

# CYBER NEWS

O Boletim Informativo Oficial de Gestão de Riscos em Terceiros



## NESTA EDIÇÃO

### Conscientização e Treinamento

- Phishing e Engenharia Social
- Proteção e Privacidade de Dados (LGPD)
- Prevenção de Vazamento de Informações
- Senhas Fortes e Autenticação Segura
- Navegação e Uso Seguro da Internet
- O Papel dos Colaboradores
- Boas Práticas no Trabalho Remoto e Híbrido

## CONCLUSÃO

A Segurança da Informação é um pilar fundamental para garantir a continuidade das operações, a proteção dos dados corporativos e a confiança de clientes, parceiros e colaboradores. Para mantermos um ambiente seguro e preparado, é indispensável que todos participem dos treinamentos obrigatórios relacionados aos principais riscos e boas práticas.

A seguir, destacamos os temas que compõem o programa de conscientização e que precisam ser realizados por todos os colaboradores.

### Phishing e Engenharia Social

Ataques de phishing continuam entre as maiores causas de incidentes.

**Nos treinamentos, os colaboradores aprendem:**

- Identificar e-mails, mensagens e links suspeitos.
- Reconhecer tentativas de fraude e manipulação psicológica.
- Adotar práticas seguras antes de clicar, baixar ou responder algo.

**Objetivo:** evitar acessos indevidos, roubo de credenciais e infecções por malware.



## Proteção e Privacidade de Dados (LGPD)

A empresa lida diariamente com dados pessoais, confidenciais e estratégicos.

### Os treinamentos reforçam:

- Conceitos da LGPD e obrigações legais.
- Como tratar, armazenar e compartilhar informações de forma segura.
- Uso adequado de sistemas, documentos, e-mails e plataformas corporativas.
- Princípios fundamentais: necessidade, minimização, finalidade e segurança.

**Objetivo:** garantir conformidade legal e proteger dados de clientes, parceiros e do próprio negócio.

## Prevenção de Vazamento de Informações

O vazamento de informações pode causar danos severos à empresa.

### Os treinamentos abordam:

- Como classificar corretamente informações (pública, interna, confidencial).
- Boas práticas na circulação de documentos sensíveis.
- Cuidados ao enviar anexos, relatórios e prints.
- Uso seguro de dispositivos móveis e mídias externas.
- Riscos de compartilhamento não autorizado em mensagens, redes sociais e ambientes externos.

**Objetivo:** evitar exposição de dados sigilosos, impactos financeiros e danos à reputação.

## Senhas Fortes e Autenticação Segura

Um dos controles mais simples e mais ignorados.

### Nos treinamentos, reforçamos:

- Criação de senhas fortes, únicas e difíceis de adivinhar.
- Uso obrigatório de autenticação multifator (MFA).
- Riscos de compartilhar senhas ou anotá-las em locais inseguros.

**Objetivo:** reduzir drasticamente o risco de acessos indevidos.



## Navegação e Uso Seguro da Internet

O ambiente digital precisa ser utilizado com responsabilidade.

### Os temas incluem:

- Perigos de downloads desconhecidos.
- Riscos de redes Wi-Fi públicas.
- Uso adequado das ferramentas corporativas.
- Atenção ao acesso remoto e VPN.

**Objetivo:** proteger o ambiente corporativo contra ataques externos.



## 6. Boas Práticas no Trabalho Remoto e Híbrido

### Os treinamentos orientam sobre:

- Proteção de dados fora do escritório.
- Uso de VPN, dispositivos corporativos e Wi-Fi seguro.
- Evitar conversas sobre assuntos internos em ambientes públicos.

**Objetivo:** manter o mesmo nível de segurança, independentemente do local de trabalho.

## Conclusão

A participação ativa de todos nos treinamentos de Segurança da Informação é essencial para mantermos um ambiente confiável, preparado e alinhado às melhores práticas do mercado. Cada colaborador tem um papel fundamental na proteção dos dados e na prevenção de incidentes.

Segurança da Informação é responsabilidade de todos e começa nas pequenas atitudes do dia a dia.

Fiquem atentos aos próximos boletins para mais dicas!