

CARTILHA DE BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação é responsabilidade de todos. Proteger os dados da empresa, dos clientes e dos colegas de trabalho é essencial para manter a confiança, a reputação e a conformidade com a legislação, como a LGPD.

Esta cartilha traz orientações simples, práticas e eficazes para o dia a dia profissional, com base na Política Geral de Segurança da Informação da empresa. Leia com atenção, aplique e compartilhe!

1. PROTEÇÃO DE SENHAS

- Use **senhas fortes**: no mínimo 8 caracteres, com letras maiúsculas, minúsculas, números e símbolos.
- **Troque sua senha regularmente** (pelo menos a cada 90 dias).
- **Nunca compartilhe sua senha** com ninguém — nem com colegas ou TI.
- Sempre **bloqueie a tela** ao se ausentar, mesmo por poucos minutos.

2. USO DE DISPOSITIVOS E ACESSOS

- Utilize **apenas os equipamentos autorizados** pela empresa.
- Evite usar dispositivos pessoais para acessar sistemas internos, exceto se expressamente autorizado (BYOD controlado).
- **Não instale softwares ou plug-ins** sem aprovação prévia do setor de TI.
- Ao acessar sistemas da empresa remotamente, use canais seguros (VPN, autenticação multifator, etc.).

3. CUIDADOS COM E-MAILS E INTERNET

- **Desconfie de e-mails suspeitos**, especialmente com anexos ou links estranhos.

- **Não clique** em links de remetentes desconhecidos.
- Verifique o domínio de e-mails que pedem dados sigilosos. Navegue apenas em sites seguros (endereços com "https" e cadeado).
- Nunca envie arquivos confidenciais sem criptografia ou autorização.

4. TRATAMENTO DAS INFORMAÇÕES

Classifique e trate documentos conforme sua **sensibilidade**:

- *Pública*
- *Interna*
- *Confidencial*
- *Restrita*

- Armazene arquivos sigilosos em locais seguros (pastas protegidas, sistemas criptografados).
- Evite compartilhar documentos sensíveis por e-mail ou serviços de nuvem pessoal.
- Evite deixar documentos impressos em impressoras ou sobre a mesa.

5. REMOÇÃO E DESCARTE DE INFORMAÇÕES

- **Apague informações com segurança** – use as ferramentas da empresa para descarte digital.
- Documentos em papel devem ser triturados quando contêm dados internos ou confidenciais.
- Descarte de mídias (pendrives, HDs) deve ser feito com apoio do setor de TI.

6. CONDUTA EM CASO DE INCIDENTE

- Suspeitou de algo? **Informe imediatamente a área de TI ou o Encarregado de Dados (DPO).**
- Não tente resolver incidentes por conta própria.
- Sempre registre o ocorrido: data, hora, local e tipo de incidente.

7. EXEMPLOS DO QUE NÃO FAZER

- Compartilhar sua senha com um colega “só por um momento”.
- Acessar o sistema da empresa em redes Wi-Fi públicas sem proteção.
- Baixar documentos da empresa em computadores pessoais.
- Esquecer impressões com dados de clientes na bandeja da impressora.
- Jogar fora rascunhos com anotações jurídicas sem destruir o papel.

8. LEMBRE-SE: SEGURANÇA DA INFORMAÇÃO É CULTURA.

Quando você protege uma informação, protege a reputação da empresa, a confiança dos clientes e a sua própria integridade profissional.

A segurança começa com atitudes individuais e se fortalece com o compromisso coletivo.

Dúvidas? Fale com a área de TI ou com o Encarregado de Proteção de Dados (DPO), Thiago Luiz Pontarolli OAB/PR 47.488, telefone (41) 99647-4685 e e-mail pontarolli@hotmail.com.