabelecem padrões para o uso de tecnologia, acesso à informação e comportamento digital seguro, reduzindo riscos e prevenindo incidentes cibernéticos.

01 — Uso de Dispositivos e Acessos Corporativos

- Uso exclusivo para fins profissionais – Evitar o uso pessoal de dispositivos fornecidos pela empresa.
- Bloqueio de tela – Configurar bloqueio automático de tela e utilizar senhas seguras para desbloqueio.
- Instalação de software – Somente aplicativos e programas autorizados podem ser instalados.
- Atualizações e patches – Garantir que o sistema operacional e softwares estejam sempre atualizados.

02 — Uso de E-mail e Comunicação Corporativa

- Verificação de remetentes – Sempre conferir a autenticidade do remetente antes de abrir anexos ou clicar em links.
- Evitar mensagens automáticas e respostas a desconhecidos – Atacantes podem explorar respostas automáticas para coletar informações.
- Não enviar dados sensíveis por e-mail – Sempre utilizar canais seguros para compartilhar informações confidenciais.

03 — Atualizações e Conscientização Contínua

As políticas de segurança devem ser constantemente revisadas e aprimoradas para acompanhar novas ameaças e tecnologias. Dessa forma, todos os colaboradores devem passar por treinamentos periódicos para reforçar boas práticas e garantir o cumprimento das diretrizes estabelecidas.

O QUE FAZER EM CASO DE ATAQUE?

Mesmo com todas as medidas preventivas adotadas, a possibilidade de um ataque ou incidente de segurança sempre existe. Saber como reagir rapidamente pode minimizar danos e evitar que a situação se agrave. A seguir, apresentamos um guia de ações que devem ser tomadas caso um ataque cibernético ou incidente de segurança ocorra.

01 — Identifique e Avalie a Situação

Antes de tomar qualquer ação, é importante entender o que está acontecendo.
Você recebeu um e-mail suspeito e clicou em um link desconhecido?
Seu computador está apresentando comportamentos estranhos, como lentidão extrema ou arquivos corrompidos?
Você perdeu um dispositivo corporativo (notebook, celular, pendrive) que pode conter informações sensíveis?
Detectou acessos não autorizados a sistemas ou contas corporativas?

02 — Relate o Incidente Imediatamente

Não tente corrigir o problema sozinho. Informar rapidamente o time de segurança da informação é essencial.
Relate o máximo de detalhes possíveis, quando e como o incidente ocorreu, quais dispositivos e sistemas podem ter sido afetados e também se houve vazamento ou exposição de informações.

03 — Altere Senhas Comprometidas

Se suas credenciais de acesso foram comprometidas:

- Troque suas senhas imediatamente.
- Utilize senhas fortes, preferencialmente geradas por um gerenciador de senhas.
- Se possível, ative a autenticação de dois fatores (2FA) para aumentar a segurança.

CHECKLIST DE SEGURANÇA PARA FUNCIONÁRIOS

Autoavaliação rápida:

- ▢ Minhas senhas são fortes e únicas?
- ▢ Ativei a autenticação em dois fatores (2FA)?
- ▢ Sei identificar um e-mail de phishing?
- ▢ Uso VPN para acessar sistemas remotamente?
- ▢ Meus dispositivos estão protegidos com senha e atualizados?

Treinamentos práticos e atividades interativas são essenciais para reforçar a segurança da informação.

CONCLUSÃO

A segurança da informação não é apenas uma responsabilidade da equipe de TI, mas sim um compromisso de todos dentro da organização. Pequenos descuidos podem resultar em grandes problemas, desde vazamento de dados sensíveis até ataques cibernéticos que comprometem toda a empresa.

CONTATO

Dúvidas? **Entre em contato com a equipe de segurança:**

📌 **E-mail: seguranca@empresax.com.br**

📌 **Telefone: (XX) XXXX-XXXX**

A segurança da informação é uma responsabilidade compartilhada! Pequenos descuidos podem colocar toda a empresa em risco.