Mente Segura em

SEGURANÇA DA INFORMAÇÃO

SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE ACESSO

Edição do Mês

Abril / 2026

Este material foi elaborado para orientar todos os colaboradores sobre as boas práticas de segurança cibernética e proteção de acesso no ambiente corporativo. Leia com atenção — a segurança da empresa depende de cada um de nós.

Equipe de Infraestrutura de TI | Distribuição interna

Conteúdo deste Mês

01. O que é Segurança Cibernética?

02. Ameaças mais comuns no ambiente corporativo

03. Proteção de Acesso: senhas e autenticação

04. Phishing e Engenharia Social

05. Boas práticas no dia a dia

06. O que fazer em caso de incidente

07. Quiz: Você está preparado?

08. Conteúdo extra e recursos

01. O que é Segurança Cibernética?

Segurança cibernética é o conjunto de práticas, tecnologias e processos projetados para proteger sistemas, redes e dados contra-ataques digitais, acesso não autorizado, danos ou vazamentos. No ambiente corporativo, ela não é responsabilidade exclusiva do setor de TI — cada colaborador é uma linha de defesa fundamental.

💡 Por que isso importa para você?

Um único clique em um link malicioso pode comprometer toda a rede da empresa.
Dados de clientes, financeiros e estratégicos estão sob responsabilidade coletiva.
Incidentes de segurança geram prejuízos financeiros, legais e reputacionais.

02. Ameaças mais comuns no ambiente corporativo

Conhecer as ameaças é o primeiro passo para se defender. Veja as principais que afetam empresas atualmente:

🎯 Phishing

- E-mails falsos que imitam fontes confiáveis para roubar credenciais
- Links maliciosos disfarados de mensagens legítimas
- Representa mais de 80% dos ataques cibernéticos corporativos

🔒 Ransomware

- Malware que criptografa arquivos e exige resgate para devolver o acesso
- Pode paralisar totalmente as operações da empresa

- Distribuído frequentemente via anexos de e-mail ou downloads

👤 Insider Threats (Ameaças Internas)

- Acesso indevido a dados por colaboradores ou ex-funcionários
- Uso não autorizado de credenciais corporativas
- Compartilhamento descuidado de informações sensíveis

🔗 Engenharia Social

- Manipulação psicológica para obter informações confidenciais
- Pode ocorrer por telefone, e-mail, WhatsApp ou pessoalmente
- Explora confiança, urgência e autoridade para enganar vítimas

03. Proteção de Acesso: senhas e autenticação

O controle de acesso é a primeira barreira de proteção dos sistemas corporativos. Senhas fracas ou reutilizadas são uma das principais causas de vazamentos de dados.

Regras de ouro para senhas seguras

- Use no mínimo 12 caracteres, combinando letras maiúsculas, minúsculas, números e símbolos
- Não reutilize senhas entre sistemas diferentes
- Nunca utilize informações pessoais óbvias (nome, data de nascimento, CPF)
- Troque suas senhas periodicamente ou sempre que suspeitar de comprometimento
- Utilize um gerenciador de senhas para criar e armazenar credenciais com segurança

Autenticação Multifator (MFA) — Obrigatório

O MFA adiciona uma camada extra de proteção além da senha. Mesmo que sua senha seja comprometida, o atacante ainda precisará do segundo fator para acessar o sistema.

✅ Como funciona o MFA?

1° fator: Algo que você SABE — sua senha
2° fator: Algo que você TEM — token, aplicativo autenticador ou SMS
3° fator (opcional): Algo que você É — biometria (impressao digital, facial)

Controle de Privilégios (Princípio do Menor Privilégio)

Cada usuário deve ter acesso somente ao que é necessário para realizar suas funções. Nunca compartilhe suas credenciais com colegas, mesmo em situações de urgência.

- Solicite acesso apenas ao que for necessário para sua função
- Informe imediatamente ao TI quando mudar de área ou de função
- Ao sair da empresa, todos os acessos devem ser revogados imediatamente

04. Phishing e Engenharia Social

O phishing é a técnica de ataque mais utilizada no mundo. Criminosos se passam por pessoas ou empresas confiáveis para enganar você e obter informações confidenciais ou instalar softwares maliciosos.

SINAIS DE ALERTA

⚠ Remetente desconhecido ou e-mail suspeito

⚠ Urgência ou ameaça excessiva na mensagem

⚠ Links encurtados ou com domínios estranhos

⚠ Anexos não esperados (.exe, .zip, .docm)

⚠ Solicitação de senha ou dados bancários por e-mail

⚠ Erros gramaticais ou de português suspeitos

O QUE FAZER

✓ Não clique: repasse ao time de TI/Segurança

✓ Verifique o endereço real do remetente

✓ Acesse sites sempre digitando diretamente no navegador

✓ Confirme por outro canal antes de executar qualquer anexo

✓ Nenhum sistema legítimo pede sua senha por e-mail

✓ Em caso de dúvida, sempre pergunte antes de agir

⚠ Atenção: Vishing e Smishing

Vishing: ataques por ligacão telefônica se passando por suporte técnico ou banco.

Smishing: ataques por SMS com links falsos ou solicitações urgentes.

Regra de ouro: nunca forneça dados de acesso por telefone, SMS ou WhatsApp.

05. Boas práticas no dia a dia

A segurança cibernética começa em hábitos simples praticados diariamente. Confira as principais recomendações para o seu ambiente de trabalho:

💻 Dispositivos e equipamentos

- Bloqueie sua tela sempre que se afastar do computador (Win + L)
- Não conecte pendrives ou dispositivos externos de origem desconhecida
- Manténha o sistema operacional e aplicativos sempre atualizados
- Não instale softwares sem autorização do time de TI

🌐 Navegação e internet

- Acesse apenas sites relacionados ao trabalho em equipamentos corporativos
- Evite redes Wi-Fi públicas para acessar sistemas da empresa
- Use a VPN corporativa quando trabalhar remotamente
- Não faça download de arquivos de fontes não confiáveis

📧 E-mail e comunicações

- Não encaminhe informações confidenciais para e-mails pessoais
- Criptografe documentos sensíveis antes de compartilhar
- Confirme solicitações incomuns por um canal alternativo
- Reporte e-mails suspeitos ao time de segurança imediatamente

📋 Dados e informações

- Siga a classificação de dados da empresa (público, interno, confidencial, restrito)
- Não discuta informações sensíveis em locais públicos
- Descarte documentos físicos com informações sensíveis na trituradora
- Armazene arquivos corporativos apenas nos repositórios autorizados

06. O que fazer em caso de incidente

Se você identificar ou suspeitar de um incidente de segurança, aja com rapidez. O tempo de resposta é crucial para minimizar os danos.

PASSO 1	Não entre em pânico e NÃO tente resolver sozinho
PASSO 2	Desconecte o dispositivo da rede (cabo e Wi-Fi) se suspeitar de infecção
PASSO 3	Não desligue o equipamento — preserve as evidências
PASSO 4	Contate imediatamente o time de TI ou Segurança
PASSO 5	Registre tudo: o que aconteceu, quando e como você identificou
PASSO 6	Não compartilhe informações sobre o incidente até ser orientado

🚨 Contatos de Segurança

📞 Canal de incidentes: 210 - 6139630030

📧 E-mail: Infraestrutura@memora.com.br

07. Quiz: Você está preparado?

Analise as situações abaixo e reflita sobre qual seria a atitude correta. As respostas estão na coluna ao lado.

#	Situação	Qual a atitude correta?
1	Você recebe um e-mail do "CEO" pedindo transferência urgente de valores.	*Não execute. Confirme por telefone com o remetente real e reporte ao time de segurança.*
2	Um colega pede sua senha por razões de urgência e prazo.	*Nunca compartilhe sua senha. Solicite abertura de acesso temporário ao TI.*
3	Você encontra um pendrive sem identificação na mesa do escritório.	*Não conecte ao computador. Entregue ao time de TI para análise.*
4	Seu computador trava e aparece uma mensagem pedindo pagamento em criptomoeda.	*Desconecte da rede imediatamente e acione o time de segurança urgentemente.*
5	Uma ligação do "suporte técnico" solicita suas credenciais de acesso.	*Recuse e desligue. O suporte legítimo NUNCA pede senha por telefone.*
6	Você precisa acessar o sistema da empresa de um café com Wi-Fi público.	*Use sempre a VPN corporativa antes de acessar qualquer sistema da empresa.*

Segurança é responsabilidade de todos!

Em caso de dúvida, sempre consulte a equipe de Segurança da Infraestrutura antes de agir.

Juntos somos mais fortes contra as ameaças cibernéticas.