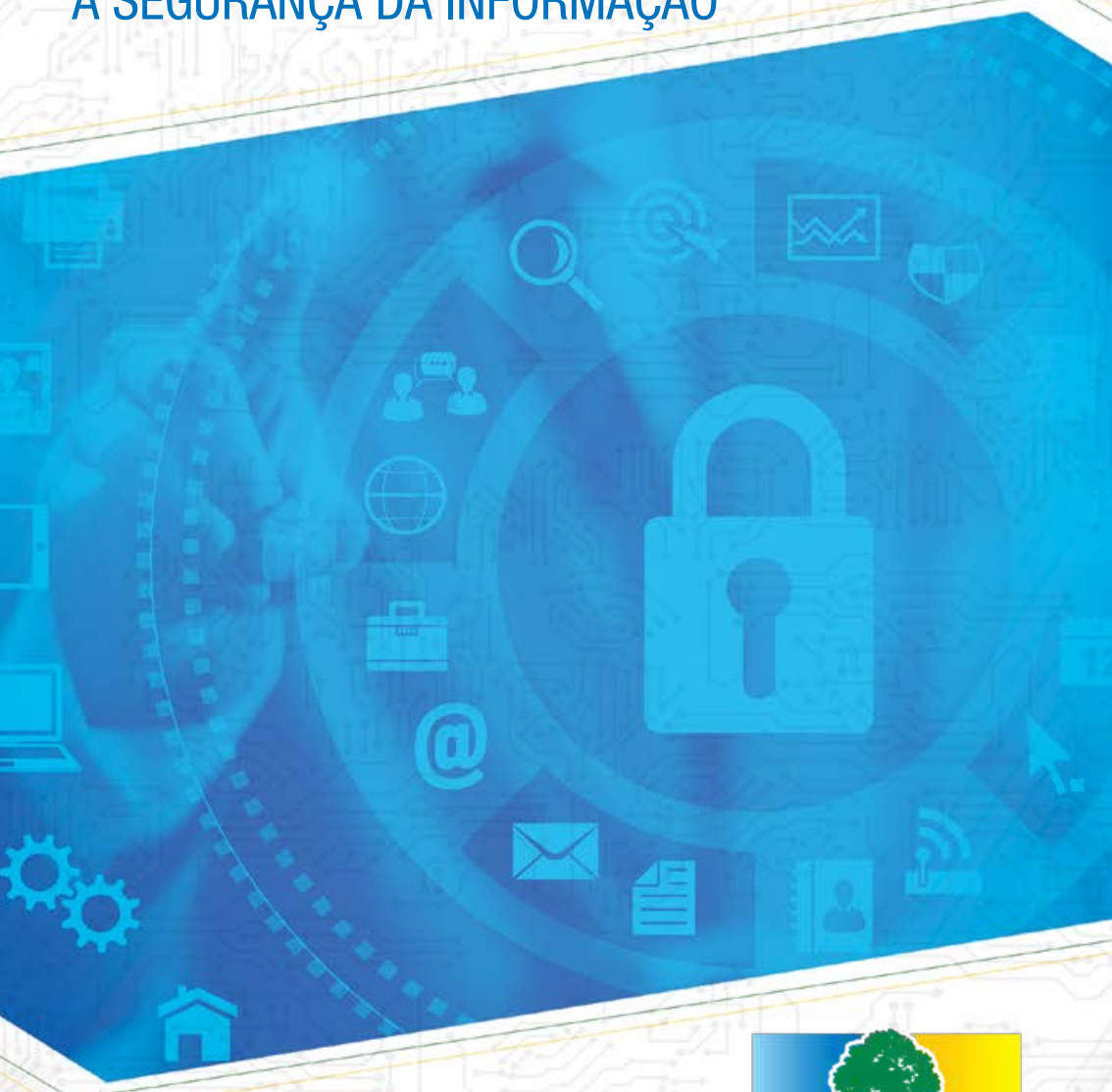
# COLABORADOR SEGURO NA INTERNET:

## RECOMENDAÇÕES ESSÊNCIAIS À SEGURANÇA DA INFORMAÇÃO



Ministério Público
do Estado do Amapá

# COLABORADOR SEGURO NA INTERNET:
## RECOMENDAÇÕES ESSÊNCIAIS À SEGURANÇA DA INFORMAÇÃO

Olá colaborador do **MINISTÉRIO PÚBLICO DO ESTADO DO AMAPÁ (MP-AP).**

Esta cartilha apresenta os principais temas sobre a **Segurança da Informação** e deve estar sempre com você, principalmente, durante suas atividades ligadas ao **MP-AP.** Por meio destas medidas buscamos juntos garantir a Segurança da Informação em nosso dia a dia, seja em relações internas ou externas à **instituição**, como em audiências e até mesmos em nossas casas.

### UMA RESPONSABILIDADE DE TODOS

O **MP-AP** trabalha com informações confidenciais sobre processos, colaboradores e investigações, com as quais estamos envolvidos em diversos momentos durante nossas atividades. Portanto, é importante que tenhamos a consciência de que a Segurança da Informação no **Ministério Público** é uma responsabilidade de **TODOS**, devendo ser tratada em conformidade com a **legislação nacional**, as **melhores práticas** de segurança e consequentemente com esta **cartilha**.
É necessário reforçar que diversas informações presentes no **MP-AP** possuem caráter público e devem estar acessíveis para os cidadãos a partir de sua respectiva solicitação e por meio dos trâmites indicados junto à Lei nº 12.527/2011 (Lei de acesso à informação -LAI). Todavia, essa cartilha indicará medidas de segurança da informação voltadas principalmente aos conteúdos que não fazem parte das previsões legais de LAI.

### A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Vivemos na Era do Conhecimento e a Informação é o nosso maior bem, seja no **SERVIÇO PÚBLICO** ou na vida pessoal. Assim sendo, a **Segurança da Informação** é essencial na nossa rotina, principalmente quando nos deparamos com os novos meios de comunicação como a Internet, a telefonia móvel e outros. Nesse cenário é indispensável que todos saibam dos inúmeros riscos aos quais estamos expostos e que respeitem diariamente as leis e as normas desta cartilha.

- Divulgação de dados sigilosos do **Ministério Público do Estado do Amapá** seja de maneira direta e intencional ou indireta, por exemplo, enviando informações confidenciais por meio de softwares não autorizados e não seguros como WhatsApp, Telegram, Messenger e outros;
- A não atualização ou verificação dos dados com os softwares de segurança indicados pela equipe de Tecnologia da Informação;
- Spoofing, phishing, ransomware, vírus e outros: softwares ou práticas de usuários mal-intencionados e alheios ao sistema da Instituição que aguardam e criam oportunidades para inserir informações falsas em nosso sistema, derrubá-lo, acessá-lo indevidamente ou sequestrar seus dados;
- Violação de Direitos Autorais por meio do uso de softwares ou conteúdos piratas;
- Ocorrência de fraudes por meio de softwares piratas ou aplicativos maliciosos de dispositivos móveis;
- Uso antiético dos componentes eletrônicos e de comunicação, que podem causar danos à imagem da Instituição;
- O vazamento de informações pessoais e íntimas de colaboradores do MP-AP em redes sociais, serviços de comunicação instantânea e na Internet em geral, as quais podem afetar a vida pessoal e profissional.

**LEMBRE-SE:** a Segurança da Informação é uma responsabilidade de todos!

# ÍNDICE

# SENHAS 1

Você emprestaria a chave do seu carro para outra pessoa? Claro que não, pois esta conduta gera um risco e traz responsabilidade para você, proprietário do equipamento. O mesmo ocorre quando tratamos da Segurança da Informação. Sua senha é a "chave" que abre o seu computador, dando acesso aos seus dados e também às redes e informações do MP-AP, como aplicativos, e-mail, Internet, rede institucional e outros. Portanto, esteja sempre atento ao uso da senha, tratando-a com confidencialidade e não a transferindo para nenhum outro colaborador ou indivíduo, seja amigo ou familiar, conforme indicado no art.8, inciso V, do Ato Normativo 002/2014-GAB/PGJ.

A seguir apresentamos algumas informações necessárias ao uso adequado da senha:

- **Sua senha é pessoal, intransferível e confidencial!** Você deve memorizá-la. Não a anote de maneira permanente ou que possa ser acessada ou vista por qualquer pessoa;
- **Jamais compartilhe seu login e senha** com demais colaboradores, amigos ou familiares, pois ela é pessoal e intransferível e será usada como prova de autoria;
- **Crie senhas fortes**, ou seja, que não possam ser adivinhadas com facilidade. Essa medida possui como finalidade **prevenir os riscos de roubo de identidade ou de invasão da rede Ministério Público**. Para criar uma senha forte siga as dicas abaixo:
    - Utilize no mínimo oito caracteres e se possível prefira senhas mais extensas;
    - Faça composições entre letras maiúsculas e minúsculas, números e caracteres especiais (! % #@$);
    - Crie senhas com frases mnemônicas: MffBN7a (Meu filme favorito é o Branca de Neve e os 7 anões);
    - Crie senhas utilizando o estilo de escrita usado em mensagens de texto "torpedo": T42&24ta5 (Tea for two and two for tea at 5);
    - Troque sua senha periodicamente (60 dias).

**LEMBRE-SE:** a sua senha é a primeira barreira de proteção das informações. Ela deve ser sempre confidencial e intransferível.


Username or email
login

# PROTEJA SEU EQUIPAMENTO

Em nosso dia a dia, como colaboradores do **MP-AP**, entramos em contato com computadores (Desktop), Laptops e outros dispositivos móveis como celulares e tablets, os quais podem ter acesso às redes da **Instituição** ou não. Entretanto, todos esses dispositivos merecem sempre a nossa atenção e cuidado diário, segundo as indicações apresentadas abaixo para cada tipo de dispositivo.

## COMPUTADOR

O computador é a nossa principal ferramenta de trabalho. Ele constitui uma valiosa fonte de informações, devendo ser protegido ao máximo em sua integridade interna e externa. Os computadores estão sujeitos a riscos como acesso indevido, vazamento, perda, furto ou roubo de informações e infecção por arquivos maliciosos (vírus, malwares e outras pragas virtuais).

Abaixo apresentamos algumas medidas voltadas especificamente para a **proteção do seu computador**.

- Não altere a configuração padrão entregue pelo **Ministério Público** presente em todos os computadores, desktops ou laptops;
- **Sempre bloquei manualmente o seu computador**, usando as teclas Ctrl + Alt + Delete e selecionando a opção bloquear ou clicando diretamente nas teclas Windows + L, ao sair da sua estação de trabalho;
- **Desligue o computador ao final do dia**, exceto em ocasiões excepcionais por indicação do Departamento Tecnologia da Informação;
- **Dados e informações profissionais devem ser armazenadas corretamente na rede institucional do MP-AP**, evitando perdas de conteúdo e acesso não autorizado por terceiros.

## LAPTOP

O uso de laptop exige medidas adicionais de segurança, tendo em vista a grande mobilidade que esse dispositivo

2

permite. Fique atento e faça uso seguro do laptop, protegendo as informações da **Instituição. Mantenha seu equipamento sempre à mão e seguro**, não o transportando de maneira exposta ou deixando-o em lugares de fácil identificação e remoção.

## DISPOSITIVOS MÓVEIS – CELULARES E TABLETS

Celulares e tablets já fazem parte da nossa rotina, tanto profissional como pessoal. Sendo assim, a nossa segurança não pode ser reduzida nesses dispositivos, principalmente quando se trata da privacidade de nossos colaboradores e da proteção das informações do **Ministério Público do Estado do Amapá**.

- Jamais deixe seu **dispositivo móvel desprotegido ou desbloqueado**. Utilize sempre uma **senha de bloqueio** para o seu dispositivo móvel, configurando-o para travamento automático após um período sem uso;
- Tenha seu **dispositivo móvel sempre à mão**, não o deixando em lugares indevidos ou visíveis, como em cima de mesas, facilitando a ocorrência de furtos ou roubos;
- Tenha sempre um **antivírus** instalado e atualizado;
- Habilite o backup em seu dispositivo;
- Jamais altere configurações padrões de programação do seu dispositivo, por exemplo, inserindo sistemas operacionais piratas ou paralelos;
- **Não instale aplicativos** que solicitam acesso a informações do seu dispositivo que não estejam ligadas diretamente às funções do aplicativo.

**LEMBRE-SE:** em caso de furto ou roubo do seu dispositivo proceda imediatamente com o boletim de ocorrência junto à autoridade policial competente.

# CORREIO ELETRÔNICO 3

**Simples e rápido, o correio eletrônico é um instrumento de uso diário. Seja um usuário de e-mail cuidadoso.**

**Antes de enviar quaisquer informações de caráter confidencial ou que envolvam assuntos sensíveis verifique novamente os destinatários**, pois uma pequena distração que provoque o envio de mensagem para pessoa errada pode ser prejudicial. Lembre-se, conteúdo digital não tem devolução. Depois de enviada, não é possível bloquear a leitura da mensagem nem desfazer o envio. Por isso, é preciso muita atenção.

**Conteúdos que devem ser excluídos e não compartilhados ou abertos:**

- Mensagens cujo **emissor** ou o **conteúdo** lhe pareçam **duvidosos**.
- As correntes de amizade, bem como anúncios de vírus que não tenham sido enviados pelo Departamento de Tecnologia da Informação.
- Questionários ou sondagens cuja origem não seja o **Ministério Público**.
- Evite deixar sua senha de acesso ao e-mail automaticamente salva em seu dispositivo;
- **Não envie conteúdos institucionais para e-mails pessoais ou serviços externos** não pertinentes as atividades do **MP-AP**.
- Leia a Portaria nº 0403/2011 – GAB/PGJ.

# INTERNET 4

**A Internet nos permite ter acesso a uma grande variedade de serviços, porém nem todos estes são coerentes com as normas do Ministério Público e com a atividade profissional de nossos colaboradores.**

O envio ou recebimento de conteúdos na Internet depende, por exemplo, da localização precisa da sua máquina na rede, o que ocorre por meio do número de IP (Internet Protocol). No **MP-AP** os dispositivos ligados à rede institucional do **Ministério Público** possuem IP institucional, portanto é necessário ter muita cautela ao utilizar a Internet em nossas instalações, pois acessos indevidos a conteúdos ilegais podem trazer sérios riscos à **Instituição** e inviabilizar ou dificultar o acesso à Internet por outros colaboradores.

**LEMBRE-SE:** o número de usuários não é um indicativo de legitimidade de um serviço. Ou seja, o fato de familiares e amigos fazerem uso de plataformas torrents para baixar filmes, por exemplo, não implica que este serviço está juridicamente autorizado. Portanto, fique atento e em caso de dúvida entre em contato com o Departamento Tecnologia da Informação.

**Para utilizar a Internet com precaução siga as recomendações abaixo:**

- **Apenas acesse sites, portais ou conteúdos,** permitidos pelo Provimento nº 004/2013 PGJ do **Ministério Público, adequados ao ambiente de trabalho e relacionados às suas atividades, evitando todo e qualquer ambiente on-line** que possa trazer danos à imagem da **Instituição**.
- Cuidado com o **uso das ferramentas de buscas.** Não devem ser utilizados métodos de busca que possam expor informações do **MP-AP**.
- A atuação em **fóruns de discussão** necessita de cuidado redobrado, pois a divulgação de informações nestes pode implicar em responsabilidade pessoal e causar prejuízo à **Instituição**.
- O uso de **sites de armazenamento externo** não é permitido. Utilize as ferramentas disponibilizadas pelo Departamento de Tecnologia da Informação para transferência e armazenamentos externos de informações.
- Cuidado ao efetuar **compras ou pagamentos on-line**. Sempre verifique se os sites possuem reputação confiável e se possuem criptografia nas transações on-line (HTTPS).
- Leia o Provimento nº 004/2013 PGJ do **MP-AP**.

**LEMBRE-SE:** tudo na Internet fica documentado e registrado. Pense sempre duas vezes antes de realizar qualquer procedimento.

# DISPOSITIVOS EXTERNOS DE ARMAZENAMENTO

5

Dispositivos externos para armazenamento de dados, como memory stick, pen-drive e hd´s portáteis, permitem a mobilidade de grande quantidade de dados de maneira simplificada e facilitada. Todavia, essa mobilidade apresenta sérios riscos à integridade das informações do **Ministério Público**, principalmente em caso de perdas e furtos. Portanto, o uso desses dispositivos deve ser focado apenas no **trânsito temporário de dados**, não em seu armazenamento.

**CORRETA E SEGURA CONSERVAÇÃO DE DADOS MINISTÉRIO PÚBLICO DO ESTADO DO AMAPÁ**

Os dados e as informações são o maior patrimônio do **MP-AP.** Por essa razão, a proteção e o armazenamento devidos são indispensáveis em nossas atividades. A seguir apresentamos as principais dicas quanto a estes procedimentos.

- As informações e dados armazenados em nossos dispositivos estão sujeitos a falhas, sabotagem ou danos que impossibilitem o acesso. Portanto, é indispensável que estes **conteúdos sejam salvos adequadamente na rede do Ministério Público**, permitindo a organização das informações, o acesso de outros colaboradores envolvidos no processo e a sua conversação;
- O armazenamento em dispositivos externos como chave USB e outros, não são apropriados para a conservação ou o arquivamento permanente de dados, devendo ser utilizado de maneira segura e em casos temporários de trânsito apenas.

# RESPEITO À LEGISLAÇÃO 6

Além de suas normas internas, o **MP-AP** reforça aos seus colaboradores a necessidade de atender as seguintes diretrizes:

- Princípio da boa-fé;
- Princípios de dignidade humana;
- Privacidade de dados pessoais;
- Respeito aos direitos autorais e a propriedade industrial;
- Sigilo relativo à correspondência e à comunicação;
- Sigilo profissional.

O uso dos Sistemas de Informação do **MINISTÉRIO PÚBLICO** deve respeitar sempre os princípios de ordem pública e bons costumes, bem como os interesses e a reputação da instituição.

# REDES SOCIAIS

7

As redes sociais permitem o compartilhamento e a criação de conteúdos de maneira coletiva e descentralizada. Contudo, também trazem sérios riscos, portanto, fique atento aos princípios apresentados abaixo.

- Utilize as redes sociais com precaução e bom senso;
- A sua imagem é uma extensão da imagem do **MP-AP.** Tome atitudes digitais sempre pensando na maior proteção da sua imagem pessoal e da **Instituição**;
- Não compartilhe conteúdos confidenciais ou sigilosos do **Ministério Público** nas redes;
- Não aborde questões ou incidentes internos do **MP-AP** nas redes sociais;
- Os perfis e as informações disponibilizados na Internet podem ser falsos, por isso não conceda informações sobre o **Ministério Público** de maneira direita e indireta para nenhuma pessoa por estes serviços;
- Não compartilhe agendas de trabalho, compromissos ou rotas nas redes sociais.

**LEMBRE-SE:** a sua imagem é uma extensão da imagem da **Instituição**.

# ATUAÇÃO PROFISSIONAL À DISTÂNCIA

8

A atuação profissional à distância exige ainda maior cuidado frente à proteção dos dados, tendo em vista que dados confidenciais do **Ministério Público** podem ser enviados e recebidos a todo o momento de um dispositivo ligado externamente à rede do **MP-AP**. A seguir apresentamos as principais medidas de proteção que você deve levar em consideração.

- Garantir a confidencialidade do acesso aos dados e aos terminais;
- Armazenar conteúdos do **Ministério Público** apenas nos dispositivos gerenciados pela **Instituição**;
- Garantir a proteção dos dispositivos de acesso remoto à rede do **MP-AP**;
- Utilizar conexão segura à internet, com dispositivos que tenham antivírus habilitado, especialmente em ambientes de terceiros como hotéis e locais públicos;
- Descarte correta e seguramente os documentos do **Ministério Público do Estado do Amapá**, retornando-os ou triturando-os;
- Não realizar uso indevido ou impróprio dos dispositivos do **MP-AP** ou da rede institucional.

# PROTEGENDO SUA FAMÍLIA: INTERNET E DISPOSITIVOS MÓVEIS

9

Os impactos dos avanços tecnológicos na vida pessoal transpassam a figura da pessoa em si, alcançando também instituições sociais como a família e a escola. Por isso, preocupado com a saúde também da família do colaborador do **Ministério Público do Estado do Amapá**, apresentamos aqui algumas dicas de uso familiar consciente das redes sociais e dispositivos móveis.

- Mantenha a porta digital fechada, utilizando senha de acesso nos dispositivos accesspoint e desligando o recurso wireless em horários não utilizados pela família;
- Celular não é brinquedo, por isso, acompanhe de perto e monitore as atividades dos seus filhos. Na internet e nas redes sociais existem recursos que exigem idade mínima que deve ser seguida;
- Leia sempre os termos de uso dos serviços e das redes sociais que você e seus filhos utilizam, pois é fundamental conhecer as regras do jogo;
- Realize buscas periódicas na Internet para saber o que aparece sobre você e sua família nos buscadores. Proteja a reputação digital da sua família;
- Conheça os amigos digitais dos seus filhos, com quem eles conversam no celular, no WhatsApp, no Skype, nos jogos pela Internet, além dos seus sites favoritos;
- Mantenha máquinas e dispositivos sempre com os softwares de segurança devidamente instalados e atualizados e utilize software de controle parental;
- Não utilize máquinas e dispositivos corporativos do **MP-AP** para acessar ou deixar à disposição de terceiros, ainda que familiares. O recurso tecnológico de trabalho deve ser utilizado apenas para finalidade profissional;
- Para proteger a família acesse conteúdos sobre ética e segurança digital como os do Instituto iStart (www.familiamaissegura.com.br/i-start/).

# CONTATO 10

Caso você ainda possua alguma dúvida sobre as informações apresentadas neste guia, não deixe de nos contatar ou de ler e acompanhar as nossas normas internas

Quando houver incidentes relacionados com a Segurança da Informação, entre em contato o mais rápido possível com:

- A Central de TI pelo telefone (96) 3198-1611 ou por e-mail dti@mpap.mp.br.
- Maiores informações sobre atos e normas podem ser obtidas em nosso Portal Corporativo (MP Conectado) junto aos arquivos do Departamento de TI.

**LEMBRE-SE:** esta cartilha possui as dicas essenciais à segurança da informação da sua família e do **Ministério Público do Estado do Amapá**. Fique sempre atento e não esqueça que você, colaborador do **MP-AP**, é uma peça fundamental para proteger a **Instituição**. A Segurança da Informação é uma responsabilidade de **todos**!

# Ministério Público
do Estado do Amapá

CRÉDITO DE AUTORIA:

PATRICIA PECK PINHEIRO
TREINAMENTOS