Mini Guia de Boas Práticas

CAMPANHA DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO E LGPD NA SECRETARIA MUNICIPAL DA SAÚDE



SUS

PREFEITURA DE SÃO PAULO
SECRETARIA DA SAÚDE



1 PROTEJA SUA SENHA

Sua senha é pessoal e intransferível!

- Nunca compartilhe sua senha.
- Utilize senhas fortes e diferentes.
- Não anote senhas em locais expostos.
- Altere sua senha quando houver suspeita de acesso indevido.



Lembre-se

Sua senha protege o acesso aos sistemas da SMS

2 DUPLO FATOR DE AUTENTICAÇÃO (MFA)

Mais uma camada de proteção!

- Utilize o duplo fator de autenticação sempre que solicitado.
- Nunca compartilhe códigos de verificação.
- Não aprove acessos que você não iniciou.
- Se receber uma solicitação suspeita, comunique a equipe responsável.



Segurança começa com você!

3 PROTEJA OS DADOS DOS MUNÍCIPES

Dados pessoais exigem cuidado!

- Acesse apenas os dados necessários para o seu trabalho
- Não compartilhe informações de munícipes sem autorização e necessidade.
- Evite deixar prontuários e informações pessoais expostos.
- Mantenha o sigilo das informações de saúde.



Respeitar a privacidade é responsabilidade de todos!

4 CUIDADO COM DOCUMENTOS E INFORMAÇÕES

Evite a exposição de dados!

- Não deixe documentos com dados pessoais sobre a mesa.
- Guarde prontuários e documentos em locais seguros.
- Não descarte informações confidenciais no lixo comum.
- Verifique os destinatários antes de enviar documentos.



Um documento exposto pode comprometer a privacidade de alguém

5 BLOQUEIE SUA ESTAÇÃO DE TRABALHO

Saiu da mesa? Bloqueie o computador!

- Bloqueie a tela sempre que se afastar.
- Não permita que outras pessoas utilizem seu acesso.
- Mantenha o computador em local seguro.
- Não deixe sistemas abertos sem supervisão.



Um simples bloqueio ajuda a proteger os dados da SMS

6 IDENTIFICOU UM INCIDENTE? COMUNIQUE!

Não ignore situações suspeitas.

- Recebeu um e-mail suspeito? Comunique.
- Perdeu um equipamento? Informe imediatamente.
- Identificou acesso indevido? Relate.
- Enviou dados para o destinatário errado? Avise a equipe responsável.



Quanto mais rápido o incidente for comunicado, mais rápido poderá ser tratado.

7 MANTENHA SEU COMPUTADOR SEGURO

Atualizações ajudam a proteger os sistemas!

- Não interrompa atualizações de segurança autorizadas.
- Utilize apenas programas permitidos pela SMS.
- Não instale softwares sem autorização.
- Comunique mensagens de erro ou alertas de segurança.





8 CUIDADO AO COMPARTILHAR ARQUIVOS

Compartilhe informações com segurança!



- Verifique o destinatário antes de enviar arquivos.
- Compartilhe apenas os dados necessários.
- Não utilize ferramentas não autorizadas pela SMS.
- Evite disponibilizar documentos com dados pessoais em links públicos.

Compartilhar com responsabilidade também é proteger dados!

9 CUIDADO COM PEN DRIVES E DISPOSITIVOS USB

Um dispositivo desconhecido pode colocar os sistemas em risco!

- Não conecte pen drives desconhecidos.
- Utilize dispositivos autorizados.
- Não copie dados institucionais sem necessidade.
- Comunique comportamentos suspeitos ao suporte responsável.



Antes de conectar, verifique a origem!

10 CUIDADO COM GOLPES POR TELEFONE E MENSAGENS

Nem toda solicitação é confiável!

- Confirme a identidade de quem solicita informações.
- Não compartilhe senhas ou códigos de acesso.
- Não compartilhe dados pessoais ou sensíveis.
- Desconfie de pedidos urgentes e incomuns.
- Confirme solicitações pelos canais oficiais.



Na dúvida, pare e verifique antes de agir!

11 ACESSE SOMENTE O NECESSÁRIO

Cada acesso deve ter uma finalidade de trabalho!

- Consulte somente os dados necessários para sua atividade.
- Não acesse prontuários por curiosidade.
- Não realize consultas sem finalidade profissional.
- Respeite as permissões de acesso aos sistemas.



Acesso autorizado deve ser utilizado com responsabilidade

12 PROTEJA OS DADOS E OS BACKUPS

Informações importantes precisam de proteção!

- Salve os arquivos institucionais nos locais autorizados.
- Não mantenha dados de trabalho apenas no computador local.
- Não exclua arquivos institucionais sem autorização.
- Siga as orientações da equipe de TI para armazenamento e recuperação.



Proteger os dados é garantir a continuidade do atendimento!

13 CUIDADO COM E-MAILS SUSPEITOS (PHISHING)

Não caia em golpes!

- Não clique em links desconhecidos.
- Não abra anexos suspeitos.
- Confira o remetente antes de responder.
- Nunca informe senhas por e-mail.



Suspeitou? Não clique
Comunique a equipe responsável pela Segurança da Informação

14 USE A INTELIGÊNCIA ARTIFICIAL COM SEGURANÇA

IA pode ajudar. Mas os dados da SMS precisam ser protegidos!

Antes de utilizar uma ferramenta de Inteligência Artificial, pare e verifique o que você está compartilhando.



NÃO insira:

Dados pessoais de munícipes ou colaboradores. Nome, CPF, CNS, endereço ou telefone. Dados de saúde ou informações de prontuários. Senhas, credenciais ou informações de acesso. Números de balanços, relatórios ou informações internas não públicas. Documentos ou informações sigilosas da SMS.

PODE fazer:

Utilizar a IA para revisar ou melhorar textos. Criar ideias, modelos e conteúdos genéricos. Resumir informações desde que não contenham dados protegidos. Tirar dúvidas sobre assuntos gerais. Trabalhar com informações públicas ou devidamente anonimizadas.

Lembre-se:

A Inteligência Artificial é uma ferramenta de apoio. A responsabilidade pelo conteúdo inserido também é sua. Antes de enviar, pergunte: "Esses dados podem ser compartilhados?"

Proteja os dados. Use a IA com responsabilidade

15 Cuidado com a Engenharia Social

Nem sempre o golpe acontece pela tecnologia. Às vezes, ele começa com uma conversa!

- Desconfie de solicitações incomuns ou urgentes.
- Confirme a identidade de quem está solicitando informações.
- Nunca compartilhe senhas, códigos ou dados de acesso.
- Não forneça informações institucionais sem verificar a necessidade.
- Em caso de dúvida, confirme a solicitação pelos canais oficiais.



Lembre-se

Golpistas podem se passar por colegas, gestores ou equipes de suporte.
Pare. Verifique. Só depois responda.
Segurança da Informação é responsabilidade de todos!

16 Proteja os Dados do Munícipe

Os dados precisam de proteção do início ao fim!



Cuidado ao compartilhar:

Não envie exames, diagnósticos ou fotos de fichas médicas em grupos pessoais ou de trabalho. Evite compartilhar dados pessoais pelo WhatsApp.

Utilize sempre os sistemas e canais oficiais da SMS.

Cuidado ao descartar:

Não jogue fichas, rascunhos ou documentos com dados pessoais no lixo comum. Utilize a fragmentadora, se houver, e rasgue os papéis para um descarte correto.

Antes de descartar, verifique se o documento contém informações pessoais ou sigilosas.

Lembre-se:

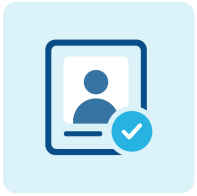
Dados de saúde são informações que exigem cuidado e proteção. Compartilhe somente quando necessário e descarte de forma segura.

Proteger os dados é proteger o cidadão!

17 Uso de Imagem

A imagem de uma pessoa também é um dado pessoal. Proteja a privacidade!

- Não fotografe ou grave: É proibido registrar imagens de pacientes, munícipes, prontuários ou procedimentos médicos sem autorização prévia e formal;
- Respeite a finalidade: A imagem só pode ser usada para o fim exato que foi autorizado no documento (exemplo: campanhas oficias da SMS ou finalidades assistenciais do paciente);
- Separe o pessoal do profissional: Nunca publique fotos do seu ambiente de trabalho ou de atendimentos nas suas redes sociais pessoais, mesmo que os pacientes consintam verbalmente.



Na dúvida, não compartilhe!

Canal de Dúvidas:

Ficou com dúvida se uma ação fere a LGPD?
Pergunte para nossa equipe e à DPO da SMS pelo e-mail:
smslgpd@PREFEITURA.SP.GOV.BR



SUS

PREFEITURA DE
SÃO PAULO
SECRETARIA
DA SAÚDE