



13590833



08006.000110/2020-85



Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Coordenação de Infraestrutura de TIC

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

INTRODUÇÃO

Conforme previsto no artigo 11 da INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019, a elaboração dos Estudos Técnicos Preliminares da Contratação serve essencialmente para definição e especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição. A análise comparativa das soluções, deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

É na elaboração dos Estudos Técnicos Preliminares da Contratação que diversos aspectos devem ser levantados com maior profundidade para que os gestores se certifiquem, de que através de uma necessidade da área de negócio, claramente definida, há condições de atendê-la, tendo como premissa que os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente, além de embasar a elaboração do Termo de Referência, que somente é elaborado se a contratação for considerada viável.

A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica para a contratação de Licenças de Softwares e Serviços de Computação em Nuvem da Microsoft, pelo período de 48 (quarenta e oito) meses, com vistas a atender as necessidades do Ministério da Justiça e Segurança Pública - MJSP.

Referência: Art. 11 da IN SGD/ME nº 1/2019.

1 - DEFINIÇÃO DAS NECESSIDADES, REQUISITOS E JUSTIFICATIVA DA CONTRATAÇÃO (Art. 11, Inciso I da IN 01/2019 SGD/ME)

VISÃO GERAL DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA E SEUS OBJETIVOS ESTRATÉGICOS:

O Ministério da Justiça e Segurança Pública - MJSP é um órgão da Administração Pública Federal direta, que tem dentre suas competências a defesa da ordem jurídica, dos direitos políticos e das garantias constitucionais; a coordenação do Sistema Único de Segurança Pública; e a defesa da ordem econômica nacional e dos direitos do consumidor. O MJSP atua também no combate ao tráfico de drogas e crimes conexos, inclusive por meio da recuperação de ativos que financiem essas atividades criminosas ou dela resultem, bem como na prevenção e combate à corrupção, à lavagem de dinheiro e ao financiamento do terrorismo.

Conforme o Decreto nº 9.662, de 1º de janeiro de 2019 o MJSP é composto de várias unidades em sua estrutura, dentre as principais:

- a) **Órgãos de assistência direta e imediata ao Ministro:** Assessorias Especiais, Gabinete do Ministro, Secretaria Executiva e Consultoria Jurídica;
- b) **Órgãos específicos singulares:** Secretaria Nacional de Justiça - SENAJUS, Secretaria Nacional do Consumidor - SENACON, Secretaria Nacional de Políticas sobre Drogas - SENAD, Secretaria Nacional de Segurança Pública - SENASP, Secretaria de Operações Integradas - SEOPI, Departamento Penitenciário Nacional - DEPEN, Polícia Federal - PF, Polícia Rodoviária Federal - PRF e Arquivo Nacional - AN;
- c) **Órgãos colegiados:** Conselho Federal Gestor do Fundo de Defesa dos Direitos Difusos - CFDD, Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual - CNPCP, Conselho Nacional de Políticas sobre Drogas - CONAD, Conselho Nacional de Política Criminal e Penitenciária - CNCP, Conselho Nacional de Segurança Pública - CNSP, Conselho Gestor do Fundo Nacional de Segurança Pública - CFNSP, Conselho Nacional de Imigração - CNI e Conselho Nacional de Arquivos - CNA;
- d) **Entidade vinculada:** Conselho Administrativo de Defesa Econômica - CADE, Fundação Nacional do Índio;

Como pode ser observado, a estrutura do MJSP é bastante considerável e complexa, possuindo diversas áreas de atuação que merecem tratamento diferenciado e proporcional às suas especificidades, tanto do ponto de vista de suas dimensões, quanto ao grau de sensibilidade e sigilo que as áreas necessitam para o desempenho de suas atividades.

Alguns temas sensíveis podem ser destacados em cada um dos Órgãos específicos singulares e de acordo com as competências do Ministério com base no Decreto nº 9.662, de 01 de janeiro de 2019:

...

Art. 13. À Secretaria Nacional de Justiça compete:

...

II - coordenar, em parceria com os órgãos da administração pública, a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro - Enccl e outras ações do Ministério relacionadas com o enfrentamento da corrupção, da lavagem de dinheiro e do crime organizado transnacional;

III - coordenar a negociação de acordos e a formulação de políticas de cooperação jurídica internacional, civil e penal, e a execução dos pedidos e das cartas rogatórias relacionadas com essas matérias;

IV - coordenar as ações relativas à recuperação de ativos;

...

Art. 17. À Secretaria Nacional do Consumidor compete:

I - formular, promover, supervisionar e coordenar a política nacional de proteção e defesa do consumidor;

II - integrar, articular e coordenar o Sistema Nacional de Defesa do Consumidor;

...

X - receber e encaminhar consultas, denúncias ou sugestões apresentadas por consumidores, entidades representativas ou pessoas jurídicas de direito público ou privado;

Art. 20. À Secretaria Nacional de Políticas sobre Drogas compete:

I - assessorar e assistir o Ministro de Estado quanto às políticas sobre drogas relacionadas com a redução da oferta e a repressão da produção não autorizada e do tráfico ilícito de drogas;

...

VI - indicar bens apreendidos e não alienados em caráter cautelar, a serem colocados sob custódia de autoridade ou de órgão competente para desenvolver ações de redução da demanda e da oferta de drogas, para uso em tais ações ou em apoio a elas;

Art. 23. À Secretaria Nacional de Segurança Pública compete:

I - assessorar o Ministro de Estado na definição, na implementação e no acompanhamento de políticas, programas e projetos de segurança pública, prevenção social e controle da violência e da criminalidade;

II - coordenar e promover a integração da segurança pública no território nacional em cooperação com os demais entes federativos;

...

V - implementar, manter e modernizar redes de integração e de sistemas nacionais de informações de segurança pública, em conformidade com disposto na [Lei nº 12.681, de 4 de julho de 2012](#);

VI - promover a articulação e a integração dos órgãos de segurança pública, incluídas as organizações governamentais e não governamentais;

VII - coordenar as atividades da Força Nacional de Segurança Pública;

VIII - promover e fomentar a modernização e o reaparelhamento dos órgãos de segurança pública;

Art. 29. À Secretaria de Operações Integradas compete:

I - assessorar o Ministro de Estado nas atividades de inteligência e operações policiais, com foco na integração com os órgãos de segurança pública federais, estaduais, municipais e distrital;

II - implementar, manter e modernizar redes de integração e de sistemas nacionais de inteligência de segurança pública, em conformidade com disposto na [Lei nº 13.675, de 11 junho de 2018](#);

III - promover a integração as atividades de inteligência de segurança pública, em consonância com os órgãos de inteligência federais, estaduais, municipais e distrital que compõem o Subsistema de Inteligência de Segurança Pública;

IV - coordenar o Centro Integrado de Comando e Controle Nacional e promover a integração dos centros integrados de comando e controle regionais; e

V - estimular e induzir a investigação de infrações penais, de maneira integrada e uniforme com as polícias federal e civis.

Art. 32. Ao Departamento Penitenciário Nacional cabe exercer as competências estabelecidas nos [art. 71 e art. 72 da Lei nº 7.210, de 11 de julho de 1984 - Lei de Execução Penal](#), e, especificamente:

I - planejar e coordenar a política nacional de serviços penais;

...

IV - prestar apoio técnico aos entes federativos quanto à implementação dos princípios e das regras da execução penal;

...

XIII - promover a gestão da informação penitenciária e consolidar, em banco de dados nacional, informações sobre os sistemas penitenciários federal e dos entes federativos.

...

Merece também destaque os órgãos colegiados do Ministério, que atuam em temas sensíveis, e de importância nacional, como por exemplo o Conselho Nacional de Combate à Pirataria e aos Delitos contra a Propriedade Intelectual (CNCP). Esse órgão, é a instância que trata do assunto pirataria no Brasil, sendo responsável pela aplicação de abordagens e metodologias inéditas para o tratamento

da questão, elaborando diretrizes para a formulação e proposição de plano nacional para o combate à pirataria, à sonegação fiscal dela decorrente e aos delitos contra a propriedade intelectual.

Outro importante órgão colegiado é o Conselho Nacional de Políticas sobre Drogas - CONAD, sendo o órgão máximo brasileiro que regulamenta e pesquisa o uso de substâncias químicas e determina quais são drogas e quais não são e sua classificação. Este conselho também realiza campanhas de esclarecimento quanto às drogas e projetos como o de dano mínimo.

Destaca-se também o Conselho Nacional de Política Criminal e Penitenciária - CNCP, que preconiza a implementação, em todo o território nacional, de uma nova política criminal e principalmente penitenciária a partir de periódicas avaliações do sistema criminal, criminológico e penitenciário, bem como a execução de planos nacionais de desenvolvimento quanto às metas e prioridades da política a ser executada.

O Ministério possui também em sua estrutura o Conselho Nacional de Segurança Pública - CNSP, que tem o objetivo de propor diretrizes para prevenir e conter a violência e a criminalidade no País. O CNSP está previsto na lei nº 13.675, de 11 de junho de 2018, que instituiu o Sistema Único de Segurança Pública (Susp) e a Política Nacional de Segurança Pública e Defesa Social (PNSPDS), o órgão será composto por representantes da União, dos estados, Distrito Federal, municípios e sociedade civil.

De acordo com o Planejamento Estratégico Institucional 2020-2023 ([PEI 2020-2023](#)) e a Estratégia de Governo Digital 2020-2022 ([EGD 2020-2022](#)), publicada pelo Decreto 10.332/2020, o MJSP possui os seguintes objetivos estratégicos:

- a) Ampliar a escala e a efetividade das ações de defesa da concorrência e do consumidor; (OE.PEI.06)
- b) Aperfeiçoar a coordenação estratégica e a integração dos órgãos de segurança pública; (OE.PEI.03)
- c) Oferta de Serviços Públicos Digitais; (OE.EGD.01)
- d) Otimização das infraestruturas de tecnologia da informação; (OE.EGD.16)

Dentre os vários projetos estratégicos definidos pela Alta Administração do MJSP no PDTIC 2020 (SEI nº 10812779; Ata de aprovação no CTIC. – SEI nº 10873439), existem os que tratam da necessidade de construção de serviços e sistemas para tratamento de grandes volumes de dados, dentre os quais podem ser elencados os projetos P426 - SINESP Big Data e inteligência artificial, P402 - Rede de Centros Integrados de Inteligência, P419 - Fortalecimento da Rede Integrada de Bancos de Perfis Genéticos, P411 - Sistema para Processamento de Solicitações de Reconhecimento da Condição de Refugiado - SICONARE, P401 - Disponibilização do sistema Recall.gov.br. Os investimentos planejados pela Diretoria de Tecnologia da Informação e Comunicação visam atender às necessidades de todos esses projetos.

Salienta-se que os projetos elencados, se referem a órgãos em que a DTIC/MJSP apoia diretamente com recursos de TIC. Os órgãos como: Polícia Federal - PF, Polícia Rodoviária Federal - PRF, Arquivo Nacional - AN, Fundação Nacional do Índio - FUNAI e o Conselho Administrativo de Defesa Econômica - CADE, possuem estruturas independentes de TIC para suportar suas necessidades específicas de Tecnologia da Informação, no entanto o compartilhamento de informações entre esses órgãos é crucial para a execução de políticas públicas.

As ações de compartilhamento de dados previstas no Decreto Nº 10.046, de 9 de outubro de 2019 irão demandar que as instituições públicas sejam capazes de adotar mecanismos rígidos de governança de dados (políticas de controle de acesso, identificação das fontes de dados, classificação das informações e gestão da qualidade dos dados), a fim de viabilizar a sua utilização nos diferentes contextos de aplicação de políticas públicas. No caso específico do MJSP, foi verificada a necessidade de realizar um trabalho extenso de catalogação das fontes de dados capazes de potencializar ações institucionais nas suas diversas áreas de atuação, que vão desde a implementação de políticas mais eficazes de segurança pública e de combate à corrupção até a adoção de melhores mecanismos para garantir os direitos do consumidor. Para atingir esses objetivos foi publicada a [Portaria nº 260/2019 – MJSP](#), que instituiu o grupo de trabalho que será responsável pela implantação da política de governança de dados no Ministério da Justiça e Segurança Pública.

Para que todos os órgãos da estrutura do Ministério possam atuar de maneira eficiente e eficaz, e com os recursos necessários para o pleno desenvolvimento de suas atividades, **são necessários mecanismos tecnológicos que sejam capazes de gerar valor e entregar as informações necessárias, de forma a permitir a produção de conhecimento útil e tempestivo à tomada de decisão**, seja em nível estratégico, tático ou operacional.

Um aspecto relevante a ser considerado é a **natureza das informações com as quais o Ministério da Justiça e Segurança Pública deve lidar para a execução das suas competências, e o nível de sigilo que deve ser a elas assegurado**. Em muitos casos trata-se de dados com características que ensejam o controle estrito do acesso, seja porque são informações que dizem respeito a intimidade e vida privada de cidadãos, seja porque incluem atos preparatórios para a execução de ações de segurança pública e investigação criminal ou ainda porque trata-se de informações com imposição da observância de sigilo por determinação legal.

Tais características contraindicam, nos termos da [Norma Complementar nº 14 da Instrução Normativa nº 01/2008-DSIC/GSI](#), a utilização de forma irrestrita de recursos de computação em nuvem, o que se enquadra nas exceções às [recomendações](#) do Ministério da Economia de dar preferência a contratações de serviços de nuvem pública ou privada para suportar os serviços da Administração Pública Federal.

A Norma Complementar nº 14 veda também a utilização de nuvem para o armazenamento de informações classificadas nos graus de sigilo (ultrassecreta, secreta ou reservada) estabelecidos pelo Art. nº 24 da [Lei nº 12.527/2011 \(Lei de Acesso à Informação\)](#). Todas as essas restrições implicam na necessidade de investimento em ativos de TIC e na infraestrutura do Data Center para suportar os projetos do MJSP que irão necessitar de recursos de tecnologia da informação.

Importante destacar, que a Segurança Pública é um processo, ou seja, uma sequência contínua de fatos ou operações que apresentam certa unidade ou que se reproduzem com certa regularidade, que compartilha uma visão focada em componentes preventivos, repressivos, judiciais, saúde e sociais.

Trata-se de um processo sistêmico, pela necessidade da integração de um conjunto de conhecimentos e ferramentas estatais que devem interagir a mesma visão, compromissos e objetivos. Deve ser também otimizado, pois dependem de **decisões rápidas, medidas saneadoras e resultados imediatos**. Sendo a ordem pública um estado de serenidade, apaziguamento e tranquilidade

pública, em consonância com as leis, os preceitos e os costumes que regulam a convivência em sociedade, a preservação deste direito do cidadão só será amplo se o conceito de segurança pública for aplicado.

A segurança pública não pode ser tratada apenas como medidas de vigilância e repressiva, mas como um sistema integrado e otimizado envolvendo instrumento de prevenção, coação, justiça, defesa dos direitos, saúde e social. O processo de segurança pública se inicia pela prevenção e finda na reparação do dano, no tratamento das causas e na reinclusão na sociedade do autor do ilícito.

Para isso, houve a criação do Sistema Único de Segurança Pública (SUSP), que é um marco divisório na história do país. Implantado pela Lei nº 13.675/2018, sancionada em 11 de junho, o SUSP dá arquitetura uniforme ao setor em âmbito nacional e prevê, **além do compartilhamento de dados, operações e colaborações nas estruturas federal, estadual e municipal.**

Com a criação do SUSP, surgem novas regras, em que os órgãos de segurança pública, como as polícias civis, militares e Federal, as secretarias de Segurança e as guardas municipais serão integrados para atuar de forma cooperativa, sistêmica e harmônica.

Como já acontece na área de saúde, os órgãos de segurança do SUSP já realizam operações combinadas. Elas podem ser ostensivas, investigativas, de inteligência ou mistas e contar com a participação de outros órgãos, não necessariamente vinculados diretamente aos órgãos de segurança pública e defesa social – especialmente quando se tratar de enfrentamento a organizações criminosas.

O fato, é que para exercer todas suas competências de modo cada vez mais eficaz, o MJSP precisa incorporar novas ferramentas de tecnologia da informação capazes de realizar o processamento e a análise de volumes massivos de dados com diferentes formatos e gerados de forma ininterrupta, dentro do conceito de *Big Data*. Atualmente, várias unidades do MJSP (por exemplo, SENASP, SEOP, DRCI, DPF e DPRF) demandam a disponibilização de ferramentas capazes de processar grandes volumes de informações e gerar conhecimento e insights relevantes para a aplicação de políticas públicas nas áreas da segurança pública e do combate à corrupção e à lavagem de dinheiro.

A capacidade que as ferramentas de análise, pesquisa e cruzamentos de dados da administração pública federal possuem para potencializar o embasamento de políticas públicas e o combate às fraudes foi brilhantemente demonstrada pelo trabalho da SEFI/TCU apresentado no [Acórdão nº 2.587/2018 – Plenário](#). A metodologia de trabalho envolveu o cruzamento de dados disponibilizados por diferentes instituições para a investigação de determinadas tipologias (fatos que estariam em desconformidade com a legislação ou que denotariam a ocorrência, ao menos em tese, de fraudes ou ilícitos). A partir dos dados analisados foram identificadas diversas ocorrências destas tipologias em diferentes ações ou programas de governo, em um espectro de análises que englobaram, por exemplo, ocorrências não usuais e contrárias à legislação em licitações e contratações públicas, fatos suspeitos na execução financeira e orçamentária de órgãos públicos e a existência de possíveis fraudes em programas de governo como o Bolsa-Família e o Minha Casa Minha Vida.

O mesmo potencial demonstrado pelas análises realizadas no Acórdão TCU 2.587/2018 **pode ser aplicado às ações vinculadas às políticas de segurança pública e de combate à corrupção, mas, para isso, alguns entraves precisam ser vencidos.** Notadamente, existem ainda hoje uma série de dificuldades de ordens técnica e político-administrativa para um compartilhamento efetivo de dados entre os órgãos da Administração Pública, mesmo após a edição do Decreto nº 10.046, de 9 de outubro de 2019, que estabelece como regra o compartilhamento de informações entre as diversas entidades da Administração Pública Federal para viabilizar a execução e o monitoramento de políticas públicas.

Considerando esse prisma, a DTIC/MJSP tem envidado esforços técnicos e administrativos para equacionar da melhor maneira possível o atendimento ao previsto na INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019, na INSTRUÇÃO NORMATIVA GSI/PR Nº 1, DE 13 DE JUNHO DE 2008, notadamente a Norma Complementar 14/IN01/DSIC/SCS/GSI/PR e os desafios tecnológicos frente à quantidade de projetos estratégicos essenciais para a sociedade brasileira.

1. Identificação das necessidades de negócio	
1.1	Garantir a efetividade da prestação de serviços de TIC;
1.2	Garantir a integração entre plataformas;
1.3	Prover sistemas operacionais para as estações de trabalho;
1.4	Fornecer sistemas operacionais para os servidores de processamento de dados;
1.5	Disponibilizar ferramentas de escritório para manipulação de documentos de texto, apresentações, realizações de operações financeiras e contábilísticas para todos os usuários;
1.6	Prover ferramentas de gravação de vídeos e de reuniões de áudio/videoconferências;
1.7	Prover infraestrutura adequada e ferramenta de serviço de mensagens instantâneas e conferências;
1.8	Fornecer infraestrutura adequada e ferramenta de envio de mensagens de correio eletrônico para todos os usuários;
1.9	Prover infraestrutura adequada e ferramenta para controle de projetos;
1.10	Disponibilizar infraestrutura para viabilizar serviços colaborativos de intranet, extranet e internet;
1.11	Prover infraestrutura adequada para implantação e controle de banco de dados;
1.12	Prover ferramenta para criação e edição de diagramas diversos;

1.13	Prover infraestrutura e ferramentas para acesso remoto ao ambiente de TIC;
1.14	Garantir conexões seguras entre pessoas, dispositivos, aplicativos e dados em uma solução única e holística de identidade que ofereça flexibilidade e controle;
1.15	Prover ferramenta que permita análise de dados de negócio para utilização por parte dos usuários do MJSP;
1.16	Atender a Política de Segurança da Informação e Comunicações do Ministério da Justiça e Segurança Pública POSIC/MJSP;
1.17	Os dados e informações da CONTRATANTE devem residir exclusivamente em território nacional, incluindo replicação e cópias de segurança (backups), de modo que a contratante disponha de todas as garantias da legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas;
1.18	Deverá adotar o foro brasileiro para dirimir quaisquer questões jurídicas relacionadas aos contratos firmados entre o contratante e o fornecedor do serviço;
1.19	Controle de trabalho em equipe, com compartilhamento de arquivos, chat permanente, planejamento e gerenciamento de projetos colaborativos;
1.20	A contratação se dará pelo modelo do tipo subscrição, onde o CONTRATANTE remunerará a CONTRATADA apenas pelas licenças e serviços efetivamente utilizados, além disso a aquisição se dará sob demanda, ou seja, não há obrigação de consumir o total de licenças ou serviços que compõem o objeto da presente contratação;
1.21	Disponibilizar serviços e sistemas com escalabilidade, elasticidade e pagamento sob demanda;
2. Identificação das necessidades tecnológicas	
2.1. Subscrição de software	
2.1.1	Todos os produtos contratados devem permitir a atualização para novas versões que forem disponibilizadas, bem como incorporar benefícios do avanço tecnológico aos usuários;
2.1.2	Os produtos e serviços devem permitir a sincronização com o ambiente Active Directory;
2.1.3	Compatibilidade com o ambiente de correio eletrônico do Microsoft Exchange On-Premises (interno) e Híbrido, plataforma servidora de correio eletrônico utilizada atualmente pelo MJSP;
2.1.4	Suporte à manutenção de contas de correio institucionais e contas de recursos (salas de reunião, etc.), sem custos adicionais de licenciamento, além daqueles já aplicáveis aos usuários pessoais;
2.1.5	Ferramentas de segurança, compartilhamento e intercâmbio de arquivos;
2.1.6	Disponibilizar aplicações tanto em ambiente local como web;
2.1.7	Proporcionar experiências de reunião avançadas com funcionalidades de chamada avançada e um hub único para reuniões, chat, conteúdo e chamada;
2.1.8	Gerenciar o trabalho com eficiência entre indivíduos, equipes e organizações;
2.1.9	Detectar e investigar ameaças avançadas em ambientes locais e de nuvem;
2.1.10	Proteger o MJSP contra ações mal-intencionadas com inteligência e de forma adaptável;
2.1.11	A solução deve permitir a publicação, em ambiente WEB, dos relatórios ou painéis produzidos, sendo que a consulta a tais publicações poderá ser realizada sem a necessidade de autenticação, sem a necessidade de aquisição de licenças adicionais e sem restrições prévias quanto ao número de acessos simultâneos;
2.1.12	A solução deve permitir a publicação de gráficos e relatórios por meio da inserção do conteúdo em páginas html utilizando códigos de inserção/compartilhamento;
2.1.13	É de responsabilidade da CONTRATADA, como escopo do serviço de subscrição, a execução dos serviços de entrega e ativação das licenças contratadas e demandadas;
2.1.14	A CONTRATADA fica obrigada a fornecer documentação oficial do fabricante da solução com informações que permitam aferir a validade dos produtos adquiridos, como identificador da licença, descrição, quantitativo, part number, modelo, versão, data de validade, indicador se está incluído o direito a atualização, garantia e suporte técnico, período de garantia e preço praticado;
2.1.15	Disponibilizar o monitoramento e manutenção de conformidade, com a possibilidade de instalação/atualização automatizada e padronizada de softwares das estações de trabalho e de computadores móveis;

2.1.16	Para acionamento do suporte técnico em garantia, serão abertos chamados por parte da CONTRATANTE para a CONTRATADA/FABRICANTE;	
2.1.17	A garantia deverá englobar qualquer atividade relacionada ao funcionamento dos produtos, como manutenção evolutiva, preventiva e corretiva em software, sem nenhum ônus para a contratante;	
2.2. Serviço de Computação em nuvem		
2.2.1	Para garantir a continuidade do negócio e possibilitar a transição contratual, o serviço a ser contratado deverá permitir a portabilidade de dados e aplicativos e as informações da CONTRATANTE deverão estar disponíveis para transferência de localização, em prazo adequado e sem custo adicional;	
2.2.2	As informações sob custódia da CONTRATADA serão tratadas como informações sigilosas, não podendo ser usadas por este fornecedor ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal do CONTRATANTE;	
2.2.3	O ambiente do serviço contratado deverá estar em conformidade com a norma ABNT NBR ISO/IEC 27001:2013, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação;	
2.2.4	Auto-provisionamento sob demanda (“on-demand self-service”): o consumidor pode ter a iniciativa de provisionar recursos na nuvem, e ajustá-los de acordo com as suas necessidades ao decorrer do tempo, de maneira automática, sem a necessidade de interação com cada provedor de serviços;	
2.2.5	Acesso amplo pela rede (“broad network access”): os recursos da nuvem estão disponíveis para acesso pela rede por diferentes dispositivos (tais como: estações de trabalho, tablets e smartphones) através de mecanismos padrões.	
2.2.6	Compartilhamento através de pool de recursos (“resource pooling”): Os recursos computacionais do provedor são agrupados para servir a múltiplos consumidores (modelo multi-tenant), com recursos físicos e virtuais sendo alocados e realocados dinamicamente, de acordo com a demanda dos seus consumidores. Há uma ideia geral de independência de localização, uma vez que o cliente geralmente não possui controle ou conhecimento sobre a localização exata dos recursos providos. No entanto, é possível especificar este local em um nível mais alto de abstração (por exemplo: país, estado ou data center). Os serviços são concebidos como um padrão, com a finalidade de atender à demanda de vários consumidores de maneira compartilhada, não sendo focados em necessidades customizadas de um único consumidor.	
2.2.7	Rápida elasticidade: os recursos podem ser elasticamente provisionados e liberados, e, em alguns casos, de maneira automática, adaptando-se à demanda. Do ponto de vista do consumidor, os recursos disponíveis para provisionamento parecem ser ilimitados, podendo ser alocados a qualquer hora e em qualquer volume.	
2.2.8	Serviços medidos por utilização (“measured service”): os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos, através de mecanismos de medição utilizados em nível de abstração associado ao tipo de serviço utilizado (por exemplo: armazenamento, processamento, largura de banda, e contas de usuário ativas). A utilização dos recursos pode ser monitorada, controlada e reportada, fornecendo transparência tanto para provedores como para consumidores. Portanto, a precificação, se houver, será balizada pelo uso dos serviços.	
3. Demais requisitos necessários à escolha da solução de TIC		
3.1	Requisitos Temporais	A reunião de alinhamento deverá ocorrer após a assinatura do contrato e ser executada em, no máximo, 5 (cinco) dias corridos após a assinatura do contrato;
3.2	Requisitos Segurança	Atendimento à legislação pertinente a Segurança da Informação, principalmente à Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que disciplina a gestão de segurança da Informação e Comunicações na Administração Pública Federal, bem como ao Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, além da NC14/IN01/DSIC/GSIPR, que estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem;
3.3	Requisitos de metodologia de trabalho	A CONTRATADA deverá registrar o chamado informando a CONTRATANTE seu número de registro, permitindo desta forma o acompanhamento do chamado;
3.4	Requisitos Legais	A demanda ora apresentada deve estar em conformidade com a legislação federal e normas internas (Decreto-Lei 200/67; Lei nº 8.666/93; Instrução Normativa SGD/ME nº 01/2019; Plano Plurianual - PPA, Planejamento Estratégico Institucional – PEI ou Plano Diretor de Tecnologia da Informação – PDTI);
3.5	Requisitos Sociais, Ambientais e Culturais	Aplicação, no que couber, da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010 que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional;

2 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

O ritmo das mudanças no cenário globalizado e altamente digitalizado exige das organizações públicas uma maior flexibilidade para inovar e prestar serviços de TIC de forma ágil, integrada e eficiente. Isto posto, a Diretoria de Tecnologia da Informação e Comunicação - DTIC vem observando nos últimos anos um crescimento das demandas dos diversos órgãos integrantes da estrutura do Ministério da Justiça e Segurança Pública - MJSP por serviços de Tecnologia da Informação e Comunicação, tornando-se necessária a busca por soluções que proporcionem uma infraestrutura tecnológica robusta, escalável, corporativa e atualizada com o mercado.

Um bom exemplo disso está ocorrendo nesse momento. No dia 22/03/2020, através da Portaria Ministerial nº 132/2020, foram estabelecidas medidas de proteção para enfrentamento ao novo coronavírus (COVID-19), com a implantação do regime de trabalho remoto para alguns grupos de servidores, empregados públicos e estagiários no âmbito do MJSP. Isso só foi possível graças a um conjunto de soluções que permitiram que as equipes continuassem a executar suas atividades de forma remota.

A título de ilustração, durante esse período tivemos os seguintes números para umas das principais ferramentas utilizadas: o Teams.

ATIVIDADES DO TEAMS 22/03/2020 a 09/07/2020	MÉDIA (DIÁRIA)	PICO DE UTILIZAÇÃO (DIÁRIA)
Mensagens de Canal	194	982
Mensagens de Chat	7.460	14.205
Chamadas (Calls)	115	298
Reuniões	94	186

Tabela 1 - Utilização do Teams

Nesse sentido, a adoção de tecnologias modernas, como serviços em nuvem, deixou de ser uma tendência e passou ser uma realidade nas grandes corporações e por consequência também na Administração Pública, que deve estar alinhada às mais modernas e eficientes práticas de mercado.

Atualmente o Ministério da Justiça e Segurança Pública conta com os quantitativos previstos no 1º Termo Aditivo ao Contrato nº 28/2018 (SEI 8964029) para atendimento das suas necessidades. No entanto, tais quantitativos vêm se mostrando insuficientes em decorrência da expansão da atuação da instituição que está se refletindo no aumento do número de usuários das soluções de TIC corporativas e na ampliação do quantitativo de projetos que requerem recursos de TIC. Por exemplo, hoje temos no atual contrato 2.800 subscrições do Microsoft 365, no entanto, pelo último levantamento, temos em torno de 4.663 usuários válidos; para o ambiente de servidores, temos hoje 296 licenças de Windows Datacenter, para estarmos compliance necessitaremos de 315; para o Microsoft SQL Server Enterprise temos 14 licenças, mas necessitamos de 34.

2.1 COLABORAÇÃO E PRODUTIVIDADE/IDENTIDADE E SEGURANÇA

O parque de estações de trabalho do MJSP é composto de vários desktops e notebooks adquiridos no decorrer dos anos (de várias gerações/modelos de processadores diferentes). Além disso, temos diversos perfis de usuários, com diferente necessidades. Nesse sentido, a DTIC encaminhou consulta a algumas unidades organizacionais do MJSP com algumas sugestões de versões do Microsoft Office (que é a atual solução em utilização) a serem utilizadas pelos usuários, além de suas respectivas diferenças de funcionalidades, considerando os perfis dos usuários e o histórico de utilização.

Para uma **estimativa** do quantitativo e tipos de licenças, foram definidas as seguintes premissas iniciais:

- Suite de escritório instalada no computador:** Somente para servidores, mobilizados, alguns terceirizados da área administrativa e técnica, parte do estagiários, agentes federais administrativos e engenheiros temporários;
- Suite de escritório Web:** Para parte dos estagiários e parte dos terceirizados.
- Identidade e Segurança:** Para todos os usuários;
- Recursos avançados de Identidade e Segurança:** Para todos os usuários (RedeLab somente EMS E3)

Após uma checagem e atualização no Active Directory (AD), tomando como referência o campo *Description* e através do cruzamento de informações encaminhadas pelas unidades (Processo SEI nº 08006.000119/2020-96), chegou-se aos seguintes quantitativos e tipos de usuários:

RESUMO AD:*

- Total Geral de Usuários: 24.067;
- Total de Usuários Ativos: 5.398; (são todos aqueles que fizeram login nos últimos 90 dias. Após esse prazo, sem registro de acesso, automaticamente a conta é inativada)
- Total de Usuários Válidos: 4.663; (subconjunto dos Usuários Ativos, desde que não tenham as seguintes *Descriptions*: "Conta de Serviço", "Conta Acesso SEI", "CONSELHEIRO", "INATIVO", "Conta Institucional" e Contas HealthMailbox)

*Dados extraídos em 13/07/2020

DETALHAMENTO:

- Conta de Serviço:** Conta de acesso à rede corporativa necessária a um procedimento automático (aplicação, *script*, etc) sem qualquer intervenção humana no seu uso. Não terão nenhum tipo de licenciamento. Total: 104.

b) Conta Acesso SEI: São usuários de outros órgãos que apenas utilizam o SEI do MJSP (Ex: Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis - CONPORTOS, Ministério da Mulher, da Família e dos Direitos Humanos - MMFDH). Não terão nenhum tipo de licenciamento nem e-mail institucional. Total: 302.

c) Conselheiro: São usuários da Comissão de Anistia - CA, que atualmente estão vinculados ao Ministério da Mulher, da Família e dos Direitos Humanos - MMFDH. Esses usuários atuam em sessões de julgamento dos processos da CA, estas autoridades se reúnem durante as sessões de julgamento de processos daquela Comissão. Atualmente o único vínculo desses usuários com o MJSP é a necessidade de acesso ao SEI-MJSP. Não terão nenhum tipo de licenciamento nem e-mail institucional. Total: 33.

d) Conta Institucional: Conta de secretarias, coordenações e demais unidades, para envio e recebimento de e-mail (e-mail corporativo). Não necessitam de licenciamento, pois está vinculada à conta dos usuários administradores da caixa. Total: 81.

e) Contas HealthMailbox: O Exchange usa a disponibilidade gerenciada para monitorar sua própria integridade. Uma parte essencial desse monitoramento é o uso de transações sintéticas que imitam a atividade do usuário, como enviar e receber e-mail. A Caixa de Correio de Integridade é, para todos os efeitos, como uma caixa de correio normal com uma conta do Active Directory. Não terão nenhum tipo de licenciamento. Total: 203

f) Conta Acesso PE: Conta para autenticação e acesso ao Planejamento Estratégico, criada para atender a necessidade de servidores de outros órgãos que precisam de um usuário ativo no AD do MJSP visando atualizar o site de indicadores do Planejamento Estratégico. Não terão nenhum tipo de licenciamento nem e-mail institucional. Total: 12.

g) Colaborador Eventual: Conta que podem ter e-mail corporativo, acesso ao SEI, acesso ao SATI (Sistema de Atendimento Técnico) e demais sistemas internos. São usuários, por exemplo, das Secretarias Estaduais de Segurança que atuam em colaboração com alguma unidade do MJSP. Total: 169.

h) Mobilizados da Secretaria de Operações Integradas - SEOPI

Através do Ofício nº 394/2020/SEOPI/MJ (11008031), a SEOPI informou um quantitativo de 222 mobilizados, com previsão de crescimento de 138 usuários para os próximos 2 anos, totalizando 360 usuários. Na solicitação encaminhada à SEOPI foi solicitado que não fossem incluídos mobilizados com DAS ou os servidores efetivos do quadro do Ministério da Justiça e Segurança Pública - MJSP, visto que esses serão contabilizados na listagem encaminhada pela CGGP - Coordenação-Geral de Gestão de Pessoas. Somente os mobilizados sem vínculo que necessitam de login e/ou e-mail na rede do MJSP.

Essa Secretaria tem como uma de suas competências assessorar o Ministro de Estado nas atividades de inteligência e operações policiais, com foco na integração com os órgãos de segurança pública federais, estaduais, municipais e distrital. Os mobilizados, em sua maioria, são servidores das Secretarias de Segurança Pública do Estados e DF (mas lotados no MJSP, em Brasília), sendo classificados como usuários com perfil avançado. Foi informado um quantitativo de 222 usuários, com previsão de ampliação para 138, nos próximos 2 anos. **Total: 360.**

i) Mobilizados da Diretoria da Força Nacional de Segurança Pública - DFNSP

Por meio do processo SEI nº 08106.002563/2020-18 a DFNSP informou o efetivo lotado no MJSP, que executam funções prioritariamente administrativa para gestão das operações, aos quais se destinariam as "licenças mais completas" (pacote de escritório instalado localmente), totalizando em torno de 305 (trezentos e cinco) mobilizados. Foi informado ainda que cerca de 1.205 (mil duzentos e cinco) mobilizados estariam distribuídos nas diversas Operações da Força Nacional por todo o país, sendo que esses necessitariam de licenças mais simples.

Após o cruzamento dos nomes informados pela DFNSP (SEI nº 11247844) com os usuários cadastrados no AD, constatou-se que do efetivo informado pela DFNSP ($305+1205 = 1.510$), 412 estavam cadastrados no AD (considerando a *Description* "Mobilizado DFNSP"); Desse modo, estaremos considerando como elegíveis a "licenças mais completas" os 305 mobilizados informados pela DFNS e o restante dos 412, (os 107) serão atribuídas apenas licenças do pacote de Identidade e Segurança. Os mobilizados, em sua maioria, são servidores das Secretarias de Segurança Pública do Estados e DF, lotados no MJSP, mas outros em operação nos Estados e DF. **Total: 412 (305 + 107).**

j) Mobilizados da Secretaria Nacional de Segurança Pública - SENASP

Através do Despacho nº 195/2020/CITIC/CGISE/DTIC/SE/MJ (10972689) a DTIC solicitou à SENASP o quantitativo de servidores mobilizados da SENASP que utilizam a rede do MJSP, bem como expectativa de ampliação ou redução desse quantitativo para os próximos 2 anos. Como a DFNSP é subordinada à SENASP, foi solicitado que os mobilizados da DFNSP não fossem quantificados na resposta. Ainda na solicitação encaminhada à SENASP foi solicitado que não fosse incluído mobilizados com DAS ou os servidores efetivos do quadro do Ministério da Justiça e Segurança Pública - MJSP, visto que esses serão contabilizados na listagem encaminhada pela CGGP - Coordenação-Geral de Gestão de Pessoas.

Em resposta (SEI nº 11030271), a SENASP informou um quantitativo de 214 mobilizados, com previsão de ampliação de 116, nos próximos 2 anos. **Total: 330**

k) Servidores/Estagiários da Coordenação-Geral de Gestão de Pessoas - CGGP

Por intermédio do Despacho nº 184/2020/CITIC/CGISE/DTIC/SE/MJ (10964966) foi solicitado à CGGP o quantitativo de servidores públicos ativos que necessitam de login e/ou e-mail na rede do MJSP (Requisitado, Sem vínculo, Exercício Descentralizado Carreira, Contrato Temporário, Exercício Temporário, Natureza Especial, Cedido, Outros), incluindo os servidores do DEPEN, além dos estagiários.

A CGGP respondeu da seguinte forma (SEI nº 11027136 e 11020216): 1.170 servidores (excluindo-se o DEPEN) e 275 estagiários (já com previsão de mais 46 nos próximos 2 anos. Incluindo-se o DEPEN). **Total: 1.445.**

l) Servidores do Departamento Penitenciário Nacional - DEPEN

Os estabelecimentos penais federais têm por finalidade promover a execução administrativa das medidas restritivas de liberdade dos presos, provisórios ou condenados, cuja inclusão se justifique no interesse da segurança pública ou do próprio preso e também abrigar presos, provisórios ou condenados, sujeitos ao regime disciplinar diferenciado, previsto no art. 1º da Lei no 10.792, de 1º de dezembro de 2003. Atualmente estão em funcionamento cinco Penitenciárias Federais: Catanduvas/PR, Campo Grande/MS, Mossoró/RN, Porto Velho/RO e Brasília/DF. Além das Penitenciárias Federais, o DEPEN conta ainda com sua sede, em Brasília. Nesse tópico, faremos a identificação e quantificação dos tipos de servidores (agentes federais: administrativos e plantonistas) informados pela CGGP, além dos terceirizados dos contratos geridos pelo DEPEN (essa unidade conta com uma certa autonomia administrativa).

O regime de trabalho nas Penitenciárias Federais, de forma resumida, é dividido entre os agentes e terceirizados que trabalham na área administrativa (SEAD), com o horário comercial, e os agentes plantonista, que atuam nas vivências, torres e portarias, esses, têm atuação administrativa bastante restrita.

Em sua resposta, o DEPEN informou a necessidades de 118 (56+62) licenças avançadas ("Licença Office tipo 2") para os terceirizados administrativos (Sede e Penitenciárias) (SEI nº 11399122 e 11252964);

Para os Agentes Federais (Plantão Operacional), Reserva Técnica e Quota Novo Concurso: 1.120 (726+240+309/2), foi solicitado "Licença Office tipo 1"; Para os Agentes Federais (Jornada Normal), Engenheiro Temporário, Reserva Técnica e Quota Novo Concurso, foi solicitado "Licença Office tipo 2" 1.077 (1444-726+100+105+309/2) (SEI nº 11252964). **Total: 2.315** (2.197 [Servidores], 118 [Terceirizados])

m) Terceirizados da Coordenação-Geral de Gestão Documental e Serviços Gerais - CGDS

A CGDS é a Coordenação Geral responsável por um dos contratos com o maior quantitativo de terceirizados do MJSP, o contrato de Secretariado, Recepcionista e Serviço de Contínuo. Nesse sentido, a DTIC encaminhou o Ofício Nº 138/2020/CITIC/CGISE/DTIC/SE/MJ (11189740) solicitando o enquadramento dos terceirizados dentro dos seguintes perfis: 1 – Acesso à internet (rede wi-fi); 2 – Acesso ao SEI; 3 – Acesso ao Word, Excel, e-mail, etc.

Através do Ofício Nº 166/2020/CGDS/SAA/SE/MJ (SEI nº 11235789) a CGDS encaminhou a relação, com os respectivos perfis de acesso (350 terceirizados; filtro Desabilitar = N;). Posteriormente, a DTIC encaminhou o Ofício Nº 201/2020/CITIC/CGISE/DTIC/SE/MJ (11371654) sugerindo a adoção de uma versão Suite de escritório Web (Office 365 E1 como referência). Em anexo foi encaminhado um documento contendo as diferenças de funcionalidades entre as versões do Office 365 E1 e Office 365 E3 (utilizada atualmente). **Total: 350.**

n) Terceirizados da Coordenação-Geral de Arquitetura e Engenharia - CGAE

Na CGAE temos algumas das empresas que prestam serviço de engenharia e arquitetura ao MJSP. De acordo com o Despacho nº 145/2020/CGAE/SAA/SE/MJ (11442770) alguns desses usuários necessitam de acesso ao Word e Excel, e também a "aplicativos web" (9 usuários). Para outro grupo, somente acesso à rede wireless do MJSP em virtude da comunicação com os técnicos e o acompanhamento de seus serviços se dar através de aplicativo e internet. **Total: 9**

o) Terceirizados da Coordenação-Geral de Sistemas, Informações e Dados - CGSID

Na CGSID há duas Coordenações: Coordenação de Desenvolvimento de Sistemas (CDS) e Coordenação de Informações e Dados (CID). Nessa Coordenação-Geral estão os diversos terceirizados responsáveis pelos contratos de Desenvolvimento e Gestão de Dados. A CDS solicitou 120 (100+20) licenças Office (SEI nº 11112003); Para a CID 68 licenças Office (11054610). Estaremos considerando a Suite de escritório Web. Além dessas, foram disponibilizadas 14 licenças de suite de escritório instalada no computador. **Total: 202** (188+14)

p) Terceirizados da Coordenação-Geral de Infraestrutura e Serviços - CGISE

Na CGISE há três Coordenações: Coordenação de Infraestrutura de TIC - CITIC, Coordenação de Serviços de TIC - CSTIC e Coordenação de Sistemas de Produção e Banco de Dados de Segurança Pública - CSPBD. Nessa Coordenação-Geral estão os diversos terceirizados responsáveis pelo contrato de Infraestrutura de TIC, atendimento aos usuários e gestão Banco de Dados e Sistema em Produção.

Foram concedidas 20 licenças para os técnicos presenciais do N2, para esse grupo estaremos considerando a Suite de escritório Web (18 Central IT + 1 Simpress + 1 3Corp). Além do atendimento presencial, há também os técnicos do Nível 1, Analistas do bi-modal que atendem remotamente (77 usuários Central IT). Para esse grupo está sendo previsto somente o pacote de identidade e

segurança. Além dessas, foram disponibilizadas 14 licenças de suite de escritório instalada no computador. **Total: 143.** (109 N1 + 20 N2 + 14 N3) (SEI nº 12183066 "Levantamento CGISE Terceirizados")

q) Contas Administrativas

Usuários administrativos são as contas utilizadas pelos servidores e terceirizados da DTIC para a administração dos recursos de Infraestrutura TIC. São, portanto, contas com privilégios avançados.

Nesse sentido, conforme solicitação da Coordenação-Geral de Gestão e Governança de TIC - CGGOV (Despacho nº 111/2020/CRS/CGGOV/DTIC/SE/MJ - SEI 11143502), para esse grupo de usuários, tendo em vista a sensibilidade e privilégios de acesso, foi solicitada uma camada extra de proteção, com ferramentas que ampliassem o controle de acesso e auditoria dos eventos (recursos avançados de Identidade e Segurança). **Total: 85.**

r) Usuários VIPs

De acordo com a definição do atual contrato de suporte de Infraestrutura (Contrato 40/2019) o usuário é classificado como VIP de acordo com a posição de chefia ocupada dentro da estrutura organizacional. O número máximo de VIP's previsto é de 100 (cem) usuários. Para qualquer um dos usuários definidos como "VIP", o impacto e a urgência do incidente ou requisição devem ser sempre classificados como "críticos", não importando a natureza do serviço afetado.

Apesar da previsão de 100 usuários VIPs, hoje o MJSP já conta com 181 (SEI nº 12183066, "VIPS.pdf"); para essas contas, conforme solicitação da Coordenação-Geral de Gestão e Governança de TIC - CGGOV (Despacho nº 111/2020/CRS/CGGOV/DTIC/SE/MJ - SEI 11143502), está sendo previsto, além da suite de escritório, recursos avançados de Identidade e Segurança. **Total: 181**

s) Contrato Temporário - Edital nº 20/2020

O Ministério da Justiça e Segurança Pública publicou em 11 de maio de 2020 o edital para a contratação de 35 novos profissionais para a área de tecnologia ([Link DOU](#)). As vagas ofertadas são para as áreas de Big Data, especificamente aos cargos de analista de governança de dados (13), cientista de dados (12) e engenheiro de dados (10). **Total: 35.**

t) Rede-Lab

Trata-se de manifestação contida no Ofício nº 152/2020-Rede-Lab (12231133), com relação a demanda de licenciamento da suite de produtividade Microsoft Office 365 para atendimento das necessidades da Rede Nacional de Laboratórios de Lavagem de Dinheiro.

A necessidade está vinculada ao Projeto Estratégico "Reestruturação e Reorganização da Rede Nacional de Laboratórios de Lavagem de Dinheiro - REDE-LAB", que foi incluída no Planejamento Estratégico do Ministério da Justiça e Segurança Pública para os anos 2020-2023. Conforme consta no OFÍCIO Nº 152/2020/Rede-Lab/DRCI/SENAJUS/MJ (12231133), a demanda está justificada pela necessidade de um ambiente seguro para a troca de informações:

Embora concebida como rede, a Rede-Lab possui enormes desafios relacionados à ausência nas unidade de Lab-LD de ambiente restrito de videoconferência e mensageria, de ferramentas integradas para trabalhos colaborativos, de base de conhecimento, de mapeamento de perfis de competência, entre outros.

Foi solicitado a disponibilização de licenças do Office 365 E1 em conjunto com o "Enterprise Mobility and Security E3", para viabilizar as funcionalidades de segurança e de gestão de identidades de usuários que são consideradas necessárias para o uso com a finalidade proposta pela Rede-Lab. **Total: 557.**

DEFINIÇÃO DO QUANTITATIVO DE LICENÇAS

Inicialmente, em consulta às unidades organizacionais quanto às versões do Office 365 a serem adquiridas, foi sugerido a utilização da versão online (E1) para alguns tipos de usuários, onde os requisitos de usabilidade não fossem tão elevados, tais como: estagiários, terceirizados administrativos e agentes federais em regime de plantão, conforme a tabela abaixo. A proposta foi a de provocar uma mudança cultural e obter uma economia de recursos com a não aquisição de versões mais caras do Office que não eram plenamente utilizadas em toda a sua extensão por todos os perfis de usuários.

Unidade		Quantidade Imediata	Próximos 2 anos	Total
CGGP - Estagiários	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	229	46	275
CGDS - Terceirizados Administrativos	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	350	0	350
DEPEN - Terceirizados Administrativos (SEDE)	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	56	0	56
DEPEN - Terceirizados Administrativos (Penitenciárias)	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	62	0	62
DEPEN - Agente Federal (Plantão Operacional)	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	726	154	880
DEPEN - E1 (Majoração)	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	0	240	240
CGAE - Terceirizados	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	9	0	9
CGSID/CDS - Terceirizados	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	45	75	120
CGSID/CID - Terceirizados	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	9	59	68
CGISE - Terceirizados	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	20	0	20

Tabela 2 - Quantitativo inicialmente proposto para as licenças Office 365 E1

Ocorre que posteriormente confirmou-se que a versão E1 tinha mais algumas limitações além das informadas no documento SEI nº 11372212, especificamente com relação a impossibilidade de edição/criação (direta) de arquivos localmente utilizando o Office E1.

Em consulta à Microsoft, foi verificado que a funcionalidade constava no *backlog* para implementação, mas que ainda não estava incluída em seu *roadmap*.

Dessa forma, para os usuários que utilizem o Office E1 para abertura de arquivos locais, a produtividade ficaria comprometida, pois haveria necessidade de, após a alteração do documento, copiá-lo do Sharepoint ou OneDrive para o seu destino original, localmente.

Sendo assim, com o objetivo de sanar essa limitação, foram substituídas as licenças E1 por E3 em relação ao proposto originalmente para uma parte desses usuários que necessitarão da versão local para edição direta de documentos, conforme tabelas abaixo:

Unidade		Quantidade Imediata	Próximos 2 anos	Total
CGGP - Estagiários	M365 E3 + Office ATP Plan2 + Azure ATP	114	23	137
CGDS - Terceirizados Administrativos	M365 E3 + Office ATP Plan2 + Azure ATP	350	0	350
DEPEN - Terceirizados Administrativos (SEDE)	M365 E3 + Office ATP Plan2 + Azure ATP	56	0	56
DEPEN - Terceirizados Administrativos (Penitenciárias)	M365 E3 + Office ATP Plan2 + Azure ATP	62	0	62
DEPEN - Agente Federal (Plantão Operacional)	M365 E3 + Office ATP Plan2 + Azure ATP	726	154	880
DEPEN - E1 (Majoração)	M365 E3 + Office ATP Plan2 + Azure ATP	0	240	240

Tabela 3 - Quantitativo alterado de licenças E3

Unidade		Quantidade Imediata	Próximos 2 anos	Total
CGGP - Estagiários	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	114	23	137
CGAE - Terceirizados	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	9	0	9
CGSID/CDS - Terceirizados	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	45	75	120
CGSID/CID - Terceirizados	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	9	59	68
CGISE - Terceirizados	E1 + EMS E3 + Win E3 + Office ATP Plan2 + Azure ATP	20	0	20

Tabela 4 - Quantitativo atualizado de licenças E1

Em relação às soluções de identidade e segurança integradas à suíte de produtividade e colaboração, foram acrescentados os licenciamentos para o Office Advanced Threat Protection Plan2 (Office ATP Plan 2) para todos os usuários que possuem licenças Office E1 ou E3, licenças do Azure ATP, do Azure Active Directory Plan 2 e do Cloup App Security (CASB) para todas as contas pessoais de domínio e contas administrativas do Ministério da Justiça, e licenças da solução de Endpoint Protection/EDR Defender ATP para todas as contas pessoais de domínio (considerando que estas utilizam Desktops corporativos). As justificativas para esses quantitativos foram apresentadas pela Coordenação de Segurança e Riscos de TIC da DTIC/MJSP, e estão nos documentos SEI 11143502 e 13581729.

A tabela abaixo traz o resumo dos quantitativos de licenciamento para os produtos de produtividade, identidade e segurança na presente contratação.

Resumo: Licenças de Colaboração e Produtividade/Identidade e Segurança. Memória de Cálculo (SEI nº 13609294)

Licenças: Colaboração e Produtividade/Identidade e Segurança	Atualmente					Ampliação				
	G1	G2	G3	G4	G5	G1	G2	G3	G4	G5
[G1] M365 E3 + DATP + OATP P2 + AATP + CASB + AAD P2	3951	-	-	-	-	1079	-	-	-	-
[G2] E1 + EMS E3 + Win E3 + DATP + OATP P2 + AATP + CASB + AAD P2	-	197	-	-	-	-	157	-	-	-
[G3] EMS E3 + AATP + AAD P2	-	-	301	-	-	-	-	-	-	-
[G4] E1 + EMS E3	-	-	-	-	0	-	-	-	-	557

Tabela 5 - Resumo Licenças de Colaboração e Produtividade/Identidade e Segurança

[G1] Mobilizados Administrativos; Servidores ; Agente Federal (Jornada Normal); Quota CGSID e CGISE; Terceirizados Administrativos: DEPEN - Agente Federal (Plantão Operacional) e 50% dos Estagiários.

[G2] 50% dos Estagiários e Terceirizados

[G3] Mobilizados DFNSP não Administrativos; Contas Administrativas; Bimodal

[G4] Rede-Lab

2.2 PORTFÓLIOS E PROJETOS

Por meio do Despacho nº 27/2020/CPN/CGGOV/DTIC/SE/MJ (11180098) a Coordenação de Portfólio e Normativos de TIC encaminhou as demandas de Project conforme tabela abaixo:

TIPOS DE LICENÇAS DO PROJECT	QUANTITATIVO
PLAN 1	150
PLAN 3	200
PLAN 5	5

Tabela 6 - Demandas de Project

Conforme informado pela Coordenação de Portfólio e Normativos de TIC - CPN, esse quantitativo foi obtido através da Coordenação-Geral de Gestão Estratégica e Inovação Institucional - CGGE, que atualmente administra as licenças de Project, também, por meio da Previsão de ampliação do quadro de pessoal da DTIC, Contratação de 35 servidores temporários para atuarem na implantação do Projeto Big Data, Projeto de Transformação Digital do MJSP e Projeto Mestrado Big Data.

2.3 SELF-SERVICE BI/ANALYTICS

Os quantitativos e tipos de licenças foram dimensionados de acordo com o levantamento realizado pela Coordenação de Informações e Dados - CID através do Despacho nº 19/2020/CID/CGSID/DTIC/SE/MJ (11054610)

TIPO DE LICENÇA	JÁ EM USO	NECESSIDADE ATUAL (SINESP, SEI E OUTROS)	NECESSIDADE FUTURA CTU	NECESSIDADE FUTURA CONTRATO SERVIÇOS DE DADOS	NECESSIDADE FUTURA CRESCIMENTO "VEGETATIVO" PROJETADO PARA OS PRÓXIMOS 2 ANOS	TOTAL
Power BI PRO	191	300	35	20	60	606
Power BI Premium (P1)	0	3	0	0	0	3
Power BI Embedded (Azure)	0	R\$ 65.346,84	0	0	R\$ 65.346,84	R\$ 130.693,68

Tabela 7 - Quantitativo Power BI

a) Power BI Free

Com uma licença gratuita (Free), é possível explorar o Power BI para visualização e análise de dados pessoais usando o "Meu Workspace", mas não é possível compartilhar com outros usuários. O único método de compartilhamento é através de um relatório aberto para usuários com licença gratuita que é publicado na Web. Isso torna o relatório disponível publicamente em app.powerbi.com. Essa publicação na Web permite compartilhar relatórios com todos na Internet, mas não é segura e não deve ser usada para dados restritos. Não existe um visualizador seguro anônimo para o Power BI. A partir da publicação de um relatório na Web, ele é torna-se público e qualquer pessoa na Internet pode ter acesso.

b) Power BI Pro

Atualmente o MJSP utiliza as licenças do Power BI Pro, incorporadas ao pacote do M365 E5 (200 no total), que é cobrada por usuário. Uma licença Pro possui todos os recursos da licença gratuita, além de 10 GB de armazenamento, tamanho máximo de relatório de 1 GB, 8 atualizações automáticas por dia, com um mínimo de 30 minutos entre atualizações etc. Mas a grande diferença é que os usuários da versão Pro podem compartilhar relatórios e painéis com outros usuários.

Em seu pedido, a CID solicitou 300 licenças do Power BI Pro para atender, prioritariamente, as necessidades do Projeto SINESP, na construção de painéis (11074694, página 5). Incluiu ainda 35 licenças para os Contratados Temporário com a União (CTU), 20 para necessidades futuras em contratos de serviços de dados e 60 para ampliação.

c) Power BI Premium

Diferente de uma licença Free ou Pro, o Power BI Premium não é uma licença por usuário. Em vez disso, a licença Premium fornece uma capacidade dedicada para todos os usuários da organização. Essa capacidade dedicada, "Espaço de Trabalho Premium" ou "Premium Workspace", pode ser usado para hospedar grandes conjuntos de dados. Uma outra diferença é a capacidade de distribuição ampla do conteúdo sem uma licença do Power BI Pro para os consumidores do conteúdo.

De acordo com a CID, considerando o total de usuários válidos do MJSP (4.663*) e que haverá um total cerca de 1.000 colaboradores acessando frequentemente os painéis em Power BI Premium e que destes, 606 já terão licença Power BI, 394 serão classificados como "Usuários Freqüentes"

* valor atualizado, após reclassificação de alguns grupos de usuários.

Como seus usuários interagirão com seus relatórios e painéis?

Total de usuários : 4.663



■ Usuários Pro

606 (13.00%)

Os usuários que requerem colaboração, modelagem de dados, autoria de conteúdo, dashboard, compartilhamento, análises ad hoc e publicação de relatórios.

■ Usuários Frequentes

394 (8.45%)

Usuários que consomem os dashboards e os relatórios com frequência (várias vezes por semana).

■ Usuários Ocasionais

3.663 (78.55%)

Usuários que consomem painéis e relatórios ocasionalmente.

<https://powerbi.microsoft.com/pt-br/calculator/>

Power BI Premium

Unidades	(x) Taxas mensais	
3 Nós P1	\$4.995/nó/mês	?
Servidor de Relatórios do Power BI	Incluído com o Power BI Premium	?
(=) Total de taxas	\$14.985 /mês	

Os preços são estimativas e não são pretendidos como cotações de preços reais. ⓘ

<https://powerbi.microsoft.com/pt-br/calculator/>

De acordo com a "Calculadora Power BI Premium" seriam necessários 3 Nós do Power BI Premium. Importante ressaltar que se trata de uma estimativa. No momento da solicitação, a CID deverá demonstrar objetivamente qual será a quantidade efetiva de usuários, para que se possa dimensionar com assertividade a quantidade de Nós.

É necessário ter o Power BI Pro para usar o Power BI Premium? Sim. O Power BI Pro é necessário para publicar relatórios, compartilhar dashboards, colaborar com colegas em workspaces e participar de outras atividades relacionadas. O Power BI Pro não é necessário para consumir o conteúdo na capacidade Premium.

d) Power BI Embedded

Tem como objetivo simplificar a maneira como os ISVs (Fornecedor Independente de Software/Desenvolvedores de Software) usam as funcionalidades do Power BI com a análise integrada. O Power BI Embedded simplifica as funcionalidades do Power BI integrando a visualização de relatórios e dashboards aos aplicativos. Como nos aplicativos criados no Microsoft Azure, é possível usar serviços como Machine Learning e IoT permitindo que os ISVs tomem decisões rápidas.

Qual é a diferença entre o Power BI Premium e o Power BI Embedded? A capacidade do Power BI Premium é direcionada a organizações que desejam uma solução de BI completa para fornecer uma exibição única da organização, dos parceiros, dos clientes e dos fornecedores. O Power BI Premium ajuda a organização na tomada de decisões. O Power BI Premium é um produto SaaS que permite aos usuários consumir conteúdo por meio do [portal do Power BI](#), de aplicativos móveis e de aplicativos desenvolvidos internamente.

O Power BI Embedded é para ISVs que desejam inserir visuais em seus aplicativos. O Power BI Embedded ajuda os clientes a tomar decisões por ser destinado aos desenvolvedores de aplicativos, de modo que os clientes desses aplicativos, incluindo qualquer pessoa dentro ou fora da organização, podem consumir o conteúdo armazenado na capacidade do Power BI Embedded.

Para a previsão do quantitativo desse item, a CID utilizou a Calculadora do Azure, tendo como parâmetro o projeto do "SINESP Análise Aplicação", que vai utilizar o PowerBI Embedded. Foi baseado em uma estimativa empírica da quantidade de renderizações por hora que a solução deve utilizar. Como o projeto ainda não está em Produção, a CID comunicou que não havia como informar exatamente a real necessidade, mas foi estimada uma média de 400 a 500 renderizações por hora, que se enquadraria dentro do node type A2, de 301 e 600 renderizações por hora em média. Como a calculadora coloca o valor mensal de R\$ 5.445,57, para 12 meses (1 ano), estima-se o custo de R\$ 65.346,84. (E-mail SEI nº 12183066, "Power BI Embedded.pdf")

2.4 FERRAMENTA PARA MODELAGEM DE DADOS, FLUXOGRAMA E DIAGRAMAS

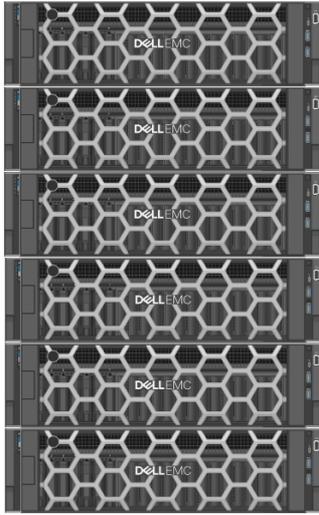
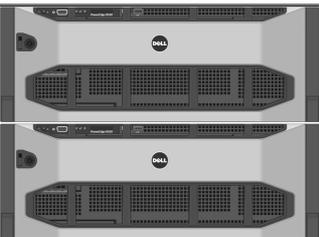
O Microsoft Visio é um programa da Microsoft que permite compor diversos tipos de gráficos de organização diferentes, como fluxogramas, organogramas e diagramas em geral. O Microsoft Visio disponibiliza diversas ferramentas para auxiliar no gerenciamento de projetos e milhares de figuras, formas e desenhos diferentes, permitindo desenhar desde o planejamento de uma estrutura de rede para aplicação em uma empresa até um organograma empresarial, além de WBS, fluxograma, diagramas de modelagem para desenvolvimento, entre outros.

Foi feita uma consulta a respeito de quais áreas do MJSP necessitariam desse tipo de licença. Em resposta, foram solicitadas 15 licenças do Microsoft Visio Professional (SEI nº 12183066, "Visio-email.pdf"). O público-alvo são os usuários que atuam na DTIC e nas áreas de projetos.

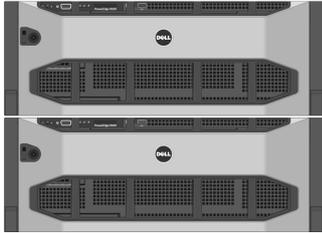
2.5 SISTEMA OPERACIONAL SERVIDOR

O atual ambiente de processamento do MJSP é composto pelos seguintes servidores físicos:

a) Data Center do Núcleo Central (Esplanada dos Ministérios):

	
<p>02 Blades HP, com 16 lâminas (cada). 2 CPUs de 10 cores com 128 GB de memória RAM, cada lâmina.</p>	<p>06 Dell R940. 4 CPUs de 12 cores com 1.5 TB, cada servidor (com suporte e garantia até 12/12/2023)</p>
	
<p>02 Dell R930. 4 CPUs de 16 cores com 512 GB, cada servidor (será movimentado para o CICCEN)</p>	<p>02 Dell R910. 4 CPUs de 10 cores com 384 GB, cada servidor.</p>

b) Data Center - CICCEN (Setor Policial)

	
<p>02 Dell R930. 4 CPUs de 16 cores com 512 GB cada.</p>	<p>01 Blade Dell M520, com 16 lâminas. 2 CPUs de 8 cores com 128 GB de memória RAM, cada lâmina.</p>

c) Penitenciárias Federais

	
<p>PFBRA (Penitenciária Federal de Brasília) - 02 Riverbeds 1 CPU de 2 cores com 16 GB de memória RAM, cada appliance.</p>	<p>PFCAT (Penitenciária Federal de Catanduvas) - 01 Riverbed / 01 Dell R910. 1 CPU de 6 cores com 16 GB de memória RAM. (Riverbed) 2 CPUs de 10 cores com 64 GB. (R910)</p>
	
<p>PFCG (Penitenciária Federal de Campo Grande). 01 Riverbed / 01 Dell R910. 1 CPU de 6 cores com 16 GB de memória RAM. (Riverbed) 2 CPUs de 8 cores com 64 GB. (R910)</p>	<p>PFMOS (Penitenciária Federal de Mossoró) - 01 Riverbed / 01 Dell R910. 1 CPU de 6 cores com 16 GB de memória RAM. (Riverbed) 2 CPUs de 10 cores com 64 GB. (R910)</p>
	
<p>PFPV - (Penitenciária Federal de Porto Velho) 01 Riverbed / 01 Dell R910. 1 CPU de 6 cores com 16 GB de memória RAM. (Riverbed) 2 CPUs de 8 cores com 64 GB. (R910)</p>	

2.5.1 Proposta de Licenciamento

a) Windows Server Datacenter

A proposta é que se licencie todo parque R910, R930, R940 do Núcleo Central/CICCN com licenças Datacenter, não sendo vantajosa a utilização da edição Standard. Os quantitativos estão detalhados na Tabela 5 desse ETP.

Considerando que o quantitativo de licenças Windows Server está vinculado a quantidade de cores, optou-se por privilegiar máquinas com maior quantidade de memória RAM e menor quantidade de cores. Nesse sentido, as 02 Blades HP serão utilizadas para

máquinas Linux.

Observe que ao se licenciar o Cluster R940, será consumido quase metade da quantidade de licenças de Windows Server, ao invés de licenciar o Cluster Blades HP e com a vantagem do dobro de memória RAM.

NOME CLUSTER	CORES	MEMÓRIA RAM	TOTAL DE LICENÇAS WINDOWS SERVER
Cluster Dell R940 (6x)	288	9 TB	144
Cluster Blades HP (2x)	640	4 TB	320

Tabela 8 - Comparativo

Entre os benefícios desse modelo:

- Permite que sejam realizados a segregação de ambiente;
- Possibilidade de crescimento futuro de hardware;
- Previsibilidade de projetos futuros;
- Margem de crescimento vegetativo do parque atual;
- Priorização para a utilização de máquinas com mais quantidade de memória RAM em contraposição a quantidade de Cores;
- Alta disponibilidade: cujo objetivo é manter os serviços disponibilizados o máximo de tempo possível. Para garantir a ausência de interrupções de serviços é necessário, muitas vezes, dispor de hardware redundante que entre em funcionamento automaticamente quando da falha de um dos componentes em utilização;
- Balanceamento de carga: o fato de ambos servidores se encontram em funcionamento e ligados à rede não implica, contudo, que se encontrem a desempenhar as mesmas tarefas. Essa é uma decisão por parte do administrador;
- Tolerância a falhas: consiste, basicamente, em ter hardware redundante que entra em funcionamento automaticamente após a detecção de falha do hardware principal.

SERVIDOR FÍSICO	LOCALIZAÇÃO	QNTD. PROCESSADORES	QNTD. CORES P/ PROC.	QNTD. MÍNIMA DE CORES POR PROCESSADOR	QNTD. MÍNIMA DE CORES POR SERVIDOR	QNTD. LICENÇAS (PACOTE DE 2 CORES)
Dell_R940#01	Infoseg	4	12	12	48	24
Dell_R940#02	Infoseg	4	12	12	48	24
Dell_R940#03	Infoseg	4	12	12	48	24
Dell_R940#04	Infoseg	4	12	12	48	24
Dell_R940#05	Infoseg	4	12	12	48	24
Dell_R940#06	Infoseg	4	12	12	48	24
Dell_R930#01	Infoseg	4	16	16	64	32
Dell_R930#02	Infoseg	4	16	16	64	32
Dell_R930#01	CICCN	4	16	16	64	32
Dell_R930#02	CICCN	4	16	16	64	32
Dell_R910#01	Infoseg	4	10	10	40	20
Dell_R910#01	Infoseg	4	10	10	40	20
LICENÇAS (PACOTE 2 CORES)						312

Tabela 9 - Quantitativo Microsoft Windows Datacenter

- Conforme verificado na tabela acima, em todos os servidores, o quantitativo mínimo de 8 licenças por processado foi alcançado (Qntd. Mínima de Cores por Processador);

- O mínimo de 16 licenças para cada servidor também foi alcançado (Qntd. Mínima de Cores por Servidor);

Modelo de Licenciamento

As licenças do tipo subscrição, ou seja, com todo serviço provido por assinatura, tem como característica o fornecimento do serviço por tempo definido de acordo com o pagamento devido. Enquanto o licenciamento perpétuo é mais rígido, por se tratar de compra das licenças de uso e para atender aos eventuais crescimentos, deve ser dimensionado com uma reserva técnica. Já a contratação de licenças por subscrição, por se tratar de serviço, permite aumento ou redução da quantidade de licenças ao longo da vigência contratual, nos limites estabelecidos em lei.

Quanto a economicidade, restou mais vantajoso o modelo de Subscrição, conforme simulação feita a partir de valores contidos no Catálogo de Soluções de TIC com Condições Padronizadas 2.0.0 - Microsoft da Secretaria de Governo Digital do Ministério da Economia (SGD), com Preços Máximos de Compra de Item de TIC - PMC-TIC.

ITEM	MODELO DE LICENCIAMENTO	PMC-TIC (R\$) 12 MESES	Simulação (R\$) 48 meses
CIS Datacenter (Windows Server + System Center) [SKU 9GS-00495]	Subscrição	1.212,10	4.848,40
CIS Datacenter (Windows Server + System Center) [SKU 9GS-00495]*	Perpétua + SA	1.795,20	7.180,80

Tabela 10 - Quantitativo Microsoft Windows Datacenter

Fonte: <https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-produtos-e-servicos-microsoft.pdf>

* Filtros Aplicados: **Identificador Microsoft** = 9GS-00495; **Modelo de Licenciamento** = Perpétua; **Unidade de Referência** = 12 meses; **Aplicação** = Produto Adicional (Licença que pode ser adquirida em um Contrato EA, EAS ou SCE); **Período de Compra** = Adição em novos contratos (Valor anual a ser pago referente a 1/3 de licença + 1 ano de Software Assurance. Este valor deve ser considerado somente para contratos de 36 meses)

b) Windows Server Standard

A licença de Windows Server Standard é adequada para ambientes virtualizados pequenos, pois cada licença atende a dois núcleos do processador que hospeda o sistema operacional virtualizado. Conforme já mencionado, o licenciamento do Windows Server Standard dá direito a até 2 (dois) ambientes de sistema operacional (OSEs ou máquinas virtuais) ou Contêineres do Hyper-V.

O MJSP provê serviço para o Departamento Penitenciário Nacional - DEPEN, fornecendo infraestrutura de rede e computadores para as Penitenciárias Federais de Porto Velho/RO, Campo Grande/MS, Catanduvas/PR, Mossoró/RN e Brasília/DF.



Figura 1 - Penitenciárias Federais

O acesso das Penitenciárias a aplicações críticas como SEI, Serviço de e-mail, acesso à internet, entre outros, funcionam de forma centralizada e necessitam de interligação com o Datacenter do MJSP em Brasília.

Nas Penitenciárias estão instalados servidores da marca Riverbed, que desempenham a função de aceleradores de WAN, para aumentar o desempenho do tráfego de dados entre a Penitenciária e a MJSP. Os servidores Riverbed também possuem a característica de hospedar alguns servidores virtualizados de pequeno porte.

Nos servidores virtualizados das Penitenciárias Federais são executados serviços de autenticação de usuários (com replicação dos usuários do MJSP para o ambiente da Penitenciária), Sistema de Administração Penitenciária- SIAPEN, Windows Server Update Services - WSUS, Servidor de Impressão e compartilhamento de arquivos, visando disponibilizar autonomia mínima para a Penitenciária em caso de falha do link de comunicação MPLS (Multi Protocol Label Switching), mesmo que a Penitenciária fique sem comunicação com o MJSP é possível autenticação e compartilhamento de arquivos dentro das instalações das Penitenciárias.

Para suportar os servidores virtualizados nas Penitenciárias Federais, encontra-se instaladas máquinas físicas e appliances nas Penitenciárias Federais.

LOCALIDADE	VM WINDOWS	VM LINUX
Cluster Penitenciária Federal de Brasília	2	0
Cluster Penitenciária Federal de Catanduvas	6	1
Cluster Penitenciária Federal de Campo Grande	6	1
Cluster Penitenciária Federal de Mossoró	8	1
Cluster Penitenciária Federal de Porto Velho	6	1

Tabela 11 - Cluster Penitenciárias

Servidor Físico	Localização	Qntd. Processadores	Qntd. Cores p/ proc.	Qntd. Mínima de Cores por Processador	Qntd. Mínima de Cores por Servidor	Qntd. Licenças (pacote de 2 cores)
Rivered#1	PFBRA	1	2	8	16	8
Rivered#2	PFBRA	1	2	8	16	8
Dell R910	PFCAT	2	10	10	20	10
Rivered	PFCAT	1	6	8	16	8
Dell R910	PFCG	2	8	8	16	8
Rivered	PFCG	1	6	8	16	8
Dell R910	PFMOS	2	10	10	20	10

Riverved	PFMOS	1	6	8	16	8
Dell R910	PFPV	2	8	8	16	8
Riverved	PFPV	1	6	8	16	8
LICENÇAS (PACOTE 2 CORES)						84

Tabela 12 - Quantitativo Microsoft Windows Standard

Diante do exposto, para as Penitenciárias Federais está sendo proposto a utilização da edição Standard, pois o número de VMs não justifica a contratação da versão Datacenter.

Modelo de Licenciamento

As licenças do tipo subscrição, ou seja, com todo serviço provido por assinatura, tem como característica o fornecimento do serviço por tempo definido de acordo com o pagamento devido. Enquanto o licenciamento perpétuo é mais rígido, por se tratar de compra das licenças de uso e para atender aos eventuais crescimentos, deve ser dimensionado com uma reserva técnica. Já a contratação de licenças por subscrição, por se tratar de serviço, permite aumento ou redução da quantidade de licenças ao longo da vigência contratual, nos limites estabelecidos em lei.

Quanto a economicidade, restou mais vantajoso o modelo de Subscrição, conforme simulação feita a partir de valores contidos no Catálogo de Soluções de TIC com Condições Padronizadas 2.0.0 - Microsoft da Secretaria de Governo Digital do Ministério da Economia (SGD), com Preços Máximos de Compra de Item de TIC - PMC-TIC.

Item	Modelo de Licenciamento	PMC-TIC (R\$)	Simulação (R\$)
		12 meses	48 meses
CIS Standard (Windows Server + System Center) [SKU 9GA-00006]	Subscrição	296,65	1.186,60
CIS Standard (Windows Server + System Center) [SKU 9GA-00006]	Perpétua + SA	438,60	1.754,40

Tabela 13 - Comparativo Subscrição x Perpétua + SA

Fonte: <https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-produtos-e-servicos-microsoft.pdf>

* Filtros Aplicados: **Identificador Microsoft** = 9GA-00006; **Modelo de Licenciamento** = Perpétua; **Unidade de Referência** = 12 meses; **Aplicação** = Produto Adicional (Licença que pode ser adquirida em um Contrato EA, EAS ou SCE); **Período de Compra** = Adição em novos contratos (Valor anual a ser pago referente a 1/3 de licença + 1 ano de Software Assurance. Este valor deve ser considerado somente para contratos de 36 meses)

2.6 SERVIDORES DE COLABORAÇÃO E PRODUTIVIDADE

A infraestrutura de e-mail corporativa atualmente é suportada pelo Microsoft Exchange Server e visa o atendimento do serviço de correio eletrônico do MJSP, contando com as funcionalidades: e-mail pessoal e corporativo, agendamento de reuniões, gerenciamento de recursos, gerenciamento de contatos e listas de distribuição.

Atualmente constam 7 servidores Microsoft Exchange Server, conforme apresentado na tabela abaixo.

Machine Fully Qualified Name	Edição Instalada	Versão Instalada	Status
111	Microsoft Exchange Server	2016	Em produção
112	Microsoft Exchange Server	2016	Em produção
113	Microsoft Exchange Server	2016	Em produção
114	Microsoft Exchange Server	2016	Em produção
115	Microsoft Exchange Server	2016	Em produção
116	Microsoft Exchange Server	2016	Em produção

Tabela 14 - Microsoft Exchange Server MJSP

De acordo com as políticas de licenciamento Microsoft, ao adquirir o M365, a organização poderá instalar os servidores Exchange, Skype for Business e Sharepoint, como forma de benefício, sem custo.

Microsoft Licensing – Microsoft 365

Microsoft 365 provides the best value when you are buying cloud services by providing suite discounts versus purchasing each component separately. Microsoft 365 also allows Enterprise Agreement customers to license in a true per user licensing model, giving them a consistent productivity experience on any device and on any operating system. It also provides increased manageability and simplicity as you will no longer need to count devices for the Platform Enterprise Agreement and cloud services. You can move to the cloud without modifying your Enterprise Agreement while eliminating the need for Bridge CALs and True-ups.

On-premises server rights

The following rights are included with all Microsoft 365 E3 and E5 User Subscription License (USL):

- ▶ Exchange Server, SharePoint Server, Skype for Business Server
- ▶ Rights to install the server software on on-premises servers. Downgrade rights included
- ▶ Rights to access any licensed on-premises servers

2.7 PLATAFORMA DE DADOS

Através do Despacho nº 251/2020/CITIC/CGISE/DTIC/SE/MJ (11053123) foi solicitado à Coordenação de Sistemas de Produção e Banco de Dados de Segurança Pública - CSPBD o quantitativo e tipos de licenças Microsoft SQL Server, considerando o dimensionamento dos *clusters* de SQL Server (produção) e também as demandas das áreas de negócio do Ministério para os próximos 2 anos.

Em resposta, foi encaminhado o Despacho nº 55/2020/CSPBD/CGISP/DTIC/SE/MJ (11397785) informando que a estimativa foi feita com base nos ambientes existentes e na média de consumo das aplicações desenvolvidas no MJSP, para os próximos 2 anos.

ID	Descrição	Versão	vCPUs	Total de Licenças
1	Servidor Aplicações MJSP	Microsoft SQL Server 2016	16	8
2	Servidor Aplicações MJSP	Microsoft SQL Server 2012 em AlwaysOn	12	6
3	Servidor BI e DW	Microsoft SQL Server 2016	16	8
4	Servidor Orchestrator/SCCM	Microsoft SQL Server 2016	4	2
5	Servidor Varonis	Microsoft SQL Server 2016	4	2
6	Servidor SharePoint	Microsoft SQL Server 2016	16	8
	Total			34

Tabela 15 - Resumo Servidores Microsoft SQL Server

Detalhamento:

- 1 - Para manter um nível satisfatório de disponibilidade em virtude da quantidade de aplicações que estão sendo desenvolvidas bem como das absorções e aplicações que serão migradas da versão 2012 para a 2016;
- 2 - Com a migração das bases que atualmente estão na versão 2012 para a versão 2016, essas licenças poderão ser utilizadas em outros projetos;
- 3 - Levando em consideração a absorção de 70 bases por parte do Gabinete do Ministro do MJSP conforme consta no e-mail (11980401), que tem como finalidade a criação de uma rede de BigData para a sustentação das atividades de Segurança Pública;
- 4 - Será mantida a mesma infraestrutura;
- 5 - Será mantida a mesma infraestrutura;
- 6 - Em desenvolvimento: Projeto de ferramenta de busca de arquivos (DRCI);

2.8 PLATAFORMA DE DESENVOLVIMENTO LOW CODE

A plataforma Power da Microsoft permite desenvolver aplicações de forma extremamente eficiente por meio da metodologia low-code, que requer muito menor esforço das equipes de desenvolvimento, podendo ser em muitos casos as aplicações serem desenvolvidas diretamente pelos integrantes das próprias áreas negociais (dentro do conceito de *citizen developer*). Através da plataforma Power é possível o desenvolvimento de aplicações por meio de componentes e interfaces visuais, porém dentro de uma arquitetura que possibilita a governança e o correto aproveitamento dos dados institucionais em diferentes contextos de uso.

No Ministério da Justiça e Segurança Pública, diferentes áreas de negócios estão demandando cada vez mais acesso a recursos de desenvolvimento através da plataforma Power exatamente por compreenderem o potencial que a plataforma possui para a prototipação e desenvolvimento de aplicações de pequeno e médio porte que viabilizem o tratamento de processos de negócios e de dados no âmbito das unidades, sem requerer um projeto de maior porte no âmbito da Fábrica de Softwares da DTIC/MJSP. Embora a abordagem low-code não seja admitida como uma alternativa capaz de substituir o desenvolvimento de softwares de maior porte em todos os casos, ele é aplicável com vantagens em cenários mais pontuais, para os quais há a dificuldade de tratar com prioridade as demandas das unidades de negócio.

Para os casos de uso vislumbrados no Ministério da Justiça e Segurança Pública, o licenciamento mais adequado é o licenciamento "por usuário por aplicativo", que permite que um determinado usuário licenciado execute até duas aplicações e acesse até um portal personalizado. Esse modelo de licenciamento é o indicado para instituições que estão iniciando o uso da plataforma Power, por ter um valor bastante inferior à licença por usuário para aplicações ilimitadas (um quarto do valor), e permitir que cada área de negócio construa até duas aplicações que suportem seus processos de negócios.

A estimativa de licenças do "Power Apps per App" consideradas inicialmente necessárias estão apresentadas na Tabela abaixo, divididas de acordo com a demanda inicial estimada das diferentes áreas do Ministério nesta fase.

UNIDADES	QUANTIDADE DE LICENÇAS
SE/GABINETE/DTIC	100
SENAACON	50
SEOPI	50
SENASP	50
SENAJUS	50
TOTAL	300

Tabela 16 - Quantidade inicial prevista de licenças Power Apps

Outra demanda recente diz respeito à possibilidade de utilização da solução de programação de agentes de inteligência artificial (comumente conhecidos como "bots") à partir da ferramenta "Power Virtual Agents", outro componente integrante da plataforma Power.

O Ministério da Justiça vem expandindo significativamente o provimento de soluções de TIC para o universo de profissionais de segurança pública de todo o país, como é o caso dos sistemas dos projetos SINESP Big Data e Cortex, e, além destes, os sistemas providos para o Sistema Penitenciário Nacional pelo Departamento Penitenciário Nacional. Para o atendimento das demandas de suporte técnico dos usuários destes sistemas está sendo proposta a contratação de um serviço específico de suporte técnico de primeiro nível (N1), que possibilitaria o contato dos usuários através de chamada telefônica e de um portal de serviços. Existem, no entanto, preocupações relativas à segurança na implementação de atendimento para sistemas que lidam com informações sensíveis de segurança pública, que são decorrentes da terceirização dos postos de atendimento e da própria infraestrutura utilizada pela empresa de Call Center.

Uma alternativa para mitigar as preocupações de segurança e ainda minimizar os custos relativos aos postos de atendimento operados por atendentes humanos é a utilização de "bots" com inteligência artificial, que podem interagir com os usuários e fornecer respostas às solicitações e dúvidas mais simples, delegando apenas as questões mais complexas e relacionadas com problemas técnicos efetivos para os atendentes humanos em outros níveis de atendimento (N2 e N3).

A solução Power Virtual Agents é uma forma eficaz de estabelecer scripts de atendimento para as demandas dos usuários dos sistemas finalísticos de segurança pública, o que pode ser feito pela área de TIC com orientação da área de negócio, ou, em muitos casos, pela própria área negocial desde que devidamente capacitada na utilização da ferramenta, uma vez que ela utiliza recursos visuais para a elaboração dos scripts e não demanda conhecimento específico em programação.

No momento há um projeto piloto de criação de um "bot" utilizando o Power Virtual Agents para apoio aos usuários do sistema Cortex, que já conta atualmente com 35 mil usuários oriundos de 100 instituições de segurança pública de todo o país. A expectativa é que o canal de atendimento por chatbot integrado à aplicação possa atenuar a demanda desses usuários por atendimento técnico na utilização da plataforma.

O licenciamento proposto para o Power Virtual Agents é na modalidade de blocos de interações, sendo que cada licença permite um conjunto de 2 mil interações mensais (sendo cada interação uma sessão de chat com o "bot" até a conclusão da demanda). Considerando o modelo de licenciamento e a expectativa de expansão do uso do Power Virtual Agents para outros sistemas além do Cortex, a estimativa para o completo atendimento das demandas é de que serão necessárias 10 licenças do Power Virtual Agents. As licenças serão progressivamente ativadas na medida em que houver volume de demanda com a implantação efetiva dos "bots" de atendimento nos sistemas finalísticos de segurança pública.

2.9 SERVIÇO DE COMPUTAÇÃO EM NUVEM

O Ministério da Justiça e Segurança Pública vem adotando, desde 2018, o uso de soluções de computação em nuvem Microsoft Azure nas modalidades Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS), contratadas por meio do Contrato nº 28/2018. A computação em nuvem é o modelo de fornecimento de soluções tecnológicas a partir de um centro de dados operacionalizado pelo provedor de serviços.

Segundo estudo da IDC, algumas das principais vantagens do uso de computação em nuvem são:

- Redução de custos de infraestrutura e serviços de TI. O benefício mais significativo vem de hospedar aplicações em infraestrutura em nuvem devido à redução de custos de capital (capital expenditure - Capex) e custos operacionais (operational expenditure - Opex).
- Otimização da produtividade da equipe de TI. A mudança para o uso de IaaS, ao acelerar o desenvolvimento e a implantação de aplicações, bem como automatizar o seu gerenciamento, torna a equipe de TI mais produtiva e capaz de melhorar o suporte de operações de missão crítica.
- Melhoria da produtividade do usuário final. Os usuários finais beneficiaram-se de menor indisponibilidade do serviço e recuperação mais rápida, reduzindo o tempo de inatividade em 72% e economizando expressivos recursos de cada aplicativo por ano.
- Aumento de benefícios do negócio. Muitas das empresas estão empregando soluções em nuvem para possibilitar novos modelos de negócios e suportar aplicações de geração de receita, atingindo um maior número de usuários/clientes.

A ISACA (Information Systems Audit and Control Association), por sua vez, aponta outras vantagens da computação em nuvem no documento **Controls and Assurance in the Cloud: Using COBIT 5**:

- Melhorar capacidade de resposta. Computação em nuvem fornece serviços flexíveis e escaláveis que podem ser implementados rapidamente para fornecer às organizações a capacidade de responder a mudanças de requisitos e a períodos de picos.
- Ciclo mais rápido de inovação. No ambiente de nuvem, a inovação é tratada muito mais rápido do que dentro da empresa. O gerenciamento de patches e atualizações para novas versões tornam-se mais flexíveis.
- Redução do tempo para implementação. Computação em nuvem oferece poder de processamento e capacidade de armazenamento de dados conforme a necessidade, quase em tempo real.
- Resiliência. Computação em nuvem pode fornecer um ambiente altamente resiliente e reduzir o potencial de falha e o risco de downtime.

O Tribunal de Contas da União também abordou no seu **Acórdão nº 1739/2015-Plenário** as tecnologias de computação em nuvem, no qual relaciona vantagens observadas na utilização destes serviços para a administração pública:

- Maior agilidade da administração pública na entrega de serviços e em sua atualização tecnológica, pois os processos formais de contratação pública podem dificultar a manutenção de uma infraestrutura de TI própria atualizada e que responda rapidamente às demandas de seus usuários.
- Suporte a iniciativas de Big Data e Dados Abertos, facilitando a abertura de informações governamentais que hoje encontram-se em sistemas que controlam as operações cotidianas do Estado e portanto são fechados com acesso limitado aos seus operadores. O uso de nuvem pública permitiria ampliar o acesso a esses dados a um custo menor, sem comprometer a segurança, a disponibilidade e o desempenho operacional dos sistemas originais. Uma vez os dados governamentais estando facilmente acessíveis, torna-se possível maior participação da sociedade na criação de novos serviços baseados nesses dados.
- Atendimento a picos de demanda sazonal de serviços públicos pela Internet sem necessidade de alocar grande quantidade de recursos fixos. Várias atividades estatais acarretam picos sazonais de demanda de serviços próximos a datas limite como: entregas de declarações de imposto de renda, inscrições e resultados do Enem, resultados eleitorais e listagem de gestores públicos inelegíveis, períodos de cadastramento do INSS, listagem dos percentuais do fundo de participação dos municípios, etc.
- A contratação de serviços em nuvem de IaaS ou PaaS pode levar a uma redução de oportunidades de desvios e irregularidades, quando comparada às múltiplas contratações de máquinas, licenças de software, manutenção e suporte necessárias para a operação de CPD próprio. As ofertas de IaaS e PaaS identificadas neste levantamento são todas por contrato de adesão, utilizando métricas de precificação com custos unitários divulgados publicamente e iguais para todos os clientes, o que facilita a pesquisa de preços.
- Agilidade e economia na entrega de serviços para instituições públicas com unidades descentralizadas, que podem ter serviços disponibilizados por meio de acesso à internet, mais barato que as interconexões via redes privadas atualmente utilizadas.

O Acórdão TCU nº 1739/2015-Plenário elenca ainda uma relação de riscos relativos à contratação, à utilização e à gestão de serviços de computação em nuvem, mas é preciso salientar que houve grandes mudanças de cenário nos últimos 5 anos. Naquela ocasião o foco era na adequação dos serviços ao Decreto nº 8.135/2013, que determinava a contratação preferencial de empresas públicas para a prestação de serviços de nuvem, Decreto este que foi revogado em 2018. Além disso, atualmente os serviços de computação em nuvem de alta qualidade e larga escala estão principalmente concentrados em alguns poucos provedores de abrangência global (ex., AWS, Google, Microsoft, Oracle), os quais, na maioria dos casos, atuam no mercado nacional por intermédio de uma rede de parceiros. Muitos dos riscos relativos à segurança da informação e da infraestrutura elencados pelo TCU atualmente são bastante mitigados por aspectos que são inerentes ao uso de serviços destes provedores, tais como as definições padronizadas de acordos de nível de serviço, as certificações e qualificações que os provedores de serviços de nuvem possuem e pelo uso de criptografia como padrão em todas as etapas da transmissão e armazenamento de dados. Em relação aos riscos apontados de dependência de fornecedor e de lock-in, o Ministério da Justiça e Segurança Pública tem buscado adotar uma estratégia de provimento de serviços de forma híbrida, em parte na nuvem (utilizando mais de um provedor) e em parte em infraestrutura própria, conforme discutido na seção seguinte.

Conceitualmente, as modalidades IaaS, PaaS e SaaS estão definidas da seguinte forma:

- A Infraestrutura como Serviço (IaaS) é a mais simples das três categorias, já que funciona praticamente da mesma forma, independentemente do fornecedor de nuvem escolhido. De forma geral, a IaaS oferece uma infraestrutura de TI automatizada e escalonável (armazenamento, hospedagem, redes) de seus próprios servidores globais, sendo remunerado apenas pelo o que o usuário consome. Desta forma, em vez de adquirir licenças de software ou servidores próprios, as empresas privadas ou administração pública podem simplesmente alocar recursos de forma flexível a partir das suas necessidades.
- A Plataforma como Serviço (PaaS) abrange todos os conceitos básicos da IaaS, assim como as ferramentas e recursos necessários para desenvolver e gerenciar aplicativos com segurança sem precisar se preocupar com a infraestrutura. Trata-se de um ambiente completo para o desenvolvimento, hospedagem e entrega de aplicativos web, com segurança, processos, métodos e componentes pré-definidos necessários e dentro dos melhores padrões de mercado. Com essa camada, o foco está na gestão dos aplicativos e dados. Tudo isso é feito utilizando a infraestrutura na nuvem. Ou seja, o time de desenvolvimento tem uma infraestrutura completa e moderna à disposição, sem que sejam necessários altos investimentos.
- O Software como Serviço (SaaS) é o software de terceiros acessado diretamente pela web, geralmente bastando um login. Por esse modelo, uma empresa pode contratar um plano de assinatura e utilizar os programas necessários para os seus negócios. Neste sentido, o SaaS é muito mais interessante para o uso de aplicativos específicos, como ferramentas de escritório, controle

de atendimentos, dentre outros. No contexto do provimento de serviços de nuvem podem existir soluções de software como serviço, tais como ferramentas de monitoramento, segurança e gestão de identidades, que são compostas com outros serviços providos nas modalidades IaaS e PaaS para a disponibilização de uma solução complexa.

Uma outra forma de diferenciar as modalidades IaaS, PaaS e SaaS em contrato de serviços de computação em nuvem é visualizar de que forma as responsabilidades sobre a infraestrutura de TIC estão compartilhadas entre esses atores. Se na modalidade "software como serviço" (SaaS) a responsabilidade por todos os aspectos de infraestrutura é do provedor (o que é verificado em serviços como o Office 365 ou o Power BI), nos casos de Infraestrutura como Serviço (IaaS) e Plataforma como Serviço (PaaS) as responsabilidades são divididas. A Figura 2, extraída do site da Microsoft, apresenta a matriz de responsabilidades para os principais aspectos da gestão de TIC nas diferentes modalidades de provimento de serviços de nuvem:

Figura 2 - Modelo de Responsabilidade Compartilhada nos Serviços de TIC on premises, IaaS, SaaS e PaaS



O Ministério da Justiça e Segurança Pública possui hoje um conjunto de ações e iniciativas que dependem do uso de tecnologias de computação em nuvem para a sua realização. Portanto, a contratação visa dotar o MJSP de recursos (na forma de créditos de nuvem) suficientes para a execução dos seguintes Projetos e Objetivos Estratégicos constantes no seu Planejamento Estratégico para os anos 2020-2023, considerando suas demandas presentes e futuras:

- **Córtex e APIs de Segurança Pública** - Sistemas criados para prover em tempo real informações cadastrais e de rastreamento de veículos, e ainda informações de outras bases de dados de grande importância para as áreas de inteligência e de operações de segurança pública de todas as unidades da federação. Essas iniciativas estão relacionadas ao projeto estratégico "Sistema Inteligente de Consciência Situacional" da Secretaria de Operações Integradas (SEOPI).
- **SINESP Geo** - Processo de geo-codificação dos dados de ocorrências policiais em todo o país, viabilizando a produção de dados estatísticos e de manchas criminais e orientando as políticas e ações de segurança pública. Essa iniciativa é parte integrante dos projetos estratégicos "Em Frente Brasil" e "SINESP big data e inteligência artificial", da Secretaria Nacional de Segurança Pública (SENASP).
- **Projeto Sinesp Identidade**: Criação de diretório nacional de profissionais de segurança pública, com a utilização de mecanismos de autenticação segura, para uso nos projetos de sistemas finalísticos para a área de segurança pública conduzidos pela Secretaria Nacional de Segurança Pública. Essa iniciativa é parte integrante dos projetos estratégicos "Em Frente Brasil" e "SINESP big data e inteligência artificial", da Secretaria Nacional de Segurança Pública (SENASP).
- **SINESP-DW** - Criação de Data Warehouse e painel analítico com dados do sistema nacional de segurança pública, que são providos pelas ferramentas do SINESP. Essa iniciativa está associada ao projeto estratégico "SINESP big data e inteligência artificial", da Secretaria Nacional de Segurança Pública (SENASP).
- **Pró-Consumidor** - Internalização do sistema de processos das unidades de defesa do consumidor estaduais (PROCONS), cuja infraestrutura hoje é provida externamente pela empresa BBTS (Banco do Brasil Tecnologia e Serviços). Esta ação está vinculada ao projeto estratégico "Dinamização da plataforma Consumidor.gov.br, com foco na desjudicialização", da Secretaria Nacional do Consumidor (SENACON).
- **Projeto Rede-Lab (ambiente com Desktops Virtuais e Ferramentas Analíticas)** - Proposta de nova estrutura para a Rede de Laboratórios de Lavagem de Dinheiro do Departamento de Recuperação de Ativos e Cooperação Internacional (DRCI), utilizando tecnologias de computação em nuvem. Esta ação está vinculada ao projeto estratégico "Reestruturação e reorganização da Rede Nacional de Laboratórios de Lavagem de Dinheiro –REDE-LAB", da Secretaria Nacional de Justiça (SENAJUS).
- **Data Lake da Segurança Pública Nacional com Data Catalog** - Implantação de repositório contendo catálogo de dados de interesse para o Sistema Nacional de Segurança Pública. Ação vinculada ao Projeto Estratégico "Inteligência analítica aplicada no combate à corrupção, lavagem de dinheiro e em ações de segurança pública", do Ministério da Justiça e Segurança Pública.
- **eSIC** - Implantação de ferramentas com o objetivo de melhorar o tratamento e controle de demandas vindas pelo e-SIC da CGU para o MJSP. Ação vinculada ao Objetivo Estratégico "Fortalecer e ampliar a estrutura e os serviços de TIC" da DTIC/MJSP.
- **App de Perícia em Campo** - Desenvolvimento de aplicação móvel para execução de perícias em campo, com o uso da ferramenta Azure Maps. Esta é uma iniciativa associada ao aprimoramento das atividades de perícias em campo, o que é

também objeto do projeto "Fortalecimento da Rede Integrada de Bancos de Perfis Genéticos", da Secretaria Nacional de Segurança Pública (SENASP).

- **Application Insights** - Monitoramento do desempenho das aplicações sustentadas pela DTIC/MJSP. Ação vinculada ao Objetivo Estratégico "Fortalecer e ampliar a estrutura e os serviços de TIC" da DTIC/MJSP.
- **Log Analytics** - Registro e análise de informações geradas por sistemas e processos informatizados (logs), como forma de incrementar as capacidades de auditoria e segurança de TIC. Ação vinculada ao Objetivo Estratégico "Fortalecer e ampliar a estrutura e os serviços de TIC" da DTIC/MJSP.
- **DevOps** - Uso da ferramenta Azure DevOps para a gestão de projetos e controle de implantação de novos releases dos softwares desenvolvidos pela Fábrica de Software da DTIC. Ação vinculada ao Objetivo Estratégico "Fortalecer e ampliar a estrutura e os serviços de TIC" da DTIC/MJSP.
- **Armazenamento de dados de CFTV do Sistema Prisional Federal** - Registro de longo termo das imagens geradas pelo sistema de Circuito Fechado de Monitoramento (CFTV) através de armazenamento em nuvem. Esta iniciativa está vinculada ao projeto estratégico "Aprimoramento do monitoramento das visitas no Sistema Penitenciário Federal", do Departamento Penitenciário Nacional (DEPEN).
- **Demandas adicionais de provimento de infraestrutura e novos projetos** - Reserva de recursos para a execução de novos projetos ainda em planejamento, que poderão fazer uso de capacidade provida pela nuvem, como é o caso dos projetos estratégicos "Fortalecimento da Rede Integrada de Bancos de Perfis Genéticos" e "Sistema Nacional de Análise Balística - SINAB", ambos da Secretaria Nacional de Segurança Pública (SENASP).
- **Express Route (conexão de alta capacidade entre Datacenter e nuvem)** - Recursos para a implantação de conexão de alta velocidade entre o datacenter do MJSP e a nuvem, visando otimizar a transferência de dados e o acesso às aplicações. Ação vinculada ao Objetivo Estratégico "Fortalecer e ampliar a estrutura e os serviços de TIC" da DTIC/MJSP.
- **Desktops Virtuais para Necessidades do Ministério da Justiça e Segurança Pública** - Recursos para a implantação de infraestrutura de Desktops Virtuais para atender as necessidades do Ministério da Justiça, visando a compatibilidade de aplicações e o trabalho remoto com segurança. Ação vinculada ao Objetivo Estratégico "Fortalecer e ampliar a estrutura e os serviços de TIC" da DTIC/MJSP.
- **Desktops Virtuais para Centro Integrado de Operações de Fronteira** - Recursos para a implantação de infraestrutura de Desktops Virtuais para atender as necessidades de segurança no acesso a aplicações à partir do Centro Integrado de Operações de Fronteira (CIOF), localizado em Foz do Iguaçu-PR. Essa iniciativa está relacionada ao projeto estratégico "Programa VIGIA" da Secretaria de Operações Integradas (SEOPI).
- **Desktops Virtuais para Centros Integrados de Inteligência de Segurança Pública Regionais** - Recursos para a implantação de infraestrutura de Desktops Virtuais para atender as necessidades de segurança no acesso a aplicações à partir dos Centros Integrados de Inteligência de Segurança Pública Regionais (CIISP-R), estando prevista a implantação de um Centro em cada região do País (atualmente estão implantados os Centros de Manaus/AM, Curitiba/PR e Fortaleza/CE). Essa iniciativa está relacionada ao projeto estratégico "Rede de Centros Integrados de Inteligência" da Secretaria de Operações Integradas (SEOPI).
- **Projeto Base de Dados do Sistema Nacional de Análise Balística (SINAB)**: Criação de infraestrutura em nuvem para sustentação da base central de armazenamento e do motor de correlações de dados do Sistema Nacional de Análise Balística (SINAB). Essa iniciativa é parte integrante do projeto estratégico "Sistema Nacional de Análise Balística" da Secretaria Nacional de Segurança Pública (SENASP).

A Equipe de Planejamento realizou um esforço para, ainda que considerando as incertezas inerentes ao dimensionamento das demandas por parte das áreas de negócio, aplicar uma metodologia de planejamento do consumo de recursos de nuvem por meio do uso da ferramenta Azure Calculator (<https://azure.microsoft.com/pt-br/pricing/calculator/>), que realiza projeções tendo como referência os recursos a serem de fato provisionados para cada projeto. As projeções de recursos de nuvem feitas para cada projeto que irá utilizar recursos de computação em nuvem e dos custos correspondentes estão consolidadas no documento SEI 13582235, e estão ainda compartilhadas na internet por meio dos seguintes links:

- Projeto Cortex: <https://azure.com/e/927b5929c4034791a719b90b293872fa>
- Projeto Sinesp Geo: <https://azure.com/e/0cf46fc7ea06418f973b5a2b1637cf8d>
- Projeto Sinesp Identidade: <https://azure.com/e/2ee993d0aa424e239785ea7aac14d27e>
- Projeto Sinesp DW: <https://azure.com/e/222c2347d298431aa46e6557ba4c6d12>
- Projeto Pro Consumidor: <https://azure.com/e/a09f54b5e28043079ecc1592a778c004>
- Projeto Rede-Lab: <https://azure.com/e/02e815822f614a7fabe166ca18845899>
- Projeto Data Lake de Segurança Pública: <https://azure.com/e/f3e29726c6af4f3690bd776e12b9d5c7>
- Projeto eSIC: <https://azure.com/e/52063f0ab2754d1ebb01d24d79a3a6d7>
- Projeto App Perícia Mobile: <https://azure.com/e/c03488f6be4e4855a995f43511ac0507>
- Projeto Log Analytics: <https://azure.com/e/30e3f6b71ab9498f81736ca8c0d2dc1d>
- Projeto Application Insights: <https://azure.com/e/152f20d7ceda444aae002ebb2a51880f>
- Projeto Azure DevOps: <https://azure.com/e/d80084a43b0b4147a93f7568385742e6>
- Projeto Armazenamento de dados CFTV Sistema Prisional Federal: <https://azure.com/e/81bceec73ac4c45698365492d73949999>

- Demandas Adicionais de Infraestrutura: <https://azure.com/e/190476ffd8434a1583f7c6d980e4e0ee>
- Projeto Express Route: <https://azure.com/e/bcc363bd79d142129ca497e47010b31e>
- Projeto Desktops Virtuais (VDI) para o MJSP: <https://azure.com/e/0b29b0e883314791b7dae39d12756cc7>
- Projeto Desktops Virtuais (VDI) para o Centro Integrado de Operações de Fronteira (CIOF): <https://azure.com/e/f8e045b099bd4beeb3f835e84fe5866a>
- Projeto Desktops Virtuais (VDI) para os Centros Integrados de Inteligência de Segurança Pública (CIISPR): <https://azure.com/e/92a27d2b8d79444dad8e64a80f5941f4>
- Projeto Base de Dados do Sistema Nacional de Análise Balística (SINAB): <https://azure.com/e/aa7fe283dde44405b16abdef01c12ded>

A Tabela abaixo apresenta um resumo do novo dimensionamento dos recursos de Computação em Nuvem Azure da presente contratação, considerando a metodologia de cálculo e demais fatores aqui relatados. Para a realização das projeções de consumo foram adotadas as seguintes premissas:

- Os valores mensais para cada projeto obtidos da calculadora do Azure, e que constam nas projeções existentes no SEI, foram corrigidos com um acréscimo de 23% em virtude de ser essa a diferença percentual entre o valor base do Monetary Commitment considerado na calculadora e o Preço Estimado de Revenda (ERP) do Monetary Commitment que foi utilizado para as estimativas, conforme o mecanismo explicado na seção 6.19 deste Estudo Técnico Preliminar da Contratação.
- Todas as estimativas consideraram recursos criados na zona "Brazil South", que engloba os datacenters localizados no estado de São Paulo.
- Todas as estimativas foram feitas na modalidade pay-as-you-go, sem considerar o provisionamento de recursos por tempo preestabelecido (que permite descontos adicionais).
- No caso dos projetos que envolvem a necessidade de utilização de licenças do Windows Server e do Microsoft SQL Server, foi considerado nas estimativas o mecanismo de "benefício híbrido" (*hybrid benefit*), que elimina os custos de licenciamento destes softwares na nuvem caso o cliente possua este licenciamento para uso *on premises*. O licenciamento do Windows Server e do Microsoft SQL Server para uso *on premises* está detalhado nas seções 2.5 e 2.7 deste Estudo Técnico Preliminar da Contratação.

Projeto	Consumo Mensal - Calculadora Azure	Consumo Mensal - Valor Corrigido	Consumo Anual
Cortex	R\$ 59.565,43	R\$ 73.265,48	R\$ 879.185,75
SINESP Geo	R\$ 60.230,84	R\$ 74.083,93	R\$ 889.007,20
SINESP Identidade	R\$ 1.214,74	R\$ 1.494,13	R\$ 17.929,56
SINESP-DW	R\$ 9.702,97	R\$ 11.934,65	R\$ 143.215,84
Pro Consumidor	R\$ 21.761,74	R\$ 26.766,94	R\$ 321.203,28
Projeto Rede-Lab (ambiente com Desktops Virtuais e Ferramentas Analíticas)	R\$ 59.273,23	R\$ 72.906,07	R\$ 874.872,87
Data Lake da Segurança Pública Nacional com Data Catalog	R\$ 20.145,24	R\$ 24.778,65	R\$ 297.343,74
eSIC	R\$ 515,49	R\$ 634,05	R\$ 7.608,63
App Perícia Mobile	R\$ 556,76	R\$ 684,81	R\$ 8.217,78
Application Insights	R\$ 651,91	R\$ 801,85	R\$ 9.622,19
Log Analytics	R\$ 1.769,47	R\$ 2.176,45	R\$ 26.117,38
Azure DevOps	R\$ 6.664,87	R\$ 8.197,79	R\$ 98.373,48
Armazenamento de dados de CFTV do Sistema Prisional Federal	R\$ 42.251,80	R\$ 51.969,71	R\$ 623.636,57
Demandas adicionais de provimento de infraestrutura e novos projetos	R\$ 56.846,45	R\$ 69.921,13	R\$ 839.053,60
Express Route (conexão de alta capacidade entre Datacenter e nuvem)	R\$ 5.263,87	R\$ 6.474,56	R\$ 77.694,72
Desktops Virtuais para Necessidades do Ministério da Justiça e Segurança Pública	R\$ 17.863,23	R\$ 21.971,77	R\$ 263.661,27
Desktops Virtuais para Centro Integrado de Operações de Fronteira (CIOF)	R\$ 8.287,32	R\$ 10.193,40	R\$ 122.320,84
Desktops Virtuais para Centros Integrados de Inteligência de Segurança	R\$ 32.542,51	R\$	R\$

Pública Regionais (CIISP-R)		40.027,29	480.327,45
Sistema Nacional de Análise Balística (SINAB)	R\$ 29.918,36	R\$ 36.799,58	R\$ 441.594,99
TOTAL			R\$ 6.420.987,15
TOTAL em Azure Monetary Commitments			R\$ 1.074,25

Tabela 17 - Estimativa de Consumo de Recursos de Nuvem Azure

Portanto, de acordo com as projeções obtidas para os projetos em andamento que irão requerer recursos de computação em nuvem, conforme o memorial de cálculo existente no documento SEI 13582235, o quantitativo para o item 29 da contratação deverá ser corrigido de 995 para 1.075 Compromissos Monetários (Monetary Commitments), considerando como referência o valor do Estimated Retail Price fornecido pela Microsoft para o Monetary Commitment de R\$ 5.977,20 (conforme SEI 12259433).

3 – IDENTIFICAÇÃO DAS SOLUÇÕES

Iremos dividir a identificação das soluções em dois grupos: Subscrição de Software e Serviço de Computação em Nuvem.

3.1 SUBSCRIÇÃO DE SOFTWARE

3.1.1 Solução 1A: Portal do Software Público.

O presente cenário tem o objetivo de analisar a aquisição junto ao Portal do Software Público (<https://www.gov.br/governodigital/pt-br/software-publico>).

O Software Público Brasileiro é um tipo específico de software livre que atende às necessidades de modernização da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e é compartilhado sem ônus no Portal do Software Público Brasileiro, resultando na economia de recursos públicos e constituindo um recurso benéfico para a administração pública e para a sociedade. O que rege o Software Público Brasileiro atualmente é a Portaria N° 46 de 28 de setembro de 2016, que dispõe sobre os procedimentos para o desenvolvimento, a disponibilização e o uso do Software Público Brasileiro

Sempre que possível já são utilizados softwares disponibilizados na plataforma do Software Público no ambiente de processamento central do MJSP, como por exemplo, o Sistema de Informação Eletrônica - SEI, Sistema de Registro e Frequência Eletrônica - SISREF e o Sistema Integrado de Gestão Patrimonial - SIADS (os dois últimos, em implantação).

Conforme pesquisa no Portal de Software Público constam 69 softwares disponíveis no Portal (SEI nº 12183066 "screenshot-softwarepublico.gov.br-2020.07.19-14_17_36", no entanto, não foi identificado um conjunto de soluções que atendessem a todas as necessidades elencadas no tópico Necessidades Tecnológicas e de Negócio do presente documento.

3.1.2 Solução 2A: Software Livre.

a) Sistema Operacional Servidor

O MJSP possui em seu ambiente de virtualização Windows aproximadamente 280 servidores virtuais de rede, totalizando no conjunto em torno de 1051 vCPU alocadas, os quais processam as aplicações e dados de todas as áreas de negócio. Aplicações críticas Microsoft funcionam totalmente de forma virtualizadas, conforme exemplificado abaixo, permitindo alta disponibilidade e balanceamento de carga através de *clusters* de servidores físicos.

- a) **Infra Básica:** Active Directory, DHCP, NTP, DNS, WSUS, SCOM, RADIUS, CA - Servidor de Certificados, System Center, Exchange, Servidor on premise Sharepoint, MIM, File Server, Print Server, Trend Micro;
- b) **Servidores de aplicação:** EAD Infoseg, Internet Information Services - IIS, SIAPEN, SINDEC, ClassInd;
- c) **Servidores de BD:** Cluster SQL, Power BI Report Services;
- d) **Solução de Segurança/Backup:** Varonis, Risk Manager, NetBackup;
- e) **Sistema de Controle de Acesso Físico:** Sistema de catracas, CFTV;
- f) **Sincronização com Azure:** ADFS, HMA, MFA;

A gestão dos usuários, e-mails e serviços críticos de domínio do MJSP são providos por soluções Microsoft: Active Directory, proxy, DNS entre outros serviços implementados sobre Windows Server, com diversos serviços agregados como DNS, Proxy e file server. Desta forma, a migração para uma solução de software livre necessitaria alterar toda a forma de autenticação dos usuários para uma solução baseada em LDAP (Lightweight Directory Access Protocol) nos três datacenters que dispõe o MJSP.

Conforme informado anteriormente, estima-se que em torno de 280 servidores necessitariam ser migrados, o que envolveria a alteração de permissionamento e adaptação para a autenticação dos diversos sistemas existentes atualmente. É uma tarefa de alta complexidade, que não encontra justificativa técnica, considerando o nível de padronização existente atualmente no MJSP.

b) Plataforma de Dados

Semelhantemente ao Windows Server, diversas aplicações e sistemas do MJSP foram desenvolvidas e são sustentadas com integração ao SGBD SQL da Microsoft (a estrutura de SGBDs utilizada pelo MJSP já é diversificada e já inclui MySQL, Postgree e Oracle). A migração dessas aplicações para uma outra plataforma diferente do Microsoft SQL Server necessitaria de adequação das aplicações

utilizadas atualmente. Além disso, temos diversas aplicações legadas, o que poderia gerar indisponibilidades e em alguns casos até mesmo incompatibilidade. Dessa forma, esse cenário não se mostrou viável, pelos motivos expostos acima.

c) Colaboração e Produtividade/Identidade e Segurança

O presente cenário tem o objetivo de analisar a aquisição de uma solução de Software Livre, especificamente o LibreOffice em substituição ao Microsoft Office.

LibreOffice é uma suite de aplicativos livre para escritório disponível para Windows, Unix, Solaris, Linux e Mac OS X. A suite utiliza o formato OpenDocument — formato homologado como ISO/IEC 26300 e NBR ISO/IEC 26300 — e é também compatível com os formatos do Microsoft Office, além de outros formatos legados. Oferece as principais funções esperadas de uma suite profissional: editor de textos, planilha, editor de apresentações, editor de desenhos e banco de dados, exportação para PDF, editor de fórmulas científicas, extensões, etc. É composto dos seguintes aplicativos: Writer – Editor de texto. Calc – Planilha. Impress – Editor de apresentação. Draw – Editor de Desenho. Math – Editor de Fórmulas. Base – Banco de dados. Atualmente a suite oficial de escritório utilizada pelo MJSP é o Microsoft Office (E3 e E5).

Iremos listar as principais vantagens e desvantagens em sua adoção:

Vantagem:

- Licenciamento gratuito;
- Código fonte aberto (open source);
- Disponível para os sistemas operacionais Windows, Unix, Solaris, Linux Mac OS X.

Desvantagem:

- Não possui um aplicativo de correio eletrônico corporativo integrado (teríamos que fazer uma composição com um produto open source, como por exemplo o Mozilla Thunderbird);
- Os documentos do Microsoft Office nem sempre são exatamente iguais no LibreOffice (uma das razões é que a Microsoft usa suas próprias fontes);
- Quando você compra uma licença para o Microsoft Office, o Microsoft OneDrive é incorporado a todos os programas. O LibreOffice não inclui nenhum armazenamento em nuvem. Haveria a possibilidade de se usar serviços como o OneDrive (sem possuir o Office), o Dropbox ou outro provedor de armazenamento em nuvem para sincronizar seus arquivos na nuvem;
- Quando você paga por uma licença do Microsoft Office, também compra o suporte ao cliente. O LibreOffice, como todas as plataformas de código aberto, conta com a assistência dos usuários da comunidade que oferecem voluntariamente seus conhecimentos e tempo. Como o produto é gratuito, não há obrigação de fornecer suporte; portanto, normalmente é necessário esperar um pouco mais pelas respostas às suas perguntas;
- Possui dependência do Java Runtime Environment (JRE) para algumas funcionalidades;
- Não possui integração nativa com nenhum tipo de plataforma colaborativa e não oferece qualquer suporte próprio para isso;
- Não possui integração nativa com as tecnologias utilizadas no MJSP, tais como: Active Directory, Exchange, Skype for Business, Teams, Sharepoint, SQL Server, OneDrive for Business, etc.
- Não possui suporte para edição em dispositivos móveis (Android, iOS, Windows Mobile), bem como não possui um suporte funcional para edição via web;
- Baixa expertise técnica e experiência da equipe de profissionais do MJSP com a solução em questão;
- Baixo grau de padronização visual e modo de operação das soluções, por serem de múltiplos desenvolvedores;

d) Portfólios e Projetos

Atualmente, diversas unidades do MJSP já organizam suas atividades de gestão de projetos e equipes em ambiente de nuvem, com dispositivos de colaboração e gerenciamento de atividades projetizadas. Tais ambientes contam com uma série de customizações que facilitam o uso das ferramentas disponíveis. A ferramenta de gerenciamento de projetos utilizada no ambiente do MJSP é o Microsoft Project que está integrada ao Active Directory e ao restante do Office 365, que permite melhor gestão de atividades e tarefas com o Teams, gerenciamento de equipe e publicação de página para acompanhamento do projeto pelo Sharepoint.

Alterar a atual solução, implicaria em um retrabalho para as áreas de negócio, pois teriam que refazer o cadastramento dos projetos, prazos e cronogramas, além da customização da nova ferramenta. Além disso, a unidade responsável pela área de projetos no MJSP (CGGE) e a DTIC já se pronunciaram pela continuidade da atual solução (SEI nº 12230344), informando que o Microsoft Project OnLine atende satisfatoriamente os seus requisitos.

e) Self-service bi/Analytics

O Power BI é utilizado hoje no MJSP como a principal ferramenta de BI. Temos mais de 1.400 workspaces cadastrados (workspaces são locais para colaborar com os usuários, neles são criadas as coleções de dashboards, os relatórios e relatórios paginados). Por meio do Contrato 27/2018 (SEI nº 08006.000878/2018-34 - Lanlink Soluções e Comercialização em Informática S.A.) já foram solicitados o desenvolvimento de diversos painéis, alguns de caráter estratégico para o Ministério da Justiça e Segurança Pública.

Da análise das alternativas, concluiu-se pela continuidade da solução de BI baseada na suite Microsoft Power-BI. A integração com a atual arquitetura tecnológica do MJSP, o aproveitamento dos dashboards já desenvolvidos e a manifestação da área de Informações e Dados (SEI nº 11054610) pela manutenção da atual solução foram tomados como referência.

3.1.3 Solução 3A: G Suite.

O presente cenário tem o objetivo de analisar a utilização do G Suite da Google em substituição ao Microsoft Office.

G Suite (antigo Google Apps) é um serviço do Google que oferece versões de vários produtos Google que podem ser personalizados de forma independente com o nome de domínio do cliente. Ele oferece vários aplicativos da web com recursos similares aos de pacotes de escritório tradicionais, inclusive Gmail, Hangouts, Google Agenda, Drive, Docs, Planilhas, Apresentações, Groups, News, Play, Sites, e Vault.

Sob o ponto de vista econômico (considerando o Pregão analisado e o Catálogo disponível na Web), a solução da Google (versão Basic: R\$ 25,00 usuário/mês. PE Nº 00005/2020. UASG: 389421. CRE-CE) apresenta um custo levemente superior a versão inicial da Microsoft (Office E1: R\$ 22,21 usuário/mês. PE Nº 80/2019. UASG: 30001. TCU), com vantagem da Microsoft com relação a capacidade de e-mail (30 GB x 50 GB) e armazenamento em nuvem (30 GB x 1 TB).

Um outro ponto desfavorável à solução do Google é que enquanto a Microsoft permite que suas ferramentas sejam instaladas em diferentes plataformas, como computadores, notebooks, tablets e smartphones, a partir da versão E3, o Google tem suas soluções disponibilizadas por meio de navegadores, e, para dispositivos Android, algumas ferramentas principais, mas que podem apresentar dificuldades na usabilidade ao serem instaladas em dispositivos com telas menores, como smartphones. No atual contrato da Microsoft com o MJSP a suite de programas de escritório é instalada diretamente nos computadores (versões E3 e E5). Existem algumas diferenças entre a versão Desktop e a versão via Web do Office 365 ().

Para essa contratação, na consulta às unidades organizacionais, quanto aos tipos de versões do Microsoft 365, como o início para uma mudança cultural e visando economia de recursos, foi sugerido a utilização da versão online (E1) para alguns tipos de usuários, onde o requisito de usabilidade não fosse tão elevado. No entanto, entendemos que ainda há alguns entraves técnicos e de performance para a utilização em massa da versão online para todos os tipos de usuários.

Além disso, há ainda no MJSP um legado significativo de código de macros em linguagem VBA (Excel/Access/Word), utilizados em processos de trabalho, tanto nas áreas finalísticas, como nas áreas-meio, além da necessidade de migração e treinamento da equipe.

3.1.4 Solução 4A: Contratação de Licenças de Softwares Microsoft.

O presente cenário tem o objetivo de analisar a continuidade na utilização das ferramentas Microsoft no âmbito do MJSP. Especificamente com relação à solução de colaboração e produtividade, o Ministério disponibiliza para os usuários finais o Microsoft 365 - E3. PART NUMBER: AAA-10756 e Microsoft 365 - E5. PART NUMBER: AAA-28605. Tecnicamente a solução atende bem aos requisitos dos usuários finais, apresenta boa interatividade e é de fácil utilização. Além disso, está totalmente integrada com os diversos aplicativos e serviços que compõem a solução (M365 = Enterprise Mobility + Security + Office 365 + Windows), por serem do mesmo fabricante e serem comercializados em conjunto. Outro aspecto importante é com relação a cultura organizacional. Todos os usuários já estão bem familiarizados com o Office, partir para uma das soluções dos cenários anteriores, além de não atender por completo os requisitos dos usuários, ainda geraria custo de integração, de gerenciamento, de implementação e treinamento dos usuários.

Com relação à suite de Portfólios e Projetos, o MJSP utiliza atualmente o Microsoft Project que está integrada ao Active Directory e ao restante do Office 365. A unidade responsável pelo gerenciamento de Projetos da DTIC, subsidiada pela Coordenação-Geral de Gestão Estratégica e Inovação Institucional - CGGE, se manifestou pela manutenção da atual solução. (SEI nº 12230344)

Para a solução de Self-service BI/Analytics, a unidade responsável pelo gerenciamento de Dados da DTIC, se manifestou pela manutenção da atual solução. (SEI nº 11054610)

Importante destacar que nesse cenário não haverá gastos de implantação, nem de treinamento, tendo em vista que a equipe técnica já tem conhecimento da tecnologia e essa se encontra implantada.

3.1.4.1 Análise de Viabilidade

Durante a elaboração desse ETP, a Equipe de Planejamento da Contratação verificou a necessidade de que houvesse uma previsão normativa por parte do MJSP para que fosse respaldada a utilização dos serviços em nuvem.

Diante do exposto, a Equipe de Planejamento da Contratação entende como viável o presente cenário para a manutenção e continuidade dos atuais serviços prestados via Microsoft. Alertamos, no entanto, que a análise aqui realizada não pretende verificar a adequação do uso dos serviços de nuvem às políticas de segurança da informação institucionais, e nem compete à equipe de planejamento realizar uma análise mais abrangente dos riscos relativos à segurança da informação associados ao uso dos recursos de nuvem. Quando, e se for solicitada a ativação ou utilização desses serviços, a equipe de fiscalização deverá seguir o Modelo de Execução do Contrato constante no Termo de Referência, conforme previsto pela IN 1/2019 ME/SGD.

O uso dos recursos de computação em nuvem deve estar alinhado com a política de segurança da informação da instituição, e ainda à Norma Complementar nº 14 da IN 01/2008-DSIC/GSI, que define que somente podem ser utilizados recursos de nuvem aprovados pela alta administração (DAS 6 e acima) com o acompanhamento do Gestor de Segurança da Informação e Comunicação.

6.1 A Alta Administração de cada órgão ou entidade da APF, no âmbito de suas competências, é responsável pela segurança das informações tratadas em ambiente de computação em nuvem, em conformidade com as orientações contidas nesta norma e legislação vigente; e

6.2 O Gestor de Segurança da Informação e Comunicação do órgão, no âmbito de suas atribuições, é responsável pelas ações de implementação da gestão de risco de segurança das informações tratadas em ambiente de computação em nuvem. **(Norma Complementar nº 14 da IN 01/2008-DSIC/GSI)**

3.2 COMPUTAÇÃO EM NUVEM

3.2.1 Solução 1B: Não contratação do serviço de Computação em Nuvem

A Administração Pública Federal está gradativamente adotando o direcionamento preferencial para a contratação de serviços de computação em nuvem ("cloud-first") em detrimento do modelo de serviços de TIC providos à partir das próprias sedes dos órgãos públicos (denominado modelo "on premises"), conforme pode ser verificado na Instrução Normativa Nº 1 de 4 de abril 2019 da Secretaria de Governo Digital, que estabelece em seu Anexo, item 4, o seguinte:

4. **CONTRATAÇÃO DE INFRAESTRUTURA DE CENTRO DE DADOS, SERVIÇOS EM NUVEM, SALA-COFRE E SALA SEGURA:**

4.1. Os órgãos e entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação.

4.2. As contratações de serviços em nuvem devem observar o disposto na Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e suas Normas Complementares, notadamente a Norma Complementar 14/IN01/DSIC/SCS/GSIPR.

4.2.1. Os órgãos e entidades devem exigir mediante justificativa prévia, no momento da assinatura do contrato, que fornecedores privados de serviços em nuvem possuam certificações de normas de segurança da informação aplicáveis ao objeto da contratação, assim como outros requisitos que objetivem mitigar riscos relativos à segurança da informação.

4.2.2. Os órgãos e entidades devem assegurar, por meio de cláusulas contratuais, que os serviços em nuvem a serem contratados permitirão a portabilidade de dados e softwares e que as informações do contratante estarão disponíveis para transferência de localização, em prazo adequado.

Uma vantagem dos serviços de nuvem ainda pouco enfatizada na Administração Pública, mas que recebeu destaque nas avaliações realizadas pelo IDC, ISACA e TCU, é a capacidade dos serviços de nuvem de alavancar projetos, acelerar entregas e otimizar resultados para o contratante, em especial na utilização de soluções de Plataforma como Serviço e Software como Serviço. Este tipo de solução permite abstrair diversos aspectos da infraestrutura que são apenas insumos para sustentar os processos de negócio, e focar diretamente naqueles aspectos da tecnologia que de fato geram valor comercial, o que permite executar muito mais em tempo muito menor. A DTIC/MJSP tem feito uso de soluções de computação em nuvem em determinados projetos de grande abrangência e resultado, e a avaliação é que tal resultado seria inviável para esses projetos no caso da utilização de ferramentas executadas no modelo "on premises" e contratadas no formato tradicionalmente utilizado para as contratações públicas.

A computação em nuvem se apresenta nos dias de hoje como uma das tecnologias ditas "desruptivas", capazes de provocar grandes transformações em setores inteiros da economia. A Administração Pública nas diferentes esferas da federação compreende cada vez melhor a sua utilidade e a sua capacidade para promover e acelerar a transformação digital, levando a serviços públicos melhores e mais efetivos. A caminhada para a nuvem parece ser um caminho inequívoco a ser trilhado por instituições públicas e privadas.

Desse modo, seguindo as melhores recomendações dos órgãos de controle e do SISP, o serviço de computação nuvem, utilizado de forma criteriosa, pode de fato trazer grandes benefícios para as organizações públicas, se tornando imprescindível a sua utilização. Pelo exposto, esse cenário não se mostra viável sem que haja prejuízo para Ministério da Justiça e Segurança Pública.

3.2.2 Solução 2B: Contratação de empresa especializada no serviço de Computação em Nuvem pública por licitação sem definição de provedor

Desde o ano de 2018 o Ministério da Justiça e Segurança Pública tem feito uso cada vez maior dos serviços de computação em nuvem Microsoft Azure, que foram adquiridos por meio do Contrato nº 28/2018, para vários de seus projetos. A experiência obtida nesse período demonstrou de forma inequívoca o potencial que o uso da computação em nuvem possui para viabilizar projetos que dependem de soluções dinâmicas de tecnologia da informação, em especial no que diz respeito a ferramentas capazes de possibilitar o processamento e a análise de grandes volumes de dados.

Além da nuvem Microsoft Azure, existem soluções de outros provedores de computação em nuvem, como, por exemplo, Google Cloud, Amazon AWS e Oracle Cloud, que possuem ofertas de serviços amplas e adequadas para determinados cenários. Para exemplificar, a DTIC/MJSP realizou recentemente (por meio do Processo SEI 08006.000238/2020-49) a contratação de serviços da Oracle Cloud, por ser esta a alternativa considerada viável para a internalização do sistema do sistema Consumidor.gov.br, da Secretaria Nacional do Consumidor, sistema este que presta relevante serviço público para a sociedade no campo dos direitos do consumidor. Naquela circunstância, por haver uma dependência tecnológica do sistema a ser internalizado com soluções da empresa Oracle, restou caracterizado por meio do Estudo Técnico Preliminar da Contratação (ETPC) que seria inviável naquela circunstância a contratação de solução de computação em nuvem de outros provedores para essa finalidade.

Do mesmo modo, para os projetos em andamento no Ministério da Justiça e Segurança Pública relacionados na seção 2.8, a solução considerada viável é a realização de processo de contratação para a manutenção e ampliação dos serviços atualmente prestados pela nuvem Microsoft Azure. Um dos motivos para essa conclusão é que vários dos projetos em curso no Ministério da Justiça e Segurança Pública fazem uso de soluções de Plataforma Como Serviço (PaaS) e Software como Serviço (SaaS) providas pela Microsoft Azure, tais como Azure Event Hubs, Azure Stream Analytics, Azure Functions, Azure Logic Apps, Azure Maps, Application Insights, Azure Active Directory, etc. Vários dos projetos em desenvolvimento e em produção atualmente no MJSP somente se tornaram viáveis após a adoção destas e outras soluções PaaS e SaaS da nuvem Microsoft Azure, como foram o caso dos projetos Cortex e Sinesp Geo, e estes são projetos que já se tornaram essenciais para as áreas de negócios responsáveis por eles (SEOPI e SENASP), não sendo, portanto, possível prescindir dos serviços. Ademais, a DTIC realizou grande investimento nos últimos 18 meses para adquirir conhecimento

técnico para a melhor utilização dos recursos da nuvem Microsoft Azure, incluindo a realização de treinamentos e participação em eventos nacionais e internacionais, estando hoje com as suas equipes em condições de extrair um resultado muito mais significativo dos serviços disponibilizados, sempre objetivando atender as necessidades das áreas de negócio do MJSP que dependem de soluções de Tecnologia da Informação. Por todos esses aspectos, a perspectiva de substituição do provedor de serviços de computação em nuvem Microsoft Azure por serviços de outro provedor para os projetos estratégicos em curso na DTIC implicaria em paralisação de serviços hoje providos continuamente para diferentes áreas do MJSP e para o Sistema Único de Segurança Pública, e implicaria ainda na necessidade de gastos adicionais com o re-desenvolvimento dos softwares e com a nova capacitação das equipes, sendo, portanto, considerada inviável.

3.2.3 Solução 3B: Contratação de empresa especializada no serviço de Computação em Nuvem pública Microsoft Azure mediante licitação

O presente cenário tem o objetivo de analisar a manutenção e ampliação dos serviços atualmente prestados pela nuvem Microsoft Azure. Conforme já demonstrado nos dois cenários anteriores, o uso de computação em nuvem é um caminho natural para a Administração Pública, e Ministério da Justiça não pode prescindir, no atual contexto, da adoção de um serviço em nuvem. Por outro lado, a instituição já possui diversos projetos implantados através da nuvem Microsoft Azure que sofreriam prejuízo caso houvesse a substituição do fornecedor dos serviços. Desta forma, fica caracterizado que a solução viável para o MJSP é a manutenção e ampliação dos serviços de computação em nuvem Microsoft Azure prestados atualmente por meio do Contrato nº 28/2018. A contratação dos serviços de nuvem Microsoft Azure deve ocorrer por meio de procedimento licitatório por Pregão Eletrônico, uma vez que a Microsoft comercializa o serviço por intermédio da sua rede de parceiros.

A adoção de tecnologias de Plataforma como Serviço (PaaS) e de Software como Serviço (SaaS) em nuvem pode suscitar questões à respeito de dependência tecnológica e de aprisionamento (*lock-in*) em relação a soluções de um fornecedor em particular. Essa é uma preocupação constante dos gestores de TIC, pois o custo de migração/re-desenvolvimento de soluções em uso por instituições públicas é normalmente significativo, o que traz consigo o risco de vulnerabilidade às políticas de preços do fornecedor. No entanto é preciso salientar que, na área de tecnologia da informação, esse risco já é hoje uma condição generalizada, que não é substancialmente menor no caso da utilização de licenças de software adquiridas para uso em infraestrutura própria (*on premises*). Além disso, o risco de *lock-in* deve ser sopesado com o benefício que as soluções PaaS e SaaS trazem para a execução de projetos institucionais que, de outra forma, dificilmente seriam viáveis. Deve ainda ser considerado que o futuro aponta para um cenário onde muitas das novas tecnologias só estarão disponíveis ou poderão ser acessadas na nuvem, como já é o caso de várias soluções de aprendizado de máquina, processamento cognitivo e inteligência artificial (ex., processamento de linguagem natural, reconhecimento de fala e imagem, etc.).

Organismos de referência no aconselhamento de profissionais da área de TIC, como é o caso do *Gartner Group*, vêm se debruçando sobre essas questões. Em linhas gerais, as pesquisas e análises feitas pelo Gartner apontam que dificilmente os gestores de TIC, não importa se atuando no setor público ou no setor privado, poderão prescindir da nuvem se esperam seguir com a evolução da qualidade dos serviços informatizados. De acordo com os levantamentos realizados pelo Gartner, 75% das organizações que usam a nuvem atualmente consideram ser ela a primeira alternativa para o desenvolvimento de novos projetos. O Gartner enfatiza ainda a necessidade das organizações desenvolverem uma estratégia de adoção da nuvem, que, no documento "*Formulate a Cloud Strategy in the Context of Your Overall Strategy*", analista David Smith detalha como deve ser:

"Uma estratégia de nuvem deve ser um ponto de vista claro e conciso na nuvem e seu papel na sua organização. Não é um plano migrar tudo para a nuvem. De fato, se você fizer dessa estratégia um plano para migrar tudo para a nuvem, seu pessoal poderá evitá-la porque talvez não queira ir para a nuvem. Deve ser um documento curto, um documento vivo - algo que funcione em conjunto com outros planos estratégicos, como uma estratégia de data center e uma estratégia de compras. Sua estratégia de nuvem não é uma tentativa de resolver tudo. Em vez disso, deve se concentrar na identificação de outras atividades que precisam ser realizadas para implementar e operacionalizar a estratégia."

Outro organismo de aconselhamento e consultoria, o *Forrester Research*, realizou extensa pesquisa no estudo "*Multicloud Arises From Changing Cloud Priorities*", que aponta que a estratégia preferida da maioria dos gestores de TIC envolve a adoção de soluções de provedores de nuvem diferentes em conjunto com soluções de nuvem *on premise* (o que vem se denominando estratégia *multi-cloud* ou de *cloud híbrida*) como a forma preferencial de mitigar os riscos de *lock-in* de fornecedor e ainda possibilitar a melhor entrega possível de serviços. De acordo com o estudo, 86% das companhias pesquisadas apontam que sua estratégia de nuvem envolve a contratação de serviços de mais de um provedor. Esta combinação de abordagens que envolve a contratação de serviços de nuvem de mais de um fornecedor combinada com a utilização de serviços *on premise* é exatamente a estratégia que vem sendo adotada pela DTIC/MJSP para garantir a continuidade e a expansão dos serviços com o mínimo de dependência possível em relação aos seus fornecedores.

É importante também salientar que a manutenção e ampliação dos serviços de nuvem Microsoft Azure apresenta várias vantagens de ordem técnica e econômica para o MJSP decorrentes do atual cenário de uso de soluções tecnológicas da Microsoft na instituição. Os serviços da nuvem Microsoft Azure oferecem integração nativa e direta com os serviços Microsoft instalados no datacenter atual do Ministério da Justiça e Segurança Pública, garantindo assim alta disponibilidade e redundância, conectividade e expansão do parque atual de máquinas já instaladas com pouco esforço. Também é possível se utilizar do benefício exclusivo de nuvem híbrida (*Hybrid Benefits*) da Microsoft que permite que as licenças de Office, Windows Client, Windows Server e SQL Server contratadas pelo Ministério da Justiça e Segurança Pública para o ambiente local, sejam utilizadas concomitantemente no ambiente local e na nuvem Azure, gerando assim uma economia na aquisição de licenças. Isso quer dizer que cada licença já comprada pode ser utilizada também no ambiente de nuvem ao mesmo tempo, dobrando a capacidade de uso dessas tecnologias, e reduzindo à metade seu custo.

Abaixo são relacionadas algumas das demais vantagens da contratação de serviços de nuvem Microsoft Azure em conjunto com o licenciamento de softwares Microsoft:

- **Office e Windows:** As licenças do Office e Windows podem ser migradas e utilizadas concomitantemente nas versões remotas através do serviço do Office 365 e Virtual Desktop, permitindo a possibilidade de teletrabalho com o serviço do Azure chamado

Azure Virtual Desktop. Não há a necessidade de licenciamentos adicionais.

- **Active Directory:** A Rede do Ministério da Justiça e Segurança Pública utiliza o Microsoft Active Directory como plataforma de gestão de identidade e ativos, gestão de direitos e permissões. É uma tecnologia já amplamente adotada no mercado e no governo federal e garante a segurança e gestão da rede e da infraestrutura de TI do Ministério da Justiça e Segurança Pública. Como proposta de evolução desta plataforma para garantir maior proteção aos usuários, informações e infraestrutura de TI do Ministério da Justiça e Segurança Pública, o Azure oferece o Azure AD. O serviço de identidade empresarial do Azure AD (Azure Active Directory + Intune + AIP) oferece logon único e autenticação multifator para ajudar a proteger usuários contra 99,9 por cento dos ataques de segurança cibernética. Além disso, o Azure AD dá suporte a mais de 2.800 aplicativos SaaS (software como serviço) pré-integrados.
- **System Center:** O Ministério da Justiça e Segurança Pública possui sistema de monitoramento de infraestrutura de TI baseado em Microsoft System Center. Este serviço pode ser interligado ao Azure Monitor, que é o serviço de monitoramento de nuvem que permite o monitoramento centralizado da infraestrutura local e remota. Com a integração do System Center com o Azure Monitor, é possível a utilização de Inteligência Artificial para geração de alertas de segurança, utilização de máquinas e otimização de ambiente. Além disso, o Azure Monitor permite a integração com o APM da Microsoft, Application Insights, gerando alertas, métricas, mapeamento e track de toda a solução de infraestrutura e aplicações;
- **SQL Server 2008, Windows Server 2008 e Windows 7:** Hoje o Ministério da Justiça e Segurança Pública possui em seu ambiente algumas máquinas com SQL Server 2008, Windows Server 2008, e Windows 7 cujo suporte Microsoft acaba em 2019. Com a migração para a nuvem Azure, a Microsoft assegura o suporte estendido por mais três anos, bem como a utilização da licença já adquirida;

É possível estabelecer análises comparativas entre diferentes provedores de nuvem e demonstrar a vantajosidade econômica da opção pela nuvem Azure em determinados cenários, como os de utilização de Máquinas Virtuais com sistema operacional Windows Server e do banco de dados Microsoft SQL Server. Consideramos que este cenário é bastante representativo do todo, pois estes softwares sustentam parcela significativa dos sistemas corporativos em uso atualmente no Ministério da Justiça e Segurança Pública. Serão considerados na análise apenas os principais provedores de cloud que estão na categoria *hyperscale* (Microsoft Azure, Amazon AWS, Google Cloud), por consideramos que apenas estes atendem a todas as premissas (possuem datacenter no Brasil, permitem optar pelo licenciamento como serviço incluso no custo da máquina virtual), e, portanto, possuem características comparáveis para este estudo.

Exemplificativamente, serão aqui considerados dois cenários de recursos de TIC com as características acima que são representativos da utilização típica de infraestrutura de servidores e bancos de dados no Ministério da justiça:

- Servidor virtual com Sistema Operacional Windows Server, 04 núcleos de processamento (VPCUs), 16 Gigabytes de RAM, 1 Terabyte de disco rígido tipo SSD Standard (até 500 iops e 60 MBps de taxa de transferência)
- Servidor de Bancos de Dados SQL Server Enterprise rodando em Sistema Operacional Windows Server, 04 núcleos de processamento (VPCUs), 16 Gigabytes de RAM, 1 Terabyte de disco rígido tipo SSD Standard (até 500 iops e 60 MBps de taxa de transferência)

Para a análise será considerada para o cenário de utilização dos recursos na nuvem Microsoft Azure a utilização do benefício híbrido, que permite eliminar os custos de licenciamento dos softwares caso o cliente possua o mesmo licenciamento para uso em infraestrutura própria (on premises). Foram ainda adotadas as seguintes premissas para o estudo comparativo:

- Criação dos recursos computacionais exclusivamente em datacenters localizados em território brasileiro.
- Estimativa realizada apenas na modalidade pay-as-you-go, sem considerar o provisionamento de recursos por tempo preestabelecido (que permite descontos adicionais).
- Análise comparativa realizada diretamente com o valor provido pelas calculadoras públicas das plataformas em dólares (USD), visto que as calculadoras de alguns provedores de nuvem só fazem estimativas nesta moeda.

A Tabela abaixo traz o resultado da análise comparativa do custo mensal de cada cenário realizada por meio das calculadoras do Azure (<https://azure.microsoft.com/pt-br/pricing/calculator/>), AWS (<https://calculator.aws/#/estimate>) e Google Cloud (<https://cloud.google.com/products/calculator>):

	Azure	AWS	Google Cloud
Servidor virtual com Sistema Operacional Windows Server, 04 núcleos de processamento (VPCUs), 16 Gigabytes de RAM, 1 Terabyte de disco rígido tipo SSD Standard (até 500 iops 60 MBps)	389,47 USD	473,06 USD	439,62 USD
Servidor de Bancos de Dados SQL Server Enterprise rodando em Sistema Operacional Windows Server, 04 núcleos de processamento (VPCUs), 16 Gigabytes de RAM, 1 Terabyte de disco rígido tipo SSD Standard (até 500 iops 60 MBps)	389,47 USD	1.568,07 USD	930,16 USD*
TOTAL	778,94 USD	2.041,13 USD	1.369,78 USD

Tabela 18 - Análise comparativa de custos mensais entre provedores de cloud nos cenários estabelecidos

* Foi considerado o acréscimo de licenças SQL Server Enterprise para 04 VPCUs (490,54 USD), uma vez que a Google Cloud não oferece a opção de licenciamento de SQL Server embutido no custo da VM

Desta forma, na impossibilidade de se realizar análises comparativas de custo de soluções entre provedores de nuvem para todos os possíveis cenários, foi definido um cenário representativo da utilização de recursos de infraestrutura por parte do Ministério da Justiça e Segurança Pública, e, no cenário considerado, fica demonstrada a grande vantagem econômica da opção pela nuvem Azure quando considerada a utilização do Benefício Híbrido. As evidências da análise realizada estão no documento SEI 13581711.

Os serviços de computação em nuvem Azure utilizados atualmente pelo MJSP são providos à partir de centros de dados localizados em território brasileiro, o que é uma exigência estabelecida pela Norma Complementar nº 14 da Instrução Normativa nº 01/2008-DSIC/GSI, que estabelece em seu item 5.3 que "*deve ser assegurado que dados, metadados, informações e conhecimentos, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro*".

Portanto, considerando todas as variáveis aqui apresentadas, a contratação dos serviços da nuvem Microsoft Azure é a única que se apresenta viável para a continuidade e expansão dos projetos estratégicos do MJSP que envolvem o uso de tecnologias de nuvem, é a que apresenta a maior vantagem do ponto de vista econômico considerados determinados cenários característicos de utilização, e também a que inclui as maiores vantagens quando considerada a integração com as demais soluções já utilizadas pela instituição.

Durante a elaboração desse ETP, a Equipe de Planejamento da Contratação verificou a necessidade de uma previsão normativa por parte do MJSP para que fosse respaldada a utilização dos serviços em nuvem.

Diante do exposto, a Equipe de Planejamento da Contratação entende como viável o presente cenário para a manutenção e continuidade dos atuais serviços prestados via Microsoft. Alertamos, no entanto, que a análise aqui realizada não pretende verificar a adequação do uso dos serviços de nuvem às políticas de segurança da informação institucionais, e nem compete à equipe de planejamento realizar uma análise mais abrangente dos riscos relativos à segurança da informação associados ao uso dos recursos de nuvem. Quando, e se for solicitada a ativação ou utilização desses serviços, a equipe de fiscalização deverá seguir o Modelo de Execução do Contrato constante no Termo de Referência, conforme previsto pela IN 1/2019 ME/SGD.

O uso dos recursos de computação em nuvem deve estar alinhado com a política de segurança da informação da instituição, e ainda à Norma Complementar nº 14 da IN 01/2008-DSIC/GSI, que define que somente podem ser utilizados recursos de nuvem aprovados pela alta administração (DAS 6 e acima) com o acompanhamento do Gestor de Segurança da Informação e Comunicação.

6 RESPONSABILIDADES

6.1 A Alta Administração de cada órgão ou entidade da APF, no âmbito de suas competências, é responsável pela segurança das informações tratadas em ambiente de computação em nuvem, em conformidade com as orientações contidas nesta norma e legislação vigente; e

6.2 O Gestor de Segurança da Informação e Comunicação do órgão, no âmbito de suas atribuições, é responsável pelas ações de implementação da gestão de risco de segurança das informações tratadas em ambiente de computação em nuvem. (Norma Complementar nº 14 da IN 01/2008-DSIC/GSI)

3.1 – ANÁLISE COMPARATIVA DE SOLUÇÕES

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1A		x	
	Solução 2A	x		
	Solução 3A	x		
	Solução 4A	x		
	Solução 1B			x
	Solução 2B	x		
	Solução 3B	x		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1A		x	
	Solução 2A		x	
	Solução 3A		x	
	Solução 4A		x	
	Solução 1B			x
	Solução 2B			x
	Solução 3B			x

Requisito	Solução	Sim	Não	Não se Aplica
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1A		x	
	Solução 2A	x		
	Solução 3A		x	
	Solução 4A		x	
	Solução 1B			x
	Solução 2B			x
	Solução 3B			x
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1A			x
	Solução 2A			x
	Solução 3A			x
	Solução 4A			x
	Solução 1B			x
	Solução 2B			x
	Solução 3B			x
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1A			x
	Solução 2A			x
	Solução 3A			x
	Solução 4A			x
	Solução 1B			x
	Solução 2B			x
	Solução 3B			x
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1A			x
	Solução 2A			x
	Solução 3A			x
	Solução 4A			x
	Solução 1B			x
	Solução 2B			x
	Solução 3B			x

4 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Conforme § 1º do art. 11, da INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019, as soluções identificadas e consideradas inviáveis serão registradas com breve descrição e justificativa.

Solução 1A: Portal do Software Público: Pelos fatos expostos, conclui-se que não foi possível localizar softwares disponíveis no Portal de Software Público para o atendimento das necessidades do MJSP, tornando essa solução inviável.

Solução 2A: LibreOffice (Software Livre): Este cenário não se mostrou como a solução mais eficiente no momento, devido à necessidade de uniformização e orquestração dos vários produtos e serviços que viessem a ser contratados. Além disso, poderia haver a necessidade de ter várias empresas prestando suporte para os diversos produtos adquiridos de forma separada, tornando essa solução inviável, considerando o nível de padronização que MJSP conta atualmente.

Solução 3A: G Suite: Esse cenário, pelo menos nesse momento, não se mostrou vantajoso, levando em conta o aproveitamento dos investimentos já realizados, as customizações já efetuadas pelo MJSP nos últimos anos, além da indisponibilidade da versão on-premisse da suite de escritório da Google, tornando, assim, essa solução inviável.

Solução 1B: Não contratação do serviço de Computação em Nuvem: Este cenário não se mostrou viável devido a imprescindibilidade dos serviços de computação em nuvem para o alcance do objetivos estratégicos do Ministério da Justiça e Segurança Pública.

Solução 2B: Contratação de empresa especializada no serviço de Computação em Nuvem pública, mediante realização de certame licitatório: Considerando a necessidade de manutenção dos atuais serviço disponibilizados pelo Microsoft Azure e tendo em vista todo o investimento já efetuado e a necessidade de migração/re-desenvolvimento dos atuais serviços, caso se optasse por outro provedor de nuvem, este cenário se mostrou inviável.

5 – ANÁLISE COMPARATIVA DE CUSTOS (TCO)

Não se aplica, pois apenas 1 (uma) solução de cada tipo se mostrou viável não sendo possível realizar comparação com outra, conforme previsto no art. 11, § 1º da INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019.

6 – DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

6.1 MICROSOFT 365 E3 = Office 365 E3 + Windows 10 + EMS [SKU AAD-33204]

O Microsoft 365 reúne o Office 365, Windows 10 e Enterprise Mobility + Security para fornecer uma solução completa de colaboração e produtividade. Ele foi projetado para dar o poder da criatividade nas organizações com as ferramentas de produtividade do Office 365, enquanto o Windows 10 ajuda a otimizar o gerenciamento de dispositivos da empresa e dados em vários ambientes e o Enterprise Mobility + Security oferece as ferramentas de gerenciamento e segurança necessárias. O Microsoft 365 E3 é composto pelas seguintes soluções:

a) Office 365 E3

Por ser uma subscrição com mais recursos e instalada localmente, será adotada preferencialmente para: servidores, mobilizados, alguns terceirizados da área técnica, agentes federais administrativos e engenheiros temporários do DEPEN.

O Office 365 E3 inclui:



Figura 3 - Composição do Office 365 E3

Benefícios do Office 365 E3:

- **Exchange Online:** Permite trabalhar de forma mais inteligente com 100 GB de email e calendários corporativos;
- **OneDrive for Business:** Possibilita a utilização de 1 a 5 TB de armazenamento em nuvem pessoal de praticamente qualquer lugar, em qualquer dispositivo, além de compartilhar documentos facilmente com outras pessoas dentro ou fora da organização e controlar quem pode exibir e editar cada arquivo;
- **Proteção de informações:** As informações são protegidas com criptografia de mensagens do Office e possui prevenção contra perda de dados de e-mails e arquivos do Office 365;
- **Recursos de conformidade adicionais:** Inclui a Descoberta Eletrônica Principal e auditoria básica aos seus recursos de conformidade;
- **SharePoint Online:** Compartilha e gerencia conteúdo, conhecimento e aplicativos com armazenamento ilimitado do SharePoint Online, promovendo o trabalho em equipe, encontre informações rapidamente e colabore de forma fácil com toda a organização;
- **Bookings:** Simplifica a forma de agendamento de horários e gerenciamento de reservas;
- **Proteção de Informações do Azure:** Controla e protege e-mails, documentos e dados privados compartilhados fora da empresa;
- **Aplicativos do Office 365:** Instala os aplicativos do Office 365, como Word, Excel, PowerPoint, OneNote e Access, em até cinco PCs ou Macs, cinco tablets e cinco telefones por usuário;
- **Aplicativos móveis do Office 365:** Usa aplicativos do Office 365 desenvolvidos para dispositivos móveis e tablets;
- **Outlook:** Mantém a organização com e-mail, calendário e contatos em um só lugar;

- **Microsoft Teams:** Possibilita conversar, compartilhar arquivos e usar aplicativos de negócios em um espaço de trabalho compartilhado;
- **Grupos do Office 365:** ferramenta colaborativa de trabalho que permite redigir documentos, criar planilhas, trabalhar em planos de projetos, agendar reuniões ou enviar e-mail, além das ferramentas do Office 365;
- **Skype for Business Online:** Reune a equipe facilmente compartilhando um link;
- **Microsoft Stream:** Carregua, organiza e compartilha conteúdo de vídeo;
- **Power Apps:** Desenvolve aplicativos de negócios necessários;
- **Power Automate:** Facilita tarefas repetitivas com a automação de fluxos de trabalho;
- **Microsoft To Do:** Realiza o planejamento do dia e gerencia a rotina;
- **MyAnalytics:** Explora padrões de trabalho e otimiza formas de trabalhar com mais inteligência, melhorando seu foco, bem-estar, contatos e colaboração;
- **Gerenciamento de Dispositivo Móvel:** Protege e gerencia os dispositivos móveis dos usuários com o MDM (Gerenciamento de Dispositivo Móvel) do Office 365, através de políticas de segurança, limpeza remota e relatórios detalhados do dispositivo;
- **Aplicativos do Office para Web:** Permite a criação e compartilhamento de forma colaborativa onde quer que esteja;
- **Office Delve:** Gerencie seu perfil do Office 365 com o Delve. Além disso, descubra e organize as informações mais relevantes imediatamente em todos os aplicativos do Office;
- **Microsoft Whiteboard:** Colabore sobre ideias e conteúdo com um canvas digital de forma livre, agora integrado com o Microsoft Teams;
- **Microsoft Kaizala Pro:** Conecte-se e coordene o trabalho em toda a sua organização, além de fornecedores, parceiros, distribuidores e clientes usando este aplicativo de chat móvel baseado em número de celular simples e seguro;
- **Yammer:** Conecte-se e gere envolvimento com redes sociais empresariais;
- **Microsoft Sway:** Crie boletins informativos, apresentações e documentos visualmente impressionantes em minutos;
- **Microsoft Forms:** Crie facilmente pesquisas, testes e votações;
- **Microsoft Planner:** Organize o trabalho em equipe, crie novos planos, atribua tarefas, compartilhe arquivos, converse e receba atualizações sobre o progresso;
- **Microsoft Shifts:** Permite que os trabalhadores de linha de frente e os gerentes deles administrem cronogramas e mantenham contato por meio de dispositivos móveis;
- **API do Microsoft Graph:** Acessa recursos de serviços do Microsoft Cloud através desta API web RESTful;
- **Logon único:** Sincroniza o Active Directory local para SSO;
- **Conformidade:** Facilita a conformidade jurídica com arquivamento de e-mail, pesquisa de conteúdo, auditoria básica, políticas de retenção manual e rótulos de confidencialidade;

b) Windows 10: O Windows 10 Enterprise foi desenvolvido para lidar com as necessidades de organizações de grande e médio porte ao oferecer aos profissionais de TI. A padronização em uma única versão simplifica as implantações e as atualizações, além de fornecer dispositivos prontos para o ambiente corporativo a seus usuários direto do fabricante.

c) Enterprise Mobility + Security: O Microsoft Enterprise Mobility + Security é uma plataforma de segurança e gerenciamento da mobilidade inteligente. Ele ajuda a proteger e garantir a segurança das organizações e capacita seus funcionários a trabalhar de maneiras novas e flexíveis. Todas as contas atualmente do MJSP que necessitam acessar via VPN algum serviço, é obrigatório que o usuário tenha feito a habilitação do Multifator de Autenticação (Microsoft Azure Multi-Factor Authentication).

O licenciamento do EMS E3 é baseado em usuários e a licença inclui:

- Azure Active Directory Premium P1: O Azure AD (Active Directory) é o serviço de gerenciamento de identidade e de acesso baseado em nuvem da Microsoft. Além dos recursos gratuitos, o P1 também permite que seus usuários híbridos acessem recursos locais e de nuvem. Ele também dá suporte à administração avançada, como grupos dinâmicos, gerenciamento de grupo de autoatendimento, Microsoft Identity Manager (um conjunto de gerenciamento de acesso e identidade local) e recursos de write-back de nuvem, que permitem a redefinição de senha por autoatendimento para os usuários locais;
- Microsoft Endpoint Manager: O Microsoft Endpoint Manager ajuda a fornecer o local de trabalho e o gerenciamento modernos para manter seus dados seguros, na nuvem e no local. O Endpoint Manager inclui os serviços e as ferramentas que você usa para gerenciar e monitorar dispositivos móveis, computadores desktop, máquinas virtuais, dispositivos inseridos e servidores;
- Azure Information Protection Premium P1: A Proteção de Informações do Azure (conhecida como AIP) é uma solução baseada em nuvem que ajuda as organizações a classificar e, opcionalmente, proteger documentos e e-mails aplicando rótulos. Os rótulos podem ser aplicados automaticamente por administradores que definem regras e condições, manualmente pelos usuários ou uma combinação na qual os usuários recebam recomendações;
- Licença cliente de acesso padrão: Client Access License (CAL), aos serviços on-premises do Windows Server, RMS e Microsoft Identity Management CAL;
- Licença cliente de acesso padrão: Client Access License (CAL), aos serviços on-premises do System Center Configuration Manager e System Center Endpoint Protection Management License (ML);

d) CALS de acesso: para ambiente híbrido e servidores de produtividade Exchange Server, Skype For Business Server e SharePoint Server.

6.2 OFFICE 365 E1 [SKU T6A-00024]

Será utilizada preferencialmente para estagiários, terceirizados administrativos e agentes federais em regime de plantão.

O Office 365 E1 inclui aplicativos baseados na Web, como o Excel e o Outlook, integrados a serviços de nuvem, como o OneDrive e o Teams, possibilitando a produtividade em praticamente qualquer lugar.

Benefícios do Office 365 E1:

- **Aplicativos do Office para dispositivos móveis:** Possibilita baixar aplicativos do Office em dispositivos iOS, Android e Windows¹ com tela de tamanho igual ou inferior a 10,1 polegadas. Cada usuário pode instalar aplicativos móveis do Office em até cinco tablets e cinco telefones. Os aplicativos de área de trabalho do Office não estão incluídos.
- **Outlook:** Permite conectar-se e manter a organização com e-mail, calendário e contatos em um só lugar.
- **SharePoint Online Plano 1:** Possibilita compartilhar e gerenciar conteúdo, conhecimento e aplicativos com 1 TB de armazenamento do OneDrive por usuário, promovendo o trabalho em equipe, permitindo acessar as informações rapidamente e colaborar de forma fácil com toda a organização.
- **OneDrive for Business:** Possui 1 TB para armazenamento em nuvem pessoal de praticamente qualquer lugar, em qualquer dispositivo. Com isso, é possível compartilhar documentos facilmente com outras pessoas, dentro e fora da sua organização e controlar quem pode exibir e editar cada arquivo.
- **Exchange Online Plano 1:** E-mail corporativo seguro e confiável com uma caixa de correio de 50 GB por usuário. Permite trabalhar de forma mais inteligente, e em praticamente qualquer lugar, com o e-mail hospedado para empresas.

6.3 ENTERPRISE MOBILITY + SECURITY E3 [SKU AAA-10732]

Conforme já mencionado anteriormente o EMS E3 está contido no M365 E3. No entanto, é possível a sua aquisição de forma avulsa. Isso se faz necessário para contemplar os usuários que utilizarão o Office 365 E1 (estagiários, terceirizados administrativos e agentes federais em regime de plantão). As suas funcionalidades já foram explanadas na alínea "c" do subitem 6.1 desse ETP.

6.4 WINDOWS E3 [SKU AAA-10787]

Upgrade de sistema operacional do Windows 10 Enterprise E3 com benefícios de: App-V; BranchCache; DirectAccess e Always On VPN ; Windows Defender Application Control e AppLocker; Windows Defender Credential Guard; e Windows Defender Application Guard. Necessário para os usuários que utilizarão as licenças do Office 365 E1.

6.5 MICROSOFT DEFENDER ATP [SKU QLS-00003]

Trata-se de uma proteção avançada contra ameaças para endpoint incluindo detecção, investigação e resposta. No Windows 10, ele é totalmente sem agente. Serão atribuídas licenças para todos os usuários corporativos, conforme solicitação da área de Segurança e Risco. (DTIC/CGGOV/CRS)

Abaixo, alguns dos pontos mais importantes que a solução oferece:

- Sem uso de agentes e construído na nuvem;
- Uso do Microsoft Inteligente Graph: Threat intel usando base de inteligência com cerca de 8 trilhões de sinais;
- Segurança automatizada: Eleva o nível da sua segurança, passando do alerta para a correção em minutos – em grande escala;
- Compartilha os sinais de detecção e exploração entre dispositivos, identidade para agilizar a resposta e a recuperação;
- Gerenciamento de Vulnerabilidades e Ameaças;
- Especialistas em Ameaças da Microsoft: Conte com o apoio dos Threat Experts da Microsoft para obter conhecimento aprofundado para lidar com ameaças avançadas;

6.6 OFFICE 365 ATP PLANO 2 [SKU FSZ-00002]

A proteção avançada contra ameaças do Office 365 (ATP) é um serviço de filtragem de e-mail baseado em nuvem que ajuda a proteger as organizações contra malware e vírus desconhecidos, fornecendo proteção robusta de dia zero e inclui recursos para proteger as organizações contra links prejudiciais em tempo real. A ATP tem recursos ricos de relatórios e de rastreamento de URL que dão aos administradores a percepção do tipo de ataques que ocorrem na sua organização.

Esse serviço é necessário para proteção aos usuários do subitem 6.1 (Microsoft 365 E3) e 6.2 (Office 365 E1) desse ETP.

Ele é apresentado em duas versões: Office 365 ATP Plano 1 e Plano 2.

O plano 2 do Office 365 ATP está incluído no Office 365 E5, no Office 365 A5 e no Microsoft 365 E5. No entanto, é possível a sua aquisição de forma individualizada.

A tabela a seguir resume o que está incluído em cada plano.

Plano 1 do Office 365 ATP	Plano 2 do Office 365 ATP
Capacidade de configuração, proteção e detecção:	Recursos do Plano 1 do Office 365 ATP
Anexos seguros	+
Links seguros	Recursos de automação, investigação, correção e formação educacional:
ATP para SharePoint, OneDrive e Microsoft Teams	- Rastreadores de ameaças
Proteção antiphishing da ATP	- Explorador de ameaças
Detecções em tempo real	- Investigação e resposta automatizadas
	- Simulador de ataque

Tabela 19 - Comparativo Office ATP

A seguir estão as principais maneiras de usar a ATP para proteção de mensagens:

- Em um cenário somente de filtragem, o ATP do Office 365, a ATP fornece proteção de e-mail baseada em nuvem para seu ambiente local do Exchange Server ou qualquer outra solução de e-mail SMTP local;
- O Office 365 ATP pode ser habilitado para proteger caixas de correio hospedadas na nuvem do Exchange Online;
- Em uma implantação híbrida, o ATP do Office pode ser configurada para proteger seu ambiente de mensagens e controlar o roteamento de e-mail quando você tem uma combinação de caixas de correio locais e em nuvem com o Exchange Online Protection para filtragem de e-mail de entrada;

6.7 AZURE ATP [SKU G5F-00002]

O ATP (Proteção Avançada contra Ameaças) do Azure é uma solução de segurança baseada em nuvem que aprimora os sinais locais do Active Directory para identificar, detectar e investigar ameaças avançadas, identidades comprometidas e ações de pessoas internas mal-intencionadas, direcionadas à sua organização.

Add-on para usuários do subitem 6.1 (Microsoft 365 E3) e 6.2 (Office 365 E1) desse ETP, além dos usuários sem pacote Office (Contas Administrativas, subitem 2.1, alínea "q" e Bi-modal Central, alínea "p")

O Azure ATP permite aos analistas de SecOp (uma abordagem de gerenciamento que conecta equipes de segurança e operações, semelhante a como o DevOps unifica desenvolvedores de software e profissionais de operações) e profissionais de segurança que lutam para detectar ataques avançados em ambientes híbridos:

- Monitorar usuários, comportamento de entidade e atividades com a análise baseada em aprendizado;
- Proteger as identidades do usuário e as credenciais armazenadas no Active Directory;
- Identificar e investigar atividades de usuário suspeitas e ataques avançados em toda a cadeia do ataque cibernético;
- Fornecer informações claras sobre incidentes em uma linha do tempo simples para triagem rápida;

6.8 MICROSOFT CLOUD APP SECURITY [SKU 2ER-00002]

O Microsoft Cloud App Security é um Agente de Segurança de Acesso à Nuvem que oferece suporte a vários modos de implantação, incluindo coleta de log, conectores de API e proxy reverso. Ele fornece visibilidade avançada, controle sobre a viagem de dados e análises sofisticadas para identificar e combater ameaças cibernéticas em todos os seus serviços de nuvem da Microsoft e de terceiros. Esse serviço é necessário para proteção aos usuários do subitem 6.1 (Microsoft 365 E3) e 6.2 (Office 365 E1) desse ETP.

O Microsoft Cloud App Security integra-se nativamente às principais soluções da Microsoft e foi desenvolvido com profissionais de segurança em mente. Ele fornece implantação simples, gerenciamento centralizado e recursos de automação inovadores.

O Cloud App Security integra visibilidade à nuvem ao:

- Usar o Cloud Discovery para mapear e identificar seu ambiente de nuvem e os aplicativos na nuvem que sua organização está usando;
- Aprovar e desaprovar aplicativos em sua nuvem;
- Usar conectores de aplicativos de fácil implantação que aproveitam as APIs do provedor para visibilidade e governança de aplicativos aos quais você se conecta;
- Usar a proteção de Controle de Aplicativos de Acesso Condicional para obter visibilidade e controle em tempo real do acesso e das atividades em seus aplicativos na nuvem;

- Ajudar você a ter controle contínuo ao configurar as políticas e depois ajustá-las continuamente;

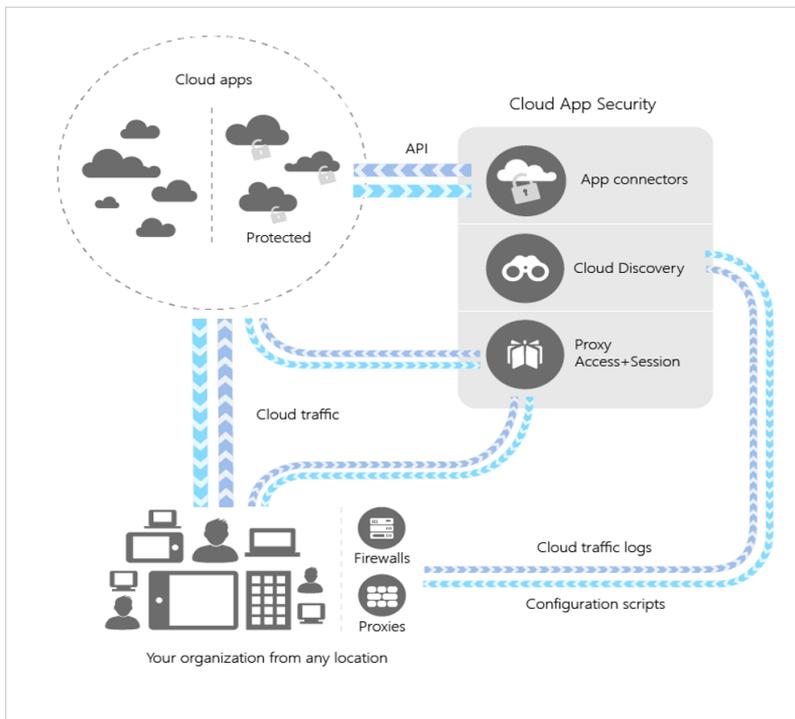


Figura 4 - Funcionamento do Cloud App Security

6.9 AZURE AD PREMIUM P2 [SKU 6E6-00004]

O Azure AD (Active Directory) é o serviço de gerenciamento de identidade e de acesso baseado em nuvem da Microsoft, que ajuda aos usuários a se conectar e acessar os recursos em:

- Recursos externos, como o Office 365, o portal do Azure e milhares de outros aplicativos SaaS;
- Recursos internos, como aplicativos em sua rede corporativa e intranet, juntamente com outros aplicativos de nuvem desenvolvidos por sua organização;

Ele é apresentado em três versões:

Azure Active Directory Gratuito. Fornece gerenciamento de usuários e de grupos, sincronização de diretório local, relatórios básicos, autoatendimento para alteração de senha e logon único no Azure, no Office 365 e em muitos aplicativos SaaS populares.

Azure Active Directory Premium P1. Além dos recursos gratuitos, o P1 também permite que seus usuários híbridos acessem recursos locais e de nuvem. Ele também dá suporte à administração avançada, como grupos dinâmicos, gerenciamento de grupo de autoatendimento, Microsoft Identity Manager (um conjunto de gerenciamento de acesso e identidade local) e recursos de write-back de nuvem, que permitem a redefinição de senha por autoatendimento para os usuários locais.

Azure Active Directory Premium P2. Além dos recursos nos planos Gratuito e P1, o P2 também oferece o Azure Active Directory Identity Protection, a fim de fornecer Acesso Condicional baseado em risco para seus aplicativos e dados críticos da empresa, e o Privileged Identity Management, para ajudar a descobrir, restringir e monitorar os administradores e o acesso deles a recursos e fornecer acesso Just-In-Time quando for necessário.

Esse add-on será atribuído aos usuários do subitem 6.1 (Microsoft 365 E3) e 6.2 (Office 365 E1) desse ETP, além dos usuários sem pacote Office (Contas: Administrativas, subitem 2.1, alínea "q" e Bi-modal Central, alínea "p")

6.10 PROJECT PLAN 1/ PROJECT PLAN 3/PROJECT ONLINE PREMIUM [SKU TRS-00002; SKU 7LS-00002;SKU 7SY-00002]

A Microsoft disponibiliza atualmente três versões do Project:

Características

Project Plano 1: Permite gerenciar projetos facilmente por meio do navegador da Web.

Project Plano 3: Executa projetos com facilidade através de ferramentas familiares de agendamento, escolhendo o navegador da Web ou o cliente de área de trabalho.

Project Plano 5: Possibilita otimizar o portfólio de projetos para priorizar iniciativas e obter os resultados desejados com a escolha do navegador da Web ou cliente de área de trabalho.

Funcionalidades	Project Plano 1	Project Plano 3	Project Plano 5
Página inicial do Project	Incluído	Incluído	Incluído

A partir de uma exibição centralizada, cria novos projetos com facilidade, acessa rapidamente projetos importantes ou abre os projetos com trabalho mais recente.			
Modo de exibição de grade Planeja e gerencia projetos, usando uma lista ordenada de tarefas.	Incluído	Incluído	Incluído
Modo de exibição de quadro Acompanha visualmente as tarefas do projeto para ter um melhor fluxo de trabalho e status, usando painéis de tarefas fornecidos com o programa ou personalizados.	Incluído	Incluído	Incluído
Modo de exibição de linha do tempo (Gantt) Acompanha e compreenda datas, tarefas e os relacionamentos das tarefas do projeto no modo de exibição de linha do tempo visual.	Incluído	Incluído	Incluído
Colaboração e comunicação Trabalhe em conjunto em projetos, usando o Microsoft Teams.	Incluído	Incluído	Incluído
Coautoria Trabalhe em conjunto com stakeholders e membros da equipe para editar e atualizar listas de tarefas, agendamento de projetos e muito mais simultaneamente.	Incluído	Incluído	Incluído
Planejamento e agendamento de projetos Inclui ferramentas de agendamento conhecidas para atribuir tarefas de projeto aos membros da equipe e usar diferentes modos de exibição, como Grade, Quadro e Linha do tempo (gráfico de Gantt) para supervisionar o cronograma.	Incluído	Incluído	Incluído
Relatórios Use relatórios pré-criados para acompanhar o andamento de seus projetos, recursos, programas e portfólios.	Não incluído	Incluído	Incluído
Roteiro Crie roteiros visuais e interativos, agregando diferentes tipos de projetos em sua organização para obter visibilidade.	Acesso somente leitura	Incluído	Incluído
Envio de quadro de horários Capture o tempo gasto dentro e fora do projeto para fins de folha de pagamento, faturamento e outras tarefas comerciais.	Não incluído	Incluído	Incluído
Gerenciamento de recursos Defina a equipe do projeto, solicite recursos para ele e atribua tarefas do projeto a esses recursos.	Não incluído	Incluído	Incluído
Cliente de área de trabalho Use o aplicativo Project para área de trabalho totalmente instalado e atualizado. Uma licença abrange até cinco PCs por pessoa.	Não incluído	Incluído Em até 5 PCs	Incluído Em até 5 PCs
Otimizar e selecionar portfólios Modele diferentes cenários de portfólio para determinar o melhor caminho estratégico, ponderando propostas de projetos com drivers de negócios estratégicos.	Não incluído	Não incluído	Incluído
Gerenciamento de demanda Capture e avalie ideias de projetos de qualquer lugar na organização por meio de um processo padronizado.	Não incluído	Não incluído	Incluído
Gerenciamento e planejamento de recursos empresariais	Não incluído	Não incluído	Incluído

Exiba e compare como os recursos são usados nos projetos para otimizar as atribuições.			
--	--	--	--

Tabela 20 - Comparativo Project

Fonte: <https://www.microsoft.com/pt-br/microsoft-365/project/compare-microsoft-project-management-software>

6.11 POWER BI PRO [SKU NK4-00002]

Segundo o Gartner, “**self-service business intelligence**” é o conceito em que o usuário não técnico cria e implanta suas próprias análises apoiando na estruturação de uma arquitetura corporativa e de ferramentas que entreguem autonomia na concepção e modelagem para a implementação de relatórios e dashboards.

Atualmente o MJSP utiliza a versão Power BI Pro, incluída dentro da licença M365 E5. No entanto, economicamente é mais vantajosa a aquisição individual da subscrição ao invés da aquisição do M365 E5.

De forma resumida o **Power BI** é uma coleção de serviços de software, aplicativos e conectores que trabalham juntos para transformar suas fontes de dados não relacionadas em informações coerentes, visualmente envolventes e interativas. Os dados podem estar em uma planilha do Excel ou em uma coleção de data warehouses híbridos locais ou baseados na nuvem. Com o Power BI, você pode se conectar facilmente a fontes de dados, visualizar e descobrir conteúdo importante e compartilhá-lo de acordo com a necessidade da organização.

Em regra, o Power BI pode ser licenciado por usuário (versões Free e Pro) ou por capacidade (versão Premium). Discorreremos sobre as características e cada um deles.

Abaixo, alguns conceitos importantes:

Consumidor

Como um usuário final ou *consumidor*, recebe o conteúdo (dashboards, relatórios e aplicativos) dos demais usuários. Possibilita trabalhar na versão online ou móvel do Power BI, que é chamada de Serviço do Power BI, revisando e interagindo com o conteúdo a fim de tomar decisões de negócios. Como um consumidor, não há acesso a todos os recursos do Power BI, porque o Serviço do Power BI será utilizado para análise, monitoramento, exploração e tomada de decisões. Com um conteúdo *compartilhado*, uma licença **gratuita** será suficiente.

Aplicativos

Um *aplicativo* é um tipo de conteúdo do Power BI que combina dashboards e relatórios relacionados em um só lugar. Um aplicativo pode ter um ou mais dashboards e um ou mais relatórios, todos agrupados. Os aplicativos são criados por *designers* do Power BI que distribuem e compartilham os aplicativos com *consumidores* como você.

Relatórios

Um relatório do Power BI é uma exibição de um conjunto de dados em várias perspectivas, com visuais que representam as diferentes descobertas e informações obtidas por meio desse conjunto de dados. Um relatório pode ter um único visual ou páginas repletas de visuais. Os relatórios são criados por *designers* do Power BI que distribuem e compartilham os relatórios com *consumidores* como você.

Dashboards

Um dashboard do Power BI é uma página única, geralmente chamada de tela, que usa as visualizações para contar uma história. Como ele é limitado a uma página, um dashboard bem projetado contém apenas os elementos mais importantes da história.

O Power BI Pro é uma licença individual de usuário que permite que eles leiam e interajam com relatórios e painéis publicados por outras pessoas no serviço do Power BI. Os usuários com esse tipo de licença podem compartilhar conteúdo e colaborar com outros usuários do Power BI Pro. Somente os usuários do Power BI Pro podem publicar ou compartilhar conteúdo com outros usuários ou consumir conteúdo criado por outros usuários, a menos que uma capacidade do Power BI Premium hospede esse conteúdo.

6.12 POWER BI PREMIUM P1 [SKU GSL-00002]

Com o Power BI Premium os usuários podem usar o serviço do Power BI com melhor desempenho e capacidade de resposta. Por exemplo, com uma assinatura do Power BI Premium, os usuários têm acesso a:

- Maior dimensionamento e desempenho;
- Flexibilidade para licença por capacidade;
- Unifique o BI corporativo e de autoatendimento;
- Estenda o BI local com o Servidor de Relatórios do Power BI;
- Suporte para residência de dados por região (Multi-Geo);
- Compartilhe dados com qualquer pessoa sem comprar uma licença por usuário;

Diferente de uma licença Free ou Pro, o Power BI Premium não é uma licença por usuário. Em vez disso, a licença Premium fornece uma capacidade dedicada para todos os usuários da organização.

6.13 POWER BI EMBEDDED

O Microsoft Power BI Embedded permite que os desenvolvedores de aplicativos insiram dashboards e relatórios totalmente interativos em aplicativos, sem o tempo e o custo de terem que criar seus próprios controles desde o princípio.

Com o Power BI Embedded, os ISVs e desenvolvedores têm maior flexibilidade para inserir inteligência em seus aplicativos usando as APIs do Power BI. Os ISVs e desenvolvedores podem aproveitar a minimização dos esforços de desenvolvimento para chegar ao mercado com mais rapidez e diferenciar-se por inserir um mecanismo de análise de classe mundial da Microsoft em seu aplicativo. Da mesma forma, os desenvolvedores podem dedicar seu tempo à solução para atender às demandas do cliente, em vez de desenvolver recursos de análise visual. Além disso, o Power BI Embedded permite que você trabalhe em ambientes de desenvolvimento familiares, como o Visual Studio e o Azure, que você já usa.

O Power BI Embedded é indicado para ISVs (fornecedores de software independentes) e para desenvolvedores que criam aplicativos para seus clientes. Você pode usá-lo como um serviço de business intelligence de terceiros que permite visualizar dados de aplicativo, em vez de criar esse serviço por conta própria. O Power BI Embedded é uma solução de análise de PaaS (plataforma como serviço), que permite aos desenvolvedores inserir relatórios e dashboards em um aplicativo para seus clientes. O Power BI Premium é uma solução de análise de SaaS (software como serviço) que oferece à organização uma exibição única dos seus dados de negócios mais críticos.

O Power BI Embedded é um recurso pago conforme o uso, enquanto o Power BI Premium requer uma taxa mensal.

6.14 VISIO PLANO 2

Para criação de fluxogramas, diagramas, organogramas, plantas baixas, designs de engenharia e muito mais com sofisticação. Permite formas e modelos modernos de maneira fácil e intuitiva.

Recursos:

- **Elementos versáteis e flexíveis:** Permite trabalhar rapidamente com modelos, temas e 250 mil formas prontas no ecossistema de conteúdo do Visio.
- **Diagramas simples:** Possibilita dar destaque aos diagramas visualmente com sobreposições de dados, ícones, cores e gráficos, inclusive com a visualização de dados do Excel em uma etapa.
- **Importe arquivos de desenho (DWG):** É possível adicionar dados ou formas inteligentes a designs importados do AutoCAD (suporte até o DWG 2013), simplificar ou aprimorar as visualizações avançadas com facilidade.
- **Crie uma capacidade de programação personalizada:** Permite acessar a arquitetura robusta de aplicativos e criar funcionalidades personalizadas com um Software Development Kit disponível.
- **Use modelos que possam dar suporte aos padrões do setor:** Aproveita modelos do Visio com suporte para UML (Unified Modeling Language) 2.5, BPMN (Business Process Model and Notation) 2.0 e IEEE (Institute of Electrical and Electronics Engineers).
- **Colabore com facilidade:** Finaliza diagramas mais rapidamente de forma colaborativa, através do compartilhamento de seu trabalho como um link baseado na Web, anexo, PowerPoint, imagem ou PDF.
- **Use o armazenamento em nuvem do OneDrive for Business:** Possibilita armazenar e compartilhar suas ideias e diagramas de forma segura com os 2 GB incluídos de armazenamento gratuito na nuvem do OneDrive.

6.15 WINDOWS SERVER STANDARD + SYSTEM CENTER STANDARD [SKU 9GA-00006] / WINDOWS SERVER DATACENTER + SYSTEM CENTER DATACENTER [SKU 9GS-00495]

O Windows Server 2019 é um sistema operacional que une ambientes locais com os serviços do Azure.

Visão Geral:

Edição do Windows Server 2019	Ideal para	Modelo de licenciamento	Requisitos CAL ^[1]
Datacenter ^[2]	Datcenters e ambientes de nuvem altamente virtualizados	Baseado em núcleo	Windows Server CAL
Standard ^[2]	Ambientes físicos ou minimamente virtualizados	Baseado em núcleo	Windows Server CAL

Tabela 21 - Comparativo Windows Server

Diferencial de recursos do Windows Server 2019:

Legenda de suporte a recursos
 Recurso disponível Recurso não disponível

Recurso	Standard Edition	Datacenter Edition
Funcionalidade básica do Windows Server	●	●
Integração híbrida	●	●
Infraestrutura hiperconvergente	○	●
Contêineres de OSEs*/Hyper-V	2 [1]	Ilimitado
Contêineres do Windows Server	Ilimitado	Ilimitado
Serviço Guardião de Host	●	●
Réplica de Armazenamento [2]	●	●
Máquinas virtuais (VMs) blindadas	○	●
Rede definida por software	○	●
Armazenamento definido por software	○	●

[1] A licença do Windows Server Standard Edition inclui permissão para dois OSEs ou VMs.

[2] A licença do Windows Server Standard Edition limita-se a um único volume da Réplica de Armazenamento de até 2 TB.

Tabela 22 - Comparativo Windows Server

6.15.1 Regra de Licenciamento para o Windows Server

O licenciamento do Microsoft Windows Server 2019 considera unicamente o número de cores físicos por servidor. Todos os núcleos físicos do servidor devem ser licenciados. Não são considerados servidores virtuais; unicamente cores físicos dos servidores. Podem ser comprados em pacotes de 2 cores físicos ou 16 cores físicos.

Requisitos mínimos no licenciamento:

- Todos os cores físicos de cada servidor físico devem ser licenciados;
- 1 licença contempla 2 cores, com um mínimo de 8 licenças por cada processador (mesmo que o processador tenha menos de 8 cores);
- Um mínimo de 16 licenças por core para cada servidor (mesmo que o servidor tenha menos de 16 cores);

Physical Cores per Processor	2	4	8	10	12	14	16	Processors per server
Number of 2-core packs needed	8	8	8	8	8	8	8	1 processor
	8	8	8	10	12	14	16	2 processors
	12	12	12	15	18	21	24	3 processors

Tabela 23 - Regra de Licenciamento Windows Server

No modelo acima, temos *Processors per server* (Processadores por servidor) e *Physical cores per processor* (Núcleos físicos por processador). Por exemplo, um servidor com apenas 1 processador físico, com 2 cores. A princípio necessitaríamos de apenas uma licença, pois 1 licença contempla 2 cores, no entanto, a regra impõe, ainda, que se adquira um mínimo de 8 licenças, independentemente se o processador tenha menos de 8 cores.

6.15.2 Versões Windows Server

Existem basicamente 2 edições que podem ser utilizadas pelo MJSP:

- **Datacenter:** suportando um número ilimitado de OSEs*/Hyper-V containers; é indicado para ambientes altamente virtualizados;
- **Standard:** suporta 2 (dois) OSEs*/Hyper-V containers, ideal para servidores físicos ou com até 2 VMs (Máquinas Virtuais);
- **Outras diferenças:** <https://docs.microsoft.com/pt-br/windows-server/get-started-19/editions-comparison-19>;

6.15.3 Virtualização

O hypervisor que será utilizado é indiferente; o licenciamento deve ser de todos os núcleos dos processadores físicos de um host para cobrir o número máximo de máquinas virtuais do Windows Server possíveis (independentemente do tempo) que possam ser executadas nesse host. Ou seja, nós de cluster devem ser licenciados igualmente para atender ao failover e vMotion/Live Migration.

Adicionalmente, as regras permanecem praticamente as mesmas em relação aos benefícios das edições Standard e Datacenter. No caso do Windows Standard, você recebe 2 VOSEs (Virtual OSEs) para cada vez que licenciar todos os núcleos de um host; no Windows Datacenter, número ilimitado de VOSEs.

Por exemplo, se você tem um host vSphere com processadores de 10 núcleos duplos (20 núcleos), e quer licenciar essa máquina para suportar 4 máquinas virtuais Windows Server. Começa-se licenciando os 20 núcleos com 10 licenças do WS2016 Standard. Isso licencia 2 instalações virtuais do Windows Server. Para licenciar mais 2 instalações virtuais do Windows Server, é necessário adquirir mais 10 licenças do WS2016 Standard para esse host. Dessa forma, chega-se aos 4 VOSEs que agora pode ser usado para licenciar as 4 máquinas virtuais.

6.16 SQL SERVER ENTERPRISE CORE

SQL Server é um Sistema Gerenciador de Banco de Dados (SGDB) desenvolvido e mantido pela Microsoft. Seu principal objetivo é retirar da aplicação cliente a responsabilidade de gerenciar o acesso, a manipulação e a organização dos dados. O SGDB disponibiliza uma interface para que seus clientes possam incluir, alterar ou consultar dados previamente armazenados. Em bancos de dados relacionais a interface é constituída pelas APIs (Application Programming Interface) ou drivers do SGDB, que executam comandos na linguagem SQL (Structured Query Language).

Especificamente no MJSP, o SQL Server é responsável por gerenciar diversos bancos de dados. Ele é oferecido em duas edições principais:

- A Enterprise Edition é ideal para aplicativos que exigem desempenho crítico em memória, segurança e alta disponibilidade.
- A Standard Edition oferece recursos completos de bancos de dados para aplicativos e datamarts de camada intermediária.

Existem dois modelos principais de licenciamento:

Servidor + CAL: fornece a opção de licenciar usuários e/ou dispositivos, com acesso de baixo custo ao SQL Server incremental implantações.

- Cada servidor executando o software SQL Server requer um servidor licença;
- Cada usuário e / ou dispositivo acessando um SQL Server licenciado requer uma CAL do SQL Server com a mesma versão ou mais recente - por exemplo, para acessar um SQL Server 2012 Standard Edition servidor, um usuário precisaria de uma CAL do SQL Server;
- Cada CAL do SQL Server permite acesso a vários Servidores SQL licenciados;

Por núcleo: O licenciamento baseado em núcleo fornece aos clientes uma medida mais precisa do poder de computação e uma métrica de licenciamento mais consistente, independentemente de as soluções serem implantadas em servidores físicos no local, em ambientes virtuais ou em nuvem. Ele é apropriado quando os clientes não conseguem contar usuários/dispositivos, têm cargas de trabalho ou sistemas de Internet/Extranet.

Regra básica para licenciamento: 1 licença contempla 2 núcleos; no entanto, é necessário licenciar no mínimo 4 núcleos para cada processador, ou seja: é necessário comprar no mínimo 2 licenças para cada processador. A mesma lógica é aplicada aos núcleos virtuais em um ambiente virtual. As licenças SQL Server Developer e Express são gratuitas (a natureza do dado armazenado nessas versões NÃO pode ser produtivo).

A figura abaixo ilustra os requisitos de licenciamento para três máquinas virtuais diferentes no modelo de licenciamento por núcleo:

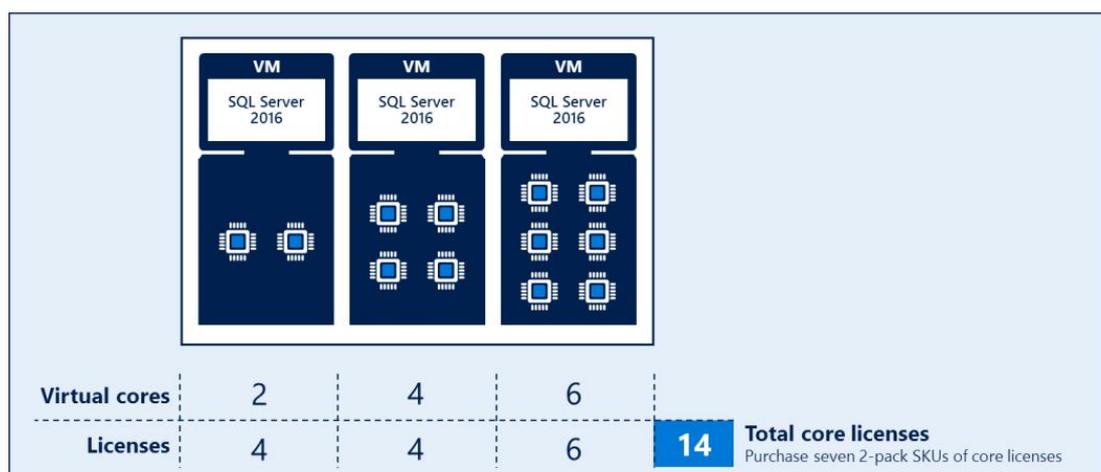


Figura 5 - Regra de Licenciamento Microsoft SQL Server
(Adquirir **sete** skus de 2 pacotes de licenças principais)

6.17 POWER APPS PER APP PLAN [SKU SEQ-00001]

O Power Apps permite criar aplicativos de nível profissional de maneira fácil, aumentando a agilidade em toda a organização com a criação rápida de aplicativos com pouco código que modernizam processos e solucionam desafios complexos.

Para a adoção do Power Apps no Ministério da Justiça, foi escolhido o licenciamento "por usuário por aplicativo", por ser a forma que permite um maior aproveitamento do investimento feito no licenciamento para os casos em que as licenças serão utilizadas para

apoiar um número limitado de processos de negócio por usuário.

A tabela abaixo demonstra as capacidades inclusas no licenciamento do Microsoft Power Apps "por usuário por aplicativo".

Entitlement Summary for Power Apps per app license

Plans and capabilities		Power Apps per app plan
Run custom apps / portals	Run custom apps (both canvas and model driven)	2 apps
	Access custom portals	1 custom portal
Connect to your data	Standard connectors 	●
	Premium and custom connectors	●
	On premises data gateway	●
Store and manage data	Utilize Dataverse (formerly Common Data Service)	●
	Create and access custom entities (includes complex entities)	●
	Dynamics 365 restricted entities access ¹	Read only
Execute flows	Automated, instant, and scheduled flows ²	Within app context
	Business process flows	
Per license capacity	Dataverse Database Capacity ³	50 MB
	Dataverse File Capacity ³	400 MB
	Daily API request limit ⁴	1,000
Infuse AI	AI Builder capacity add-on	\$

Tabela 24 - Capacidades inclusas no licenciamento do Power Apps per app plan

6.18 POWER VIRTUAL AGENTS 2K SESSIONS [SKU RYT-00001]

O Power Virtual Agents permite criar rapidamente chatbots sofisticados habilitados por IA que podem resolver problemas comuns e responder a perguntas 24 horas por dia. Com o Power Virtual Agents é possível criar e gerenciar chatbots eficientes, sem a necessidade de código ou conhecimento sobre IA, com uma interface gráfica fácil de usar.

O Ministério da Justiça tem por objetivo utilizar as capacidades do Power Virtual Agents para a construção de "bots" de auto atendimento capazes de endereçar as demandas de suporte técnico de sistemas finalísticos para a área de segurança pública, como é o caso do projeto Cortex.

Cada licença do Power Virtual Agents permite a criação de um número ilimitado de bots, considerando uma quantidade de duas mil sessões mensais de chatbot. A tabela abaixo demonstra as capacidades incluídas no licenciamento do Power Virtual Agents.

Summary of Power Virtual Agents entitlements

Plans and capabilities		Power Virtual Agents entitlements
Create and maintain intelligent chatbots ¹	Deploy chatbots in all channels	●
Chat Sessions	Sessions / tenant / month ¹	2k
Create flows	Automated, instant, scheduled, and business process flows	Within the context of Power Virtual Agents bots
	Standard connectors	
Connect to your data	Premium and custom connectors	●
	On-premises data gateway	●
Store and manage data	Dataverse (formerly Common Data Service) use rights	●
Per license capacity	Dataverse – Database Capacity	10GB
	Dataverse – File Capacity	20GB
	Dataverse – Log Capacity	2GB

Tabela 25 - Capacidades Inclusas no licenciamento do Power Virtual Agents 2K Sessions

6.19 AZURE

O Microsoft Azure é uma plataforma de computação em nuvem pública com soluções que incluem Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS) que podem ser usadas para serviços analíticos, máquinas virtuais, armazenamento, rede, entre outros. Conforme explanado na seção 3.2 desse Estudo Técnico, a contratação desse serviço é imprescindível para o alcance dos objetivos estratégicos do Ministério da Justiça e Segurança Pública.

A contratação de serviços de computação em nuvem representa um novo paradigma para as contratações públicas, pois a sua sistemática de utilização é por meio da aquisição de créditos (unidades monetárias) aplicáveis dentro do ambiente de nuvem para a criação de quaisquer serviços disponíveis, tais como máquinas virtuais, bancos de dados, plataformas de aplicações ou ferramentas para processamento analítico. Trata-se, portanto, de serviço utilizado mediante demanda, mensurado com base em uma relação de

valores unitários que variam de acordo com o recurso utilizado. Em alguns casos os serviços de nuvem podem incluir tanto a infraestrutura quanto o licenciamento necessário para executar as cargas de trabalho (workloads) associadas aos projetos.

No caso da nuvem Microsoft Azure, as contratações públicas (incluindo o contrato atual de serviços do MJSP) utiliza a unidade *Monetary Commitment* (compromisso monetário), *Part Number/SKU 6QK-00001*, que equivale a um valor de USD 1.200,00 por ano em valores "de tabela", sem a adição de impostos ou margens de revenda, para consumo dentro da plataforma. O valor estimado de revenda (*ERP - Estimated Retail Price*) do *Monetary Commitment* para o consumidor final foi fixado pela Microsoft em R\$ 5.977,20 para o presente exercício (ano fiscal) conforme atesta o comunicado oficial da empresa (SEI 12259433). Considerando este valor, o quantitativo de créditos previstos para atender a demanda do Ministério da Justiça e Segurança Pública seria equivalente a 1074,25 *Monetary Commitments* (aqui arredondados para 1075 *Monetary Commitments*).

O *Monetary Commitment* foi estabelecido originalmente como uma forma de comercialização de créditos de nuvem no sistema pré-pago. O uso desta modalidade em um contrato do tipo *Enterprise Agreement* (Acordo Empresarial) envolvia a aquisição e aplicação prévia dos créditos à conta de serviços de nuvem, créditos esses que passariam a estar disponíveis e deveriam ser utilizados no prazo máximo do ciclo de prestação de serviços do Azure (um ano). Os créditos remanescentes que não fossem empregados ao término do ciclo seriam simplesmente perdidos, e não poderiam ser utilizados para o ciclo seguinte. Essa modalidade de contratação e de uso dos recursos não é aderente ao regramento de contratação de serviços de TIC constante na Instrução Normativa nº 01/2019-SGD. Para contratações públicas, a Microsoft estabelece a possibilidade de execução na modalidade pós-paga, no qual a execução dos serviços em um período de apuração (normalmente um mês) gera um débito (*overage*) a ser pago na fatura subsequente. Nesta perspectiva, o *Monetary Commitment* não tem a função de unidade fundamental ou "grão" à partir do qual os créditos devem ser adquiridos e consumidos.

As contratações de serviços de computação em nuvem devem estar adequadas ao regramento que baliza as contratações públicas de serviços de TIC, o que tem se mostrado bastante desafiador. Em particular, há manifestações recentes do TCU no Acórdão nº 1.508/2020-TCU/Plenário contrárias à contratação de serviços de TIC por demanda com base em unidades abstratas (ex. Unidade de Serviço Técnico) em situações onde não exista um catálogo padronizado no qual os custos unitários estejam estabelecidos:

9.1.3. a fim de que, em novas contratações de serviços de tecnologia da informação, sejam observados os seguintes procedimentos:

9.1.3.1. abstenham-se de criar unidades de medida de forma unilateral, sem a ciência, a avaliação técnica e econômica e a padronização do órgão supervisor, com vistas a mitigar o risco de compartilhamento de metodologias e práticas sem a devida consistência e sem justificativas técnica e econômica, além de riscos inerentes a cenários de incomparabilidade de preços, de heterogeneidade e de assimetria de informações entre a administração e o mercado;

9.1.3.2. avaliem a economicidade dos preços estimados e contratados, realizando a análise crítica da composição de preços unitários e do custo total estimado da contratação, complementando-a com a análise da planilha de composição de custos e formação de preços dos serviços e com a análise do fator-k, submetendo as referidas análises para a avaliação e a autorização da autoridade competente, com vistas a mitigar a assimetria de informações e o risco de sobrepreço e de superfaturamento;

9.1.3.3. todos os parâmetros, pesos ou quaisquer variáveis quantitativas adotadas, que impactem o cálculo da quantidade de serviços e de seu preço, sejam devidamente justificados técnica e economicamente, com vistas a mitigar o risco de sobrepreço e superfaturamento, tendo em vista a disseminação da prática de não justificar técnica e economicamente tais parâmetros, pesos ou variáveis;

9.1.3.4. sejam implantados controles internos que assegurem a existência dos catálogos de serviços, juntamente com todos os detalhamentos cabíveis de cada serviço, como perfis profissionais, tempo estimado de execução e produtos e resultados esperados, a fim de mitigar o risco de antieconomicidade e de inobservância dos normativos já existentes, que versam sobre a clareza da solução de tecnologia da informação demandada;

9.1.3.5. os catálogos de serviços apresentem o respectivo valor monetário estimado de cada serviço, independentemente da métrica ou unidade utilizada; e

9.1.3.6. considerando os riscos inerentes às contratações baseadas em UST, entre outras denominações similares, o uso de UST em contratações por meio do Sistema de Registro de Preços (SRP) deve ocorrer somente se restar demonstrada a compatibilidade entre o uso de UST (e similares)

Por outro lado, o próprio TCU no Acórdão nº 1739/2015-Plenário (que discute a contratação de serviços de computação em nuvem pela Administração Pública) estabelece como uma vantagem o fato de que os serviços de nuvem são contratados "por contrato de adesão, utilizando métricas de precificação com custos unitários divulgados publicamente e iguais para todos os clientes", o que "facilita a pesquisa de preços" e "pode levar a uma redução de oportunidades de desvios e irregularidades, quando comparada às múltiplas contratações de máquinas, licenças de software, manutenção e suporte necessárias para a operação de CPD próprio".

Quando interpretado dentro do contexto das contratações públicas, o *Monetary Commitment* se aproxima bastante do conceito de Unidade de Serviço Técnico (e é assim chamada em vários processos), mas ele isoladamente não define um detalhamento em relação aos custos unitários dos serviços, ou seja, não há preliminarmente uma relação explícita entre o *Monetary Commitment* e os custos unitários dos serviços da nuvem Azure. No entanto, os serviços da nuvem Microsoft Azure possuem um catálogo público e uma calculadora (disponível no endereço <https://azure.microsoft.com/pt-br/pricing/calculator/>) que estabelecem os valores unitários para os serviços em diferentes moedas, inclusive em Reais. O catálogo do Azure contém uma relação enorme de itens, sendo cada item de serviços mensurado por um conjunto de critérios associados a diferentes valores unitários. Para exemplificar, o custo do item "Conta de Armazenamento" (*Blob Storage*) é modificado por diversos parâmetros utilizados na criação do item, como o tipo de redundância (local ou global), o tipo de tier utilizado pelo storage (quente ou frio), etc. Para definir o custo efetivo do storage são utilizados parâmetros de uso que são mensurados em valores unitários, como o custo unitário de armazenamento (em Gigabytes por mês) e o custo unitário associado ao número de operações de leitura e escrita realizados (em blocos de 10 mil operações), porém os valores unitários variam de acordo com os parâmetros utilizados na criação da Conta de Armazenamento. Os valores unitários da calculadora

pública do Azure são valores que não consideram os impostos e a margem do revendedor, ou seja, não representam os custos efetivos de comercialização dos serviços, mas são a referência para o emprego dos créditos adquiridos por meio do "*Monetary Commitment*".

As contratações de serviços da nuvem Microsoft Azure são tipicamente realizadas por meio de processo licitatório via Pregão Eletrônico, uma vez que a Microsoft comercializa os serviços no Brasil por meio da sua rede de parceiros. O mecanismo licitatório normalmente utilizado é o de menor lance para o valor do *Monetary Commitment* (Part Number/SKU 6QK-00001). A aquisição de um *Monetary Commitment* equivale ao cliente ter à sua disposição a USD 1.200,00 ou R\$ 4.858,97 (a calculadora pública do Azure estabelece a equivalência de 1 USD = R\$ 4,04914) para consumir em recursos na nuvem, de acordo com os valores estabelecidos pela calculadora, porém o custo final do *Monetary Commitment* para o cliente tipicamente excede esse valor, pois aqui não estão incluídos os impostos e a margem do revendedor. A *Microsoft* denomina essa diferença entre o valor pago pelo *Monetary Commitment* e o valor fundamental em créditos ao que ele dá direito dentro da nuvem de *markup*, e esta mesma diferença em termos percentuais é aplicada linearmente no preço de cada serviço presente no catálogo do Azure em relação aos valores da calculadora para estabelecer o valor final dos serviços que é apresentado ao cliente na ferramenta de gerenciamento de custos (os custos relativos aos serviços que foram consumidos pelo cliente podem ser acessados por meio do portal do *Enterprise Agreement* ou do próprio portal de gerenciamento do Azure).

Portanto, consideramos que o catálogo e a calculadora públicos do Azure atendem as recomendações do TCU no que diz respeito à necessidade de existência de um catálogo de serviços padronizado e precificado para a contratação de serviços por demanda utilizando métrica abstrata. Deve ser considerado, no entanto, que os valores unitários presentes no catálogo e na calculadora públicos do Azure não serão os valores finais dos serviços, devendo ainda ser acrescentado sobre eles a margem percentual que virá da diferença (*markup*) entre o valor básico do *Monetary Commitment* (R\$ 4.858,97) e valor da proposta vencedora por esse item. Considerando a necessidade de materializar o catálogo de serviços no processo de contratação, deverá ser feita a sua publicação, relacionando os itens unitários de serviços por meio dos seus SKUs (*stock-keeping units*), contendo no mínimo a descrição do serviço, a zona geográfica de prestação do serviço, a família de serviços do Azure, a métrica utilizada para mensuração e o valor unitário em reais. Abaixo, um resumo da metodologia utilizada.

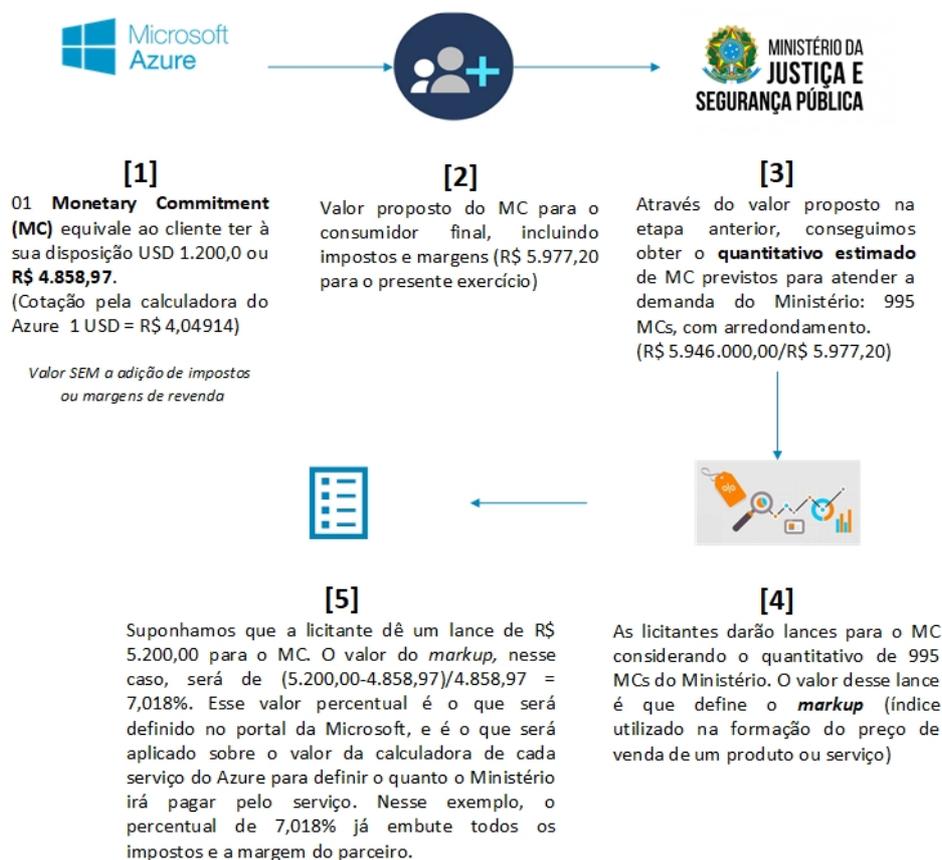


Figura 6 - Resumo metodologia Azure

7 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

O presente Estudo Técnico Preliminar (ETP) evidenciou que a contratação da Solução 4A (Contratação de Licenças de Softwares Microsoft) e Solução 3B (Contratação de empresa especializada no serviço de Computação em Nuvem pública Microsoft Azure) é viável do ponto de vista técnico, de negócio e economicamente mais vantajoso, desde que sejam adotadas as premissas e conclusões descritas neste estudo conforme preconizado na IN. 1, de 4 de abril de 2019.

Benefícios a serem alcançados com a contratação:

- a) Ampliação do volume de licenças e serviços atualmente disponibilizados por meio do Contrato nº 28/2018;
- b) Adequação das licenças e serviços às necessidades atuais do Ministério da Justiça e Segurança Pública;
- c) Contratação de volume de serviços de computação em nuvem Azure suficientes para as novas necessidades e para a expansão dos projetos em andamento;
- d) Realização de contratação conjunta entre o Ministério da Justiça e Segurança Pública e as instituições vinculadas (DPF, DPRF, CADE, FUNAI), de forma a obter ganhos de volume e redução dos custos de contratação;
- e) Adequação do formato da contratação de serviços por demanda mensurados por Unidade de Serviço Técnico às recentes deliberações do TCU, por meio da elaboração de catálogos de serviços que estabeleçam entregas quantificáveis e de valor aferível pelo ente público.

8 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Conforme o "Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação" V 3.0 do SISP, o orçamento informado nesse momento é preliminar. Ele deverá ser suficiente na análise de custo total de propriedade para a escolha da solução. **O orçamento detalhado será realizado na confecção do Termo de Referência.**

A participação dos órgãos ou entidades vinculadas ao Ministério da Justiça e Segurança Pública na presente contratação será fundamentada na compatibilidade do Estudo Técnico Preliminar e outros documentos de planejamento da contratação do órgão interessado na participação com o Termo de Referência do MJSP, sendo de responsabilidade exclusiva dos órgãos ou entidades partícipes as justificativas e os quantitativos solicitados.

A contratação conjunta visa a integração tecnológica entre o Ministério da Justiça e Segurança Pública e as demais instituições vinculadas que são partícipes do presente processo, viabilizando a utilização de ferramentas comuns para a comunicação e o intercâmbio de dados e informações, além de possibilitar projetos de TIC conjuntos entre as instituições.

Conforme previsto na Instrução Normativa Nº 2, DE 4 DE ABRIL DE 2019:

Art. 2º Os órgãos e entidades previstos no art. 1º deverão submeter à Secretaria de Governo Digital do Ministério da Economia proposta para aprovação de:

I - contratação de bens ou serviços de TIC com valor global estimado do objeto superior a 20 (vinte) vezes o previsto no art. 23, inciso II, alínea "c", da Lei nº 8.666, de 21 de junho de 1993; e

II - atas de registro de preços de serviços de TIC passíveis de adesão por parte de órgãos ou entidades não participantes, para efeito do disposto no art. 22, § 10, inciso II, do Decreto nº 7.892, de 2013.

§ 1º Para contratações no sistema de registro de preços, o valor global estimado que trata o inciso I deverá contemplar o montante das demandas dos órgãos participantes da licitação, incluindo os volumes previstos para possíveis utilizações da ata de registro de preços por órgão ou entidade não participante, e considerar os Decretos de atualizações expedidos na forma do art. 120 da Lei nº 8.666, de 1993.

...

Art. 4º As solicitações de aprovação deverão conter todos os documentos referentes à fase de planejamento da contratação, quais sejam: Documento de Oficialização da Demanda, Estudo Técnico Preliminar, Termo de Referência ou Projeto Básico, documentos relacionados à pesquisa de preços e o Mapa de Gerenciamento de Riscos.

Considerando que o valor estimado da presente contratação ficou superior ao previsto no inciso I do Art. 2º da supracitada IN (1,43 milhões x 20 = 28,6 milhões) será necessário o encaminhamento dos documentos referentes à fase de planejamento da contratação para apreciação por parte da SGD.

Informa-se ainda que foram consideradas somente as licenças que tivessem o modelo de Subscrição. Licenças de natureza perpétua, pela incompatibilidade do modelo adotado por esse Ministério, não foram consideradas.

Referência:

- a) DPRF: OFÍCIO Nº 58/2020/DIGEF/CGT/DTIC (SEI nº 12291028) e SEI nº 13158346;
- b) CADE: OFÍCIO Nº 5632/2020/SESIN/CGTI/DAP/CADE (SEI nº 12290819) e SEI nº 13047034;
- c) DPF: OFÍCIO Nº OFÍCIO Nº 48/2020/DTI/PF (SEI nº 12322906);
- d) FUNAI: OFÍCIO Nº 1454/2020/PRES/FUNAI (SEI nº 12243153).

ITEM	SKU	DESCRIÇÃO COMPLEMENTAR	UNIDADE	VALOR ESTIMADO MENSAL (R\$)	VALOR ESTIMADO ANUAL (R\$)	QTDE MJSP	QTDE DPRF	QTDE CADE	QTDE DPF	QTDE FUNAI	QTD TOTAL	VALOR TOTAL ESTIMADO ANUAL (R\$)
1	AAD-33204	Microsoft 365 E3 (Windows 10, Enterprise Mobility + Security, Office 365 E3, CALs de acesso para ambiente híbrido e servidores de produtividade Exchange Server, Skype For Business Server e Sharepoint Server)	Usuário	120,02	1.440,24	5030	0	500	0	0	5530	7.964.527,20
2	T6A-00024	Office 365 E1	Usuário	26,69	320,28	911	0	400	0	1000	2311	740.167,08
3	AAA-10842	Office 365 E3	Usuário	73,53	882,3	0	1000	0	0	1000	2000	1.764.600,00
4	4SY9-00004	Office 365 E5	Usuário	128,61	1.543,26	0	100	0	0	0	100	154.326,00
5	AAA-10732	Enterprise Mobility + Security E3 - Gerenciamento de identidade, dispositivos e proteção das informações	Usuário	32,13	385,56	1212	0	0	0	0	1212	467.298,72
6	AAA-12414	Core CAL Bridge para Office 365	Usuário	9,35	112,2	0	0	0	0	2000	2000	224.400,00

7	AAA-10787	Windows E3	Usuário	24,06	288,66	354	0	20	0	0	374	107.958,84
8	6VC-01252	Windows Server Remote Desktop CAL	Usuário	12,54	150,45	0	0	0	1000	0	1000	150.450,00
9	QLS-00003	Microsoft Defender ATP - Proteção avançada contra ameaças para endpoint incluindo proteção, detecção, investigação e resposta.	Usuário	18,53	222,36	5384	0	0	0	0	5384	1.197.186,24
10	FSZ-00002	Office 365 ATP Plano 2 - Proteção avançada contra ameaças para e-mail incluindo configuração, proteção, detecção, automação, investigação, correção e educação	Usuário	15,64	187,68	5384	0	0	0	0	5384	1.010.469,12
11	G5F-00002	Azure ATP - Proteção avançada contra ameaças e análise de comportamento para domínio incluindo identificar, detectar e investigar ameaças avançadas, identidades comprometidas e ações de pessoas internas mal-intencionadas.	Usuário	15,98	191,76	5685	0	0	0	0	5685	1.090.155,60
12	2ER-00002	Microsoft Cloud App Security - Agente de Segurança de Acesso à Nuvem incluindo funcionalidades de shadow IT, proteção das informações, proteção contra ameaças cibernéticas e anomalias e análise de conformidade dos apps em nuvem.	Usuário	10,97	131,58	5384	0	0	0	0	5384	708.426,72
13	6E6-00004	Azure AD Premium P2 - Step Up do Azure AD P1 para Azure AD P2 - Serviço de diretório adicionando as funcionalidades de proteção de identidade e governança de identidade.	Usuário	8,76	105,06	5685	0	0	0	0	5685	597.266,10
14	TRS-00002	Project Plan 1 - Recursos e membros de projeto	Usuário	31,28	375,36	150	60	60	0	0	270	101.347,20
15	7LS-00002	Project Plan 3 - Gerentes de Projeto	Usuário	93,76	1.125,06	200	40	60	0	0	300	337.518,00
16	7SY-00002	Project Online Premium - Gerente de Portfólio	Usuário	171,79	2.061,42	5	4	20	0	0	29	59.781,18
17	NK4-00002	Power BI Pro	Usuário	31,2	374,34	606	160	20	0	100	886	331.665,24
18	GSL-00002	Power BI Premium P1 - Plano com 8 virtual cores e implantação SaaS ou PaaS	Processamento	15.598,78	187.185,30	3	3	5	0	0	11	2.059.038,30
19	N9U-00002	Visio Plano 2	Usuário	46,92	563,04	15	20	20	0	0	55	30.967,20
20	DDW-00003	Dynamics 365 for Customer Services Enterprise - Usuário para gestão de relacionamento, processos, demandas e ocorrências.	Usuário	349,1	4.189,14	0	300	0	0	0	300	1.256.742,00
21	PRX-00002	Armazenamento de Dados na Plataforma Dynamics, por Gb	Armazenamento	146,97	1.763,58	0	100	0	0	0	100	176.358,00
22	PSM-00002	Armazenamento de Logs na Plataforma Dynamics, por Gb	Armazenamento	36,81	441,66	0	100	0	0	0	100	44.166,00
23	PSG-00002	Armazenamento de Arquivos na Plataforma Dynamics, por Gb	Armazenamento	7,4	88,74	0	100	0	0	0	100	8.874,00
24	RVT-00001	Pacote de 2 mil sessões de agente virtual (bot)	Sessão	3.674,04	44.088,48	10	5	0	0	0	15	661.327,20
25	SEQ-00001	Power Apps Per App - Usuários com direito de acesso a até duas aplicações e um portal que utilizem conectores premium.	Usuário	36,81	441,66	300	600	0	0	0	900	397.494,00
26	9GA-00006	CIS Standard Core - Windows Server Standard + System Center Standard	Núcleo	24,72	296,65	84	0	100	0	80	264	78.315,60
27	9GS-00495	CIS Datacenter Core - Windows Server Datacenter + System Center Datacenter	Núcleo	101,01	1.212,10	312	40	400	0	80	832	1.008.467,20
28	7JQ-00341	SQL Server Enterprise Core	Núcleo	1.529,86	18.358,30	34	0	32	0	6	72	1.321.797,60
29	6QK-00001	Créditos de Azure para serviços de nuvem híbrida	Compromisso Monetário	498,1	5.977,20	1075	550	150	496	150	2421	14.470.801,20
TOTAL											38.521.891,54	

Tabela 26 - Quantitativos Consolidados da Contratação

9 – APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela Portaria SAA Nº 22, de 02 de julho de 2020 (12059507), conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

Integrantes Técnicos

Nome	Simão Pedro Miranda de Sousa
Matrícula/SIAPE	1795258
Nome	Sérgio Paulo Futer
Matrícula/SIAPE	9221554

Integrante Requisitante

Nome	Leonardo Garcia Greco
------	-----------------------

Matrícula/SIAPE	1447905
Autoridade Máxima da Área de TIC	
Nome	Rodrigo Lange
Matrícula/SIAPE	0480055



Documento assinado eletronicamente por **Leonardo Garcia Greco, Integrante Requisiteante**, em 06/01/2021, às 11:56, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.



Documento assinado eletronicamente por **Sergio Paulo Futer, Integrante Técnico(a)**, em 06/01/2021, às 11:59, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.



Documento assinado eletronicamente por **Rodrigo Lange, Diretor(a) de Tecnologia da Informação e Comunicação**, em 06/01/2021, às 13:52, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.



A autenticidade do documento pode ser conferida no site <http://sei.autentica.mj.gov.br> informando o código verificador **13590833** e o código CRC **AE53D44**

O trâmite deste documento pode ser acompanhado pelo site <http://www.justica.gov.br/aceso-a-sistemas/protocolo> e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.