

# MANUAL EXECUTIVO

## **USO **SEGURO** DO CELULAR**

PARA **GESTORES PÚBLICOS**



**2025**

## 1. PROTEÇÃO FÍSICA

- Mantenha o celular sempre sob sua supervisão.
- Não empreste o aparelho nem o entregue a terceiros.
- Use apenas carregadores e cabos próprios.
- Utilize power banks pessoais de marcas confiáveis.

## 2. CONFIGURAÇÕES DO SISTEMA

- Ative o bloqueio por biometria ou Face ID e utilize senhas fortes.
- Desative Bluetooth, NFC e Localização quando não estiver usando esses recursos.
- Mantenha o sistema operacional sempre atualizado.
- Ative o modo avião em reuniões sensíveis.
- Revise e limite permissões de apps frequentemente.
- Use apenas apps instalados via lojas oficiais.

### 3. COMUNICAÇÃO SEGURA

- Priorize apps com criptografia de ponta a ponta: como Signal, Wire, Threema e iMessage.
- Evite WhatsApp, Telegram (exceto "chats secretos") e SMS para comunicações sensíveis.
- Nunca envie informações críticas por e-mail ou mensagens não criptografadas.
- Ative a opção de autodestruição de mensagens nos apps que permitem.
- Use VPN corporativa em qualquer rede Wi-Fi pública.

#### Apps com criptografia de ponta a ponta

APP	PLATAFORMA	DESCRIÇÃO
Signal Private Messenger	Android / iOS	Criptografia de ponta a ponta, mensagens autodestrutivas e chamadas seguras
Wickr Me / Pro	Android / iOS	Comunicação criptografada com autodestruição e anonimato
Silent Phone / Silent Text	Android / iOS	Usado por órgãos governamentais e de inteligência
Threema	Android / iOS	Não exige número de telefone, comunicação totalmente criptografada

## 4. REDES E CONEXÕES

- Use firewall pessoal e monitore tráfego com apps de segurança.
- Confirme manualmente o nome da rede antes de se conectar.
- Prefira conexões 4G ou 5G.
- Configure pontos de acesso (hotspot) com senha forte.
- Desative conexões automáticas a redes conhecidas.

## 5. APLICATIVOS E ACESSOS

- Instale apenas apps essenciais e confiáveis.
- Remova apps com permissões excessivas ou desnecessárias.
- Nunca use apps de origem desconhecida ou lojas de terceiros.
- Utilize apps de segurança com análise de comportamento.
- Verifique periodicamente o consumo de bateria e dados.

### Navegação anônima e privacidade

APP	PLATAFORMA	DESCRIÇÃO
Ortob (Tor para Android)	Android	Roteia tráfego através da rede Tor para anonimato
Firefox Focus / DuckDuckGo Privacy Browser	Android / iOS	Bloqueiam rastreadores e não armazenam histórico
NetGuard	Android	Firewall sem root para bloquear conexões indesejadas

## 6. GESTÃO DE IDENTIDADE E SENHAS

- Utilize senhas fortes e únicas para cada serviço.
- Use gerenciadores de senha seguros (Bitwarden, 1Password etc).
- Ative autenticação multifator (MFA) sempre que possível.
- Não compartilhe logins com assessores ou terceiros.

### Antivírus e detecção de malware

APP	PLATAFORMA	DESCRIÇÃO
Kaspersky Mobile Security	Android / iOS	Proteção contra phishing, spyware e sites maliciosos
Bitdefender Mobile Security	Android / iOS	Firewall de apps, proteção contra rastreamento
Malwarebytes	Android / iOS	Deteção de adware, ransomware e spyware
Certo Mobile	Android / iOS	Detecta spyware avançado, como Pegasus

### Gerenciamento de senhas

APP	PLATAFORMA	DESCRIÇÃO
Bitwarden	Android / iOS / Desktop	Gratuito, open source, sincronização segura
1Password	Android / iOS / Desktop	Interface intuitiva e muito segura
LastPass	Android / iOS / Desktop	Bem conhecido, mas teve falhas no passado
KeePassDX (Android)	Android	Controle total sobre suas senhas

## 7. CONDUTA E BOAS PRÁTICAS

- Diferencie o uso pessoal do institucional.
- Não registre, armazene ou compartilhe informações sensíveis via celular.
- Oriente a equipe sobre segurança digital e práticas recomendadas.
- Evite fotografar documentos confidenciais.
- Não aceite brindes tecnológicos desconhecidos.

## 8. INCIDENTES E RISCOS

- Se perder ou tiver o celular roubado:
  - Bloqueie e apague os dados remotamente.
  - Altere imediatamente todas as principais senhas.
  - Registre boletim de ocorrência.
- Caso note sinais de invasão (lentidão, aquecimento, ou o surgimento de apps desconhecidos), procure suporte técnico imediatamente.

## 9. COMUNICAÇÃO CRÍTICA (ZERO TRUST DIGITAL)

- Em situações críticas, prefira:
  - Conversas presenciais (sem dispositivos por perto).
  - Linhas fixas seguras.
  - Rádios criptografados ou entrega manual de mensagens.
- Tenha palavras-código com sua equipe para indicar comprometimento do canal.

## 10. USO INTERNACIONAL

- Em viagens internacionais, evite usar o mesmo chip ou número institucional.
- Considere o uso de celular alternativo com chip local pré-pago não vinculado a dados pessoais.

## 11. DISPOSITIVOS RECOMENDADOS

- Prefira celulares atualizados com suporte oficial ativo (iPhone ou Android com patch recente).

## 12. ORIENTAÇÃO PARA ASSESSORIAS

- Todos os assessores diretos devem seguir os mesmos protocolos.
- Crie grupo restrito de contatos autorizados com instruções de segurança.

## 13. AUDITORIAS E REVISÕES

- Realize revisões semestrais com equipe técnica especializada.
- Solicite varreduras físicas e digitais nos aparelhos utilizados.

## 14. PROTOCOLOS EM AMBIENTES DE DECISÃO

- Proibir celulares em reuniões estratégicas ou salas de decisão.
- Utilizar bolsas de bloqueio de sinal (Faraday bags), se necessário.



## CHECKLIST DE AÇÕES DE SEGURANÇA

- ✓ Mantenha o celular longe do alcance de terceiros.
- ✓ Utilize senhas fortes e ative o bloqueio automático da tela.
- ✓ Ative autenticação multifator.
- ✓ Mantenha o sistema operacional atualizado.
- ✓ Utilize apps conhecidos e de fontes confiáveis.
- ✓ Ative a função de autodestruição de mensagens.
- ✓ Não compartilhe logins e senhas.
- ✓ Realize revisões periódicas e solicite varreduras físicas e digitais.

*prodam*



PREFEITURA DE  
**SÃO PAULO**