MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA
DIRETORIA DE GESTÃO E INTEGRAÇÃO DE INFORMAÇÕES

CARTILHA DE ORIENTAÇÕES DE SEGURANÇA DA INFORMAÇÃO

PARA O USUÁRIO SINESP

Sinesp
Sistema Nacional de Informações de Segurança Pública

APRESENTAÇÃO

Esta cartilha é um guia prático elaborado pela Diretoria de Gestão e Integração de Informações (DGI), da Secretaria Nacional de Segurança Pública, do Ministério da Justiça e Segurança Pública, especialmente para você.

Seu objetivo é fortalecer a segurança da informação no ambiente de trabalho, com foco na utilização do Sinesp e de suas soluções, alinhando boas práticas de proteção de dados às diretrizes da LGPD e da Portaria MJSP nº 2/2022.

A iniciativa busca promover a preservação, o uso ético e a proteção de informações institucionais e pessoais diante das ameaças digitais.

Cibersegurança não é apenas uma questão de tecnologia, mas também de cultura, responsabilidade e mentalidade.

Ao seguir estas orientações, você contribui para reduzir riscos, prevenir golpes e manter suas informações mais seguras.

Lembre-se: A segurança da informação é responsabilidade de todos. Pequenas atitudes diárias fazem uma grande diferença na proteção dos dados institucionais e pessoais!

I. USO SEGURO DE EQUIPAMENTOS E SISTEMAS

COMPUTADORES E DISPOSITIVOS MÓVEIS

- Bloqueie a tela do computador ao se ausentar (Winkey + L, Ctrl + Alt + Del e dar enter no Windows / Cmd + Ctrl + Q no Mac).
- Utilize senhas fortes com no mínimo 12 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos em todos os dispositivos e sistemas.
- Nunca compartilhe suas senhas ou deixe-as anotadas em locais visíveis.
- Não utilize a mesma senha em sistemas distintos.
- Utilize preferencialmente dispositivos corporativos para atividades institucionais.

E-MAILS E COMUNICAÇÃO

- Verifique remetentes de e-mails antes de clicar em links ou baixar anexos.
- Nunca compartilhe dados sensíveis por e-mail sem criptografia.
- Desconfie de mensagens urgentes ou que solicitem informações pessoais.
- Ao enviar e-mails para mais de um destinatário, utilize a funcionalidade de Cópia Oculta (CCO), preservando os dados sigilosos dos destinatários.

USO DE SOFTWARES E SISTEMAS

- Utilize apenas softwares autorizados e licenciados em dispositivos de acesso aos sistemas institucionais.
- Evite baixar programas ou arquivos de fontes não confiáveis.
- Mantenha antivírus e ferramentas de segurança sempre atualizados.
- Atualize regularmente os sistemas operacionais e aplicativos nos dispositivos pessoais que utilize para acessar sistemas institucionais.

II. PROTEÇÃO DE DADOS INSTITUCIONAIS E PESSOAIS

DOCUMENTOS FÍSICOS E DIGITAIS

- Mantenha documentos confidenciais em locais seguros (armários trancados, pastas protegidas).
- Evite imprimir documentos sensíveis desnecessariamente.
- Realize descarte seguro de documentos físicos com uso de fragmentadoras.

ACESSO E COMPARTILHAMENTO DE DADOS

- Conceda acesso a informações apenas para colaboradores autorizados, e que tenham necessidade de serviço em saber a informação.
- Utilize plataformas seguras para compartilhamento de arquivos (ex.: sistemas corporativos internos).
- Não utilize dispositivos pessoais para armazenar dados institucionais.
- Jamais insira dados corporativos como e-mail, endereço, descrição e detalhamento de funções em cadastros para fins comerciais.
- Evite utilizar os canais de comunicação corporativos, como e-mail, conta Teans coorporativa, ou telefones do setor para tratar de assuntos privados, e/ou comerciais.

III. INTERNET E REDE CORPORATIVA

ACESSO À INTERNET

- Evite acessar sites não confiáveis ou realizar downloads não autorizados.
- Passe o cursor sobre o link antes de clicar para ler a URL ou endereço. Não clique se o endereço não for familiar.
- Não conecte dispositivos pessoais à rede corporativa sem necessidade.
- Utilize redes Wi-Fi seguras. Nunca acesse sistemas corporativos em redes públicas ou abertas sem uma VPN confiável.

SENHAS E AUTENTICAÇÃO

- Habilite a autenticação em dois fatores sempre que possível.
- Troque senhas periodicamente e não reutilize senhas antigas e não grave senhas em navegadores.
- Use, preferencialmente, e-mail diferente do fornecido em sites comerciais, nos seus cadastros de sistemas públicos.

IV.COMPORTAMENTOS PREVENTIVOS NO AMBIENTE DE TRABALHO

IDENTIFICAÇÃO DE AMEAÇAS

- Fique atento a e-mails, mensagens ou ligações suspeitas solicitando informações.
- Faça de forma habitual varredura completa na estação de trabalho, a fim de verificar se há dispositivos desconhecidos conectados.
- Certifique-se de que todos os dispositivos conectados sejam verificados por um antivírus.

USO DE DISPOSITIVOS EXTERNOS

- Evite conectar pendrives ou dispositivos USB desconhecidos.
- Evite utilizar dispositivos externos.
- Realize varredura de antivírus antes de abrir arquivos em dispositivos externos.

PRESERVAÇÃO DO AMBIENTE

- Evite conversas sobre informações sensíveis em locais públicos.
- Certifique-se de que documentos confidenciais estejam protegidos antes de sair da mesa.
- Evite publicar em redes sociais informações que permitam identificar ações específicas que esteja fazendo no trabalho, assim como, atribuições e responsabilidades institucionais. A publicação indevida pode torná-lo alvo de cyber criminosos.

V. GERENCIAMENTO DE INCIDENTES DE SEGURANÇA

IDENTIFICAÇÃO DE INCIDENTES

A identificação de incidentes cibernéticos envolve sinais como acesso não autorizado a sistemas ou dados, indicando possíveis invasões, e perda ou roubo de dispositivos corporativos, que podem expor informações críticas. Outros indícios incluem acessos desconhecidos no histórico de login, sugerindo credenciais comprometidas, e mensagens de phishing ou malware, utilizadas para roubo de informações ou introdução de ameaças. Reconhecer esses sinais é essencial para mitigar riscos e proteger dados corporativos.

AÇÕES IMEDIATAS

- Informe imediatamente o setor de TI de seu órgão, ao identificar incidentes que possam ameaçar a segurança.
- Verifique, sempre que chegar a estação de trabalho, se há algum dispositivo estranho conectado ao seu computador.
- Não tente resolver problemas de segurança por conta própria.
- Desconecte dispositivos comprometidos da rede.

VI. TREINAMENTO E RESPONSABILIDADE PESSOAL

TREINAMENTO CONTÍNUO E CONSCIENTIZAÇÃO

- Participe regularmente de treinamentos de segurança da informação, conforme estabelecido na POSIC.
- Fique atualizado sobre novas ameaças e boas práticas.
- Promova uma cultura de segurança ao compartilhar boas práticas com colegas.

IMPORTÂNCIA DA CONSCIENTIZAÇÃO DOS USUÁRIOS

A manutenção da segurança dos sistemas depende do compromisso diário de cada usuário.
É essencial seguir as diretrizes desta cartilha, aplicando práticas seguras no uso de sistemas e dispositivos.

Reportar imediatamente comportamentos inseguros ou incidentes ao setor de TI contribui para a rápida mitigação de riscos.

Além disso, cada usuário deve proteger as informações sensíveis sob sua responsabilidade, garantindo que sejam armazenadas e compartilhadas de forma segura.

A colaboração de todos é fundamental para a construção de um ambiente digital seguro e confiável.

@mjsp_gov @senaspgov

www.gov.br/mj/pt-br

Ministério da Justiça e Segurança Pública

Ministério da Justiça e Segurança Pública

Escaneie o QR Code e acesse a cartilha.

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Segurança Pública
Diretoria de Gestão e Integração de Informações

Sala 520 - Anexo II
Esplanada dos Ministérios, Brasília - DF.
Fone: (61) 2025-3333

Sinesp
Sistema Nacional de Informações de Segurança Pública

SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO