CAO DEFESA DE DADOS PESSOAIS E INTELIGÊNCIA ARTIFICIAL

Cartilha de Aplicativos Homologados MPMT

Navegue Seguro: Seu Guia de Aplicativos Oficiais e Como Usar

3ª Edição

MPMT Ministério Público DO ESTADO DE MATO GROSSO | DTI - Departamento de Tecnologia da Informação

CAO/MPMT DEFESA DE DADOS PESSOAIS E INTELIGÊNCIA ARTIFICIAL

O uso exclusivo de aplicativos homologados e a segurança institucional

“A utilização exclusiva de aplicativos homologados é prática fundamental para a proteção de dados sensíveis, prevenção de vulnerabilidades e mitigação de riscos que possam comprometer a integridade da instituição.

No contexto da contrainteligência, o uso de soluções não autorizadas representa uma porta de entrada para ações hostis, vazamentos de informações e comprometimento das estruturas institucionais. Além disso, a observância das diretrizes fixadas assegura a conformidade com a Lei Geral de Proteção de Dados (LGPD), promovendo o uso ético e seguro dos recursos tecnológicos.

O Centro de Segurança e Inteligência ratifica: a adesão a essa política (PSI - Ato Adm. 495-2015-PGJ) baseada nas melhores práticas de segurança da informação internacionais e implantadas pelo Departamento de Tecnologia da Informação, é um compromisso com a segurança institucional e a proteção dos nossos mais valiosos ativos.”

Mauro Zaque de Jesus
Coordenador do Centro de Segurança e Inteligência-CSI

SUMÁRIO

Objetivo da Cartilha

Esta cartilha foi elaborada com o objetivo de orientar membros e servidores do Ministério Público no uso seguro, eficiente e responsável dos aplicativos homologados pela instituição. Em um ambiente cada vez mais digital, é fundamental que as ferramentas tecnológicas utilizadas estejam em conformidade com as normas de segurança da informação e com a legislação vigente.

A PSI (Politica De segurança Institucional) instituída através do Ato Adm. 495-2015-PGJ, estabelece diretrizes claras de segurança e proteção do ambiente tecnológico, onde o uso de softwares homologados representa um importante passo esta finalidade.

Nesse contexto, o uso consciente dos aplicativos homologados é essencial para garantir a conformidade legal e a integridade das informações tratadas no âmbito institucional.

Para facilitar a consulta e promover uma melhor compreensão, **esta cartilha foi organizada em quatro edições**, abordando de forma clara e objetiva os principais aspectos relacionados ao uso adequado dos aplicativos, à proteção de dados, à segurança da informação e às responsabilidades dos usuários.

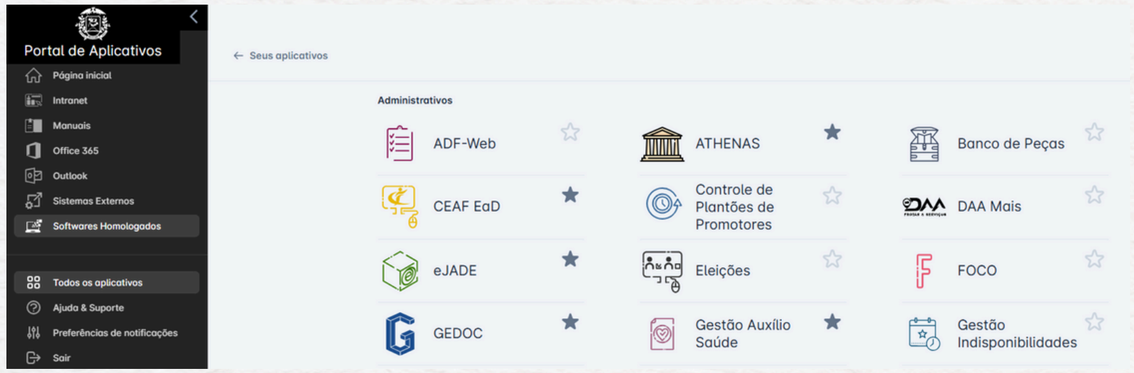
Ao adotar as boas práticas aqui apresentadas, membros e servidores contribuem ativamente para a construção de um ambiente digital mais seguro, ético e eficiente. A proteção de dados é uma responsabilidade coletiva e contínua, que exige atenção, comprometimento e atualização constante.

Público Alvo: Membros e Servidores do MPMT

Passo a passo para baixar qualquer um dos seguintes aplicativos:

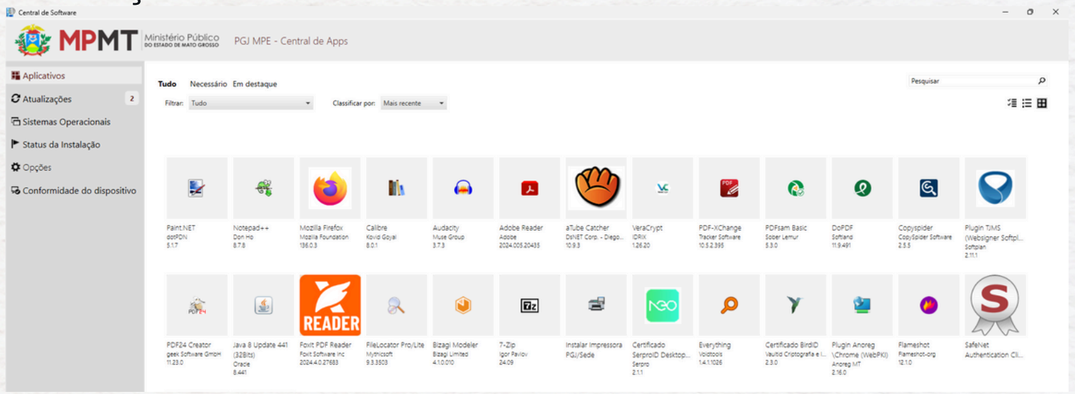
Obs: Esse passo a passo só funciona para instalação em computadores institucionais.

1. Abra o portal de aplicativos e, na lateral esquerda, clique em “Softwares Homologados”



2. Ao abrir essa janela, clique no ícone em azul claro em Abrir SCCliente.

3. Então se abrirá essa tela com todos os aplicativos disponíveis para instalação segura e gratuita. Escolha o aplicativo desejado, clique em instalar e então aguarde a instalação.



Obs: Caso a central de software não abra ou apareça algum erro. Acione a central de serviços por meio dos seguintes canais:

- Telefone - 3613 5166; ou
- Portal de serviços - https://suporte.mpmt.mp.br/

5. Multimídia

5.1.aTube Catcher

O que é?

- Programa gratuito que permite baixar vídeos de sites como YouTube, Vimeo e outros.
- Converte vídeos para vários formatos (MP4, MP3, AVI, entre outros).
- Possui funções extras como gravação de tela, captura de áudio e criação de DVDs.

Funcionalidades:

- Download de vídeos e músicas.
- Conversão de formatos para diferentes dispositivos.
- Gravação de tela (aulas, tutoriais, reuniões).
- Criação de DVDs e CDs.

Boas Práticas:

- Respeite os direitos autorais: Use apenas para conteúdos livres, pessoais ou autorizados.
- Não compartilhe vídeos com dados pessoais sem permissão dos envolvidos.
- Verifique se o conteúdo é legal para download, especialmente músicas, filmes ou materiais protegidos.
- Use a gravação de tela de forma ética, com consentimento em reuniões ou aulas.
- Mantenha o programa atualizado para evitar falhas de segurança e garantir melhor desempenho.

Link para baixar na web: aTube Catcher

5.2.Audacity

O que é?

Audacity é um editor de áudio digital gratuito e de código aberto. Ele oferece ferramentas de gravação, edição e mixagem de áudio, sendo adequado tanto para iniciantes quanto para profissionais. Pode ser usado para criar podcasts, editar música e realizar várias outras tarefas relacionadas ao áudio.

Funcionalidades:

- Gravação de áudio de microfone, mixer ou dispositivos externos.
- Edição de áudio (cortar, copiar, colar, remover ruídos, normalizar).
- Aplicação de efeitos (eco, reverberação, equalização, compressor).
- Suporte a vários formatos: MP3, WAV, OGG, FLAC, entre outros.

Boas Práticas:

- Remova informações pessoais ou sensíveis dos áudios antes de compartilhar.
- Use formatos de exportação seguros, como WAV ou FLAC, para preservar qualidade e integridade.
- Salve projetos no formato .AUP (projeto do Audacity) para manter todas as edições acessíveis.
- Faça backup dos projetos antes de realizar edições grandes.
- Respeite os direitos autorais ao editar músicas, trilhas ou conteúdos de terceiros.
- Mantenha o Audacity atualizado para garantir estabilidade e segurança.

Link para baixar na web: Audacity

6.1.Veracrypt

O que é?

O VeraCrypt é um programa gratuito e de código aberto usado para criptografar arquivos, pastas, pendrives, discos e partições inteiras, protegendo informações contra acessos não autorizados. Ele cria um tipo de cofre digital seguro, onde os dados só podem ser acessados mediante uma senha forte. Muito utilizado por empresas, profissionais e qualquer pessoa que deseja garantir a privacidade e a segurança dos seus dados, o VeraCrypt utiliza algoritmos de criptografia avançados, tornando praticamente impossível que alguém acesse as informações sem a senha correta.

Funcionalidades:

- Criptografia de volumes: Cria um arquivo criptografado que funciona como um disco virtual protegido por senha.
- Criptografia de discos inteiros: Protege o HD, SSD ou pendrive inteiro.
- Criptografia de partições: Protege partições específicas do sistema.
- Proteção forte: Utiliza algoritmos robustos como AES, Serpent e Twofish.
- Funciona em Windows, Linux e macOS.

Boas Práticas:

1. Crie senhas fortes: → Use combinações de letras maiúsculas, minúsculas, números e símbolos.
2. Anote e guarde sua senha em local seguro: → Se perder a senha, não há como recuperar os dados.
3. Escolha algoritmos de criptografia confiáveis: → AES é o mais recomendado, equilibrando segurança e desempenho.
4. Mantenha backups seguros: → Criptografar não substitui ter cópias de segurança dos dados.
5. Verifique a integridade dos arquivos criptografados regularmente: → Isso evita perda acidental de dados por corrompimento.
6. Desmonte (unmount) o volume quando não estiver usando: → Mantê-lo montado expõe os dados caso alguém acesse seu computador.
7. Atualize o VeraCrypt sempre que possível: → Corrige vulnerabilidades e melhora a segurança.
8. Use o VeraCrypt apenas em computadores confiáveis: → Se houver vírus ou keyloggers, sua senha pode ser roubada mesmo com a criptografia.
9. Evite nomear arquivos criptografados com nomes que revelem seu conteúdo: → Isso aumenta a sua segurança e discrição.

Link para baixar na web: Veracrypt

6.2.SafeNet

O que é?

O SafeNet é uma solução de segurança digital desenvolvida pela empresa Thales, utilizada para proteger informações sensíveis, controlar acessos e garantir a confidencialidade dos dados. Ele é muito usado para geração e gerenciamento de senhas, autenticação forte (como tokens e certificados digitais), criptografia de dados e proteção de identidades. No Brasil, o SafeNet é bastante conhecido por ser utilizado na geração de senhas para acesso seguro a sistemas de instituições públicas e privadas, além de proteger transações online, ambientes corporativos e documentos eletrônicos.

Funcionalidades:

- Autenticação forte: Geração de senhas temporárias (token) para acesso seguro.
- Proteção de identidade: Garante que só o usuário autorizado acesse sistemas.
- Assinatura digital: Permite assinar documentos eletrônicos com validade jurídica.
- Criptografia: Protege arquivos e dados contra acessos não autorizados.
- Acesso seguro a sistemas: Protege logins em redes corporativas e plataformas.
- Gestão de usuários e acessos: Controle centralizado de permissões e dispositivos.

Boas Práticas:

1. Mantenha seus tokens ou dispositivos SafeNet em local seguro para evitar perda ou uso indevido.
2. Nunca compartilhe sua senha ou PIN associado ao SafeNet com outras pessoas.
3. Atualize as senhas regularmente, conforme as políticas de segurança da sua instituição.
4. Utilize o SafeNet apenas em dispositivos confiáveis, livres de vírus e malwares.
5. Em caso de perda ou roubo do dispositivo, comunique imediatamente à equipe de segurança ou suporte.
6. Mantenha o software do SafeNet sempre atualizado, garantindo proteção contra falhas e vulnerabilidades.
7. Desconecte o dispositivo SafeNet quando não estiver em uso, evitando acessos não autorizados.

Link para baixar na web: SafeNet

6.3.SerproID

O que é?
O Certificado SerproID é um certificado digital, uma espécie de identidade digital para o ambiente online.

Funcionalidades:

- **Autenticação Segura:** Acessar sistemas e plataformas online com um nível de segurança muito maior do que apenas com login e senha. É como ter um crachá digital que comprova quem você é, impedindo acessos não autorizados. Isso é crucial para serviços governamentais, bancos e outras plataformas que exigem alta confiabilidade.
- **Assinatura Digital de Documentos:** Permite que você assine documentos eletronicamente com a mesma validade jurídica de uma assinatura feita à mão. Isso significa que contratos, declarações e outros documentos importantes podem ser assinados de forma rápida, eficiente e segura, sem a necessidade de impressão e reconhecimento de firma.

Boas Práticas:

- **Mantenha seu Certificado Protegido:** O SerproID geralmente é armazenado em um dispositivo físico (como um token USB ou cartão inteligente) ou em nuvem. Trate-o como se fosse a chave de sua casa. Não o deixe desacompanhado e certifique-se de que ele esteja sempre em um local seguro.
- **Use Senhas Fortes e Exclusivas:** O acesso ao seu SerproID é protegido por uma senha (PIN ou passphrase). Crie uma senha forte, com uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Nunca use senhas óbvias (como datas de aniversário) e nunca a compartilhe com ninguém.
- **Cuidado com Phishing e Fraudes:** Esteja sempre alerta para e-mails ou mensagens suspeitas que solicitem informações sobre seu Certificado SerproID ou que peçam para você clicar em links desconhecidos. O Serpro ou qualquer outra instituição séria nunca solicitará sua senha ou informações sensíveis por e-mail ou telefone.
- **Mantenha seu Sistema Atualizado:** Utilize sempre um sistema operacional e um navegador de internet atualizados. Isso garante que você tenha as últimas correções de segurança e que o SerproID funcione corretamente.
- **Instale o Software Necessário:** Para usar o SerproID, você precisará instalar softwares específicos (como os drivers do token ou o software de gerenciamento do certificado). Certifique-se de baixar esses softwares somente dos canais oficiais do Serpro ou da certificadora.

Link para baixar na web: SerproID

6. Segurança e Certificação Digital

6.4.BirdID

O que é?

O BirdID é um certificado digital projetado para ser sua identidade segura no mundo digital. Ele funciona como uma credencial eletrônica que garante a autenticidade e a integridade de suas transações e documentos online. Sua principal finalidade é proporcionar um ambiente virtual mais seguro e confiável para indivíduos e organizações.

Funcionalidades:

- **Autenticação Segura:** Comprovar sua identidade de forma robusta ao acessar diversos sistemas e plataformas online. Isso é crucial para acessar serviços governamentais, sistemas corporativos e qualquer outra aplicação que exija um alto nível de segurança para evitar acessos indevidos.
- **Assinatura Digital:** Uma das funcionalidades mais poderosas do BirdID é a capacidade de assinar documentos eletronicamente com validade jurídica. Essa praticidade agiliza processos e reduz custos.
- **Realização de Operações Seguras Online:** O BirdID permite que você execute uma variedade de operações online com a certeza de que seus dados estão protegidos e sua identidade está verificada. Isso abrange desde transações financeiras até o envio de informações sigilosas, garantindo a integridade e a confidencialidade dos dados.

Link para baixar na web: BirdID

Boas Práticas:

- **Proteja sua Senha (PIN):** O acesso é protegido por uma senha. Crie uma senha forte e exclusiva, combinando letras maiúsculas e minúsculas, números e símbolos. Nunca compartilhe sua senha com ninguém e evite anotá-la em locais de fácil acesso.
- **Mantenha o Certificado em Local Seguro:** Mantenha-o em um local seguro e evite deixá-lo conectado a computadores públicos ou desprotegidos.
- **Cuidado com Tentativas de Phishing:** Esteja sempre atento a e-mails, mensagens ou chamadas telefônicas que solicitem sua senha, dados do certificado ou que o direcionem para sites suspeitos. Empresas e instituições legítimas nunca pedirão essas informações por esses canais.
- **Verifique a Validade do Certificado:** Certificados digitais possuem um prazo de validade. Fique atento à data de expiração do seu BirdID e providencie a renovação com antecedência para evitar interrupções no uso.
- **Mantenha seu Software Atualizado:** Certifique-se de que seu sistema operacional, navegador e o software de gerenciamento do BirdID estejam sempre atualizados. Isso garante que você tenha as últimas correções de segurança e compatibilidade.
- **Instale Apenas Drivers Oficiais:** Ao instalar os drivers ou softwares necessários para o seu BirdID, baixe-os apenas dos canais oficiais da Autoridade Certificadora que emitiu seu certificado.

7. Plugins e Ferramentas Específicas

7.1.Plugin TJMS

O que é?

O Plugin TJMS é uma ferramenta essencial desenvolvida para aprimorar a experiência de advogados e profissionais do direito que atuam junto ao Tribunal de Justiça de Mato Grosso do Sul (TJMS). Ele serve como uma ponte, facilitando a comunicação e a interação com os sistemas judiciais eletrônicos, tornando o trabalho desses profissionais mais ágil e eficiente. Em essência, ele moderniza e simplifica o acesso à Justiça no estado.

Funcionalidades:

- **Acesso Simplificado a Processos Judiciais:** Com o plugin, o acesso a informações e documentos de processos torna-se mais rápido e intuitivo. Ele pode automatizar ou facilitar etapas de login e navegação, permitindo que os profissionais encontrem o que precisam com menos cliques e de forma mais organizada, seja para consultar andamentos, despachos ou documentos anexados.
- **Facilitação da Realização de Petições Eletrônicas:** O envio de petições e outros documentos ao TJMS é uma tarefa constante para os profissionais do direito. O plugin agiliza esse processo, potencialmente otimizando o carregamento de arquivos, a assinatura digital e o envio para o sistema, garantindo que as petições sejam protocoladas corretamente e sem complicação.

Boas Práticas:

- Utilize Navegadores Compatíveis: O TJMS geralmente indica quais navegadores de internet são compatíveis e mais recomendados para o uso do plugin (como o Mozilla Firefox ou Google Chrome). Certifique-se de usar um desses navegadores e de que ele também esteja atualizado para sua versão mais recente.
- Certificado Digital em Ordem: O uso do Plugin TJMS, especialmente para assinatura de documentos, depende diretamente do seu certificado digital (e-CPF ou e-CNPJ) estar válido e corretamente instalado em seu computador. Mantenha os drivers do seu certificado atualizados e verifique sua validade regularmente.
- Atenção às Configurações de Segurança: Alguns navegadores ou antivírus podem, por padrão, bloquear a execução de plugins. Verifique as configurações de segurança do seu navegador e do seu software de proteção para garantir que o Plugin TJMS não esteja sendo impedido de funcionar. Se necessário, adicione o site do TJMS como uma exceção confiável.
- Busque Suporte Oficial: Se você encontrar problemas ou tiver dúvidas sobre o funcionamento do plugin, procure o suporte técnico oferecido pelo Tribunal de Justiça de Mato Grosso do Sul ou consulte os manuais e tutoriais disponíveis em seu portal.

Link para baixar na web: Plugin TJMS

7.2.Plugin Anoreg

O que é?

Ferramenta digital desenvolvida para otimizar e simplificar a interação de profissionais com os serviços notariais e de registros em todo o Brasil. Ele atua como uma ponte entre o usuário e os sistemas dos cartórios, tornando a comunicação e a execução de diversas tarefas mais eficientes e seguras no ambiente digital. Em um cenário onde a digitalização é cada vez mais presente, esse plugin se torna um aliado fundamental para quem lida diariamente com a burocracia dos registros públicos.

Funcionalidades:

- **Interação Simplificada com Sistemas de Cartórios:** A principal função do plugin é permitir uma comunicação fluida com as plataformas digitais dos cartórios. Isso pode envolver desde a consulta de matrículas de imóveis, buscas de certidões, até o acompanhamento de processos de registro. Ele pode automatizar o preenchimento de formulários, facilitar o upload de documentos e otimizar a navegação entre diferentes sistemas.
- **Acesso Direto a Serviços de Registro:** Além da interação geral, o plugin pode oferecer atalhos ou interfaces diretas para serviços específicos, como o pedido de certidões online, a solicitação de averbações ou o envio de documentos para registro, tudo de forma integrada e segura

Boas Práticas:

- **Utilize Navegadores Compatíveis:** Certifique-se de usar um navegador de internet que seja compatível e recomendado pela Anoreg ou pelas plataformas dos cartórios. Manter o navegador atualizado também é crucial para evitar problemas de funcionamento.
- **Certificado Digital em Dia:** Muitas operações realizadas através do plugin, como a assinatura de documentos ou a autenticação, exigem o uso de um certificado digital válido (e-CPF ou e-CNPJ). Garanta que seu certificado esteja ativo, corretamente configurado e com os drivers instalados.
- **Atenção às Configurações de Segurança do Navegador:** Alguns navegadores ou softwares de segurança podem, por padrão, bloquear a execução de plugins. Verifique as configurações do seu navegador e, se necessário, adicione os sites da Anoreg e dos cartórios como exceções confiáveis para permitir o funcionamento do plugin.
- **Busque Suporte Oficial:** Em caso de dúvidas ou problemas técnicos com o plugin, procure os canais de suporte oficiais da Anoreg ou da entidade responsável pelo desenvolvimento e manutenção da ferramenta. Evite buscar soluções em fontes não-oficiais.

Link para baixar na web: Plugin Anoreg

Ministério Público do Estado de Mato Grosso

Centro de Apoio Operacional de Defesa de Dados Pessoais e Inteligência Artificial

– DICAS DO CAO DDPIA –

Equipe do Centro de Apoio Operacional de Defesa de Dados Pessoais e Inteligência Artificial

Membro Coordenador do CAO - DDPIA

Adalberto Ferreira de Souza Junior – Promotor de Justiça do Ministério Público do Estado de Mato Grosso

Membro Coordenador Adjunto do CAO - DDPIA

Fabrício Miranda Mereb – Promotor de Justiça do Ministério Público do Estado de Mato Grosso

Membro Colaborador do CAO - DDPIA

Adalberto Biazotto Junior – Promotor de Justiça do Ministério Público do Estado de Mato Grosso

Servidor

Maria Cristina Alves Ormond - Auxiliar Ministerial.

Residente

Pedro Carlos Nogueira Felix

Elaboração do Material :

Adalberto Ferreira de Souza Junior - Promotor de Justiça e Coordenador.

Fabrício Miranda Mereb - Promotor de Justiça e Coordenador Adjunto.

Adalberto Biazotto Junior - Promotor de Justiça e Colaborador

Maria Cristina Alves Ormond - Auxiliar Ministerial.

Pedro Carlos Nogueira Felix - Residente

Apoio na Elaboração do Material :

DTI - Departamento de Tecnologia da Informação

CSI - Centro de Segurança e Inteligência

CAO

DEFESA DE DADOS PESSOAIS E INTELIGÊNCIA ARTIFICIAL

MPMT Ministério Público DO ESTADO DE MATO GROSSO