Google apontou as supostas ilegalidades:

II.1. DESCABIMENTO DE EXIGÊNCIA DE DECLARAÇÃO DO FORNECEDOR

5. Primeira ilegalidade verificada diz respeito à descabida exigência de apresentação de declaração emitida pelo fornecedor do enquadramento dos proponentes como revendedores autorizados, prevista pelos itens 4.2.1. a 4.2.3. do Termo de Referência, Anexo I do Edital ("TR"), por ausência de amparo legal ou de evidências de sua razoabilidade.

4.2.1. A LICITANTE deverá, obrigatoriamente, apresentar cópia autenticada de declaração emitida pela Microsoft de que é uma revenda autorizada Microsoft (LSP – Licensing Solution Provider), demonstrando desta forma estar habilitada a operacionalizar contratos de licenciamento por volume, inclusive para médias e grandes organizações.

No Setor Público, o modelo de atuação da Microsoft no Brasil é indireto, com a necessária atuação de revendas credenciadas, seguindo-se, desta forma, uma política rigorosa de transparência e isonomia, observando fatores como capacidade financeira, aderência às políticas de Compliance da Microsoft, estrutura de pré-vendas, vendas e pós-vendas, estrutura de marketing, licenciamento e operações, histórico de vendas, capilaridade de cliente, entre outros fatores. Alinhado as estes fatores, também às regras de compras no território brasileiro, regidas pela Lei 8666/93 (e outras regras relacionadas). Mais detalhadamente, para os contratos de licenciamento em volume Enterprise Agreement e Select a participação nos certames públicos é feita pelos LSP (Large Solution Partners), anteriormente denominados LAR (Large Account Reseller). São as empresas habilitadas para tais contratos de licenciamento, e que se encontram aqui listadas. https://partner.microsoft.com/pt-br/licensing/parceiros%20lsp

4.2.2. A LICITANTE deve ser autorizada pela Microsoft para fornecer seus licenciamentos de volume para instituições governamentais (categoria Government Partner), o que será verificado através de declaração emitida por este fabricante.

A Administração Pública, via de regra, segue com o modelo de contratação por instrumento próprio, seguindo modelos pré-definidos. De outro lado, por tratar-se de licenciamento específico, a Microsoft tem seus padrões e modelos de contrato. Assim, existe o que se chama Government Partners – GP, que são parceiros habilitados pela Microsoft para atuar no segmento público, com o objetivo de assinar os contratos nos modelos dos clientes e o Government Integrator Agremment – GIA da Microsoft, que significa o contrato entre o parceiro e a Microsoft, relacionado ao primeiro firmado pelo parceiro com a Administração Pública.

Quanto à participação nos certames públicos, para se garantir as mesmas condições de participação a todos as revendas, a Microsoft segue uma política de isonomia de canais, que prevê que todas as empresas parceiras terão as mesmas condições de participação no certame licitatório, sem qualquer privilégio, de qualquer natureza, ao parceiro local ou específico. Isso implica em respeito às regras concorrenciais e competição saudável no mercado, além de cumprimento aos princípios da economicidade e competividade previstos pela legislação vigente, não estabelecendo qualquer restrição à concorrência ou participação em certames, mas sim a ampla concorrência, com a necessária capacitação ao correto atendimento à Administração e aos interesses públicos.

4.2.3. A LICITANTE deverá, obrigatoriamente, apresentar cópia autenticada de declaração emitida pela Microsoft ou através da página do fabricante (indicando a devida URL) de que possui as seguintes competências técnicas, em nível GOLD ou SILVER:

Para o processo em questão, pretende-se, junto a aquisição das licenças de software, também a aquisição de serviços técnicos especializados Microsoft sob demanda, os quais são fornecidos por Provedores de Soluções Credenciados e Reconhecidos pela fabricante, os provedores de soluções certificados pela Microsoft são especializados em fornecer soluções atualizadas baseadas na tecnologia da Microsoft em todo o mundo, conforme pode ser observado neste link https://www.microsoft.com/pt-br/solution-providers/home. Dessa forma, em tempo de especificação técnica do processo de contratação, procurou-se observar a necessidade de que, as licitantes que venham participar do certame, já sejam reconhecidas, pela própria fabricante, em relação a sua capacidade na execução e entrega de projetos.

Com isso, o Ministério do Desenvolvimento Regional (MDR), terá confiança em relação a qualidade dos serviços que serão demandados à CONTRATADA e, sobretudo, reduzirá os riscos e custos de gestão e operação em tempo de execução do contrato.

Abaixo a relação de competências que tem sinergia com o objeto contratado e detalhadas nos seus respectivos links de comprovação:

- *Collaboration and Content Demonstra habilidades e recursos técnicos no desenvolvimento de práticas eficientes e eficazes de colaboração e comunicação em um ambiente corporativo em plataformas como o SharePoint (online, na infraestrutura local e híbrida), o OneDrive e o Teams. https://partner.microsoft.com/pt-br/membership/collaboration-and-content-competency*
- *Data Platform: Demonstra a capacidade técnica para garantir que os sistemas de banco de dados de cliente operem de forma eficiente, protejam dados de acesso não autorizado e categorizem dados para que eles possam ser transformados em insights de negócios. https://partner.microsoft.com/pt-br/membership/data-platform-competency*
- *Messaging: Demonstra habilidades e recursos técnicos para implementação de ações voltadas para os recursos de mensagens do Microsoft 365 e do Exchange necessários para implantar, configurar e monitorar destinatários, permissões e fluxo de emails em ambientes híbridos e na nuvem. https://partner.microsoft.com/pt-br/membership/Messaging-competency*
- *Cloud Platform: Demonstra habilidades e recursos técnicos na administração de recursos técnicos na implantação, migração e manutenção de aplicativos e serviços na nuvem no Microsoft Azure, ajudando seus clientes a fazer uso de soluções seguras na nuvem, escaláveis e confiáveis. https://partner.microsoft.com/pt-br/membership/Cloud%20Platform-competency*
- *Data Analytics: Demonstra habilidades e recursos técnicos para criação de soluções de business intelligence e demonstrar sua proficiência para conectar fontes de dados, realizar transformações de dados e modelar e visualizar dados. https://partner.microsoft.com/pt-br/membership/Data%20Analytics-competency*
- *Enterprise Mobility Management: Demonstra habilidades e recursos técnicos no planejamento, implantação e gerenciamento de serviços de mobilidade e segurança do Microsoft 365 para manter os clientes corporativos seguros, em conformidade e conectados. https://partner.microsoft.com/pt-br/membership/Enterprise%20Mobility%20Management-competency*
- *Application Integration: Demonstra habilidades e recursos técnicos em tarefas avançadas de integração e configuração, mostrando aos clientes como integrar aplicativos e dados para aumentar a eficiência e impulsionar os resultados dos*

negócios. https://partner.microsoft.com/pt-br/membership/Application%20Integration-competency

- *Communications: Demonstra habilidades e recursos técnicos na implementação de estratégias de comunicação unificadas para os clientes por meio do projeto, planejamento, implantação e manutenção de soluções do Skype for Business e Microsoft Teams. https://partner.microsoft.com/pt-br/membership/Communications-competency*
- *Cloud Productivity: Demonstra habilidades e recursos técnicos para fornecer soluções inovadoras do Office 365, mostrando como ajudar os clientes a implantar e gerenciar aplicativos como o Exchange Online, o SharePoint Online, o Teams e o Skype for Business. https://partner.microsoft.com/pt-br/membership/Cloud%20Productivity-competency*
- *Windows and Devices: Demonstra habilidades e recursos técnicos para fornecer serviços, oferecer dispositivos ou criar, testar e manter aplicativos otimizados para o ambiente Windows. https://partner.microsoft.com/pt-br/membership/Windows%20and%20Devices-competency*
- *Application Development: Demonstra habilidades e recursos técnicos para elaboração de projeto, desenvolvimento e monitoramento de e aplicativos baseados na Web e na nuvem para clientes no Azure ou no Microsoft 365. https://partner.microsoft.com/pt-br/membership/Application%20Development-competency*
- *Small and Midmarket Cloud Solutions: Demonstra habilidades e recursos técnicos para fornecer produtividade em nuvem e soluções de segurança para clientes de pequeno e médio porte que estão implantando ou migrando para o Office 365. https://partner.microsoft.com/en-us/membership/small-midmarket-cloud-solutions-competency*
- *Datacenter: Demonstra habilidades e recursos técnicos para criar, implementar e manter uma infraestrutura do Windows Server em um ambiente dimensionado e altamente virtualizado. https://partner.microsoft.com/pt-br/membership/Datacenter-competency*
- *Security: Demonstra habilidades organizacionais na implementação, gerenciamento e monitoramento de soluções de segurança e conformidade para ambientes na nuvem e híbridos. https://partner.microsoft.com/pt-br/membership/Security-competency*
- *Project and Portfolio Management: Demonstra habilidades, recursos técnicos e experiência em projetar, criar e implantar soluções de Gerenciamento de Projetos baseadas no Project para a Web, o Power Platform. https://partner.microsoft.com/pt-br/membership/project-portfolio-management-competency*

II.2. DA INSUFICIENTE MOTIVAÇÃO DO OBJETO DO CERTAME

A Medida Provisória nº 870, de 1º de janeiro de 2019 estabeleceu uma nova organização básica dos órgãos da Presidência da República e dos Ministérios, formando o Ministério do Desenvolvimento Regional, composto pela integração dos órgãos Ministério da Integração Nacional (MI) e Ministério das Cidades (MCid). Diante do cenário de fusão de Órgãos, o Ministério do Desenvolvimento Regional passou a possuir 2 instrumentos contratuais com objeto similar a solução pretendida no Pregão Eletrônico nº 01/2021, sendo eles:

ÓRGÃO	CONTRATO	VIGÊNCIA	OBJETO

MI	18/2017-MI	23/08/2020	O presente contrato tem por objeto a Renovação e Expansão de Licenciamento e Serviços Microsoft, com garantia, suporte pelo período de 36 (trinta e seis) meses e a consultoria técnica especializada à plataforma de produtos Microsoft em operação nos equipamentos servidores e estações de trabalho do Ministério da Integração Nacional - MI conforme especificações previstas no Termo de Referência - Anexo I, do edital do Pregão Eletrônico SRP n.º 08/2017.
MCid	14/2018	30/08/2021	O contrato tem por objeto a contratação de empresa especializada para a aquisição e renovação de solução de software Microsoft e fornecimento de serviços técnicos especializados aos softwares Microsoft, de acordo com as especificações técnicas, nos termos e nas condições contidas no Termo de Referência e no Estudo Técnico preliminar, de modo a atender às necessidades da Contratante, nos termos e condições constantes do citado edital do pregão eletrônico e seus anexos, doravante denominado simplesmente "contrato de fornecimento" ou "fornecimento".

Desta forma, um fator de extrema relevância a ser considerado com a execução desse projeto será a racionalização dos contratos com objetos similares, remanescentes dos extintos Ministérios que integraram o Ministério do Desenvolvimento Regional (MDR), com o objetivo de evitar o prejuízo ao erário público ao se considerar os custos envolvidos na formalização, gestão e fiscalização dos contratos administrativos.

Resta claro que a Coordenação Geral de Tecnologia da Informação possui a incumbência de assegurar que os serviços de TIC sejam prestados de forma satisfatória, com a finalidade de garantir o Princípio da Eficiência, o qual aduz que a "atividade administrativa deve ser exercida com presteza, perfeição e rendimento funcional, exigindo resultados positivos para o serviço público e satisfatório atendimento das necessidades".

Assim, em função desse princípio, a Administração Pública possui o dever de planejar adequadamente suas aquisições e contratações, com vistas a buscar a melhor solução para o total atendimento do interesse que se busca satisfazer, através de processo licitatório que irá selecionar a proposta mais vantajosa para tal fim.

Neste sentido, o Ministério do Desenvolvimento Regional, através da Coordenação Geral de Tecnologia da Informação, visa a contratação de empresa especializada para o fornecimento de licenças de softwares aplicativos e sistemas operacionais Microsoft, destinados aos usuários finais, à camada cliente/servidor e banco de dados, em atendimento às necessidades do Ministério.

Posto isso, cabe ressaltar que, ambos os Ministérios que hoje compõem o Ministério do Desenvolvimento Regional, já possuíam em seus respectivos parques computacionais um legado expressivo de soluções fornecidas pela fabricante Microsoft, seja para atender as soluções do ambiente de Datacenter local, seja para as necessidades dos usuários finais com soluções de

colaboração, comunicação e produtividade, como também para o ambiente em nuvem pública. O impacto da mudança dessas tecnologias iria além da possibilidade de mudança de fabricantes, foram observados questões como:

- A familiaridade dos usuários em relação as soluções já em uso pelo Ministério;
- O esforço e custo envolvidos na Migração para uma nova plataforma, seja ela de Datacenter local, nuvem pública e colaboração, comunicação e produtividade;
- Capacitação dos usuários finais e equipe técnica do Ministério;
- Capacidade de manutenção da nova plataforma, uma vez que hoje o Ministério já possui em seu quadro técnico uma equipe familiarizada e capacitada para operação das soluções em operação;
- Dentre outros fatores.

Dessa forma, decidiu-se pela manutenção do atual parque tecnológico fornecido pela Microsoft.

II.3. DA ILEGAL ESCOLHA DE MARCA E INDEVIDO DIRECIONAMENTO DO PREGÃO

- **II.3.1. Premissa inafastável: a indicação de marca é medida absolutamente excepcional nas licitações, que deve sempre vir respaldada em justificativa sólida**

II.3.2. Insuficiente motivação do objeto do certame para respaldar a escolha exclusiva por produtos da Microsoft

- **a) Ausência de motivações técnicas que evidenciem que os produtos da Microsoft são os únicos capazes de atender os interesses do MDR**
- **b) Insuficiência da mera referência a contrato anterior envolvendo produtos similares.**
- c) **As funcionalidades dos softwares da Microsoft são plenamente compatíveis com outras marcas e podem igualmente ser atendidas por produtos similares**
- **d) Desconsideração das vantagens econômicas da competição entre fornecedores.**

II.3.3. Conclusão parcial: a escolha antecipada da solução Microsoft compromete a economicidade, a competitividade e a isonomia do certame

O Google Workspace (antigo G Suite) 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.

As suítes Microsoft Office 365 e Google Workspace são as mais largamente utilizadas globalmente para provimento de soluções de escritório e produtividade, incluindo aqui o serviço de e-mail em nuvem. No entanto, análise realizada pelo Gartner Inc. em 2019 no documento "Survey Analysis: Google and Microsoft Battle It Out in a Growing Cloud Email Market" demonstra a grande superioridade da preferência pela solução Office 365 em escala global, quando consideradas companhias de diferentes setores e tamanhos.

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 MDR a suite de programas de escritório é instalada diretamente nos computadores (versões E3 e E5).

Para a atual contratação foi realizada consulta às unidades organizacionais quanto às versões do Microsoft Office 365 necessárias, visando o início de uma mudança cultural por meio da adoção quando possível da solução online (acessível exclusivamente por browser) e a consequente economia de recursos. Foi portanto definido inicialmente o uso da versão online (E1) do Office 365 para um conjunto de 500 usuários, essas licenças foram cedidas pela Microsoft para apoio ao teletrabalho no início da Pandemia, notadamente aqueles para os quais os requisitos de usabilidade não fossem tão elevados. No entanto, foi verificado que persistem alguns entraves técnicos e de performance para a utilização exclusiva da versão online para a grande maioria dos usuários. Devido à observância desta realidade, o quantitativo de licenças F1 previsto para o MDR teve que ser limitado a cerca de 8% do total de licenças do Microsoft 365 previsto para aquisição.

Deve ser considerado ainda que parte significativa da contratação consiste em licenças do Microsoft M365 E3 (item 2 do processo licitatório), que engloba em um único pacote as soluções de produtividade da suíte Microsoft Office 365 acrescidas do licenciamento da suíte de identidade e segurança EMS E3 (Enterprise Mobility and Security E3) e ainda do licenciamento Windows Enterprise para Desktops, que possibilita que os usuários dos Desktops utilizados na instituição recebam sempre a última versão do Microsoft Windows 10 e suas atualizações. O pacote M365 E3 traz grande vantagem econômica em relação à aquisição em separado dos itens que o compõem.

Adicional ao exposto acima, a equipe da Coordenação Geral de Tecnologia da Informação, atenta ao momento de transformação das práticas de trabalho na Administração Pública Federal, as quais estão cada vez mais voltadas ao teletrabalho, se viu no desafio de manter seus servidores produtivos, de qualquer lugar, com qualquer dispositivo e, sobretudo, com camadas de segurança adicionais, as já existentes no Ministério.

Para atender essa necessidade, a Microsoft disponibiliza uma solução completar ao Office 365 e Windows Enterprise chamada: Enterprise Mobility + Security (EMS). O EMS, segundo a própria fabricante, fornece um conjunto de soluções de segurança orientada por identidade, as quais oferecem uma abordagem holística aos desafios de segurança nessa era de foco em dispositivos móveis e na nuvem, essas tecnologias ajudam a proteger a organização e identificar violações no âmbito das soluções em nuvem da fabricante, antes que estas possam causar danos. Abaixo um breve resumo das funcionalidades observadas pelo Ministério:

- 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. O Premium 1 (P1) foi projetado para capacitar organizações com mais necessidades de gerenciamento de identidades e acesso, a edição Azure Active Directory Premium adiciona capacidades de gerenciamento de identidades de nível empresarial e ricas em recursos, permitindo que usuários híbridos acessem perfeitamente as capacidades locais e na nuvem. Essa edição inclui tudo o que é necessário para profissionais da informação e administradores de identidade em ambientes híbridos em termos de acesso de aplicativos, IAM (gerenciamento de identidades e acessos) de autoatendimento e segurança na nuvem. Conforme pode ser observado quadro comparativo abaixo:

	GRATUITO	APLICATIVOS DO OFFICE 365	PREMIUM P1	PREMIUM P2
Gerenciamento de Identidade e Acesso Núcleo				
Objetos do diretório1	500.000 Limite de objeto	Sem limite de objeto	Sem limite de objeto	Sem limite de objeto
SSO (logon único) (ilimitado)2	Disponível	Disponível	Disponível	Disponível
Provisionamento do usuário	Disponível	Disponível	Disponível	Disponível
Autenticação federada (ADFS ou IDP de terceiros)	Disponível	Disponível	Disponível	Disponível
Gerenciamento de usuários e grupos (adicionar/atualizar/excluir)	Disponível	Disponível	Disponível	Disponível
Registro do dispositivo	Disponível	Disponível	Disponível	Disponível
Autenticação de nuvem (autenticação de passagem, sincronização de hash de senha e SSO simples)	Disponível	Disponível	Disponível	Disponível
Sincronização do Azure AD Connect (estender diretórios locais para o Azure AD)	Disponível	Disponível	Disponível	Disponível
Alteração de senha de autoatendimento para usuários na nuvem	Disponível	Disponível	Disponível	Disponível
Ingresso no Azure AD: recuperação do bitlocker do administrador e SSO de desktop	Disponível	Disponível	Disponível	Disponível
Proteção por senha (senha banida global)	Disponível	Disponível	Disponível	Disponível
Autenticação Multifator3	Disponível	Disponível	Disponível	Disponível
Relatórios de uso e segurança básica	Disponível	Disponível	Disponível	Disponível
Identidades externas				

Proteger e gerenciar clientes e parceiros				
Gerenciamento de Identidade e Acesso para aplicativos do Office 365				
Identidade visual da empresa (personalização das páginas de logon/logoff e painel de acesso)	Não disponível	Disponível	Disponível	Disponível
Redefinição de senha self-service para usuários na nuvem	Não disponível	Disponível	Disponível	Disponível
Contrato de Nível de Serviço (SLA)	Não disponível	Disponível	Disponível	Disponível
Dispositivo com write-back (sincronização de duas vias de objetos de dispositivo entre diretórios locais e do Azure)	Não disponível	Disponível	Disponível	Disponível
Recursos Premium				
Proteção por senha (senha banida personalizada)	Não disponível	Não disponível	Disponível	Disponível
Proteção por senha para o Active Directory do Windows Server (senha banida global e personalizada)	Não disponível	Não disponível	Disponível	Disponível
Redefinição/alteração/desbloqueio de senha self-service com write-back local	Não disponível	Não disponível	Disponível	Disponível
Gerenciamento de acesso ao grupo	Não disponível	Não disponível	Disponível	Disponível
Microsoft Cloud App Discovery4	Não disponível	Não disponível	Disponível	Disponível
Ingresso no Azure AD: inscrição automática do MDM e personalização da política de administrador local	Não disponível	Não disponível	Disponível	Disponível

Ingresso no Azure AD: recuperação de autoatendimento do Bitlocker e Enterprise State Roaming	Não disponível	Não disponível	Disponível	Disponível
Relatórios de uso e segurança avançada	Não disponível	Não disponível	Disponível	Disponível
Identidades híbridas				
Proxy de aplicativo	Não disponível	Não disponível	Disponível	Disponível
CAL do usuário do Microsoft Identity Manager5	Não disponível	Não disponível	Disponível	Disponível
Connect Health6	Não disponível	Não disponível	Disponível	Disponível
Gerenciamento avançado de acesso a grupos				
Grupos dinâmicos	Não disponível	Não disponível	Disponível	Disponível
Delegação de permissão para criar grupos	Não disponível	Não disponível	Disponível	Disponível
Política de nomenclatura do grupo	Não disponível	Não disponível	Disponível	Disponível
Término do grupo	Não disponível	Não disponível	Disponível	Disponível
Diretrizes de uso	Não disponível	Não disponível	Disponível	Disponível
Classificação padrão	Não disponível	Não disponível	Disponível	Disponível
Acesso condicional				
Acesso Condicional com base no grupo, na localização e no status do dispositivo	Não disponível	Não disponível	Disponível	Disponível

Integração da Proteção de Informações do Azure	Não disponível	Não disponível	Disponível	Disponível
Acesso limitado ao SharePoint	Não disponível	Não disponível	Disponível	Disponível
Termos de Uso (configure os termos de uso para acesso específico)	Não disponível	Não disponível	Disponível	Disponível
Autenticação Multifator com Acesso Condicional	Não disponível	Não disponível	Disponível	Disponível
Integração do Microsoft Cloud App Security	Não disponível	Não disponível	Disponível	Disponível
Integração de parceiros de governança de identidade de terceiros	Não disponível	Não disponível	Disponível	Disponível
Proteção de identidade				
Detecção de vulnerabilidades e contas de risco	Não disponível	Não disponível	Não disponível	Disponível
Investigação dos eventos de risco	Não disponível	Não disponível	Não disponível	Disponível
Políticas de Acesso Condicional baseadas em risco	Não disponível	Não disponível	Não disponível	Disponível
Governança de Identidade				
PIM (Privileged Identity Management)	Não disponível	Não disponível	Não disponível	Disponível
Revisões de Acesso	Não disponível	Não disponível	Não disponível	Disponível
Gerenciamento de direitos	Não disponível	Não disponível	Não disponível	Disponível
Preço	Gratuito	O365 E1, E3, E5, F3	$6 usuário/mês	$9 usuário/mês

Fonte: https://azure.microsoft.com/pt-br/pricing/details/active-directory/

- Microsoft Intune: O Microsoft Intune é um serviço baseado em nuvem que se concentra no MDM (Gerenciamento de Dispositivo Móvel) e no MAM (Gerenciamento de Aplicativo Móvel). Este serviço permitirá o Ministério controlar como os dispositivos são usados para acesso aos dados corporativos, incluindo telefones celulares, tablets e laptops. Através dete serciço, é possíve ltambém configurar políticas específicas para controlar aplicativos. Por exemplo, é possível impedir que emails sejam enviados para pessoas de fora do MDR. O Intune também permite que os usuários do Ministério usem dispositivos pessoais para escola ou trabalho. Em dispositivos pessoais, o Intune ajuda a garantir que os dados o MDR permaneçam protegidos e pode isolar os dados da organização de dados pessoais de cada servidor.

Fonte: https://docs.microsoft.com/pt-br/mem/intune/fundamentals/what-is-intune

- Proteção de Informações do Azure P1: Este serviço fornece uma camada adicional ao controle e proteção de emails, documentos e dados confidenciais que que são compartilhados para fora do MDR, independentemente do local em que eles estão armazenados ou de com quem são compartilhados. Abaixo um quadro comparativo dos recursos.

RECURSO	GRATUITO	PROTEÇÃO DE INFORMAÇÕES DO AZURE PARA OFFICE 365	PROTEÇÃO DE INFORMAÇÕES DO AZURE PREMIUM P1	PROTEÇÃO DE INFORMAÇÕES DO AZURE PREMIUM P2
Consumo de conteúdo de Proteção de Informações do Azure usando contas corporativas ou de estudante de aplicativos e serviços com reconhecimento de política de Proteção de Informações do Azure	Disponível	Disponível	Disponível	Disponível
Proteção para conteúdo do Microsoft Exchange Online, Microsoft SharePoint Online e Microsoft OneDrive for Business	Não disponível	Disponível	Disponível	Disponível
BYOK (Bring Your Own Key) para ciclo de vida de provisionamento de chaves gerenciado pelo cliente2	Não disponível	Disponível	Disponível	Disponível

Modelos personalizados, incluindo modelos departamentais	Não disponível	Disponível	Disponível	Disponível
Proteção para conteúdo local do Exchange e do SharePoint por meio do conector do Rights Management	Não disponível	Disponível	Disponível	Disponível
Criação de conteúdo de Proteção de Informações do Azure usando contas corporativas ou de estudante	Não disponível	Disponível	Disponível	Disponível
Criptografia de mensagens do Office 365	Não disponível	Disponível	Disponível	Disponível
Controle administrativo3	Não disponível	Disponível	Disponível	Disponível
Kit para desenvolvedores de software de Proteção de Informações do Azure para proteção para todas as plataformas – Windows, Windows Mobile, iOS, Mac OSX e Android	Não disponível	Não disponível	Disponível	Disponível
Proteção para formatos de arquivo que não são do Microsoft Office, incluindo PTXT, PJPG e PFILE (proteção genérica)	Não disponível	Não disponível	Disponível	Disponível
Classificação de documentos em manual, padrão e obrigatório	Não disponível	Não disponível	Disponível	Disponível
Scanner da Proteção de Informações do Azure para descoberta de	Não disponível	Não disponível	Disponível	Disponível

conteúdo de arquivos locais correspondentes a qualquer um dos tipos de informações confidenciais				
Scanner da Proteção de Informações do Azure para aplicar um rótulo a todos os arquivos em um repositório ou servidor de arquivos local	Não disponível	Não disponível	Disponível	Disponível
Conector do Rights Management com compartilhamentos de arquivos do Windows Server locais usando o conector de FCI (Infraestrutura de Classificação de Arquivos)	Não disponível	Não disponível	Disponível	Disponível
Acompanhamento e revogação de documentos	Não disponível	Não disponível	Disponível	Disponível
O SDK (Kit de Desenvolvimento de Software) de Proteção de Informações da Microsoft para aplicar rótulos e proteção a emails e arquivos para todas as plataformas – Windows, iOS, Mac OSX, Android e Linux	Não disponível	Não disponível	Disponível	Disponível
Configurar as condições para classificação automática e recomendada	Não disponível	Não disponível	Não disponível	Disponível
Definir rótulos para aplicar automaticamente a	Não disponível	Não disponível	Não disponível	Disponível

proteção S/MIME pré-configurada no Outlook				
Controle o compartilhamento excessivo de informações ao usar o Outlook (avise, justifique ou bloqueie emails).	Não disponível	Não disponível	Não disponível	Disponível
HYOK (Hold Your Own Key) que engloba a Proteção de Informações do Azure e o AD (Active Directory) Rights Management para cenários altamente regulamentados	Não disponível	Não disponível	Não disponível	Disponível
Scanner da Proteção de Informações do Azure para proteção, rotulagem e classificação automatizadas de arquivos locais compatíveis	Não disponível	Não disponível	Não disponível	Disponível

Fonte: https://azure.microsoft.com/pt-br/pricing/details/information-protection/

- Microsoft Cloud App Security: O Microsoft Cloud App Security trabalha como um CASB (agente de segurança de acesso à nuvem) que dá suporte a vários modos de implantação, incluindo coleta de log, conectores de API e proxy reverso. A solução 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 até mesmo de terceiros.

Fonte: https://docs.microsoft.com/pt-br/cloud-app-security/what-is-cloud-app-security

- Microsoft Advanced Threat Analytics (ATA): O ATA (Advanced Threat Analytics) é uma plataforma local que contribui na proteção da organização contra vários tipos de ataques cibernéticos avançados e ameaças internas.

  O ATA aproveita um mecanismo de análise de rede proprietário para capturar e analisar o tráfego de rede de vários protocolos (como Kerberos, DNS, RPC, NTLM entre outros) para autenticação, autorização e coleta de informações. Essas informações são coletadas pelo ATA por meio de:

  - Espelhamento de porta de seus controladores de domínio e servidores DNS para o Gateway do ATA e/ou
  - Implantação de um LGW (Gateway Lightweight do ATA) diretamente nos Controladores de domínio

O ATA obtém informações de várias fontes de dados, como eventos e logs em sua rede, a fim de aprender o comportamento dos usuários e de outras entidades na organização e cria um perfil comportamental sobre eles. O ATA pode receber eventos e logs de:

- Integração do SIEM
- WEF (Encaminhamento de Eventos do Windows)
- Diretamente do Coletor de Eventos do Windows (para o Gateway Lightweight)

Fonte: https://docs.microsoft.com/pt-br/azure-advanced-threat-protection/what-is

- Proteção Avançada contra Ameaças do Azure (ATP): O ATP (Azure Advanced Threat Protection) 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 ao ambiente corporativo. Tais como:
    - 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

Fonte: https://docs.microsoft.com/pt-br/azure-advanced-threat-protection/what-is

- Microsoft Secure Score: Essa solução, permite avaliar qual o status de segurança atual da organização e identificar possíveis melhorias em todas as suas cargas de trabalho do Microsoft 365 com visibilidade centralizada do Secure Score.

- Azure Azure Rights Management (RMS): O Azure RMS é um serviço de proteção baseado em nuvem que usa políticas de criptografia, identidade e autorização para ajudar a proteger arquivos e emails entre vários dispositivos, incluindo telefones, tablets e PCs. As configurações de proteção permanecem com seus dados mesmo quando eles extrapolam os limites da sua organização, mantendo seu conteúdo protegido dentro e fora da organização.

Já a suíte Google Workspace apresenta alternativa (ainda que com funcionalidades limitadas em certos aspectos) apenas para o primeiro e segundo item, e não oferece alternativa similar para os demais produtos e funcionalidades presentes nos demais itens. Outra necessidade do MDR não coberta pela suíte Google Workspace é que está presente nos itens 1 e 2 da contratação é a disponibilidade de plataforma para o gerenciamento de dispositivos móveis Microsoft Intune, ferramenta que se tornou indispensável com o avanço do trabalho remoto em decorrência da pandemia do Coronavírus.

Outra das principais características que as ferramentas da suíte Google Workspace não preenchem é a possibilidade de implantação híbrida para as ferramentas de gestão de identidade e dos serviços de e-mail. Atualmente o MDR tem uma implementação híbrida do Active Directory e do Microsoft Exchange, com parte da gestão e do armazenamento sendo feita em ativos on premises, e parte em ambiente de cloud. A suíte Google Workspace não oferece alternativa para gestão híbrida desses recursos, forçando a migração da totalidade do serviço de e-mail para a nuvem e a utilização de uma solução de gerenciamento de identidade de

terceiros como o próprio Microsoft Active Directory, características estas que não contemplam os requisitos de negócio do MDR no presente momento.

A suíte do Google não conta ainda com ferramentas analíticas avançadas para detectar comportamentos irregulares de usuários e para mitigar riscos de identidade como o Azure Defender for Identity (antigo Azure ATP), e não oferecem o mesmo nível de integração que as ferramentas da Microsoft possuem entre a solução de identidade (Azure Active Directory) e as diversas soluções de segurança que fazem parte do portfólio da contratação, tais como as soluções de EDR (Defender ATP - Defender for Endpoints) e CASB (Cloud App Security).

As ferramentas do Google Workspace não são complemente aderentes ainda à aspectos regulatórios presentes nas normas aplicáveis à administração federal, notadamente à Norma Complementar nº 14 da Instrução Normativa nº 1/2008 do DSIC/GSI, em relação à residência dos dados armazenados em nuvem. Enquanto é possível, no caso das ferramentas Office 365, verificar que os dados do Exchange Online residem em datacenters no Brasil, para os serviços do Google Workspace é informado que as opções de localidade de dados são apenas Estados Unidos e Europa, conforme pode ser confirmado em consulta ao endereço https://support.google.com/a/answer/7630496?hl=en#zippy=%2Cstep-view-data-regions-progress.

Por fim, é relevante destacar os investimentos feitos pelo MDR na implantação de soluções corporativas que fazem uso intensivo de ferramentas presentes no Microsoft Office 365, como é o caso dos sites equipe e colaboração desenvolvidos no SharePoint Online, as ferramentas institucionais de acompanhamento de projetos que fazem uso da solução Microsoft Project integrada ao Sharepoint (Project Web Access) e ainda as integrações e automações realizadas por meio das ferramentas flow/power automate que integram funcionalidades de diferentes aplicações, como o Microsoft Teams, Sharepoint, etc. Todo o desenvolvimento e investimento feito para o uso integrado das ferramentas seria instantaneamente perdido no caso da substituição da plataforma, o que traria enorme prejuízo para a produtividade do órgão e para o serviços públicos por ele prestados.

Em relação ao principais recursos observados nas soluções da Microsoft e Google, segue abaixo comparativos:

Plano	G Suite			Office 365					
	Basic	**Business**	**Enterprise**	**F1**	**F1 + EOP1**	**F1 + EOA**	**E1**	**E1 + EOA**	**E3**
Armazenamento de correio eletrônico na nuvem / usuário	30 GB compartlhados com G Drive	Ilimitado	Ilimitado	2 GB	50 GB	2 GB + archivamento ilimitado	50 GB	100 GB + archivamento ilimitado	100 GB + archivamento ilimitado
Caixas de Correio Compartilhadas	-	-	-	50 GB	50 GB	50 GB	50 GB	50 GB	100 GB
Caixas de Correio de recursos	30 GB compartilhad	Ilimitado	Ilimitado	50 GB	50 GB	50 GB	50 GB	50 GB	50 GB

	os com G Drive								
Pastas públicas	-	-	-	-	50 GB	-	50 GB	50 GB	100 GB
Caixas de Correio de grupo	-	-	-	50 GB	50 GB	50 GB	50 GB	50 GB	50 GB
Arquivamento de correio eletrônico, eDiscovery	-	Ilimitado	Ilimitado	-	-	Ilimitado	50 GB	Ilimitado	Ilimitado
Retenção Legal	-	Incluído	Incluído	-	-	Incluído	-	Incluído	Incluído
Notas para arquivamento	Google Vault é capaz de capturar todas as mensagens enviadas e recebidas (independente da ação do usuário) e mentê-las armazenadas para consultas/exportações subsequentes. Só está disponível nas versões Business ou Enterprise.			Mecanismo similar ao Google Vault (journaling) pode ser configurado em qualquer plano do Office 365. O arquivamento e eDiscovery estão disponíveis em vários planos, limitados a um espaço de armazenamento ou ilimitado. Através do mecanismo de retenção legal que está disponível no plano E3 ou através de Add-On, qualquer mensagem enviada, recebida ou modificada em qualquer caixa de correio ou pastas se manterão no arquivamento. Realizar o registro em outra caixa postal ou em pastas públicas é posSimvel arquivar/capturar todas as mensagens enviadas e recebidas (equivalente à solução Google).					
Armazenamento de arquivos na nuvem									
Tamanho do Armazendamento Standard	30 GB compartlhado com G Drive	Ilimitado	Ilimitado	-	-	1TB	1TB	1TB	Ilimitado
Arquivamento de arquivos	-	Não	Não	Não	Não	Não	Não	Não	Sim
Arquivamento de mensageria instantânea	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Prevenção a Perda de Dados									
Proteção da informação enquanto os dados se armazenam na plataforma (correio eletrônico e arquivos)	Não	Não	Sim	Não	Não	Não	Não	Não	Sim
Proteção da informação fora da plataforma	Não	Não	Não	Não	Não	Não	Não	Não	Sim
Delegação									

Delegação de contatos, correio eletrônico e calendário	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Outlook (cliente do correio eletrônico)									
Sincronização Email, Agenda e Contato	Sim, MAPI con la herramienta Gasmo			Sim, MAPI, soporte nativo					
Microsoft Office Pro Plus (cliente instalado na máquina)	Não	Não	Não	Não	Não	Não	Não	Não	Sim. Office Pro Plus (5 desktops)
Inteligencia artificial para apoiar a criação de conteúdo	Não	Não	Não	Não	Não	Não	Não	Não	Sim
Configuração e atualização mediante tecnologia de streaming	Não	Não	Não	Não	Não	Não	Não	Não	Sim
Soporte de entrada de lápiz	Não	Não	Não	Não	Não	Não	Não	Não	Sim
Observações	G-Suite realiza a conversão de documentos do Office a um formato nativo e permite a edição neste novo arquivo. O processo de conversão introduz algumas incompatibilidades de formato e modificação de conteúdo que pode ou não ser importante. Um exemplo é a modificação de cabeçalhos e rodapés de imagens, imagens, índices, equações no Excel, perda de macros, etc.			-	-	-	-	-	Office Pro Plus requer Windows 7 ou versões posteriores
Aplicações web na nuvem									
Editor de Textos	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Compatibilidade com Microsoft Word	Conversão/Limitada	Conversão/Limitada	Conversão/Limitada	100%	100%	100%	100%	100%	100%
Editor de apresentações	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Compatibilidad com PowerPoint	Conversão/Limitada	Conversão/Limitada	Conversão/Limitada	100%	100%	100%	100%	100%	100%
Planilhas	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Compatibilidad con Excel	Conversão/Limitada	Conversão/Limitada	Conversão/Limitada	100%	100%	100%	100%	100%	100%
Macros	Script da aplicação do Google (não é compatível com o script de VB Office)	Script da aplicação do Google (não é compatível com o script de VB Office)	Script da aplicação do Google (não é compatível com o script de VB Office)	VB Script	VB Script	VB Script	VB Script	VB Script	VB Script
Formas	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Gerencia de Projetos	Não	Não	Não	Limited	Limited	Limited	Sim	Sim	Sim
Anotações e acompanhamentos de reuniões	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Chat mobile e automatização de processos de negócios	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Workflows	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Narración	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Análise e Estatísticas Pessoais	Não	Sim (beta)	Sim (beta)	Sim	Sim	Sim	Sim	Sim	Sim
Gestão de turnos/horários	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Vídeo corporativo e TV empresarial	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Gestão de Conhecimento	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim
Aplicações Móveis e Web sem código	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Colaboração em tempo real na Web	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Colaboração em tempo real entre web e clientes Office Pro Plus	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Edição Offline	Limited	Limited	Limited	Outlook	Outlook	Outlook	Outlook	Outlook	Sim
Revisão/Controle de versões	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Sincronização de arquivos armazenados localmente	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Comunicação									
Mensageria instantânea, chamadas de voz e video conferencias	Sim (25 pessoas)	Sim (25 pessoas)	Sim (50 pessoas)	Sim (250 pessoas)	Sim (250 pessoas)	Sim (250 pessoas)	Sim (250 pessoas)	Sim (250 pessoas)	Sim (250 pessoas)
Eventos corporativos online (audio/video)	Não	Não	Sim	Sim (consumo)	Sim (consumo)	Sim (consumo)	Sim (consumo)	Sim (consumo)	Sim (consumo e produção)
Capacidade de integração a redes RTC locais	Não	Não	Sim (USA e Canadá) - ou com solução de terceiros	Sim	Sim	Sim	Sim	Sim	Sim
Capacidade de designar números de telefone locais para que usuários de RTC se juntem à reunião (audio conferencing)	Somente USA	Somente USA	Sim	Não	Não	Não	Add-on (direto com Microsoft)	Add-on (direto com Microsoft)	Add-on (direto com Microsoft)
Site Intranet									
Site Intranet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Administração de conteúdo e fluxos de trabalho de publicação	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Fluxo de trabalho de soluções múltiplas para integração	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Rede Social									
Rede Social	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Eventos ao vivo na rede social	Não	Não	Não	Sim (consumo)	Sim (consumo)	Sim (consumo)	Sim (consumo)	Sim (consumo)	Sim (consumo y producion)
Seguranças e SPAM									

Antispam e proteção contra vírus	SPF (Sender Policy Framework) DKIM (Domain Key Identified Mails) DMARC			SPF (Sender Policy Framework) DKIM (Domain Key Identified Mails) DMARC					
Filtro antispam personalizado	Listas brancas e negras para dominio, IP e correio eletrônico Filtros de conteúdo			Listas brancas e negras para dominio, IP e correio eletrônico. Filtros de conteúdo					
Criptografia SSL	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Autenticação de 2 fatores com SMS	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Quarentena	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Certificações	ISO 27001,FISMA,SSAE 16/SAE 3402 Type II,SAS 70			ISO 27001,FISMA, FERPA, HIPAA-HITECH,EU MODEL CLAUSES, UK G- CLOUD IL2 & CJIS O Office 365 possui mais de 60 certificações internacionais de privacidade, conformidade e segurança.					
Suporte S/MIME	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Criptografia de correio eletrônico fora da borda	Não	Não	Não	Não	Não	Não	Não	Não	Sim
Suporte									
Comunidade / Suporte Distribuidor	Direto (remoto), foruns e parceiro			Suporte gratuito, foruns, parceiros, distribuidores, acordo direto da Microsoft para cenários de integração avançada ou outra cobertura de serviços (se necessário)					
Suporte 24x7 Empresa	Telefone e email			Telefone e correio eletrônico (gratis), opção direta com o fabricante (opcional)					
Disponibilidade 99.9% com SLA	99,90%			99,90 %					
Active Directory / LDAP									
Integração de Active Directory	Sim (replicação de identidades)			Sim (replicação de identidades)					
Replicação de contrasenha de Active Directory	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
SSO com credenciais Windows	Não (requer solução de terceiros)	Não (requer solução de terceiros)	Não (requer solução de terceiros)	Sim	Sim	Sim	Sim	Sim	Sim
Dispositivos móveis									
Correio eletrônico e calendário	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)

Editor de textos	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Planihas	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Editor de apresentaçõ es	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Formas	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Gerencia de Projetos	Não	Não	Não	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Anotações e acompanha mentos de reuniões	Não	Não	Não	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Chat mobile e automatizaçã o de processos de negócios	Não	Não	Não	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Workflows	Não	Não	Não	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Narrativas	Não	Não	Não	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Gestão de turnos / horários	Não	Não	Não	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Vídeo corporativo e TV empresarial	Não	Não	Não	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Aplicações móveis e Web sem código	Não	Não	Não	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)	Sim (iOS, Android)
Gestão de dispositivos móveis	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Integração com outras aplicações									

Integração com terceiros	Sim (mais de 5000 apps)	Sim (mais de 5000 apps)	Sim (mais de 5000 apps)	Sim. Milhares de aplicações estão disponíveis para integração direta com Office 365.					
Aplicações construídas sob medida	Sim, API completa, Google script, SSO e suporte SSL			Sim. Existem milhares de aplicações criadas por parceiros e pela Microsoft que se comunicam com o serviço através das APIs do Office. Existem APIs REST baseadas em um modeli chamado Microsoft Graph que permite a criação de aplicações que realizam operações administrativas e em dados da plataforma. Estas aplicações utilizam SSL, SSO, scripts, etc.					
Ferramentas de copia de segurança de dados									
Exportación de datos	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Ferramentas de Relatório									
Email Log Search / Tracking	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Uso de correio electrônico	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Atividade das Contas	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Informes administrativos	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Gestão de ferramentas de terceiros	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Alertas de administração	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Comparação Microsoft 365 vs G-Suite Security and Compliance

Proteção contra ameaças (correio eletrônico)			
Funcionalidade	**G-Suite Business**	**Office 365 E1 + EOA + ATP**	**Comentários**
Proteção aos usuários de correio eletrônico contra ataques cibernéticos avançados utilizando aprendizado de máquina e inteligência artificial	Atende	Atende	O Office 365 oferece esta proteção através do Advanced Threat Protection (O365 ATP)

Proteção contra malware ou virus desconhecidos com zero dias. Todas as mensagens e anexos que não possuem uma assinatura conhecida de virus/malware são roteados a um ambiente especial isolado onde técnicas de análise especificas são utilizadas para detecção (Safe Attachments)	Atende Parcialmente	Atende	O Office 365 oferece esta proteção através do Advanced Threat Protection (O365 ATP). O Google menciona na documentação que esta feature não substitui software AV/Anti Malware e que não é recomendado usar sem auxílio de tal proteção.
Proteção proativa dos usuários contra links maliciosos enviados em mensagens de correio eletrônico. Links são substituidos nas mensagens por um mecanismo de deteção e teste antes de permitir acesso aos usuários (Safe Links)	Atende	Atende	O Office 365 oferece esta proteção através do Advanced Threat Protection (O365 ATP)
Deteção de comportamento onde o remetente envia mensagens como se fosse outro usuário em sua organização (Spoof intelligence)	Atende	Atende	O Office 365 oferece esta proteção através do Advanced Threat Protection (O365 ATP)
Mensagens identificadas como spam, bulk mail, phishing, contend malware ou que casem com regra específica criada pelo administrador são redirecionada a um ambiente apartado onde o usuário tem a opção de bloquear ou liberar mensagens (Quarantine)	Atende	Atende	
Suporte a implementações e proteção aos ambiente híbridos, com servidores de correio abrigados on-premises e na nuvem (Hybrid Protection)	Atende	Atende	
Roteamento de mensagens em ambiente híbrido, onde parte dos usuários se encontram na nuvem e parte on-premises sob o mesmo domínio de correio eletrônico (Hybrid Mail Routing)	Atende	Atende	
Configuração de tráfego de correio eletrônico Seguro (criptografado) entre domínios	Atende	Atende	

específico através de Transport Layer Security (TLS).			
Disponibilidade de plug-ins e opção na interface web para que os usuários reportem eventuais mensagens que escapam da proteção de SPAM para análise (Junk Mail Reporting).	Atende	Atende	
Proteção contra virus e SPAM através de multiplos motores de detecção (Conventional AV/Malware detection)	Atende	Atende	
Capacidade de encriptação de mensagens para qualquer destinatário através de geração, gerenciamento, atribuição e comprovação de chaves de criptografia e identidades (Office 365 Message Encryption)	Não atende	Atende	Disponível com o Azure Information Protection ou para clientes dos planos E3 ou superiores. Google implementa esta feature através do G-Suite Message Encryption (GAME) oferecido pela Zix.
Geração e disponibilidade de logs de auditoria e tracking de mensagens enviadas ou recebidas pela plataforma de correio eletrônico.	Atende	Atende	
Relatórios de proteção do correio eletrônico disponíveis em planilhas compatíveis com o Excel ou através de web services (REST/Odata) disponíveis para acesso de sistemas de relatório	Atende Parcialmente	Atende	Google não oferece relatórios em formato excel ou APIs para extração de relatórios via REST. Relatórios de correio eletrônico estão limitados a entrega, spam e criptografia conforme documentação.
Administradores podem usar scripts remotos para realização de tarefas administrativas como criação de regras de transporte especificas, atualização de listas de bloqueio, configuração de quarentena, etc	Atende Parcialmente	Atende	Google apps scripts are limited to macros, custom functions, menus, dialogs and add-ons to G-Suite products. Some APIs are available for Python and other scripting languages.

Gerenciamento de dispositivos móveis			
Funcionalidade	**G-Suite Business**	**Office 365 E1 +**	**Comentários**

		EOA + ATP	
Suporte a dispositivos Windows Phone 8.1+, iOS 7.1+, Android 4+, Windows 8.1+, Windows 10+ (Device Support)	Atende Parcialmente	Atende Parcialmente	De acordo com a documentação do Google, apenas dispositivos Apple a partir da versão 8 são suportados. O gerenciamento de aplicações só é suportado em Android 5 ou iOS 8, profiles apenas no Android 5. A versão básica do MDM no Office 365 não suporta gerenciamento de aplicações.
Controle de acesso baseado em regras para o correio eletrônico, arquivos e aplicações de edição de conteúdo em núvem compatíveis (Access Control)	Atende Parcialmente	Atende	O MDM do G-Suite não permite nenhum controle de acesso aos sistemas de correio baseado em condições do dispositivo. Ele controla a presença ou não das aplicações, direitos de uso, senhas, etc, mas não é possível restringir o acesso a um determinado serviço. Algumas restrições são possíveis apenas nos dispositivos android.
Obrigação de exigir senha de acesso para cada desbloqueio do dispositivo móvel (Password to Access)	Atende	Atende	
Reset (wipe) apenas de dados corporativos e não da totalidade dos dados armazenados no dispositivo móvel (Corp Data Wipe only)	Atende Parcialmente	Atende	O Google permite esta funcionalidade apenas nos dispositivos móveis android, através do recurso de Work Profile.
Prevenir contra a definição e uso de senhas simples pelos usuários (Simple Passwords)	Atende	Atende	
Definição do número de tentativas com senhas incorretas antes de realizar um reset do dispositivo móvel	Atende	Atende	
Definição de tempo de inatividade antes de	Atende	Atende	

bloquear o dispositivo móvel			
Definição de dias para expiração da senha de acesso do dispositivo móvel	Atende	Atende	
Gerenciamento do ciclo de vida (instalação/remoção) de aplicações nos dispositivos móveis	Atende Parcialmente	Não Atende	O Google só suporta ciclo de vida dos aplicativos em dispositivos android e iOS. Apenas whitelists e aprovações individuais são suportadas.
Exigir criptografia nos dispositivo móveis	Atende	Atende	
Bloquear acesso de dispositivos violados (jailbreak)	Atende	Atende	
Criação e gerenciamento dos perfis de acesso ao correio eletrônico remotamente	Atende Parcialmente	Atende Parcialmente	O Google permite apenas para o Android através dos Work Profiles e a Microsoft apenas para iPhones e Windows Phones
Bloquear sincronização de dados de diagnóstico dos dispositivos	Não Atende	Atende Parcialmente	Google não suporta este bloqueio, Microsoft suporta apenas em alguns dispositivos.
Bloquear acesso à loja de aplicativos	Atende Parcialmente	Atende Parcialmente	Ambos os provedores suportam esta funcionalidade em parte dos sistemas operacionais dos dispositivos

Gerenciamento de aplicações e dispositivos (incluindo PCs)			
Funcionalidade	**G-Suite Business**	**Microsoft Intune**	**Comentários**
Permitir aos usuários o registro e gerenciamento de devices móveis e computadores pessoais (Mobile and PC Enrollment)	Atende Parcialmente	Atende	Google suporta apenas dispositivos móveis, PCs não são suportados.
Proteção de dados corporativos incluindo correio eletronico, aplicações e arquivos de acordo	Atende Parcialmente	Atende	Google não suporta proteção e controle de dados em PCs.

com o estado de registro do dispositivo móvel ou computador pessoal (Corporate Data Protection)			Controles avançados disponíveis apenas no Android.
Gerenciamento do ciclo de vida de aplicações instaladas nos dispositivos móveis registrados (App Management for Mobile)	Atende Parcialmente	Atende Parcialmente	Ambas soluções possuem limitações do que pode ser realizado nos dispositivos móveis. Limitações relacionadas ao suporte ou whitelist apenas.
Gerenciamento do ciclo de vida de aplicações instaladas nos computadores pessoais (App Management for PC)	Não Atende	Atende	Google não suporta ciclo de vida de aplicações nos PCs.
Inventário de aplicações instaladas nos dispositivos móveis e computadores corporativos e pessoais usados para acesso aos dados corporativos (Inventory)	Atende Parcialmente	Atende	Inventário apenas disponível para dispositivos móveis no Google.
Integracão com o System Center Configuration Manager para permitir uma mesma experiência administrativa em servidores, estações de trabalho e dispositivos móveis utilizados para acesso ou armazenamento de dados corporativos (SCCM Integration)	Não Atende	Atende	Google não possui integração com SCCM
Sem necessidade de manter infra-estrutura de gerenciamento on-premises (No On-prem Infrastructure)	Atende	Atende	
Capacidade de criar políticas de restrição para aplicações em dispositivos registrados, permitindo ao administrador bloquear copy/paste/save as, além de obrigar criptoigrafia e remover dados corporativos sem qualquer alteração nos dados pessoais (Mobile Application Management)	Atende Parcialmente	Atende	Google permite apenas remover dados corporativos em dispositivos Android com Work Profiles. Não possui esta funcionalidade em outros sistemas operacionais e não oferece controle de ações nos aplicativos.
Controle de acesso condicional permitindo que apenas dispositivos registrados e	Não Atende	Atende	Google não oferece controle de acesso condicional.

autorizados tenham a capacidade de acesso aos dados corporativos (Conditional Access)			
Políticas de controle específicas para as aplicações Office Mobile permitindo o controle de cópia, colagem, gravação bem como acesso condicional aos serviços do Office 365 (Office Mobile Control)	Não Atende	Atende	Não existem controles diferenciados para aplicações Office no Google G-Suite.
Determinação de condições de cumprimento e monitoração dos dispositivos contra as condições definidas como mínimas para acesso aos dados corporativos (Device Compliance)	Não Atende	Atende	O Google não oferece relatórios ou controles de compliance para dispositivos registrados no MDM
Distribuição e atualizações para os sistemas operacionais Windows 10 (OS Updates)	Não Atende	Atende	Atualizações de sistemas operacionais não são suportadas pelo MDM do Google.
Execução de ações remotas em dispositivos móveis, incluindo remoção de dados corporativos, reset total, bloqueio remoto, reset de senha de acesso, bypass do bloqueio de ativação, fresh start, modo de perda do dispositivo, localização do dispositivo, restart, controle remoto para dispositivos android, sincronização remota do dispositivo móvel (Device Management).	Atende Parcialmente	Atende	Parte destas features são suportadas pelo MDM do Google.

Compliance			
Funcionalidade	**G-Suite Business**	**Office 365**	**Comentários**
Gerenciamento centralizado das regras de cumprimento oferecendo avaliações de risco de segurança, informações obtidas do comportamento dos usuários, logs e processos	Não Atende	Atende	Disponíveis nos planos E3 e E5. Não disponível no Google G-Suite.

Localização previsível dos dados. O cliente sabe sempre os dados se localizam.	Não Atende	Atende	A Microsoft divulga a localização dos centros de dados e onde as cópias são mantidas. O Google possui uma arquitetura que não permite controle sobre a localização geográfica dos dados.
Possibilidade de importação e injestão de dados para permitir governança e cumprimento de normas em várias plataformas.	Não Atende	Atende	O Google não oferece serviço de injestão de dados na plataforma G-Suite.
Arquivamento, incluindo auto expansão e arquivamento de modificações realizadas em draft ou durante composição de mensagens	Atende Parcialmente	Atende	Google Vault se baseia em mecanismo de ournaling para arquivamento. Não detecta modificações realizadas nas caixas postais ou em draft.
Possibilidade de criação de políticas de retenção e expiração de dados	Atende	Atende	
Gerenciamento de registros para classificação pelo usuários final, com revisão manual e definição de disposição de dados, além de relatórios e controle de permissões.	Não Atende	Atende	Classificação por labels no Google está disponível como um recurso de organização no Gmail, não como ferramenta para definição de regras de proteção, arquivamente ou compliance. Disponível com o EOA e nos pacotes E3 e E5 do Office 365.
Classificação automática para aplicação de etiquetas nos arquivos e mensagens baseadas no tipo de dados, sensibilidade, consultas ou palavras chave.	Não Atende	Atende	Classificação automática baseada em sensibilidade, palabras chave ou tipo de dados está dispoíbel como add-on ou para os clientes do pacote E5.
Retenção baseada em eventos para disparar retenção customizada de dados	Atende Parcialmente	Atende	Regras de retenção podem ser criadas para artefatos produzidos por um certo grupo de pessoas ou armazenados sob detemrinadas condições. Google não oferece este recurso.
Ferramentas de gerenciamento de casos investigativos que podem combinar dados de múltiplos sistemas, suporte a pesquisas e exportação.	Não Atende	Atende	

Permite implementação de autorizações explicitas de acesso aos dados para os clientes durante execução de operações de suporte ou de serviço	Não Atende	Atende	Cloud LockBox permite aprovações prévias do cliente no acesso aos dados corporativos ou dos usuários que porventura sejam necessários para suporte ou por questões operacionais.
APIs REST para acesso aos eventos gerados pelos usuários ou transações na plataforma	Não Atende	Atende	

Proteção contra ameaças (geral)			
Funcionalidade	**G-Suite Business**	**Microsoft 365**	**Comentários**
Proteção de aplicações e informações contra ataques através de políticas granulares	Não Atende	Atende	Microsoft Cloud App Security. Office 365 ATP
Proteção dos dispositivos móveis e estações de trabalho contra ataques através de tecnologias de proteção embarcadas	Não Atende	Atende	Windows Defender Antivirus, Smartscreen, App/Device / Exploit Guard, WDATP
Proteção através de toda a infra-estrutura híbrida contra ataques cibernéticos	Não Atende	Atende	Azure Security Center
Detecção de comportamento anormal no uso de identidades na nuvem ou na infra-estrutura on-premises	Não Atende	Atende	Azure Advanced Threat Protection (ATP). Microsoft Advanced Threat Analytics (ATA).
Detecção de comportamento anormal em aplicações de nuvem	Atende Parcialmente	Atende	Cloud App Security

Gerenciamento de Segurança			
Funcionalidade	**G-Suite Business**	**Microsoft 365**	**Comentários**
Habilidade de gerenciar nuvem, on-premises ou ambiente híbrido	Atende Parcialmente	Atende	Google faz somente na nuvem
Visibilidade do estado de segurança dos usuários	Atende	Atende	Azure Active Directory

Controles para definir politicas e controles consistentes de segurança para os usuários	Atende	Atende	Azure Active Directory
Inteligência integradas e recomendações para usuários	Atende	Atende	Azure AD Identity Protection Security Reports
Visibilidade do estado de segurança dos dispositivos	Atende Parcialmente	Atende	Windows Defender Advanced Threat Protection. Google faz somente pra Android.
Controles para definir políticas e controles consistentes de segurança para dispositivos	Atende Parcialmente	Atende	Microsoft Intune ou System Center Configuration Management. Google faz somente para Android.
Inteligência integrada e recomendações para dispositivos	Atende Parcialmente	Atende	Microsoft Intune ou System Center Configuration Management. Google faz somente para Android.
Visibilidade do estado de segurança dos apps e dados	Atende Parcialmente	Atende	Security and Compliance Center. Google faz somente para Apps.
Controles para definir políticas e controles consistentes de segurança para apps e dados	Atende Parcialmente	Atende	Security and Compliance Center. Google faz somente para Apps.
Inteligência integrada e recomendações para apps e dados	Atende Parcialmente	Atende	Security and Compliance Center. Google faz somente para Apps.
Visibilidade de segurança do estado de segurança de workloads através de uma infraestrutura híbrida	Não Atende	Atende	Azure Security Center
Controles para definir políticas e controles consistentes de segurança para workloads através de uma infraestrutura híbrida	Não Atende	Atende	Azure Security Center

Inteligência integrada e recomendações para workloads através de uma infraestrutura híbrida	Não Atende	Atende	Azure Security Center

Identidades			
Funcionalidade	**G-Suite Business**	**Microsoft 365**	**Comentários**
Proteger a porta da frente através de acesso controlado, com MFA (Multi-Factor of Authentication).	Atende	Atende	
Habilidade de conceder políticas de acesso condicional baseadas no estado do dispositivo, sensibilidade da aplicação e localização do usuário.	Não Atende	Atende	Azure Active Directory Premium P1
Levantamento em tempo real dos riscos de autenticação / usuário baseado em dados analisados por machine learning provenientes de dispositivos, apps, email	Não Atende	Atende	Azure Active Directory Premium P1
Proteger acesso a apps 1st e 3rd party, on premises e na nuvem	Atende Parcialmente	Atende	Google faz Somente nuvem 1st party
Proteção de senha com duplo fator de autenticação que pode utilizar PIN ou biometria no seu PC	Não Atende	Atende	Windows Hello
Proteção para credenciais do usuário e administrador de chaves roubadas usadas para criar um ataque “Pass the Hash” com tokens ou usuários impersonate	Não Atende	Atende	Windows Credential Guard
Habilidade para descobrir, restringir e monitorar identidades privilegiadas	Não Atende	Atende	Azure AD Privileged Identity Management
Medidas de segurança em conformidade com GDPR para proteçao e privacidade de dados e usuários	Atende	Atende	

Proteção da Informação			
Funcionalidade	**G-Suite Business**	**Microsoft 365**	**Comentários**

Detecção, classificação e proteção de informações sensíveis no Office 365	Não Atende	Atende	Office 365 Advanced Data Governance
Detecção, classificação e proteção de informações sensíveis no Google Cloud	Atende	Atende	Microsoft Cloud App Security
Detecção, classificação e proteção de informações sensíveis no contidas em aplicações SaaS de terceiros	Não Atende	Atende	Microsoft Cloud App Security
Detecção, classificação e proteção de informações sensíveis armazenadas em servidores de arquivos locais	Não Atende	Atende	Azure Information Protection
Aplicar classificação de sensibilidade que persistem com os arquivos conforme navegam entre dispositivos, apps, services	Não Atende	Atende	Office 365 Advanced Data Governance, AIP
Bloquear compartilhamento ou envio inapropriado de conteúdo com dados sensíveis	Não Atende	Atende	Office 365 DLP
Customizar e ajustar políticas de proteção de informação	Atende	Atende	Office 365 Advanced Data Governance
Detectar uma grande quantidade de tipos de Informação pre-definidos (out-of-the-box)	Não Atende	Atende	Office 365 Advanced Data Governance e DLP
Recomendações de poítica baseadas em informações potencialmente sensíveis detectadas no ambiente	Não Atende	Atende	Office 365 Advanced Data Governance e DLP
Proteger Informação em dispositivos perdidos ou roubados através de criptografia, remoção de armazenamento e wipe remoto	Atende Parcialmente	Atende	Windows Information Protection & BitLocker. Google faz somente wipe remote.
Proteger dados de negócio em dispositivos Windows 10 permitindo divisão e contenção de informações de negócio	Não Atende	Atende	Windows Information Protection & BitLocker
Proteger dados de serem transferidos ou compartilhados em aplicação que não são de negócio, em dispositivos iOS e Android	Atende Parcialmente	Atende	Intune MDM/MAM. Google apenas no Chromebook.

Enviar emails protegidos (criptografados) para recipients internos e externos (mesmo que o recipiente use uma conta de consumidor)	Atende	Atende	Office 365 Message Encryption
Ticas de poíticas e notificações de usuário final (dentro da aplicação) quando há um trigger the política	Não Atende	Atende	AIP, O365 DLP
Automaticamente retém e deleta documentos no Office 365	Não Atende	Atende	Office 365 Advanced Data Governance
Monitorara eventos e violações de poíticas de proteção da informação	Atende	Atende	Office 365 Advanced Data Governance
Monitorar acesso e compartilhamento de documentos	Atende	Atende	Azure Information Protection
Monitorar uso de apps de nuvem	Não Atende	Atende	Cloud App Security
API para permitir eventos e atividades de proteção da Informação para ser compartilhado com SIEM de 3rd party e outros sistemas	Atende	Atende	Office 365 Management Activity API
API para permitir que serviços e apps 3rd party extendam seus cenários de segurança ou experiencias customizadas de apps	Não Atende	Atende	Information Protection SDK

Já em relação a escolha da manutenção da Nuvem Pública, o Microsoft Azure AZURE, desde o ano de 2017 o Ministério do Desenvolvimento Regional tem feito uso cada vez mais uso dos serviços de computação em nuvem Microsoft Azure, que foram adquiridos por meio do Contrato 18/2017-MI, para vários de seus projetos, o principal deles, o PISF (PISF - Projeto de Integração do Rio São Francisco com as Bacias do Nordeste Setentrional). 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.

Posto isto, para os projetos em andamento no Ministério Desenvolvimento Regional, a solução considerada viável é a realização de processo de contratação para a manutenção e ampliação dos serviços atualmente prestados pela nuvem Microsoft Azure. O principal motivo para essa conclusão é que o principal projeto em curso no Ministério do Desenvolvimento Regional, uma vez que, conforme já considerado acima neste documento, para adoção de uma nova tecnologia, deve-se levar em consideração não apenas o custo da atual em relação a outra, mas também, todo o custo relacionado à migração para uma nova plataforma, mão de obra especializada para uma tecnologia inexistente até então no MDR, capacitação, curva de aprendizagem, dentre outros.

Nesta linha, a equipe de sustentação do ambiente de TIC do Ministério do Desenvolvimento Regional, tem constantemente investido na obtenção de mais conhecimento técnico para melhor utilização da nuvem Microsoft Azure, 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 MDR 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 em curso na DTIC implicaria em paralisação de serviços hoje providos continuamente para diferentes áreas do Ministério, além de implicar ainda na necessidade de gastos adicionais, que não só os referente a aquisição da nova plataforma.

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 MDR 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 do Desenvolvimento Regional, 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 do Desenvolvimento Regional 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. Já a Reserva de Instância, permite ao MDR realizar reserva de recursos/serviços no Azure com antecedência e compromisso de uso por um período de 12 ou 36 meses, essa reservas de recursos/serviços pode resultar em uma redução de até 70% no custo inicial do serviço em nuvem. Este percentual irá variar do DataCenter e tipo de recursos que estão sendo contratados com antecedência.

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

- **Microsoft Power BI:** Atualmente toda a camada de visualização de dados analíticos do Ministério do Desenvolvimento Regional, está implementada no Microsoft Power BI, solução nativamente integrado ao Microsoft Azure e outras bases existentes no Ministério, uma eventual migração de plataforma tecnológica poderia trazer prejuízos na disponibilização desses dados até sua correta adequação. Atualmente os dados podem ser consultados no endereço público: http://paineis.mdr.gov.br/
- **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 do Desenvolvimento Regional 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 MDR. Como proposta de evolução desta plataforma para garantir maior proteção aos usuários, informações e infraestrutura de TI do Ministério do Desenvolvimento Regional, 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 do Desenvolvimento Regional 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;

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, altamente utilizados no MDR. Consideramos que este cenário é bastante representativo do todo, pois estes softwares sustentam parcela significativa dos sistemas corporativos em uso atualmente no Ministério do Desenvolvimento Regional. Serão considerados na análise apenas os principiais 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 do Desenvolvimento Regional:

- 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

* Foi considerado o acréscimo de licenças SQL Server Enterprise para 04 VCPUs (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 do desenvolvimento Regional, e, no cenário considerado, fica demonstrada a grande vantajosidade econômica da opção pela nuvem Azure quando considerada a utilização do Benefício Híbrido.

II.4 DA ILEGAL CONSOLIDAÇÃO DAS LICENÇAS A SEREM CONTRATADAS NUM EDITAL ÚNICO: PARCELAMENTO DO OBJETO OBRIGATÓRIO NO CASO CONCRETO

- **II.4.1 A conveniência do parcelamento do objeto, expressamente, recomendada pela legislação para a promoção da maior competitividade do certame**
  - **a) Falta de comprovação de ganho de economias de escala com o não-parcelamento do objeto**
  - **b) A restrição ao parcelamento por modalidade contratual do fabricante.**

- **II.4.2 Possibilidade de divisão mais benéfica à Administração comparada à proposta pelo Edital**

Com o objetivo de ampliar a competividade e gerar mais economia, a Lei nº 8.666/93 estabeleceu em seu artigo 23, §1º, a obrigatoriedade da Administração Pública em promover o parcelamento do objeto, quando houver viabilidade técnica e econômica para tanto.

Ocorre que o raciocínio de parcelamento ou adjudicação por itens não deve ser levado a termos absolutos, pois a divisão da pretensão contratual, em alguns casos, pode prejudicar a economia de escala e gerar outros custos relacionados aos diversos contratos, além de potencializar riscos e dificuldades na gestão de uma pluralidade de contratos autônomos para atendimento da mesma pretensão contratual.

O Tribunal de Contas da União - TCU já entendeu que seria legítima a reunião de elementos de mesma característica, quando a adjudicação de itens isolados onerar "o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a celeridade processual", o que pode comprometer a seleção da proposta mais vantajosa (Acórdão 5301/2013 - Segunda Câmara. Rel. Ministro André Luís de Carvalho).

Somando-se a insto, este mesmo Tribunal de Contas da União, no Acórdão nº 732/2008, se pronunciou no sentido de que "a questão da viabilidade do fracionamento deve ser decidida com base em cada caso, pois cada obra tem as suas especificidades, devendo o gestor decidir analisando qual a solução mais adequada no caso concreto".

Adicionalmente, o Professor Jorge Ulisses Jacoby Fernandes, no Parecer nº 2086/00, elaborado no Processo nº 194/2000 do TCDF, ensina que:

> "Desse modo a regra do parcelamento deve ser coordenada com o requisito que a própria lei definiu: só se pode falar em parcelamento quando háviabilidade técnica para sua adoção. Não se imagina, quando o objeto é fisicamente único, como um automóvel, que o administrador esteja vinculado a parcelar o objeto. Nesse sentido, um exame atento dos tipos de objeto licitados pela Administração Pública evidencia que embora sejam divisíveis, há interesse técnico na manutenção da unicidade, da licitação ou do item da mesma. Não é, pois, a simples divisibilidade, mas a viabilidade técnica que dirige o processo decisório. Observa-se que, na aplicação dessa norma, até pela disposição dos requisitos, fisicamente dispostos no seu conteúdo, a avaliação sob o aspecto técnico precede a avaliação sob o aspecto econômico. É a visão jurídica que se harmoniza com a lógica. Se um objeto, divisível, sob o aspecto econômico for mais vantajoso, mas houver inviabilidade técnica em que seja licitado em separado, de nada valerá a avaliação econômica. Imagine-se ainda esse elementar exemplo do automóvel: se por exemplo as peças isoladamente custassem mais barato, mesmo assim, seria recomendável o não parcelamento, pois sob o aspecto técnico é a visão do conjunto que iria definir a garantia do fabricante, o ajuste das partes compondo todo único, orgânico e harmônico. Por esse motivo, deve o bom administrador, primeiramente, avaliar se o objeto é divisível. Em caso afirmativo, o próximo passo será avaliar a conveniência técnica de que seja licitado inteiro ou dividido".

Portanto, ao se licitar por grupo único, cabe ao administrador analisar por meio dos setores técnicos acerca da viabilidade técnica e econômica de dividir-se o objeto licitatório, pois segundo Justen Filho, "*a obrigatoriedade do fracionamento respeita limites de ordem técnica e econômica. Não se admite o fracionamento quando tecnicamente isso não for viável ou, mesmo, recomendável. O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. (...) a unidade do objeto a ser executado não pode ser destruída através do fracionamento*". Esclarece-nos Carvalho Carneiro acerca do conceito de viabilidade técnica e econômica, informando que *"a viabilidade técnica diz respeito à integridade do objeto, não se admitindo o parcelamento quando tal medida implicar na sua desnaturação, colocando em risco a satisfação do interesse público em questão"*.

Nesse sentido, o grupo único é mais satisfatório do ponto de vista da eficiência técnica, por manter a qualidade da Solução de TI, haja vista que o gerenciamento permanece todo o tempo a cargo de uma gestão centralizada. 3.4.5. Por se tratar de uma solução composta por diversos softwares aplicativos, cada um contendo diversas funcionalidades, é fundamental para a garantia da qualidade do serviço, que sejam fornecidos por um mesmo fabricante, visando otimizar custos e reduzir o tempo de atendimento em caso de problemas a consultoria especializada do fabricante deverá ser adjudicado a uma mesma empresa. A adjudicação do objeto desta contratação à empresas distintas, além de aumentar seu custo administrativo, abre margem para que as empresas deixem de prestar o serviço contratado, alegando que a falha de um componente sob sua responsabilidade foi causada por falha de componente sob responsabilidade de outra CONTRATADA. De modo a impedir que esse cenário se torne realidade, comprometendo a disponibilidade de todos os serviços de TIC deste Ministério, é fundamental que os itens objeto desta contratação seja adjudicado a uma única licitante.

Cabe consignar ainda a estimativa de ganho em economia de escala com a contratação por Grupo Único, visto que as empresas certamente ofertarão menores valores visando abarcar um maior volume, podendo diferir no valor global, custos inerentes a operação própria e outros advindos da contratação, traduzindo-se em um menor custo da contratação almejado pela Administração.

Além dos benefícios elencados pela modalidade de contratação por Grupo único, citam-se as seguintes vantagens:

- Maior nível de controle pela Administração na execução dos serviços, pelo fato da existência de apenas um software de gerenciamento;
- Maior interação entre as diferentes fases da implantação/implementação;
- Redução de custos no que se refere ao Custo Total de Propriedade – TCO, considerando-se que não seria necessário adequação de hardwares (servidores) e softwares (licenciamentos) dos sistemas de gerenciamento da solução para cada um dos lotes licitados;
- Maior facilidade no cumprimento do cronograma preestabelecido;
- Diminuição da quantidade de servidores públicos a serem alocados para atividades de fiscalização e gestão do contrato, tendo em vista que cada equipe é composta por no mínimo 4 servidores (gestor, fiscal técnico, fiscal requisitante e fiscal administrativo), exigindo a alocação de recursos humanos para composição de equipes de gestão e fiscalização em função da celebração de inúmeros contratos para o mesmo objeto e, considerando o cenário atual do Ministério da Economia, no qual há notória insuficiência de força trabalho, tal estratégia demonstra-se inviável, corroborando para a realização do certame em grupo único.

Disto isto, o parcelamento do objeto dos itens do grupo 01, apesar de possível, não é tecnicamente viável, pois, embora cada tipo de licença/serviço possa ser fornecida/prestado por uma empresa diferente, a interoperabilidade entre as ferramentas que compõem a solução e trazem os principais benefícios de utilização de um ambiente colaborativo integrado poderá ser prejudicada, sob risco de não ser alcançado o objetivo da licitação. A contratação por item pode tornar a solução complexa, gerando um alto risco ao sucesso do projeto.

Os itens que compõem o grupo 01 desta contratação possuem a mesma natureza e relação entre si, o que torna seu parcelamento técnica e economicamente inviável. A adjudicação do grupo 01 desta contratação a empresas distintas, além de aumentar seu custo administrativo, poderia trazer prejuízos à qualidade e à unidade dos serviços prestados, na medida em que eventuais falhas de um contrato poderiam ser por ele imputadas às atividades desenvolvidas por outro, dificultando a atividade fiscalizadora da Administração Pública, incorrendo em alto risco de indisponibilidade dos serviços que são essenciais para o funcionamento do Órgão.

A escolha da forma mais adequada e vantajosa de adjudicação, global ou por item, deve ser feita caso a caso. Para tanto, é essencial considerar o conjunto de variáveis que caracterizam e particularizam o objeto a ser contratado, o mercado fornecedor, as condições que possam favorecer ou dificultar o funcionamento do conjunto, assim como o custo decorrente da dispersão de recursos para gestão de múltiplos contratos firmados para atender a um único objeto.

No caso em questão, não há como dissociar as licenças elencadas, uma vez que elas são complementares e instaladas no mesmo conjunto de servidores de rede utilizados na Plataforma de Análise de Dados.

Da mesma forma, não há como dissociar o fornecimento das licenças do fornecimento dos serviços de suporte e serviço especializado. O fabricante, especificamente para os serviços do Microsoft 365, faz parceria com os fornecedores para conceder serviços de gestão da migração, treinamentos, campanha de adoção, desta forma o serviço especializado deve estar associado ao fornecimento do licenciamento ou subscrição.

É importante ressaltar ainda que todos os itens de licenciamento e suporte são do mesmo fabricante, não caracterizando a adjudicação global em qualquer forma de redução de competitividade, uma vez que uma empresa que for apta a fornecer um dos itens, também será apta a fornecer os demais.

Pelo exposto, e considerando-se as características da solução, a adjudicação global do objeto revela-se, para a proposta em pauta, solução mais eficiente e vantajosa para a Administração do que a adjudicação do objeto por itens. A celebração de contratos distintos enseja elevação de riscos desnecessários com eventuais contendas de responsabilidade quanto a questões relacionadas ao funcionamento e suporte da solução, assim como de custos administrativos e com a gestão de múltiplos contratos.

Ademais, como a adjudicação global não implica nenhum tipo de restrição à competitividade e como uma empresa que esteja apta a fornecer um dos itens, também estaria a fornecer os demais, não deve ser permitida a participação de empresas em consórcio.

Conclui-se, portanto, que a contratação da solução de TI proposta neste Termo de Referência será feita em um só contrato, visto que os diversos itens da solução funcionam de forma integrada, não sendo técnica e nem economicamente viável dividir a solução.

Portanto, o objeto da presente aquisição não é parcelável

CONCLUSÃO

Diante do exposto em todo o documento, o Ministério do Desenvolvimento Regional considera improcedente as contestações apresentadas no Pedido de Impugnação, uma vez que fica demostrado que, para a realidade do Ministério do Desenvolvimento Regional, a contratação de soluções Microsoft é mais vantajosa tanto na perspectiva financeira quanto técnica.