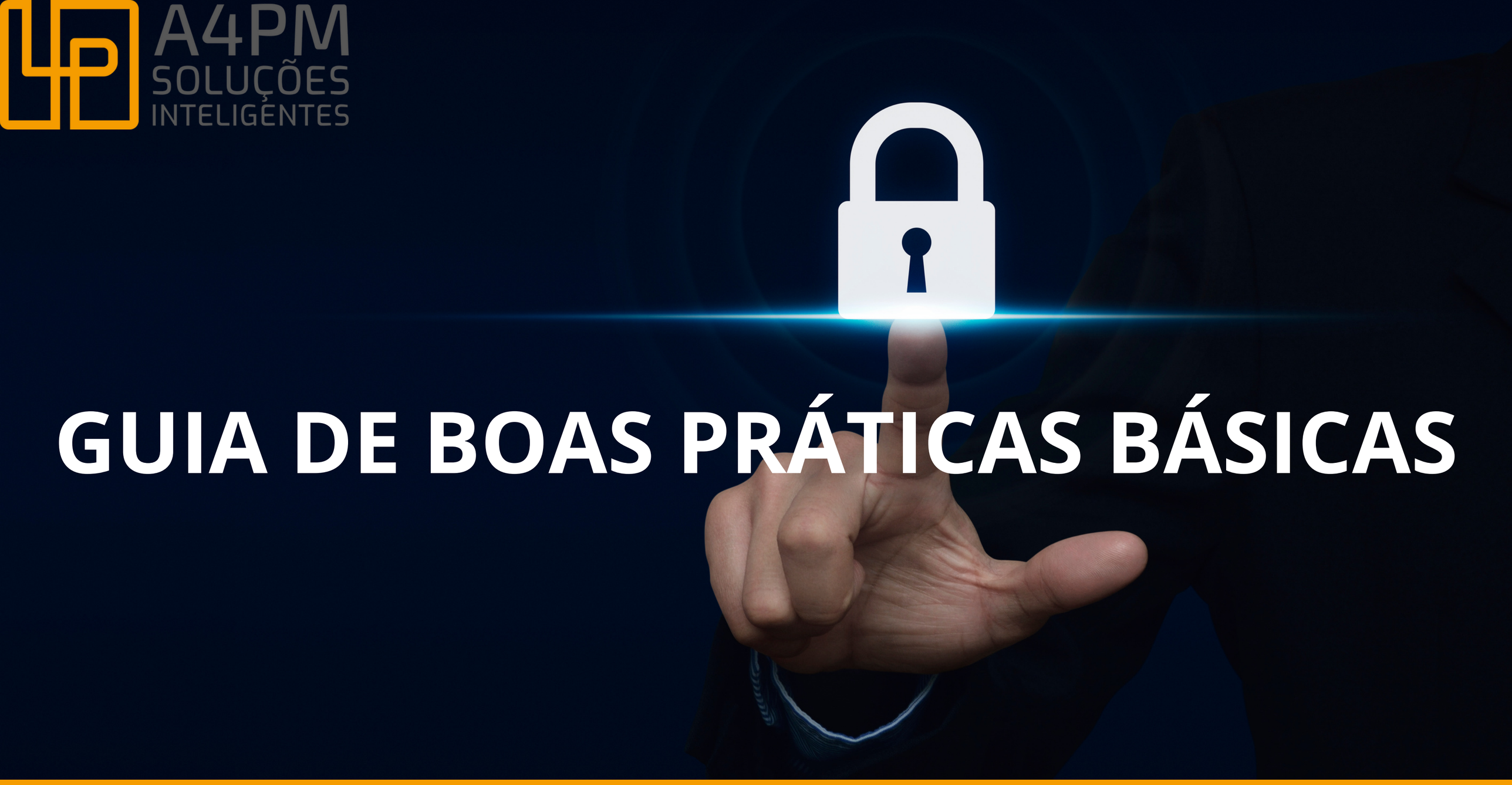
A4PM
SOLUÇÕES
INTELIGÊNTES



GUIA DE BOAS PRÁTICAS BÁSICAS

Senha Segura

- Crie senhas fortes com uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais;
- Evite senhas óbvias, como "123456" ou "senha";
- Use senhas exclusivas para cada conta;
- Atualize suas senhas regularmente;
- Nunca compartilhe senhas com ninguém;
- Nunca deixe sua senha exposta e sua máquina de trabalho livre para acesso de terceiros, tanto trabalhando presencialmente quanto em home office;
- Ative a autenticação de dois fatores sempre que possível (2FA - Camada adicional de segurança exigindo uma segunda forma de verificação).

A4PM SOLUÇÕES INTELIGENTES

Antivírus e Antimalware

- Faça uso do antivírus padrão disponibilizado pela empresa. Caso ainda não tenha entre em contato com a equipe de Infraestrutura.

Atualizações de Software

- Mantenha seu sistema operacional e software atualizados;
- Ative as atualizações automáticas sempre que possível para corrigir vulnerabilidades conhecidas;
- Reinicie sua máquina pelo menos uma vez por semana.

Segurança de Dispositivos Móveis

- Proteja seus dispositivos móveis com senhas ou PINs.

Navegação Segura

- Use conexões seguras (HTTPS) ao acessar sites sensíveis, como bancos e contas de e-mail.
- Evite sites duvidosos e de fontes não confiáveis;
- Não realize downloads de softwares pirateados. Caso necessite de algum software, consulte o catálogo de software A4PM em **software.a4pm.com.br**

Backup e Armazenamento de Dados

- Não armazene dados pessoais em sua máquina corporativa;
- Faça backups regulares de seus dados importantes;
- Armazene os backups em locais seguros, fora do alcance de ameaças físicas e digitais;
- Consulte o setor de Infraestrutura sobre onde realizar o backup de dados corporativos.

E-mails Seguros

- Desconfie de e-mails de remetentes desconhecidos;
- Não clique em links ou baixe anexos suspeitos;
- Evite fornecer informações confidenciais por e-mail.

Conscientização em Segurança

- Esteja ciente das táticas de engenharia social, como phishing;
- Relate imediatamente qualquer atividade suspeita à equipe de segurança da A4PM.

Criptografia

- Use criptografia sempre que possível para proteger informações sensíveis, como dados em trânsito e em repouso.

Rede

- Use senhas fortes para sua rede doméstica;
- Use redes Wi-Fi seguras e evite redes públicas não seguras.

Política de Acesso

- Siga as políticas de acesso da A4PM e a prática do princípio do "mínimo privilégio", onde cada usuário deve ter acesso apenas ao que é absolutamente necessário.

Denuncie Incidentes

- Se suspeitar de uma violação de segurança, relate-a imediatamente em **meuhelpdesk.com.br;**

- Lembre-se de que a segurança da informação é uma responsabilidade de todos. Seguir essas boas práticas pode ajudar a proteger sua informação pessoal e a contribuir para um ambiente de TI mais seguro. Se você estiver em uma organização, siga as políticas de segurança específicas e comunique o time de Infra e/ou LGPD caso de dúvidas ou preocupações.