



34190484



08120.000017/2026-50



MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

DOCUMENTO DE FORMALIZAÇÃO DA DEMANDA (DFD)

IDENTIFICAÇÃO DA ÁREA REQUISITANTE

UNIDADE REQUISITANTE	Divisão Administrativa da PFPV
SIGLA DA UNIDADE	DIAD-PV/PFPV/DPPF/SENAPPEN
RESPONSÁVEL PELA DEMANDA	Leandro De Souza Oliveira
MATRÍCULA/SIAPE	3160235
E-MAIL	leandro.souzaoliveir@mj.gov.br
TELEFONE	(69) 3533-8616

1. PREVISÃO DA DEMANDA NO PLANO DE CONTRATAÇÕES ANUAL - PCA (indicar o ID a que se refere a contratação no disponível no link: https://www.gov.br/mj/pt-br/aceso-a-informacao/licitacoes-e-contratosv1/se/pca/pac_se)

1. A aquisição fora adicionada ao Plano de Contratações Anual, em sua última janela (verificar o número do documento de formalização de demanda gerado no sistema comprasnet)

2. IDENTIFICAÇÃO DA DEMANDA (OBJETO)

2.1. Aquisição de Smartphones do tipo Iphone 17 PROMAX para utilização dos servidores que, por suas atribuições, possuem constante movimentação com informações sensíveis de interesse da Penitenciária Federal em Porto Velho/RO e que por essa razão exigem sistema que possuem maior segurança com relação ao tráfico de dados, conforme tabela abaixo:

Item	Objeto/Especificação	Unidade de Medida	Quantidade
------	----------------------	-------------------	------------

1	iPhone 17 PROMAX 256 GB Especificação Cor: Titânio Preto ou azul Tamanho da tela: 6,9 polegadas Super Retina XDR OLED(ProMotion de 120Hz) Resolução: 2868 x 1320 pixels(460 ppp) Processador: Chip Apple Apple A19 Pro(6 núcleos) Memória RAM: 12GB Câmeras traseiras: Sistema triplo de 48 MP (Principal, Ultra-angulares e Teleobjetiva com zoom óptico avançado) Câmera Frontal: 18MP com abertura f/1.9 Conexão: 5G, Wi-Fi 7, Bluetooth 6.0 e NFC Sistema Operacional: iOS 512 GB Todos os aparelhos devem ser homologados pela Agência Nacional de Telecomunicações (Anatel), comprovando que atendem aos padrões de qualidade e segurança exigidos para dispositivos móveis comercializados no Brasil. 12 meses de garantia 	Unidade	6
---	---	---------	---

2.2 A exigência do modelo iPhone se justifica na maior segurança do sistema operacional IOS em relação ao sistema operacional Android para tráfico de dados. O Sistema Penitenciário Federal abriga os criminosos mais perigosos do país, sendo uma importante ferramenta de combate ao crime organizado. Por se tratar de um órgão que trata de questões sensíveis envolvendo a segurança pública, com impacto na segurança nacional e soberania, a segurança dos dados é de extrema importância. Há servidores que, pela suas atribuições, cotidianamente lidam com informações sensíveis e a utilização de um smartphone funcional que não possui rígido sistema de segurança pode colocar em risco todo planejamento estratégico desta Unidade Penal Federal, sendo um verdadeiro atentado à segurança orgânica da instituição. Conforme sites especializados o IOS se mostra mais seguro do que o Android, notadamente pelas seguintes características:

- **Ambiente de Sistema Operacional Fechado (Closed Source):** O iOS opera em um ecossistema controlado e fechado, o que reduz consideravelmente a superfície de ataque. Ao contrário do Android (de código aberto e fragmentado entre diversos fabricantes), a Apple controla integralmente o hardware, o sistema operacional e a loja de aplicativos (App Store);
- **Atualizações de Segurança Imediatas e Universais :** Todos os dispositivos compatíveis da Apple recebem simultaneamente as atualizações de segurança, ao passo que o Android, muitas vezes, depende dos fabricantes e operadoras, ocasionando atrasos ou ausência de atualizações;
- **Camadas de Proteção de Dados e Criptografia Nativa :** O iOS aplica criptografia de ponta a ponta em diversas funcionalidades, como iMessage, FaceTime e dados armazenados localmente. O chip Secure Enclave presente nos iPhones gerencia chaves criptográficas com alto padrão de isolamento físico e lógico, garantindo maior proteção mesmo em caso de perda ou roubo do dispositivo.
- **Gerenciamento e Controle Remoto de Dispositivos (MDM) :** A Apple oferece soluções robustas de Mobile Device Management (MDM), permitindo que os administradores de TI da instituição configurem remotamente políticas de segurança, restrição de aplicativos, bloqueio ou formatação do dispositivo em caso de comprometimento.
- **Menor Incidência de Malware:** Estudos e relatórios periódicos de empresas como Kaspersky, Symantec e Check Point indicam que a grande maioria dos ataques via malware em dispositivos móveis ocorre em dispositivos Android, em função da fragmentação e permissividade do sistema. O ecossistema da Apple mantém um nível de curadoria muito mais rígido sobre os aplicativos distribuídos, reduzindo drasticamente esse risco.

A DINT-PV, GAEP-PV e DISED-PV exercem atividades essenciais para a segurança orgânica, protegendo o ativo mais valioso de qualquer organização, qual seja a vida dos seus servidores/colaboradores. É essencial lembrar os pilares da produção de provas nos processos de inteligência e persecução criminal, não há êxito na produção de provas, sem a juntada de imagens com boa qualidade, de modo que é de grande valia que os profissionais da área estejam munidos de equipamentos de alta tecnologia, posto a isto é essencial a aquisição dos equipamentos nos moldes expostos neste instrumento de demanda. A produção de provas incompletas, ou com qualidade que possa gerar dúvidas é prejudicial à SEGOR e pode comprometer as operações policiais de combate ao crime organizado.

É impossível mensurar o ganho em escala que a aquisição em tela poderá gerar na SEGOR e nas operações de combate ao crime organizado, pois os equipamentos visam suprir a lacuna na produção de imagens fidedignas, autêntica e íntegra.

Dessa forma, a solicitação dos Smartphones de última geração do sistema operacional IOS se mostra a melhor opção considerando a segurança no tráfico de dados, sendo fundamental à segurança orgânica da Unidade, fator prioritário a ser considerado.

Ainda, um smartphone com melhor capacidade de armazenamento (256Gb) contribuirá para maior vida útil dos aparelhos, atendendo o princípio da economicidade no uso do dinheiro público.

3. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO, CONSIDERANDO O PLANEJAMENTO ESTRATÉGICO, SE FOR O CASO.

3.1. Utilização por servidores que, por suas atribuições, lidam com informações sensíveis, exigindo maior segurança.

4. QUANTIDADE A SER CONTRATADA.

Conforme tabela prevista no item 2

5. PREVISÃO DA DATA DE INÍCIO DOS SERVIÇOS OU DA ENTREGA DOS BENS.

20 dias após o envio da Nota de Empenho.

6. INDICAÇÃO DO MEMBRO DA EQUIPE DE PLANEJAMENTO E SE NECESSÁRIO O RESPONSÁVEL FISCALIZAÇÃO.

6.1 Leandro de Souza Oliveira

6.2 Erika Mattos Faria Passos

7. OBSERVAÇÃO

7.1. O responsável pela indicação deverá cientificar o(s) servidor(es) indicado(s) no item 6, por meio de mensagem eletrônica (e-mail), a ser acostada aos autos, contendo confirmação de que o(s) mesmo(s) participará(ão) da Equipe de Planejamento. Caso o indicado esteja em período de férias ou de afastamento legal, no momento da indicação (DFD) ou durante a etapa seguinte de assinatura do Documento de Designação da Equipe de Planejamento, deverá comprometer-se a assiná-lo no seu retorno.

...



Documento assinado eletronicamente por **Leandro de Souza Oliveira, Chefe da Divisão Administrativa**, em 24/09/2026, às 13:42, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade do documento pode ser conferida no site <http://sei.autentica.mj.gov.br> informando o código verificador **34190484** e o código CRC **A0D51223**

O documento pode ser acompanhado pelo site <http://sei.consulta.mj.gov.br/> e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.