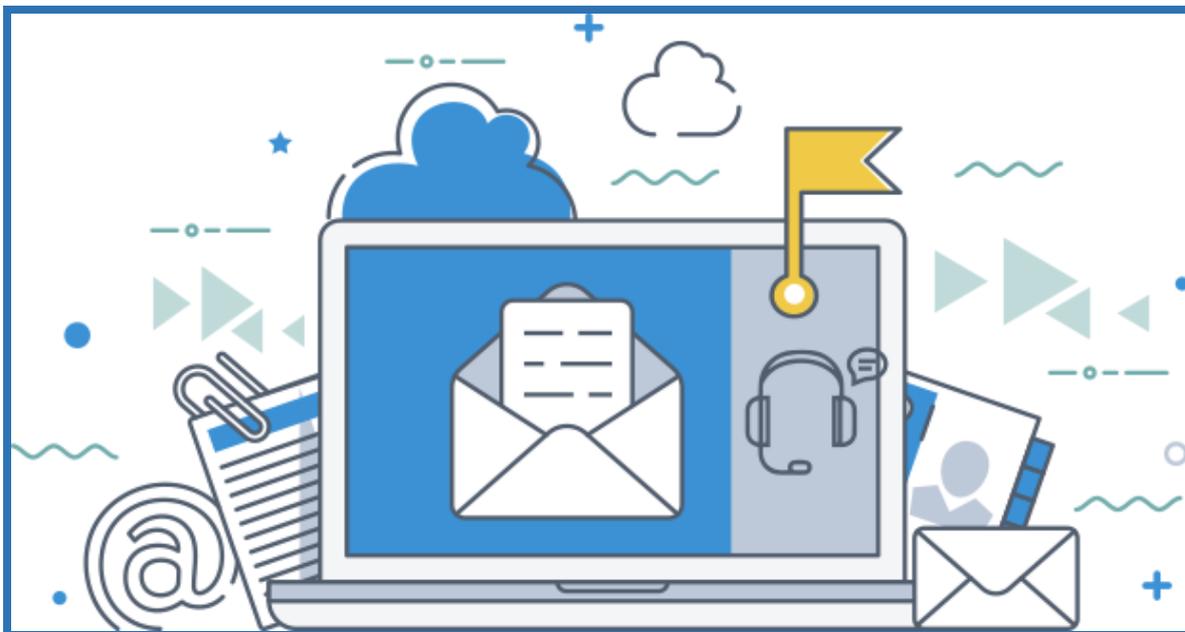




ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo n.º 10265.048398/2020-60



Contratação de Solução de Serviços Integrados para a Receita Federal do Brasil

Belo Horizonte, 25 de março de 2020.

Coordenação-Geral de Tecnologia e Segurança da Informação
Seção Especial de Tecnologia e Segurança da Informação – Sarti06 - 6ª. Região Fiscal
Av. Afonso Pena, 1316 – 10º andar – CEP: 30130-003 - Belo Horizonte/MG
www.receita.fazenda.gov.br



Histórico de Revisões

Data	Ver.	Descrição	Autor
14/02/2020	1.0	Finalização da primeira versão do documento.	Fabio Bernardo
17/02/2020	1.1	Melhorias no cenário 01, nos requisitos tecnológicos, inclusão de quadrante mágico para escolha.	Fabio Bernardo e Luiz Carlos
19/02/2020	2.0	Alteração do item 1.2.2 - Repasse de Conhecimento; 1.2.3 - Requisitos do Suporte Técnico; 1.2.4 - Operação Assistida; 1.2.5 - Operação Assistida; Nova estrutura dos títulos dos subitens; Evolução do cenário 02; Evolução do cenário 03 com a inclusão do Anexo III - ETP Security Identity Compliance GoogleComparison.pdf; Evolução do item 05- Análise comparativa de cursos (TCO); <i>Inclusão do Magic Quadrant for Endpoint Protection</i> no subitem 6.3.2; e Inclusão do item 7. Estimativa De Custo Total Da Contratação.	Fabio Bernardo
20/02/2020	2.1	Inclusão de novo texto na Solução Escolhida	Fabio Bernardo e José Fábio
28/02/2020	2.2	Criação do subitem 8.1. Justificativa para a solução escolhida e retirada do item 06 DLP do Lote Único	Fabio Bernardo
02/03/2020	2.3	Alteração do subitem 1.2.1 Sobre os principais requisitos da Solução de Serviços	Fabio Bernardo e Josivan Cararo
23/03/2020	2.4	Numeração das figuras e tabelas. Criação do subitem 8.2	Fabio Bernardo
25/03/2020	2.5	Alteração do subitem 3.1.2	Fabio Bernardo



Sumário

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS.....	4
1.1. Identificação das necessidades de negócio	4
1.2. Identificação das necessidades tecnológicas	5
1.3. Demais requisitos necessários e suficientes à escolha da solução de TIC - do Plano de Implantação, Instalação e Configuração.....	10
2. ESTIMATIVA DA DEMANDA – QUANTIDADE DE SERVIÇOS.....	12
2.1. Demanda Inicial	12
3. ANÁLISE DE SOLUÇÕES	13
3.1. Levantamento das Alternativas e Orçamento Estimado.....	13
3.1.1. Cenário 1: Renovação de Contratos em Vigência pela RFB	13
3.1.2. Cenário 2: Solução Microsoft 365	14
3.1.3. Cenário 3: Substituição pela Solução Serpro TEAMWORKS.....	17
3.1.4. Análise Comparativa de Soluções.....	21
4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS	22
4.1. Solução Consideradas Inviável.	22
5. Análise comparativa de cursos (TCO)	23
5.1. Mapa Comparativo em R\$	23
6. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA.....	24
6.1. Solução Escolhida.....	24
6.2. Descrição.....	24
6.3. Justificativa.....	24
6.3.1. Escolha Financeira	24
6.3.2. Escolha Técnica	24
6.4. Tabela comparativa entre a Solução Atual e a Solução de Serviços Integrados	27
6.5. Benefícios Esperados	28
6.6. Necessidades de Adequação do Ambiente para Execução Contratual.....	28
7. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO.....	30
7.1. Valor Total Estimado para a Contratação	30
8. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO	31
8.1. Justificativa para a solução escolhida	31
8.2. Ressalva para a solução escolhida	45
9. APROVAÇÃO E ASSINATURA	46



INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, qual seja a Contratação de Solução de Serviços Integrados para a Receita Federal do Brasil, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

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

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1. Identificação das necessidades de negócio

A Secretaria Especial da Receita Federal do Brasil – RFB, como administração tributária, faz uso intensivo de recursos de Tecnologia e Segurança da Informação. O Órgão possui atualmente um parque computacional de equipamentos de informática diversificado, dividido em estações de trabalho, notebooks, tablets, equipamentos de armazenamento híbrido, equipamentos de rede, equipamentos de videoconferência e servidores de rede utilizados como concentradores e distribuidores dos serviços corporativos e facilitadores de acesso às bases de dados da RFB e da comunicação e colaboração entre os usuários da Secretaria.

A integração desse conjunto de equipamentos e serviços, por meio da utilização de softwares, sistemas e aplicativos proporcionam diversos meios que permitem a comunicação e subsidiam os trabalhos desses usuários.

Através de investimentos no seu parque tecnológico previstos em seu PDTI, a RFB está encerrando um ciclo de soluções implementadas de infraestrutura de tecnologia. Esse ciclo se fecha pelo fim da vigência dos seus contratos administrativos ocorridos nos últimos 6 anos. De fato, a Coordenação-Geral de Tecnologia de Segurança da Informação (COTEC) adquiriu nesses últimos anos, por exemplo:

Objeto	Contrato	Empresa
Licenças MS Office 2013	2014LS0005 - RFB	Brasoftware
Sistema de Videoconferência	RFB/COPOL nº24/2014	TES Tecnologia
Solução de Colaboração – IBM Lotus Notes, Sametime, Webconfrence e Connections	RFB/COPOL nº 01/2016 18/2016	Ingram
Symantec Protection Suite e Antivirus	RFB/COPOL nº 15/2016	ISH
Receita Drive e VPN	RFB/COPOL nº 19/2018	SERPRO
Solução de Arquivamento	RFB/COPOL nº 14/2018	VA&R(14)

(Tabela 01: contratos de Soluções de TIC)



Portanto, o grande desafio neste momento é a atualização do seu parque de infraestrutura de Tecnologia da Informação (TI), tendo em vista mudanças no cenário orçamentário e tecnológico. O modelo adotado correntemente de contratações pontuais e de soluções próprias, baseadas em investimento em equipamentos e software, está em processo de transformação no serviço público, considerando restrições orçamentárias e oferecimento pelo mercado de Software como Serviços (SaaS), Infraestrutura como serviço (IaaS) e Plataformas como Serviço (PaaS).

Tendo em vista processos de trabalho mais integrados, demandas por maior produtividade, aumento da modalidade teletrabalho e restrições orçamentárias, há demandas no órgão para soluções que tragam ferramentas que possam suprir essas necessidades. Portanto, há demandas para soluções integradas, serviços em substituição a investimentos em equipamentos e licenças de softwares, soluções de serviços disponibilizados em nuvem, integração dos processos de trabalho com múltiplos dispositivos, plataformas de trabalho comuns para usuários no Órgão e em teletrabalho, integração das diversas formas de comunicação, segurança da informação integrada nas soluções de tecnologia, eliminação do conceito de proteção do perímetro da rede, entre outros.

Desta forma, o objetivo deste ETP será escolher uma solução que abranja o que os usuários da RFB demandam, com expectativa de atendê-las, após o fim das vigências contratuais. Hoje as principais soluções que provêm desses serviços são independentes: correio eletrônico, videoconferência, ferramenta de escritório e produtividade (para edição de textos, planilhas e apresentações) e proteção de dados. Outras necessidades devem ser supridas, conforme abordado no decorrer desse ETP.

1.2. Identificação das necessidades tecnológicas

Dando continuidade à identificação das necessidades dos negócios, a seguir estão relacionadas as necessidades de serviços de TIC em aderência as necessidades da Secretaria Especial da Receita Federal do Brasil:

- a. Correio eletrônico;
- b. Mensagem instantânea e Webconference;
- c. Rede Social;
- d. Solução de videoconferência;
- e. Streaming de vídeo;
- f. Ferramenta de escritório e produtividade;
- g. Solução de proteção de segurança;
- h. Gerenciamento e compliance de endpoint;
- i. Solução de Arquivamento de mensagens de correio eletrônico;



- j. Solução de acesso VPN;
- k. Integração de armazenamento seguro de dados com ambiente de produtividade; e
- l. A solução possa ser unificada e que tenha compatibilidade com dispositivos móveis.

Tendo em vista a nova realidade da RFB, a plataforma desses serviços deve ser acessada independentemente do tipo de dispositivo utilizado pelo usuário, e de onde o usuário estiver, tendo em vista o crescente uso de dispositivos móveis e pessoais e o advento do teletrabalho. Deve-se também integrar múltiplas formas de comunicação e possuir ferramentas de escritório integradas que permita ganhos de produtividade.

A segurança da informação – requisito essencial para a utilização de todos esses serviços - deve ser integrada à solução, com estratégia de proteção e conformidade de dispositivos, usuários, dados e aplicações, considerando o contexto de acesso.

Por fim, deve ser considerado na solução a ser contratada as necessidades corporativas acima citadas, as inovações tecnológicas, a situação orçamentária, a facilidade de implementar e operar, a gestão dos serviços e a segurança da informação

1.2.1. Sobre os principais requisitos da Solução de Serviços

A solução a ser contratada deverá contemplar:

- i. Uma solução de Correio Eletrônico: um serviço de e-mail para os usuários da RFB que seja dotado de arquitetura tecnológica para suportar novas funcionalidades, integração com ferramentas de colaboração e de comunicação utilizando mídias de texto, voz e vídeo e que possa agregar serviços de comunicação instantânea, para estações de trabalho fixas, móveis e outros dispositivos móveis. Deve se adaptar às mudanças de negócio com rapidez e custos adequados, seguindo políticas de segurança do órgão. As caixas postais devem ser dimensionadas de acordo com perfis de usuários. A solução deve prever ferramentas contra ameaças cibernéticas, como *spam*, *phishing* e filtros de e-mail. Deve ser possível ainda utilizar caixas corporativas, ou seja, caixas de correio que sejam compartilhadas entre vários usuários. Além disso deve ser possível usar recursos como criptografia e assinatura digital e deve suportar integração



com o AD e uso de certificado ICP/Brasil;

- ii. Uma ferramenta para a realização de Gestão de TIC que administre o parque de equipamentos, permitindo distribuir instalações de software, inventariar ativos quanto às suas características de hardware e software, gerenciar informações de configuração, monitorar em tempo real comportamentos de operação específicos;
- iii. Uma ferramenta para Segurança dos *Endpoints*: capaz de fornecer serviços de Antivírus, *Antispyware*, Proteção contra demais *malwares*; possibilidade de uma Solução conta perda de dados - DLP (*Data Loss Prevention*); suporte à criptografia de dados; firewall; dentre outro;
- iv. Editoração Eletrônica: uma Suíte de Escritório que inclui softwares para edição de texto, planilha de cálculos e software para apresentação. Sua utilização vai além das funcionalidades comuns, incluindo uso de scripts e macros, aperfeiçoando sua utilização em diversas áreas da Secretaria Especial. Deve prever o compartilhamento de arquivos, controle de versões, edição simultânea de usuários, possibilidade de salvamento de arquivo local ou em nuvem;
- v. Videoconferência: possibilidade de realização de videoconferências, a partir de qualquer de estações de trabalho e dispositivos móveis, por chamada online ou por agendamento. Deve permitir chamada de 1:N e agregar recursos multimídia. Possuir capacidade de gravar a videoconferência ou transmitir por streaming. A ferramenta deve possibilitar chamadas ou agendamento de modo amigável, sem intervenção de equipe de suporte. Deve ser possível agregar os codecs existentes na RFB, de sua solução legada, originar ou receber chamada de videoconferência, de forma a manter o conceito de sala de videoconferência com codec (mesmo que se futuramente tenha que ser comprado um *gateway* à parte). Possuir agenda integrada como a do correio eletrônico inclusive com reserva de recursos como codecs e salas.
- vi. Armazenamento de Arquivos – A solução deve apresentar serviço de armazenamento com acesso por meio de um Portal Colaborativo que permita o compartilhamento de arquivos com controle de acesso e versionamento, com segurança, e possibilidade de acessos de qualquer lugar e dispositivo. Deve permitir também a edição compartilhada, onde dois ou mais usuários possam trabalhar dentro do mesmo documento. Deve prever o uso de criptografia e a cota de armazenamento deve ser definida por perfis de usuários
- vii. Sistema de VPN - Virtual Private Network: como estratégia de redução de custos há necessidade de substituição do serviço de VPN utilizado hoje na



RFB para solução de maior vantajosidade técnica e econômica agregando solução para dispositivo móvel. Como requisito básico a solução deve prover conexão para estações de trabalho e dispositivos móveis. Deve permitir o uso de certificado digital ICP/Brasil.

- viii. Arquivamento de Mensagens: A solução de correio eletrônico utilizado hoje na RFB faz uso de software de arquivamento e retenção de e-mails automatizado. Portanto, a solução deverá implementar essa característica para a solução de e-mail ofertada, com prazos de retenção definido em políticas da RFB. Além disso deve possibilitar o *Journaling* e descoberta, um repositório de todos os e-mails, chat, e demais ferramentas de comunicação que trafegam pela organização acessível apenas para usuários autorizados e administradores. A descoberta deve possuir filtros de pesquisa que permitam a localização dos conteúdos desejados.
- ix. Rede Social: plataforma para prover a colaboração entre usuários ou grupos de trabalho, compartilhando conhecimento dentro da organização por meio de acessos compartilhados a conteúdos, reuniões, documentos, projetos comunidades, fóruns, blogs, wikis e demais ferramentas de comunicação, de forma a oferecer produtividade e eficiência aos processos de trabalho do órgão;
- x. Gerenciamento do acesso: Um requisito imprescindível para a implementação dos serviços acima descritos é uma plataforma de gerenciamento de acesso unificado. Há crescente demanda para que os recursos disponíveis sejam acessados por qualquer dispositivo e onde o usuário estiver. Portanto a solução deve prover plataforma de gerenciamento do acesso, onde sejam verificados os dispositivos, aplicações, usuário e o dado para então permitir o acesso, provendo mecanismos robustos de segurança; e
- xi. Um Sistema Operacional Cliente para que as estações de trabalho possam trabalhar de forma integrada;

1.2.2. Sobre os requisitos do Repasse de Conhecimentos da Nova Solução de Serviços Integrados

- Caso haja a troca por uma solução integrada de serviços haverá a necessidade de treinamento da equipe técnica que participa diretamente na administração das soluções envolvidas descritas no item 1.2.1 desse documento; e
- Devem ser previstos treinamento online aos usuários nas ferramentas de produtividade, colaboração e comunicação. A contratada deve auxiliar na elaboração de trilhas de treinamento e materiais de apoio à aprendizagem.



1.2.3. Sobre os requisitos do Suporte Técnico, Manutenção e Garantia da Nova Solução de Serviços Integrados

- Caso haja a troca por uma solução integrada de serviços haverá a necessidade de Suporte técnico e manutenção para todas as novas soluções a serem adquiridas

1.2.4. Sobre a Operação Assistida

- Talvez haja a necessidade de alocar profissionais da futura contratada para executar determinadas atividades na solução ofertada por um determinado período de tempo;

1.2.5. Sobre os requisitos da Migração de Dados da Nova Solução de Serviços Integrados

- Caso se escolha trocar a Solução Atual haverá a necessidade de migração dos dados;
- Entende-se pela migração a transferência da totalidade dos dados armazenados nos servidores e Storages nas soluções atuais migrada para o novo modelo a ser implementado, observando o um futuro Plano de Implantação a ser elaborado pela Contratada:
 - Os dados referem-se àqueles gerados pelas soluções de correio eletrônico; Mensagem instantânea; webconference e videoconferência; Rede Social; ferramenta de escritório e produtividade;
 - Além desses, os dados de configuração e arquitetura da infraestrutura referem-se àqueles que for aplicável para a Solução de proteção de segurança; gerenciamento e compliance de endpoint; Solução de Arquivamento de mensagens de correio eletrônico; Solução de VPN, gerenciamento de identidade e acesso; Integração de armazenamento seguro de dados com ambiente de produtividade; e Federação do Active Directory
- As atividades de migração que impactem o ambiente de produção serão realizadas em horários não úteis, fora do expediente da RFB, ou de comum acordo entre a contratante e a contratada;
- Essas atividades serão previamente agendadas, considerando as necessidades e restrições do ambiente de produção e a disponibilidade da



equipe técnica bem como as prioridades estabelecidas no planejamento de migração e implantação;;

- As atividades de migração serão executadas por profissionais treinados e qualificados pelo fabricante;
- Deve haver um planejamento da migração separado por serviço, priorizando a preparação, configuração e implantação de serviços de infraestrutura que impactem a migração de serviços aos usuários;
- O planejamento deve ser realizado pela Contratada, envolvendo equipe da Contratante. A Contratada deve realizar levantamento, junto à Contratante, do ambiente informatizado hoje existente na Contratada para determinar alterações ou configurações necessárias para permitir a entrada em produção dos novos serviços e dar apoio a essas atividades;
- Caso a configuração, arquitetura ou infraestrutura existente no órgão não seja compatível para a integração dos novos serviços, a Contratada deve fornecer suporte para resolver o problema; e
- Caso o problema implique em alterações, implementações ou contratações que causem impacto no tempo de migração, a Contratada deve propor solução provisória que mitigue o problema até que as condições definidas sejam implementadas pela Contratante;

1.3. Demais requisitos necessários e suficientes à escolha da solução de TIC - do Plano de Implantação, Instalação e Configuração

- Para a nova Solução a ser integrada, caso seja essa a escolha do Órgão, a Contratada deverá enviar à Contratante um Plano de Implantação, que constará, minimamente:
 - i. Um Cronograma de Instalação e Configuração da Solução Integrada;
 - ii. Uma Matriz de Riscos contendo os riscos inerentes à implantação da nova Solução;
 - iii. Uma listagem com os nomes e cópias dos respectivos documentos válidos dos técnicos que entrarão nas dependências da RFB para realizarem os serviços necessários;
 - iv. O procedimento de instalação e dos testes a serem realizados para o pleno funcionamento, em perfeitas condições de operação e de forma totalmente integrada ao ambiente de infraestrutura de informática da RFB;



- Em até 05 (cinco) dias úteis a Contratante realizará o Aceite ou não do Plano de Implantação, podendo pedir esclarecimentos sobre determinados pontos;
- A CONTRATADA ficará responsável por implantar o seu software de gerenciamento e/ou instalação\configuração em todas as estações de trabalho, fazendo inventário, instalação remota de aplicações e atualização de sistema operacional; e
- O Software deverá ser configurado de maneira mais otimizada, para garantir implantação eficiente de nova versão de sistema operacional ou qualquer aplicação cliente instalada nas máquinas gerenciadas;



2. ESTIMATIVA DA DEMANDA – QUANTIDADE DE SERVIÇOS

2.1. Demanda Inicial

- Foram considerados três perfis de usuários considerando uma estimativa de demanda através da consulta realizada no Sistema SA3 - Sistema de Apoio à Atividade Administrativa, são eles:
 - Terceirizados e estagiários: 4186 usuários;
 - Servidores administrativos e PSE: 5170 usuários;
 - Servidores AFRF: 14767 usuários.
- A partir dessa premissa de perfis foi criada a Tabela 02 abaixo para a formação das licenças totais por item do Lote Único x nível do Serviço (Office 365 ProPlus/F1/E1/E3/E5 and Microsoft 365 Business/F1/E3/E5 Commercial Plan Comparison)
- O maior detalhamento está presente na url: <https://docs.microsoft.com/pt-br/office365/servicedescriptions/microsoft-365-service-descriptions/licensing-microsoft-365-in-smb>

Nome do Produto	Servidores AFRF	Servidores Administr.	PSE (Externo)	Terceiriz.	Estagiár.	Outros	Total
Serviços Integrados nível 1 (e-mail, suíte de escritório, videoconferência e proteção) (licenças)				3540	646		4186
Serviços Integrados nível 2 (e-mail, suíte de escritório, videoconferência e proteção) (licenças)		3700	1470				5170
Serviços Integrados nível 3 (e-mail, suíte de escritório, videoconferência e proteção) (licenças)	14767						14767
Serviços de Mobility + Security (identidade, gestão de dispositivos e proteção da informação) nível 1 (licenças)				3540	646		4186
Serviços de Mobility + Security (identidade, gestão de dispositivos e proteção da informação) nível 2 (licenças)	14767	3700	1470				19937
Solução de Arquivamento (licenças)		3700	1470	3540	646		9356
Serviços de nuvem/AD (licenças)	14335	4132	1470	3540	646	53	24176

(Tabela 02: Estimativa de Demanda por consulta realizada no Sistema SA3 - Sistema de Apoio à Atividade Administrativa da RFB - no dia 27 de janeiro de 2020)



3. ANÁLISE DE SOLUÇÕES

3.1. Levantamento das Alternativas e Orçamento Estimado

É considerando os custos inerentes ao ciclo de vida dos bens e serviços da solução, incluindo custos diretos e indiretos, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção, etc.

Na memória de cálculo são considerados já os cálculos totais de propriedade inerentes ao ciclo de vida dos bens e serviços da solução, incluindo custos diretos e indiretos, a exemplo dos valores de **aquisição dos bens, garantia, instalação, configuração, ativação, migração de dados, manutenção, suporte, atualização, operação assistida e o repasse de conhecimento previsto.**

3.1.1. Cenário 1: Renovação de Contratos em Vigência pela RFB

Entidade: Secretaria Especial da Receita Federal do Brasil

Descrição: Reconstrução das soluções vigentes atualmente implementadas na Receita Federal do Brasil de forma atender cada necessidade pontualmente. Na tabela 03 abaixo são relacionadas as soluções existentes, bem como a projeção de custos adaptados para as variáveis atuais (quantidade de usuários, estações de trabalho, atualização de preços, etc).

Objeto	Contrato	Empresa (Anexo I a 8)	Valor
Licenças MS Office 2013	2014LS0005 - RFB	Brasoftware (I.1)	R\$6.835.968,00 (6.912 Licenças: já com o Termo Aditivo do contrato original e valor unitário a R\$989,00)
Sistema de Videoconferência	RFB/COPOL nº24/2014	TES Tecnologia (I.2)	R\$1.926.700,00 (51 equipamentos – Ativo Permanente)
	RFB/COPOL nº33/2012	TES Tecnologia (I.3)	R\$18.348.278,00 (414 Equipamentos – Ativo Permanente e diversas licenças)
Solução de Colaboração – IBM Lotus Notes, Sametime, Webconference e Connections	RFB/COPOL nº 18/2016	Ingram (I.4)	R\$ 7.196.726,90 (vide contrato original com a Ingram (IBM Domino Enterprise Client/Server/Sametime/Connections)
Symantec Protection Suite e Antivirus	RFB/COPOL nº 20/2016	ISH (I.5)	R\$7.161.015,40 (40.460 licenças da solução de segurança Symantec Protection Suite Enterprise Edition (SPSEE) for Endpoints a R\$176,99



Receita Drive e SAR\VPN	RFB/COPOL nº 19/2018	SERPRO (I.6 e I.7)	R\$2.385.175,32 ReceitaDrive (código 10567 do Contrato Serpro_anexo I 1 1) R\$2.663.125,69 SAR\VPN (código 04.02.01 do III.6 – Anexo IV.2 –Serviço de Suporte e Sustentação - Serviço de Acesso Remoto SAR)
Solução de Arquivamento	RFB/COPOL nº 14/2018	VA&R(I.8)	R\$3.815.382,00 (28.473 licenças para o Enterprise Vault para correio)
Total			R\$ 58.100.966,31
Total sem os Ativos Permanentes			R\$ 37.825.988,31

(Tabela 03: Valores de contratos sem trazer para valor presente)

Valor conforme o Anexo I.1 a I.8 ETP - Cotação para o Cenário 01: R\$ 37.825.988,31 para 12 meses de contrato (observado que o valor para o ativo permanente se dá para 60 meses de garantia)

3.1.2. Cenário 2: Solução Microsoft 365

Entidade: Solução adotada nos seguintes Órgãos:

- Ministério Público do Estado de Rondônia pelo conforme 37/2019;
- Agência Nacional de Petróleo conforme Pregão: 61/2018;
- Tribunal de Contas da União conforme Pregão: 080/2019;
- Tribunal de Justiça do Estado do Pará conforme Pregão: 093/2018;
- Agência Nacional de Aguas conforme Pregão: 008/2019;
- Conselho Nacional do Ministério Público conforme Pregão: 005/2020; e
- Superior Tribunal de Justiça conforme Pregão: 60/2019;

Descrição: Uma solução aderente aos requisitos apresentados no subitem 1 (necessidades do negócio e necessidades tecnológicas) desse Estudo seria a encontrada na Solução Microsoft 365. Os serviços que o Órgão demanda, por exemplo, são alguns dos listados abaixo:

- Suíte de Escritório Microsoft Office:

A ideia da RFB é ofertar aos nossos usuários tanto para acesso em estações Desktops, como em tablets e telefones/smartphones toda a suíte de aplicativos Office;

- E-mail e calendários:

A ideia ofertar aos usuários caixa de correio para acesso aos e-mails pela área de trabalho ou pelo navegador da Web;



- Recursos de arquivamento e retenção legal para atender às necessidades de conformidade (compliance):

A ideia da RFB é permitir o uso de suas políticas de prevenção de perda de dados (*Data Loss Prevention*) e divulgação de política para instruir os usuários para uma aplicação adicional de conformidade no e-mail;

- Controle de acesso a documentos e e-mail:

A ideia aqui é restringir o acesso a documentos e e-mails a pessoas específicas e impedir que outras pessoas as visualizem ou editem, mesmo que sejam enviadas para fora da organização;

-Criptografia de Mensagens:

A ideia aqui é permitir a aplicação de diretivas de criptografia flexíveis e prontas para uso. Além disso, permitir o controle das chaves de criptografia no Cofre de Chaves do Azure;

- Reuniões online com áudio, vídeo em alta definição e webconferência:

Esse será o grande diferencial nessa contratação (em relação a sua solução atual), isso é, será a realização de videoconferências com apenas um clique ou toque no *smartphone*, *tablet* ou PC e não ficar dependendo de agendamentos e disponibilidade de Equipamentos Cisco para a realização de videoconferências;

-- Sistema de mensagens instantâneas e conectividade do Skype/Teams:

A ideia será disponibilizar para os nossos usuários um completo sistema de mensagens instantâneas, chamadas de voz e chamadas de vídeo, com status online para mostrar quando um usuário está disponível, integrados com as demais ferramentas e que compartilhe a localização do servidor e etc, tudo com compatibilidade por estação de trabalho PC, tablets e Smartphones;

- Armazenamento e compartilhamento de arquivos:

Aqui se trata de armazenamento pessoal na nuvem para cada usuário, que pode ser acessado de praticamente qualquer lugar e em quase todos os dispositivos. Compartilhamento de documentos com outras pessoas de dentro ou fora da organização e controle de quem pode exibir e editar cada arquivo;

-Rede social corporativa:

Com o software de colaboração e os aplicativos de negócios, os servidores poderão se conectar às pessoas certas, compartilhar informações entre as equipes e se organizar em torno dos projetos;



-Gerenciamento do trabalho:

A ideia é a criação de planos, organização e atribuição de tarefas, compartilhamento de arquivos, conversas sobre o trabalho e recebimento de atualizações sobre o andamento das atividades;

- Mobilidade:

Outro diferencial em relação à Solução Atual da RFB, isso é: sincronizar e-mail, calendário e contatos; acessar sites do SharePoint; visualizar e editar documentos do Office com o Office Online usando um navegador em dispositivos Windows Phone, iOS e Android.

- Gerenciamento corporativo de aplicativos:

Trata aqui de simplificar o gerenciamento de aplicativos na organização com Diretiva de Grupo, Telemetria e Ativação de Computador Compartilhado.

- Serviço de vídeo institucional e conteúdo para a RFB:

Aqui estamos falando da criação, gerenciamento e compartilhamento de vídeos de forma segura com toda a organização. Permite que todos colaborem com vídeo e fiquem conectados ao conteúdo mais importante.

- Proteção da informação:

Trata-se do gerenciamento de direitos, a prevenção de perda de dados e a criptografia que ajudam a manter o conteúdo seguro em e-mail, mensagens instantâneas, reuniões e sites de equipe.

- Segurança e gerenciamento de acesso simplificados:

Aqui é o gerenciamento de logon único entre dispositivos, seu datacenter e a nuvem de forma centralizada.

- Acesso condicional:

Aqui é a definição das políticas que forneçam controles contextuais nos níveis de usuário, localização, dispositivo e aplicativo para permitir, bloquear ou desafiar o acesso do usuário.

- Relatórios avançados de segurança:

Monitoramento de atividades suspeitas com emissão de relatórios, auditoria e alertas, e atenuação de possíveis problemas de segurança usando recomendações concentradas.

-Gerenciamento de dispositivos móveis



Registre dispositivos corporativos e pessoais para provisionar configurações, impor a conformidade e proteger seus dados corporativos.

- Gerenciamento integrado de PCs

Centralize o gerenciamento de PCs, laptops e dispositivos móveis de um único console administrativo e produza relatórios de configuração de software e hardware detalhados.

Valor conforme anexo I.9 ETP - COTACAÇÃO Cenário 2 Planilha de Formação de Preço 2020 v2.0 Serviços Integrados para 12 meses de contrato: R\$ 28.332.290,36

3.1.3. Cenário 3: Substituição pela Solução Serpro TE-AMWORKS.

Entidade: SERPRO Proposta Comercial SERPRO no 122/2019

Descrição: solução de colaboração, criação, comunicação e armazenamento de arquivos baseada no GSuíte - a suíte de colaboração do Google - e no software de **Zimbra Collaboration**.

O SERPRO TEAMWork utiliza os conceitos de computação em nuvem, cujos componentes de infraestrutura são dotados de recursos de balanceamento de carga e escalabilidade horizontal permitindo atender a grandes volumes de comunicação e colaboração.

O SERPRO TEAMWork faz uso de servidores virtuais e cada componente do serviço pode realizar sua função suportado por múltiplos servidores. A arquitetura dispõe de:

- Ferramentas de criação e colaboração via web de edição de documentos: texto, planilhas, apresentações, formulários;
- Web conferência e mensagens instantâneas (chat);
- Diretório (LDAP) para suportar autenticações e os catálogos de endereço pessoal e corporativo;
- Banco de dados para suportar tarefas, agendas pessoais e corporativas;
- Backup para o serviço;
- Arquivamento de longo prazo (Archiving);
- Monitoramento para toda a cadeia produtiva do serviço;
- Autenticação de usuários por senha ou por certificado digital;
- Recursos de criptografia que permite ao usuário cifrar digitalmente seus e-mails;
- Uso de protocolo seguro (HTTPS) na comunicação com o servidor;



- Sistemas anti-spam e antivírus (intra e inter-domínios); e
- Uso em dispositivos móveis.

**Valor conforme anexo I.10 ETP SERPRO TEAMWORKS - COTACAÇÃO Cenário 3:
R\$12.558.000,00 para 12 meses de contrato**

Bem, apesar do Serviço Federal de Processamento de Dados (Serpro) ser considerada como a maior empresa pública de prestação de serviços em tecnologia da informação do Brasil. [As 50 maiores estatais do Brasil em 2012 acessado em Exame.com de 14 de agosto de 2012] e também ser vinculada ao Ministério da Economia, desenvolvendo e cuidando de sistemas e serviços que permitiram a realização das finalidades da Receita Federal do Brasil (Cadastro de Pessoas Físicas; Cadastro Nacional de Pessoas Jurídicas; ReceitaNet; Programa de Recuperação Fiscal; Sistema Integrado de Comércio Exterior Sistema Integrado de Informações Econômico Fiscais; Sistema Público de Escrituração Digital; e-Social e incontáveis outras soluções) achamos a solução não atende a toda a demanda levantada neste ETP.

Apesar de contar com soluções de Suítes de escritório, Email, Comunicação instantânea (voz e vídeo), Armazenamento em nuvem, Webconferência e Transmissão de vídeos, sentimos falta de uma solução mais robusta para escritório como o Office e principalmente uma completa solução de segurança que abrangeria:

- Proteção de todos os Endpoint
- Prevenção de Data Loss
- Solução de controle de Inventário;
- Solução de Deployment;
- Solução de Montiramento e análise centralizada do parque; e
- Solução de Segurança para o Data Center

Outrossim, uma análise feita pelo grupo Gartner sobre o Zimbra, apontou que:

- Apesar de não existir uma limitação técnica, normalmente o Zimbra é aplicado em ambiente de médio ou pequeno porte, girando em torno de 1000 usuários;
- De acordo com a análise, não existia um interesse do mercado sobre o produto; e
- O produto foi vendido sucessivas vezes para vários fornecedores e não se sabe até quando terão novos investimentos;

Veja o trecho no Anexo II - ETP - Gartner_SRF_WR_Zimbra:

“ *Gartner clients have expressed limited interest in Zimbra.*
As evidence:



- *Zimbra has only one review on Peer Insights. Other Gartner clients are not reviewing the product or expressing interest. <https://www.gartner.com/reviews/market/workplace-social-software/vendor/zimbra?pid=132>*
- *Zimbra has no conversations in the Gartner Peer Connect community: https://community.gartner.com/t5/forums/searchpage/tab/message?advanced=false&allow_punctuation=false&q=zimbra*
- *Every year, Gartner has thousands of interactions with Gartner clients on Microsoft Office 365 or Google Apps. Last year, Gartner clients initiated discussion on Zimbra only 15 times. We cannot provide any references from Zimbra without breaching confidentiality. However, Zimbra does share their customer stories: <https://www.zimbra.com/success-stories/>.*
- *When we have interacted with other Gartner clients in Brazil who must host their own email service due to local requirements, they ask more about Microsoft Exchange and Spamina (due to its relationship with Telefonica). ”*

Da mesma forma, o relatório do The Radicati Group, Messaging Platforms for Service Providers – Market Quadrant 2018 cita algumas fraquezas da solução (página 27), evidenciando que o produto ainda está em fase de amadurecimento e melhorias, diferente de outras soluções que já estão mais consolidadas no mercado;

Veja o trecho no Anexo II - ETP - MessagingPlatformsforServiceProviders-MarketQuadrant2018):

“

- *Zimbra is an open-source solution that includes many open-source components for key functionality such as Postfix for its message transfer agent, ClamAV and SpamAssassin for anti-malware and many others. While these open-source components are well known, they don't always deliver best in-class functionality.*
- *Social networking integration is currently only available through third party Zimlets.*
- *Zimbra currently offers basic document collaboration functionality through the Zimbra Briefcase, which allows users to create, manage and share documents and other files. A full document editing capability and integration with Zimbra Drive are on the roadmap for 2018.*



- *Zimbra has gone through many acquisitions in the past, moving from Yahoo!, to VMware, to Telligent and to Synacor, which have caused it to regularly re-assess its product portfolio. As part of Synacor, however, Zimbra has found a stable home with renewed investments in technology and product leadership.*
- *Zimbra has been late to deliver its next-generation, stateless email server in its commercial, off-the-shelf software product. However, Synacor has invested heavily into this area over the past year, and a new stateless and containerized architecture is due for release in the 2018 timeframe. “*

Interessante também mencionar o Anexo III - *ETP Security Identity Compliance GoogleComparison.pdf* onde é realizada uma comparação ponto a ponto entre a solução Microsoft 365 e a solução G-Suite em relação a segurança e a parte de conformidade legal (Compliance).

Note que na página 06 e 09 do Anexo, a solução G-Suite não apresenta quesitos essenciais de Proteção contra ameaça em geral nem habilidade de conceder políticas de acesso condicional baseadas no estado do dispositivo, sensibilidade da aplicação e localização do usuário.

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

(Figura 01: Comparativo entre G-Suite e Microsoft 365)



Funcionalidade	G-Suite Business	Microsoft 365	Comentários
Proteger a porta da frente através de acesso controlado, com MFA (Multi-Factor of Authentication).	●	●	
Habilidade de conceder políticas de acesso condicional baseadas no estado do dispositivo, sensibilidade da aplicação e localização do usuário.	○	●	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	○	●	Azure Active Directory Premium P1
Proteger acesso a apps 1 st e 3 rd party, on premises e na nuvem	◐	●	Google faz Somente nuvem 1st party
Proteção de senha com duplo fator de autenticação que pode utilizar PIN ou biometria no seu PC	○	●	Windows Hello
Proteção para credenciais do usuário e administrador de chaves roubadas usadas para criar um ataque "Pass the Hash" com tokens ou usuários <i>impersonate</i>	○	●	Windows Credential Guard
Habilidade para descobrir, restringir e monitorar identidades privilegiadas	○	●	Azure AD Privileged Identity Management
Medidas de segurança em conformidade com GDPR para proteção e privacidade de dados e usuários	●	●	

(Figura 02: Comparativo entre G-Suite e Microsoft 365)

3.1.4. Análise Comparativa de Soluções

Requisito	Id do Cenário	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	X		
	2	X		
	3	X		
A Solução está disponível no Portal do Software Público Brasileiro?	1		X	
	2		X	
	3		X	
A Solução é um software livre ou software público?	1		X	
	2		X	
	3	X		
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1	X		
	2	X		
	3	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1	X		
	2	X		
	3	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)	1			X
	2			X
	3			X

(Tabela 04: Análise das Alternativas Existentes)



(Figura 03: Análise das Alternativas Existentes. Pesquisa em <https://softwarepublico.gov.br/social/search/software> infos realizada no dia 14/02/2020)

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

4.1. Solução Consideradas Inviável.

Conforme § 1º do art. 11, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação. Tecnicamente os cenários 1, 2 e 3 são viáveis para implementação na Receita Federal do Brasil, porém, vale a pena citar que no cenário 03, uma análise feita pelo grupo Gartner e grupo The RadicaTI Group sobre o Zimbra, apontou que:

- Apesar de não existir uma limitação técnica, normalmente o Zimbra é aplicado em ambiente de médio ou pequeno porte, girando em torno de 1000 usuários;
- De acordo com a análise, não existia um interesse do mercado sobre o produto;
- O produto foi vendido sucessivas vezes para vários fornecedores e não se sabe até quando terão novos investimentos; e
- Nota-se que o produto ainda está em fase de amadurecimento e melhorias, diferente de outras soluções que já estão mais consolidadas no mercado.



5. Análise comparativa de cursos (TCO)

5.1. Mapa Comparativo em R\$

Solução Viável	Estimativa de TCO ao longo de 3 anos			Total (R\$)
	Ano 1(R\$)	Ano 2(R\$)	Ano 3(R\$)	
Solução 1	37.825.988,31	37.825.988,31	37.825.988,31	113.477.964,93
Solução 2	28.332.290,36	28.332.290,36	28.332.290,36	84.996.871,08
Solução 3*	12.558.000,00	12.558.000,00	12.558.000,00	37.674.000,00

(Tabela 05: Mapa Comparativo Dos Cálculos Totais De Propriedade - (TCO) sem contar com nenhum índice de preço para os anos futuros

***A Solução 3 não é aderente aos requisitos tecnológicos elencados no subitem 1.2, para isso, veja análise realizada no subitem 2.1.3 Cenário 03: Substituição pela Solução Serpro TEAMWORKS.)**



6. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

6.1. Solução Escolhida

- Cenário 2: Solução de Serviços Integrados da Microsoft 365

6.2. Descrição

Solução de Serviços Integrados Microsoft 365 para a Receita Federal do Brasil

6.3. Justificativa

São duas as premissas que nortearam a escolha do cenário 02.

6.3.1. Escolha Financeira

O preço para aquisição de uma Solução com serviços integrados é menor do que fazer todas as aquisições de forma separada.

Entre os cenários viáveis o percentual de vantajosidade com a escolha do cenário 2 está em aproximadamente 25% ($28.332.290,36 / 37.825.988,31 = 0,7490 \Rightarrow 1 - 0,749 = 0,251 \times 100 = 25,1\%$ de economia), que representa R\$ 9.493.697,95 (nove milhões, quatrocentos e noventa e três mil, seiscentos e noventa e sete reais e noventa e cinco centavos) de economia.

Ademais, a solução integrada do cenário 2 possibilita menor custo de manutenção, gerenciamento e de treinamento de servidores do órgão. Ganha-se também com a padronização dos softwares de produtividade uma vez que grande parte dos servidores utilizam "LibreOffice" e pequena parcela o pacote "Office 2013", já desatualizado.

6.3.2. Escolha Técnica

Uma solução com serviços integrados estaria em total alinhamento em relação às necessidades de negócio conforme a descrição da Necessidade de TI apresentada no atual PDTI da Secretaria de Receita Federal do Brasil.

Descrição da Necessidade de TI	Objetivo Estratégico Institucional	Objetivo Estratégico de TI		
		Perspectiva de Resultados	Perspectiva de Processos Internos	Perspectiva de Pessoas e Recursos



N04 - Manter e Suportar de Soluções de TI	Viabilizar recursos e otimizar sua aplicação para suprir as necessidades de infraestrutura e tecnologia	Assegurar a excelência da infraestrutura e dos serviços de TI com níveis de desempenho, segurança e disponibilidade adequados à criticidade do negócio.	Aprimorar o ambiente informatizado	Aprimorar a infraestrutura física e tecnológica para suporte às atividades de TI
---	---	---	------------------------------------	--

(Tabela 06: atual PDTI da Secretaria de Receita Federal do Brasil)

Além do mais, várias componentes que estão contemplados na Solução unificada são líderes de mercado segundo os quadrantes mágicos do grupo Gartner, além da Solução já ser adotada pelo próprio Ministério da Economia:





Magic Quadrant for Enterprise Information Archiving



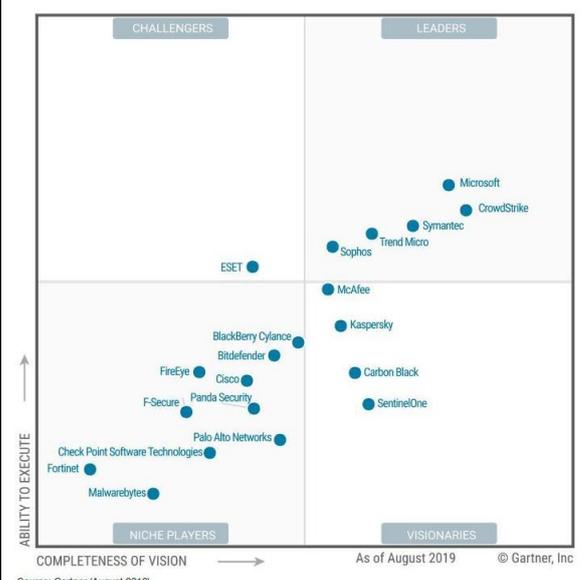
Magic Quadrant for Access Management



Magic Quadrant for Cloud Access Security Brokers



Magic Quadrant for Endpoint Protection



(Figura 04: Quadrantes mágicos do Gartner para Endpoint Protection Platforms/ Unified Endpoint Management Tools / Archiving / Access Management / Cloud Access Security Brokers/)



6.4. Tabela comparativa entre a Solução Atual e a Solução de Serviços Integrados

Nome da Solução		Soluções implantadas na RFB	Solução Microsoft 365
		Características	Características
Correio Eletrônico		Não integrado com Videoconferência, ferramentas de produtividade, fluxo de trabalho, pastas de trabalho, etc	Integrado com ferramentas de produtividade, comunicação, etc. Caixas de 2GB (F1) e 1T (E1, E3)
Web Conference		Limitada e não integrada. Equipamentos distribuídos	É o mesmo que videoconferência.
Mensagens Instantâneas		Não integrado totalmente com os dispositivos móveis.	Integrada com correio, agenda, videoconferência, produtividade
Rede Social	Atividades	Não integrado com Videoconferência e ferramentas de produtividade	Integrada com ferramenta de produtividade, comunicação, grupos de trabalho, fluxo de trabalho
	Tarefas		
	Wikis		
	Blogs		
	Fóruns		
Receita Drive		Não integrada com o espaço de trabalho do usuário, ferramentas de produtividade, fluxo de trabalho.	Integrado com ferramenta de produtividade, correio, fluxo de trabalho, grupos, etc. Espaço de até 5TB.
Perímetro definido por software ou Zero Trust		Hoje utiliza VPN ganhando acesso a toda a rede	O acesso depende de verificações: identidade de usuário, integridade do dispositivo, integridade do aplicativo e controle de privilégios e criptografia de dados.
Videoconferência		Tradicional, sem possibilidade de dispositivos móveis e videoconferência externa. Utiliza uma Central de agendamento no Lotus notes.	Possibilita videoconferência por qualquer dispositivo, agendamento na própria ferramenta, permite inclusão de codec, permite videoconferência externa, gravação e streaming
Ferramentas de Produtividade		Pacote Office instalável em um dispositivo do usuário (estimado para 10.000 usuários)	Pacote Office para F1 e E1 via browser. E3 pode instalar. Possibilidade de uso do 2013 (5000 licenças RFB).
Software de arquivamento de mensagem		Utilizado com o Notes	Arquivamento e recuperação de mensagem na solução.
Acesso VPN		Restrito a estações de trabalho da RFB	Reduz uso de VPN, restrita a acesso a sistemas
SEP – Symantec Endpoint Protection		Parte da solução de proteção de endpoints	Solução de segurança no EMS com ATP (tratamento avançado de ameaças + Intune e System Center
Plataforma para educação e treinamento.		Hoje com solução não integrada e restrita. Há demandas de plataforma de vídeo.	Possibilidade de elaboração, gerenciamento, armazenamento e distribuição de conteúdo e interação.
Atendimento à necessidade de tele trabalho		Hoje com recursos limitados para interação, fluxo de trabalho e estação dedicada.	Plataforma de comunicação colaboração, fluxo de trabalho, tarefas) e possibilidade de implantar Byod (estações/Moveel.
Atendimento das necessidades da área de Correição, Auditoria de Segurança, conformidade		Hoje sob demanda	Perfis específicos para Advance Compliance
Dispositivos móveis		Sem solução de MDM e políticas para os dispositivos.	Solução de UEM - Gerenciamento de endpoints unificado (dispositivo, aplicativo usuários e dados).

(Tabela 07: Comparação entre as soluções)



6.5. Benefícios Esperados

- Continuidade das soluções ofertadas hoje aos usuários finais da RFB, com a segurança exigida como: correio eletrônico; mensagem instantânea; webconference; rede social; solução de videoconferência; streaming de vídeo (videolan); ferramenta de escritório e produtividade; solução de proteção de segurança; gerenciamento e compliance de endpoint; solução de arquivamento de mensagens de correio eletrônico; solução de Armazenamento de Arquivos; entre outros;
- Maior confiabilidade e segurança: graças às funcionalidades de recuperação, gerenciamento global e recursos de privacidade, os dados da RFB permanecerão seguros e protegidos o tempo todo e de forma integrada e facilmente gerenciada;
- Possibilidade de Integração de serviços como ferramentas de escritório, ferramenta de colaboração e comunicação para usuários e grupos de trabalho e proteção de segurança tornando o espaço de trabalho do usuário mais eficiente e produtivo;
- Possibilidade de transição em estágios: o órgão poderá fazer a transição para a nuvem em estágios permitindo combinar serviços em suas instalações com serviços em nuvem (chamados de cenários híbridos);
- O ambiente será mais integrado para os usuários de teletrabalho, oferecendo as mesmas ferramentas disponíveis no órgão para esta modalidade de trabalho, sendo assim, aumentando a produtividade e criando mecanismos eficiente de gestão;
- Padronização da Infraestrutura e parque tecnológico pela adoção de uma única solução;
- Possibilidade de um gerenciamento centralizado e integrado pelo Datacenter de Brasília;
- Maior oferta para os nossos usuários pelo maior número de licenças para edição de textos, planilhas e apresentações
- Maior uso, usabilidade e facilidade na utilização de videoconferência pela RFB;
- Maior governança, confiabilidade e escalabilidade aos serviços de TI providos pela COTEC; e
- Redução do custo operacional, maior elasticidade ao permitir capacidade de realocar recursos de acordo com as necessidades do órgão, além do potencial ganho de performance.

6.6. Necessidades de Adequação do Ambiente para Execução Contratual

- Não há nenhuma necessidade específica de adequação do ambiente, porém, a Contratada que fornecerá a nova Solução de Serviços Integrados deverá ter



conhecimento na completa estrutura e modelo de segmentação do Parque Tecnológico da Receita Federal do Brasil.

- Como o serviço se dará em nuvem será prudente utilizar os otimizadores WAN para suportar a nova demanda de rede;



7. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

7.1. Valor Total Estimado para a Contratação

O Valor Total Estimado para essa Contratação é de **R\$ 28.332.290,36** (vinte e oito milhões e trezentos e trinta e dois mil e duzentos e noventa reais e trinta e seis centavos) tendo como base no Anexo I.9 ETP - COTACAÇÃO Cenário 2 Planilha de Formação de Preço 2020 v2.0 Serviços Integrados.

De acordo com o art. 2º da Instrução Normativa SLTI/MPOG nº5, de 27 de junho de 2014 (Alterado pela Instrução Normativa nº 7, de 29 de agosto de 2014), que trata de pesquisa de preços, temos uma ordem de preferência, a ser observada para realização da pesquisa de preços, foram eles:

- Portais de Compras Governamentais: Cotações B; C; F; G; H; I; J; e K;
- Pesquisas publicada em mídia especializada, sítios eletrônicos especializados ou de domínio amplo: Consulta ao Catálogo de Soluções de TIC com Condições Padronizadas (MICROSOFT) realizada no dia 10 de março de 2019 às 14:19: Cotação A;
- Contratações similares de outros entes públicos, em execução ou concluídos nos 180 (cento e oitenta) dias anteriores à data da pesquisa de preços: Sem sucesso; e
- Pesquisas com os fornecedores: Cotações D e E;

Processo Administrativo n.10265.048398/2020-60		Lote Único											Valor Final de Referência em R\$
		Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	Item 7	Item 8	Item 9	Item 10	Item 11	
		T6A-00024	AAA-10787	AAA-10732	JFX-00003	AAD-33204	TK6-00004	4DS-00001	KF5-00002	QLS-00003		Repasso	
		Office 365 E1	Windows E3	Enterprise Mobility + Security	Microsoft 365 F1 (Windows + Office 365 F1 + Security Kiosk)	Microsoft 365 E3 (Windows + Office 365 E3 + Mobility +)	Office 365 Advanced Compliance	Exchange Online Archiving	Office 365 ATP P1 - ATP para e-mail	Microsoft Defender ATP	Migração	Valor por Aluno	
		5.170	5.170	5.170	4.186	14.767	250	9.356	24.123	24.123		Valor por turma	
Cotação A	Catálogo de Sol. de TIC com Condições Padronizadas	R\$ 220,94				R\$ 1.193,31							
		R\$ 1.142.259,80				R\$ 17.621.608,77							
Cotação B (NOTA 01)	Pregão: 080/2019 UASG: 30001 TCU	R\$ 88,82		R\$ 427,67			R\$ 249,82		R\$ 62,62				
		R\$ 459.499,40		R\$ 2.249.536,90			R\$ 62.455,00		R\$ 1.510.682,26				
Cotação C (NOTA 02)	Pregão: 37/2019 UASG: 925040 - MPERO										R\$ 662.636,41	R\$ 763,33	
												R\$ 22.900,00	
Cotação D	Logicalis	R\$ 286,52	R\$ 206,59	R\$ 322,30	R\$ 306,67	R\$ 1.221,03	R\$ 286,52	R\$ 76,22	R\$ 49,31	R\$ 119,09			
		R\$ 1.481.308,40	R\$ 1.068.070,30	R\$ 1.666.291,00	R\$ 1.283.720,62	R\$ 18.030.950,01	R\$ 71.630,00	R\$ 713.114,32	R\$ 1.189.505,13	R\$ 2.872.808,07			
Cotação E	Brasware Informática	R\$ 437,64	R\$ 304,62	R\$ 627,46	R\$ 585,60	R\$ 1.970,22	R\$ 410,22	R\$ 145,48	R\$ 102,83	R\$ 303,14			
		R\$ 2.262.081,80	R\$ 2.039.686,63	R\$ 2.726.899,27	R\$ 2.451.321,60	R\$ 29.094.189,52	R\$ 102.554,17	R\$ 1.361.079,69	R\$ 2.480.568,09	R\$ 7.312.646,22			
Cotação F	Pregão: 60/2019 UASG: 50001 - STJ		230,40										
			R\$ 1.191.168,00										
Cotação G	Pregão: 61/2018 UASG: 323031 - ANP	R\$ 292,92											
		R\$ 1.514.396,40	R\$ 1.381.372,30										
Cotação H	Pregão: 008/2019 UASG: 443001 - ANA					R\$ 1.352,76							
						R\$ 19.976.206,92							
Cotação I	Pregão: 093/2018 UASG: 925942 - TJP				R\$ 378,91	1.145,64							
					R\$ 1.586.117,26	R\$ 16.917.665,88							
Cotação J	Pregão: 005/2020 UASG: 590001 - CNMP	R\$ 399,72						R\$ 132,84					
		R\$ 2.066.552,40						R\$ 1.242.851,04					
Cotação K (NOTA 03)	Pregão: 037/2019 UASG: 926302 - PGJBA	R\$ 340,85									R\$ 334.970,05	R\$ 656,10	
		R\$ 1.762.211,73										R\$ 19.682,89	
Preço Final de Referência para o Pregão Eletrônico													
Média de Preços para cada item (NOTA 04)		R\$ 1.379.321,53	R\$ 1.129.619,15	R\$ 1.666.291,00	R\$ 1.434.918,94	R\$ 17.523.408,22	R\$ 67.042,50	R\$ 713.114,32	R\$ 1.189.505,13	R\$ 2.872.808,07	R\$ 334.970,05	R\$ 709,71	R\$ 28.332.290,36
												R\$ 21.291,45	

(Tabela 08: Valor Total Estimado para a Contratação)



8. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Responsável pela análise de viabilidade ou não da contratação	Viável			Não viável		
	1	2	3	1	2	3
Integrantes Técnicos (ver 8.2)	X	X	X			
	4			4		
Integrantes Requisitantes	X					
Autoridade Competente (quando os Integrantes acima declararem a inviabilidade da contratação)						

(Tabela 09: Declaração de viabilidade da contratação)

Integrantes Técnicos

- 1 - Fabio R G Bernardo
- 2 – José Fábio Soares
- 3- Vicente E C de Paula

Integrante Requisitante

- 4- Luiz Carlos Ferreira

8.1. Justificativa para a solução escolhida

Resumidamente, a justificativa para a solução escolhida se encontra no subitem 6.1 e se vale por duas premissas: Financeira (economicidade) e técnica (eficácia, eficiência e efetividade).

A fim de atender explorar mais a premissa técnica, aos seus requisitos e a identificação dos benefícios a serem alcançados, além dos já previstos no subitem 6.5, levantaremos nesta seção a descrição técnica completa da Solução Escolhida e os principais benefícios que esperamos agregar à Secretaria Especial da Receita Federal do Brasil.

Vale mais uma vez destacar que, o grande desafio neste momento é a atualização do nosso parque de infraestrutura de Tecnologia, tendo em vista mudanças no cenário orçamentário e tecnológico. O modelo adotado correntemente de contratações pontuais e de soluções próprias, baseadas em investimento em equipamentos e software, está em processo de transformação no serviço público, considerando restrições orçamentárias e oferecimento pelo mercado de Software como Serviços (SaaS), ou seja, em nuvem.

Inclusive, a Instrução Normativa nº 1, de 4 de abril de 2019 do Ministério da



Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital, preconizou no seu Anexo, no subitem 4.1 que **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.**

Vale citar que já notamos tal modelo em nuvem adotado em alguns órgãos como: Ministério Público do Estado de Rondônia; Agência Nacional de Petróleo; Polícia Federal; Tribunal de Contas da União; Agência Nacional de Aguas; Conselho Nacional do Ministério Público; e Superior Tribunal de Justiça.

Tendo em vista processos de trabalho mais integrados, demandas por maior produtividade, aumento da modalidade teletrabalho e restrições orçamentárias, há demandas na própria RFB para soluções que tragam ferramentas que possam suprir essas necessidades. Portanto, há demandas para soluções integradas, serviços em substituição a investimentos em equipamentos e licenças de softwares, soluções de serviços disponibilizados em nuvem, integração dos processos de trabalho com múltiplos dispositivos, plataformas de trabalho comuns para usuários no Órgão e em teletrabalho, integração das diversas formas de comunicação, segurança da informação integrada nas soluções de tecnologia, eliminação do conceito de proteção do perímetro da rede, entre outros.

Como benefício da nova Solução de Serviços Integrados podemos observar os seguintes itens de produtos da Microsoft a serem contratados em um lote único: Office 365 E1; Windows E3; Enterprise Mobility + Security E3 (EMS E3); Microsoft 365 F1; Microsoft 365 E3; Office 365 Advanced Compliance; Exchange Online Archiving; Office 365 Advanced Threat Protection Premium P1; e o Microsoft Defender Advanced Threat Protection.

Será detalhado nas próximas linhas os principais benefícios de cada um dos itens:

<u>Item 01 - Office 365 E1</u>
Descrição: Solução integrada de colaboração e produtividade
Benefícios: <ul style="list-style-type: none">• Office para aplicativos móveis e Office para Web com Word, PowerPoint, OneNote e Excel.• E-mail e calendários – Exchange Online com experiência do Outlook, caixa de correio de 50GB, caixa de correio de arquivo morto de 50GB, caixas de correio compartilhadas de 50GB e anexos de até 150MB.



- Hub para trabalho em equipe – Microsoft Teams que reúne chats, conteúdo, pessoas e ferramentas. Pesquisa e mensagens ilimitadas, acesso para convidado, versão web dos aplicativos Word, PowerPoint, Excel e OneNote no Teams, domínio de e-mail personalizado e hospedagem de e-mails do Exchange, mais de 140 aplicativos e serviços integrados e armazenamento de arquivos.
- Reuniões online – Microsoft Teams com áudio, vídeo em alta definição, webconferência e streaming. Chamadas de áudio e vídeo online individuais e em grupo, reuniões de canal, compartilhamento de tela, reuniões agendadas, gravação de reunião, audioconferência.
- Social e intranet – Sharepoint Online e Yammer que reúnem gerenciamento de conteúdo, sites de equipes, compartilhamento de arquivos, dados, notícias e recursos, acesso para convidado, intranet móvel e inteligente, portais, notificações e aprovações, fluxos de trabalho, rede social corporativa, eventos ao vivo incluindo reuniões abertas, reuniões corporativas e treinamentos, comunidades de interesse, portal de ideias e comentários.
- Arquivos – OneDrive for Business com 1TB de armazenamento. Solução segura de arquivos em nuvem, compartilhamento, controle de acesso e edição colaborativa.
- Conteúdo – Microsoft Stream e Sway que reúnem serviço de streaming de vídeo, recursos de conversão de voz em texto, legendas automáticas e detecção de rosto, retenção de conhecimento e engajamento em treinamentos e cursos, criação e compartilhamento de relatórios interativos, histórias pessoais e apresentações.
- Gerenciamento de tarefas – Microsoft Planner e Microsoft To Do que reúnem planos e planejamentos pessoais e de equipes com controle de atividades, organização e atribuição de tarefas, compartilhamento de arquivos e chat sobre trabalho.
- Aplicativos de negócios - Microsoft Power Apps e Microsoft Power Automate que reúnem ferramentas de low-code para criação de aplicativos, fluxos de trabalho, automação de processos e formulários personalizados.
- Análise de produtividade pessoal – Microsoft MyAnalytics com insights de produtividade pessoal, conectado ao Outlook, que utilizam Inteligência artificial para sugerir formas de trabalhar com mais inteligência, melhorando foco, bem-estar, contatos e colaboração.
- Microsoft Graph API – API e gateway do Office 365 para dados e inteligência. As APIs REST ou SDKs permitem acessar pontos de extremidade e desenvolver aplicativos compatíveis com cenários que abrangem produtividade, colaboração, educação, segurança, identidade, acesso, gerenciamento de dispositivo e muito mais.
- Office Delve – Gerenciamento de perfil individual do Office 365 com ferramentas para descobrir e organizar informações importantes.
- Sincronização com Active Directory on-premises para single- sing-on.
- Gerenciamento de Dispositivos Móveis para Office 365 – funcionalidades de gerenciamento para iOS, Android e Windows Phone, inventário de dispositivos móveis



que acessam aplicações corporativas, limpeza total ou seletiva do dispositivo, definições de configuração do dispositivo móvel (comprimento do PIN, PIN necessário, tempo de bloqueio, dentre outros), certificação raiz e detecção de jailbreak, controle de acesso a e-mail e documentos corporativos com base em políticas de conformidade e relatórios.

- Licença cliente de acesso padrão, Client Access License (CAL), aos serviços on-premises do Exchange Server, SharePoint Server e Skype for Business Server

Item 02 – Windows E3.

Descrição: Upgrade de sistema operacional de desktop Windows 10 Enterprise E3

Benefícios:

- App-V – Esse recurso disponibiliza os aplicativos para os usuários finais sem instalar os aplicativos diretamente nos dispositivos dos usuários. Esse recurso também ajuda a garantir que os aplicativos sejam mantidos atualizados com as atualizações de segurança mais recentes.

- BranchCache – Permite que os PCs dos usuários armazenem em cache arquivos, sites e outros conteúdos de servidores centrais, para que o conteúdo não seja baixado repetidamente na WAN.

- DirectAccess e Always On VPN – Permite que usuários remotos acessem recursos na rede corporativa da RFB sem precisar iniciar uma VPN separada.

- User Experience Virtualization – Usado para virtualizar a personalização da área de trabalho. Segundo análise do Gartner, ele gerencia as configurações do usuário e os dados do perfil para servir a vários propósitos. Ele oferece melhores recursos do que os oferecidos pela tecnologia de perfil de usuário móvel da Microsoft, melhorando as velocidades de logon / logoff e reduzindo a probabilidade de corrupção do perfil. Ele permite que a personalização do usuário (como configurações do SO e configurações de aplicativos) permaneça consistente entre aplicativos físicos, aplicativos virtuais, ambientes de computação baseada em servidor (SBC) e HVDs.

- Windows Defender Application Control e AppLocker – Funcionalidade que gerencia o serviço de integridade de código ou "integridade de código configurável" e verifica se o código que o Windows está executando é confiável. Existem dois componentes principais: integridade do código do modo do kernel (KMCI) e integridade do código do modo do usuário (UMCI). O KMCI controla aplicativos não assinados no nível do kernel, como drivers. O UMCI controla aplicativos em nível de usuário e executa apenas código assinado e certificado. Usando políticas de integridade de código, os administradores podem criar um ambiente de controle de aplicativos de negação padrão que permite apenas que aplicativos selecionados e desenvolvedores confiáveis de aplicativos sejam executados no modo de usuário e no kernel.

- Windows Defender Credential Guard – Funcionalidade que ajuda a proteger os



tokens de acesso do usuário contra hackers, armazenando-os em um contêiner isolado de hardware seguro, derrotando uma tática importante usada para comprometer as redes.

- Windows Defender Application Guard – A funcionalidade executa o navegador Edge em um enclave virtual com apenas acesso intermediado aos serviços do SO. O Microsoft Edge abre o site em um contêiner virtual isolado, separado do sistema operacional host. O WDAG pode dificultar significativamente os ataques do navegador a comprometer outras partes do sistema operacional

Item 03 – Enterprise Mobility + Security E3 (EMS E3)

Descrição: Plataforma de segurança e gerenciamento inteligente com o objetivo de ajudar a proteger e garantir a segurança da organização em equilíbrio com as novas maneiras flexíveis de colaboração e trabalho moderno.

Composição:

- Item 3.1: Azure Active Directory Premium P1;
- Item 3.2: Microsoft Endpoint Manager;
- Item 3.3: Azure Information Protection Premium P1;
- Além de Licença cliente de acesso padrão, Client Access License (CAL), aos serviços on-premises do Windows Server, RMS e Microsoft Identity Management CAL e aos aos serviços on-premises do System Center Configuration Manager e System Center Endpoint Protection Management License (ML)

Benefícios:

Item 3.1. Microsoft Azure Active Director

- Gerenciamento de aplicativos – Capacidade de gerenciar aplicativos de nuvem e locais usando o Proxy de Aplicativo, o logon único, o portal Meus aplicativos (também conhecido como Painel de acesso) e aplicativos SaaS (software como serviço).
- Autenticação – Capacidade de gerenciar a redefinição de senha por autoatendimento do Azure Active Directory, a Autenticação Multifator, a lista personalizada de senhas banidas e o bloqueio inteligente.
- Acesso condicional – Controle de acesso condicional com base em grupo, localização e estado do dispositivo incluindo autenticação multifator.
- Azure Active Directory para desenvolvedores – Capacidade de criar aplicativos que aceitam todas as identidades da Microsoft, obtenha tokens para chamar o Microsoft Graph, outras APIs da Microsoft ou APIs personalizadas.
- Gerenciamento de dispositivo – Capacidade de gerenciar como os dispositivos de nuvem ou locais acessam dados corporativos.
- Serviços do domínio – Capacidade de adicionar notebooks e dispositivos móveis, bem como máquinas virtuais do Azure a um domínio sem usar controladores de



domínio.

- Usuários corporativos e gerenciamento avançado de acesso a grupos – Capacidade de gerenciar a atribuição de licenças, o acesso a aplicativos e configurar representantes usando grupos e funções de administrador.
- Identidade híbrida – Use o Azure Active Directory Connect e o Connect Health para fornecer uma identidade de usuário única para autenticação e autorização de todos os recursos, independentemente da localização (nuvem ou local)

Item 3.2 Gerenciamento de Dispositivos e Aplicações – Microsoft Endpoint Manager (Intune e System Center Configuration Manager):

- Gerenciamento de dispositivos flexível, escolha estar 100% na nuvem com o Intune ou ser cog gerenciado com o Configuration Manager e o Intune.
- Implantar certificados, perfis VPN (incluindo perfis específicos de aplicativos) e perfis Wi-Fi.
- Impedir recortar / copiar / colar / salvar dados de aplicativos corporativos em aplicativos pessoais (gerenciamento de aplicativos móveis).
- Visualização segura de conteúdo via aplicativos de navegador gerenciado, visualizador de PDF, visualizador de imagens e reproduzidor de AV para Intune.
- Bloqueio de dispositivo remoto via Portal da empresa de autoatendimento e via console administrativa.
- Registro e gerenciamento de coleções de dispositivos de propriedade corporativa, simplificando a implantação de políticas e aplicativos.
- Capacidade de implantar aplicativos internos de linha de negócios e aplicativos nas lojas para usuários corporativos.
- habilitar a navegação na Web mais segura usando o aplicativo Navegador gerenciado do Intune.
- Gerenciamento baseado em nuvem para PCs com Mac OS X e Windows.
- Gerenciamento de PC (por exemplo, inventário, antimalware, patch, políticas etc.).
- Implantação do SO (via System Center ConfigMgr).
- Gerenciamento de software para PC.
- Console de gerenciamento único para PCs e dispositivos móveis

Item 3.3 Governança dos dados e proteção das informações – Azure Information Protection Premium P1

- Proteção para formatos de arquivo que não são do Microsoft Office, incluindo PTXT, PJPNG e PFILE (proteção genérica).
- Classificação de documentos em manual, padrão e obrigatório.
- Scanner para descoberta de conteúdo de arquivos locais correspondentes a qualquer um dos tipos de informações confidenciais.
- Scanner para aplicar um rótulo a todos os arquivos em um repositório ou



servidor de arquivos local.

- Conector do Rights Management com compartilhamentos de arquivos do Windows Server locais usando o conector de FCI (Infraestrutura de Classificação de Arquivos).
- Acompanhamento e revogação de documentos.
- SDK (Kit de Desenvolvimento de Software) de Proteção de Informações da Microsoft para aplicar rótulos e proteção a e-mails e arquivos para todas as plataformas – Windows, iOS, Mac OSX, Android e Linux.

Item 04 – Microsoft 365 F1

Descrição: O Microsoft 365 reúne o Office 365, Windows 10 e Enterprise Mobility + Security para fornecer uma solução completa, inteligente e segura que capacita as pessoas. Ele foi projetado para liberar efetivamente o poder da criatividade na empresa 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 F1 é um licenciamento direcionado para usuários de linha de frente que não possuem um computador dedicado para o trabalho.

Composição:

Item 4.1: Office 365 E1;

Item 4.2: Enterprise Mobility e Security Kiosk

Item 4.3: Windows E3

Benefícios:

Item 4.1: Office 365 E1

• Office para aplicativos móveis e Office para Web com Word, PowerPoint, OneNote e Excel. Limitado a dispositivos com telas integradas de 10,1” na diagonal ou menos.

- E-mail e calendários – Exchange Online com experiência do Outlook Web, caixa de correio de 2GB, caixas de correio compartilhadas de 50GB e anexos de até 150MB.

- Hub para trabalho em equipe (permissão de colaboração, restrição para criação de times) – Microsoft Teams que reúne chats, conteúdo, pessoas e ferramentas. Pesquisa e mensagens ilimitadas, acesso para convidado, versão web dos aplicativos Word, PowerPoint, Excel e OneNote no Teams, domínio de e-mail personalizado e hospedagem de e-mails do Exchange, mais de 140 aplicativos e serviços integrados e armazenamento de arquivos.

- Reuniões online (permissão de chamadas 1:1 e restrição para criação de



conferências) – Funcionalidades de convidado e leitura do Microsoft Teams com áudio, vídeo em alta definição, webconferência e streaming. Chamadas de áudio e vídeo online individuais e em grupo, reuniões de canal, compartilhamento de tela, reuniões agendadas, gravação de reunião, audioconferência.

- Social e intranet (permissão de apenas leitura) – Sharepoint Online e Yammer que reúnem gerenciamento de conteúdo, sites de equipes, compartilhamento de arquivos, dados, notícias e recursos, acesso para convidado, intranet móvel e inteligente, portais, notificações e aprovações, fluxos de trabalho, rede social corporativa, eventos ao vivo incluindo reuniões abertas, reuniões corporativas e treinamentos, comunidades de interesse, portal de ideias e comentários.

- Arquivos – OneDrive for Business com 2GB de armazenamento. Solução segura de arquivos em nuvem, compartilhamento, controle de acesso e edição colaborativa. Restrição para sincronização com o desktop.

- Conteúdo (permissão de apenas leitura) – Microsoft Stream e Sway que reúnem serviço de streaming de vídeo, recursos de conversão de voz em texto, legendas automáticas e detecção de rosto, retenção de conhecimento e engajamento em treinamentos e cursos, criação e compartilhamento de relatórios interativos, histórias pessoais e apresentações.

- Aplicativos de negócios (permissão de apenas leitura) - Microsoft Power Apps e Microsoft Power Automate que reúnem ferramentas de low-code para criação de aplicativos, fluxos de trabalho, automação de processos e formulários personalizados.

- Microsoft Graph API – API e gateway do Office 365 para dados e inteligência. As APIs REST ou SDKs permitem acessar pontos de extremidade e desenvolver aplicativos compatíveis com cenários que abrangem produtividade, colaboração, educação, segurança, identidade, acesso, gerenciamento de dispositivo e muito mais.

- Sincronização com Active Directory on-premises para single- sing-on.

- Gerenciamento de Dispositivos Móveis para Office 365

Item 4.2: Enterprise Mobility e Security Kiosk

- Como o perfil de usuários elegível compreende usuários de linha de frente que não possuem um computador dedicado para o trabalho, esta licença leva o nome de Kiosk, porém, ela compreende as mesmas funcionalidades e soluções listadas no Item 3 Enterprise Mobility + Security E3 (EMS E3)

Item 4.3: Windows E3

Como o perfil de usuários elegível compreende usuários de linha de frente que não possuem um computador dedicado para o trabalho, esta licença leva o nome de Kiosk, porém, ela compreende as mesmas funcionalidades e soluções listadas no Item 2 Windows E3



Item 05 – Microsoft 365 E3

Descrição: Com o mesmo conceito do Item 4 de uma solução completa

Composição:

- Item 5.1: Office 365 E3;
- Item 5.2: Enterprise Mobility + Security Kiosk E3;
- Item 5.3: Windows E3;
- Além do Direito de executar on-premises os servidores de produtividade Exchange Server, Skype for Business Server e SharePoint Server.

Benefícios:

• **Item 5.1: Office 365 E3:**

- Aplicativos cliente do Office (Outlook, Word, Excel, PowerPoint, OneNote, Access e Publisher) em até cinco PCs/Macs + cinco tablets + cinco smartphones por pessoa com o Office 365 ProPlus;
- Office 365 para Mac;
- E-mail e calendários – Exchange Online com experiência do Outlook, caixa de correio de 100GB, caixa de correio de arquivo morto ilimitada, caixas de correio compartilhadas de 50GB e anexos de até 150MB;
- Além dos demais benefícios descritos na licença E1 e F1

• **Item 5.2: Enterprise Mobility + Security Kiosk E3**

Igual ao item 03

• **Item 5.3: Windows E3**

Igual ao item 02

Item 06 – Office 365 Advanced Compliance

Descrição: A conformidade avançada do Microsoft Office 365 inclui governança avançada de dados -Compliance Manager, descoberta eletrônica avançada - Advanced eDiscovery e caixa de bloqueio do cliente -Customer Lockbox. O pacote oferece maior valor de conformidade aos clientes e uma combinação de soluções, além de ajudar os clientes a atender aos requisitos de conformidade.

Benefícios:

- Compliance Manager – Portal para gerenciar conformidade de um só lugar, com risco contínuo avaliações nos serviços em nuvem da Microsoft, insights acionáveis e simplificados dos processos de conformidade.
- Advanced eDiscovery – Fornece um fluxo de trabalho de ponta a ponta para preservar, coletar, analisar e exportar conteúdo que responde às investigações internas e externas da sua organização. Também permite que as equipes jurídicas gerenciem todo o fluxo de trabalho de notificação de retenção legal para se comunicarem com os responsáveis envolvidos em um caso.



- **Advanced Data Governance** – O Office 365 Advanced Data Governance aplica o aprendizado de máquina para ajudar os clientes a encontrar e reter dados importantes, eliminando dados triviais, redundantes e obsoletos que podem causar riscos se comprometidos.
 - **Customer Lockbox** – O Lockbox do cliente oferece suporte a solicitações de acesso a dados no Exchange Online, no SharePoint Online e no OneDrive for Business. A Lockbox do cliente garante que a Microsoft não possa acessar seu conteúdo para executar uma operação de serviço sem a sua aprovação explícita. O Lockbox do cliente o coloca no fluxo de trabalho de aprovação para solicitações de acesso ao seu conteúdo.
 - **Customer Key** – O Office 365 fornece a linha de base e a criptografia no nível do volume habilitadas por meio do BitLocker e do DKM (Distributed Key Manager). O Office 365 oferece uma camada adicional de criptografia no nível do aplicativo para seu conteúdo. Este conteúdo inclui dados do Exchange Online, Skype for Business, SharePoint Online, OneDrive for Business e arquivos do teams. A chave do cliente criptografa dados em repouso no Office 365.
 - **Controle de Acesso ao Office 365** – O gerenciamento de acesso privilegiado permite o controle de acesso granular sobre tarefas administrativas privilegiadas no Office 365. Ele pode ajudar a proteger sua organização contra violações que usam contas de administrador privilegiadas existentes com acesso à dados confidenciais ou acesso a definições de configuração crítica.
 - **DLP para Teams Chat e conversas de canais.**
 - **Information Barriers** – Políticas para restringir comunicações entre determinadas pessoas dentro da organização.
 - **Advanced Message Encryption** – A criptografia de mensagem avançada no Office 365 ajuda os clientes a cumprir as obrigações de conformidade que exigem controles mais flexíveis sobre destinatários externos e seu acesso a e-mails criptografados. Com a criptografia de mensagem avançada no Office 365, é possível controlar e-mails confidenciais compartilhados fora da organização com políticas automáticas.
 - **Data Investigations** – Um despejo de dados ocorre quando um documento que contém conteúdo confidencial, confidencial ou mal-intencionado é liberado em um ambiente não confiável. Quando um despejo de dados é detectado, é importante conter rapidamente o ambiente, avaliar o tamanho e os locais do derramamento, examinar as atividades do usuário em torno dele e, em seguida, excluir os dados derramados do serviço. Com esta ferramenta de investigações de dados (visualização), é possível pesquisar dados confidenciais, mal-intencionados ou incorretos no Office 365, investigar o que aconteceu e tomar as medidas apropriadas para corrigir o derramamento.
 - **Supervision policies** – As políticas de supervisão no Office 365 permitem capturar comunicações de funcionários para verificação por revisores designados. É possível definir políticas específicas que capturam e-mails internos e externos, Microsoft Teams



ou comunicações de terceiros em sua organização. Os revisores podem, então, examinar as mensagens para garantir que estejam em conformidade com os padrões de mensagem da sua organização e as resolvem com o tipo de classificação

Item 07 – Exchange Online Archiving

Descrição: Solução de arquivamento baseada na nuvem e com nível empresarial, que tem como objetivo ajudar a resolver desafios de arquivamento, conformidade, normas e Descoberta Eletrônica

Benefícios:

- Arquivamento ilimitado – O recurso de arquivamento ilimitado no Office 365 (chamado arquivamento de expansão automática) fornece espaço de armazenamento adicional nas caixas de correio de arquivo morto. Cada assinante de arquivamento do Exchange Online recebe inicialmente 100 GB de armazenamento na caixa de correio de arquivamento. Quando o arquivamento de expansão automática está ativado, um espaço de armazenamento adicional é adicionado automaticamente quando a capacidade de armazenamento de 100 GB é atingida.

- Arquivo Morto no Local – Uma caixa de correio de arquivo morto é uma caixa de correio especializada que aparece ao lado das pastas de caixa de correio principal dos usuários no Outlook ou no Outlook na Web. Os usuários podem acessar o arquivo da mesma maneira que acessam suas caixas de correio principais. Além disso, eles podem pesquisar seus arquivos e caixas de correio principais. Manutenção de todos os dados importantes em um só lugar, fornecendo aos usuários uma experiência bem integrada e nativa.

- Recuperação de item excluído – Os usuários podem restaurar itens que foram excluídos de qualquer pasta de e-mail em seus arquivos. Quando um item é excluído, ele é mantido na pasta Itens Excluídos do arquivo morto. Ele permanece lá até ser removido manualmente pelo usuário ou automaticamente removido pelas políticas de retenção.

- Recuperação de caixa de correio excluída.
- Redundância de serviço de caixa de correio.

- O arquivamento do Microsoft Exchange Online permite que os usuários se conectem às caixas de correio de arquivamento a partir de uma variedade de dispositivos e plataformas. Toda a conectividade de rede ao arquivo do usuário ocorre pela Internet, e as conexões de rede virtual privada (VPN) não são necessárias.

- Políticas de retenção – O Arquivamento do Exchange Online oferece políticas de retenção para ajudar as organizações a reduzir os passivos associados ao e-mail e outras comunicações. Com essas políticas, os administradores podem aplicar



configurações de retenção a pastas específicas nas caixas de entrada dos usuários. Os administradores também podem fornecer aos usuários um menu de políticas de retenção e deixá-los aplicar as políticas a itens, conversas ou pastas específicas usando o Outlook 2010 ou posterior ou o Outlook na Web. No Arquivamento do Exchange Online, os administradores gerenciam as políticas de retenção da infraestrutura local.

- In-Place Hold e Litigation Hold – Quando existe uma expectativa razoável de litígio, as organizações são obrigadas a preservar as informações armazenadas eletronicamente (ESI), incluindo e-mails relevantes para o caso. Essa expectativa pode ocorrer antes que as especificidades do caso sejam conhecidas, e a preservação geralmente é ampla. As organizações podem preservar todos os emails relacionados a um tópico específico ou todos os emails de determinadas pessoas.

- In-Place eDiscovery – O Arquivamento do Exchange Online oferece suporte à Descoberta Eletrônica In-loco para pesquisar o conteúdo de caixas de correio em uma organização. Usando o centro de administração do Exchange ou o Windows PowerShell remoto a partir de um servidor Exchange 2013 local, administradores ou gerentes autorizados do Discovery podem pesquisar uma variedade de itens de caixa de correio - incluindo mensagens de email, anexos, compromissos de calendário, tarefas e contatos. A descoberta eletrônica no local pode pesquisar simultaneamente nas caixas de correio e arquivos principais. Os recursos avançados de filtragem incluem remetente, destinatário, tipos de mensagem, data de envio, data de recebimento, cópia carbono e cópia oculta, junto com a sintaxe da linguagem de consulta de palavras-chave (KQL).

- Criptografia entre servidores locais e arquivamento do Exchange Online – O TLS é usado para criptografar a conexão entre servidores de e-mail para ajudar a evitar falsificações e fornecer confidencialidade às mensagens em trânsito. O TLS também é usado para proteger o tráfego do servidor de correio local nos datacenters do Office 365 para arquivamento do Exchange Online.

- Criptografando entre clientes e arquivamento do Exchange Online – As conexões do cliente com o Arquivamento do Exchange Online usam o SSL para proteger o tráfego do Outlook, Outlook na Web e Exchange Web Services, usando a porta TCP 443.

- Criptografia: S/MIME e PGP

Item 08 – Office 365 Advanced Threat Protection Premium P1

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



que ocorrem na organização.

Benefícios:

- Anexos Seguros – Os anexos seguros de ATP protegem contra malware e vírus desconhecidos e fornecem proteção de dia zero para proteger seu sistema de mensagens. Todas as mensagens e os anexos que não tenham uma assinatura de vírus/malware conhecida são roteados para um ambiente especial onde a ATP usa uma variedade de técnicas de aprendizagem e análise automática para detectar conteúdo mal-intencionado. Se nenhuma atividade suspeita for detectada, a mensagem será liberada para entrega na caixa de correio.
- Links Seguros – O recurso links seguros de ATP protege usuários contra URLs mal-intencionadas em uma mensagem ou em um documento do Office. A proteção permanece sempre que o link é selecionado, pois links mal-intencionados são bloqueados dinamicamente enquanto bons links podem ser acessados.
- ATP para SharePoint, OneDrive e Microsoft Teams – Ajuda a detectar e bloquear arquivos identificados como mal-intencionados em sites de equipe e bibliotecas de documentos.
- Políticas anti-phishing – Verifica mensagens de entrada para indicadores que uma mensagem pode ser uma tentativa de phishing. Quando os usuários são cobertos por políticas ATP (anexos seguros, links seguros ou anti-phishing), as mensagens de entrada são avaliadas por vários modelos de aprendizado de máquina que analisam mensagens e a ação apropriada é executada, com base nas políticas configuradas.
- Relatórios em tempo real – Os recursos de monitoramento disponíveis no centro de conformidade & segurança do Office 365 incluem relatórios e insights em tempo real que permitem aos administradores de segurança e conformidade se concentrarem em problemas de alta prioridade, como ataques de segurança ou uma maior atividade suspeita. Além de destacar áreas problemáticas, relatórios inteligentes e insights incluem recomendações e links para exibir e explorar dados e, também, realizar ações rápidas

Item 09 – Microsoft Defender Advanced Threat Protection

Descrição: A Proteção Avançada contra Ameaças do Microsoft Defender (ATP) é uma plataforma unificada para proteção preventiva, detecção pós-violação, investigação automatizada e resposta

Benefícios:

- Gerenciamento de vulnerabilidades e ameaças – Ajuda as organizações a descobrir vulnerabilidades e configurações incorretas em tempo real, com base em sensores, sem a necessidade de agentes ou verificações periódicas. Ele prioriza vulnerabilidades com base no cenário de ameaças, detecções em sua organização, informações confidenciais sobre dispositivos vulneráveis e contexto de negócios.



- Redução da superfície de ataque – Reduz as superfícies de ataque minimizando os locais em que a organização está vulnerável a cyber threats e ataques.
- Isolamento baseado em hardware no Windows 10 – O isolamento baseado em hardware ajuda a proteger a integridade do sistema no Windows 10 e é integrado ao Microsoft Defender ATP.
- Exploit Protection – A proteção contra exploração aplica automaticamente várias técnicas de mitigação de exploração a aplicativos e processos do sistema operacional. A proteção contra exploração tem suporte a partir do Windows 10, versão 1709 e Windows Server, versão 1803.
- Proteção de rede – A Proteção de rede ajuda a reduzir a superfície de ataque de dispositivos em eventos baseados na Internet. Ela evita que funcionários usem qualquer aplicativo para acessar domínios perigosos que podem hospedar tentativas de phishing, explorações e outro conteúdo mal-intencionado na Internet.
- Controle de aplicativo – Restringe os aplicativos que os usuários têm permissão para executar e o código que é executado no núcleo do sistema (kernel). As políticas de controle de aplicativo também podem bloquear scripts não assinados e MSIs e restringir o Windows PowerShell a executar em modo de linguagem restrita (Constrained Language Mode).
- Proteção Web – A proteção pela Web permite que você proteja suas máquinas contra ameaças da Web e o ajude a controlar conteúdo indesejado.
- Acesso Controlado a Pastas – O Acesso controlado a pastas (controlled folder access) ajuda a proteger dados valiosos contra aplicativos maliciosos e ameaças, como ransomware. Ele protege seus dados verificando a lista de aplicativos confiáveis conhecidos. O acesso a pastas controladas tem suporte no Windows Server 2019, além de clientes do Windows 10.
- Proteção de próxima geração no Windows 10 e no Windows Server 2016 – O Windows Defender Antivirus é o componente de proteção de próxima geração do Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP). A proteção de última geração reúne o Machine Learning, a análise de grandes dimensões, a pesquisa sobre resistência a ameaças mais profunda e a infraestrutura de nuvem para proteger dispositivos em sua empresa.
- Detecção e resposta (endpoint detection and response – EDR) – Os recursos de detecção e resposta de ponto de extremidade do Microsoft Defender ATP fornecem detecções de ataques avançados quase em tempo real e acionáveis. Page 20 of 33
- Fila de Incidentes – A fila incidentes mostra uma coleção de incidentes que foram sinalizados de máquinas na rede. Ele ajuda a classificar incidentes para priorizar e criar uma decisão de resposta adequada.
- Filas de Alertas – A fila de alertas mostra uma lista de alertas que foram sinalizados de máquinas na rede. Por padrão, a fila exibe alertas vistos nos últimos 30 dias em uma exibição agrupada, com os alertas mais recentes mostrados na parte superior da lista, ajudando você a ver os alertas mais recentes primeiro.



- Investigações automatizadas – O Microsoft defender ATP usa recursos automatizados de investigação e correção para reduzir significativamente o volume de alertas que devem ser investigados individualmente.
- Pontuação de Segurança (Secure Score) – O painel pontuação de segurança (Secure Score) expande a visibilidade da postura de segurança geral da organização. Nesse painel, é possível rapidamente avaliar a postura de segurança da organização, ver computadores que exigem atenção, bem como recomendações de ações para reduzir ainda mais a superfície de ataque em sua organização - tudo em um só lugar. A partir daí você pode agir com base nas baselines de configurações recomendadas.
- Busca Avançada (Advanced Hunting) – Ferramenta de busca de ameaças baseada em consulta que permite explorar até 30 dias de dados brutos.
- Gerenciamento e APIs – O Microsoft defender ATP expõe muitos de seus dados e ações por meio de um conjunto de APIs programáticas. Essas APIs permitirão que automatize fluxos de trabalho e inovações com base em recursos ATP do Microsoft Defender.
- Integrações nativas do Microsoft Defender ATP – O Microsoft defender ATP integra-se nativamente com várias soluções da Microsoft, como Azure Advanced Threat Protection, Azure Security Center, Azure Information Protection, Azure Active Directory, Microsoft Cloud App Security e Office 365 Advanced Threat Protection.
- Microsoft Threat Experts – Contato com o time de especialistas em ameaças da Microsoft. É um serviço de MDR (detecção e resposta gerenciada) que fornece aos SOCs, monitoramento e análise do Expert Microsoft para ajudar a garantir que ameaças críticas em seus ambientes únicos não sejam perdidas

8.2. Ressalva para a solução escolhida

A única ressalva para a solução escolhida pelos integrantes técnicos para essa Contratação seria a falta de tempo hábil, em virtude do fim das vigências contratuais, a partir do meio desse ano, citado na Tabela 01, de fazer todos os testes de migração e prova de conceito da solução escolhida.

Vale lembrar, que ferramentas de produtividade como Microsoft Teams, além da versão web dos aplicativos Word, PowerPoint, Excel e OneNote foram amplamente testados no ambiente preparado especificamente para esse órgão: rfgov.onmicrosoft.com.

Por outro lado, ainda estamos no meio das tratativas para migração de algumas caixas postais para o Exchange Online utilizando o serviço “FastTrack” que é um serviço fornecido pela Microsoft que ajuda os clientes a integrar as soluções do Microsoft Cloud disponível para o Microsoft 365, Office 365, Azure, Dynamics 365, entre outros.



9. APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela PORTARIA RFB/SUCOR/COPOL Nº 19, de 14 de fevereiro de 2020, publicada no Boletim de Serviços da RFB em 18 de fevereiro de 2020.

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			INTEGRANTE REQUISITANTE
_____ Fabio R G Bernardo Matrícula/SIAPE: 2029585 <i>Assinado digitalmente</i>	_____ José F Soares Matrícula/SIAPE: 2090302 <i>Assinado digitalmente</i>	_____ Vicente E C de P Pessoa Matrícula/SIAPE: 1180697 <i>Assinado digitalmente</i>	_____ Luiz Carlos Ferreira Matrícula/SIAPE: 0149646 <i>Assinado digitalmente</i>

AUTORIDADE MÁXIMA DA ÁREA DE TIC

Juliano Brito da Justa Neves
Coordenador-Geral da COTEC
Matrícula/SIAPE: 1458771
Assinado digitalmente



Receita Federal

PÁGINA DE AUTENTICAÇÃO

A Secretaria da Receita Federal do Brasil garante a integridade e a autenticidade deste documento nos termos do Art. 10, § 1º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001

Histórico de atividades sobre o documento:

Documento assinado digitalmente por:

FABIO RICARDO GONCALVES BERNARDO em 26/03/2020, JOSE FABIO SOARES em 27/03/2020, LUIZ CARLOS FERREIRA em 27/03/2020, VICENTE EDUARDO COSTA DE PAULA PESSOA em 01/04/2020, JULIANO BRITO DA JUSTA NEVES em 26/03/2020.

Confira o documento original pelo Smartphone conectado à Internet:



Dúvida? Acesse

<http://sadd.receita.fazenda.gov.br/sadd-internet/pages/qrcode.xhtml>

Confira o documento original pela Internet:

a) Acesse o endereço:

<http://sadd.receita.fazenda.gov.br/sadd-internet/pages/validadocumento.xhtml>

b) Digite o código abaixo:

AP01.0420.19391.4702

Código Hash obtido através do algoritmo SHA-256:

gg9pmKWleEB4k4WSY8ZW9WvJqiAp4ACP1er+A+t9IZA=