

TERMO DE REFERÊNCIA SERVIÇOS DE TIC – LEI 14.133/2021

TR nº 001/CCA-RJ/2023

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de serviço de suporte e atualização, pelo período de 24 (vinte e quatro) meses, podendo ser prorrogado por até 10 (dez) anos, de toda a infraestrutura do correio Zimbra (13.700 caixas postais Professional Edition e 137.000 caixas postais Standard Edition); de solução de filtro de conteúdo de e-mail, para proteção da totalidade das caixas postais, incluindo sistemas de segurança contra ataques dirigidos, incluindo sistemas de segurança contra ataques dirigidos, bem como treinamento, implantação, manutenção preventiva e suporte técnico especializado 24x7, para a segurança e proteção da plataforma de e-mail da Força Aérea Brasileira; e treinamento do Zimbra para 7 (sete) pessoas em softwares de e-mail, conforme condições, quantidades e exigências estabelecidas neste instrumento., nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

LOTE	ITEM	ESPECIFICAÇÃO	REQUISIÇÃO	CATSER	MÉTRICA OU UNIDADE DE MEDIDA	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	1	Serviço de suporte e atualização por 24 meses de toda a infraestrutura do correio Zimbra (13.700 caixas postais Professional Edition e 137.000 caixas postais Standard Edition)	XYP339001TI	27014	UN	1	R\$ 1.222.387,20	R\$ 1.222.387,20
	2	Solução de filtro de conteúdo de e-mail – 24 meses	XYP339002TI	27464	UN	1	R\$ 345.600,00	R\$ 345.600,00
2	3	Treinamento para 7 (sete) pessoas	XYP339003TI	3840	UN	1	R\$ 35.291,67	R\$ 35.291,67
VALOR TOTAL DA CONTRATAÇÃO (2 ANOS)								R\$ 1.603.278,87

1.2. A presente contratação adotará como regime de execução a Empreitada por Preço Unitário, por Lote.

1.3. Motivação da contratação:

1.3.1. Considerando a importância do Correio Corporativo para apoio aos processos administrativos do COMAER e a necessidade de garantir alto índice de disponibilidade do serviço, a opção pela contratação de empresa especializada em prestar suporte ao software Zimbra se deu pelos seguintes motivos:

1.3.1.1. A ferramenta já se encontra implementada do COMAER desde 2014, tendo sido expandida para toda a FAB em 2017, sendo altamente difundida entre os usuários e administradores de TI. Haveria um custo operacional muito alto, considerando homem/hora, para migrar para outra solução, o que envolveria desde a fase de planejamento e estudo de outras soluções, até configuração da solução escolhida e de todos os clientes de correio que hoje se conectam às funcionalidades do Zimbra (IMAP, Calendário, Chat etc).

1.3.1.2. A atual solução está altamente integrada com o sistema de pessoal da FAB, tendo sido elaboradas inúmeras rotinas (scripts) de sincronização e automatização de tarefas, de acordo com as peculiaridades da Rotina militar. Manutenção automática de lista de e-mails, atualização de posto/graduação do militar, atualização de cotas de e-mail e criação/desativação de contas são exemplos de rotinas que estão sincronizadas com o sistema de pessoal da FAB, evitando trabalho manual.

1.3.1.3. A atual ferramenta também está de acordo com as necessidades administrativas da FAB, uma vez que, além do serviço de mensageria, chat e calendário, também provê funcionalidades integradas com suite office colaborativa e drive de arquivos.

1.3.1.4. Além disso, não haverá custos adicionais com o licenciamento da ferramenta Zimbra, uma vez que as licenças perpétuas Professional Edition já foram adquiridas em 2017. Haverá no entanto, custo para acrescentar ferramenta de antispam e filtro de conteúdo, uma vez que atualmente são utilizados software gratuitos. Esta última ferramenta, contudo, será necessária independentemente da solução do software de e-mail escolhido. Sua necessidade frente à permanência com o software antispam gratuito, justifica-se pela capacidade superior de atualização das bases de dados de antivírus e de blacklists de e-mail, fornecendo à administração maiores funcionalidades para proteção cibernética. Um dos principais vetores de ataques cibernéticos atualmente é a utilização do correio eletrônico para disseminação de malware ou ataques do tipo Phishing.

1.3.1.5. Apesar do CCA-RJ dispor de uma equipe dedicada ao suporte do Zimbra, a contratação de um suporte avançado se faz necessária devido à alta complexidade da solução, envolvendo a integração de mais de cinquenta servidores (máquinas virtuais) e inúmeros softwares. A alta rotatividade característica do meio militar, a dificuldade de retenção de profissionais de TI altamente capacitados e a impossibilidade de dedicação de militares a atividades puramente técnicas dificultam a manutenção do serviço com as características de segurança e disponibilidades requeridas pela Força Aérea.

1.4. O agrupamento dos itens 1 e 2 foi necessário devido à alta integração entre dois elementos. A partir do momento em que a funcionalidade do item 2, a ferramenta de antispam, é integrada, ela passa a fazer parte da solução como um todo, podendo inclusive gerar problemas no funcionamento do correio corporativo. Dessa forma, a contratação de duas empresas para realizar o suporte na mesma solução poderá ocasionar problemas, principalmente no que diz respeito a atribuição de responsabilidades e sanções por perda de dados ou indisponibilidade do serviço.

1.5. O(s) serviço(s) objeto desta contratação são caracterizados como comuns, uma vez que conforme inciso XIII do Art. 6º da Lei 14.133/2021.

1.6. O prazo de vigência da contratação é de 24 (vinte e quatro) meses contados do(a) assinatura do contrato prorrogável para até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.7. O serviço é enquadrado como continuado tendo em vista que o serviço de correio eletrônico é um meio de comunicação ágil, de grande alcance e prático, tendo seu uso de relevante importância nas atividades da FAB e, desta forma a interrupção do serviço total ou parcial pode causar transtornos e custos elevados à Administração, considerando o Estudo Técnico Preliminar.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

2.1. Suporte e atualização do software Zimbra Network Edition para 13.700 caixas postais Professional Edition e 137.000 caixas postais Standard Edition.

- 2.1.1 A contratação deve permitir que o mesmo suporte realizado no ambiente de produção seja feito no ambiente de redundância.
- 2.1.2 A contratação deve realizar suporte nas caixas postais Professional Edition que são caixas que oferecem suporte em dispositivos móveis e sua capacidade de armazenamento sendo ilimitada e dimensionada de acordo com a necessidade.
- 2.1.3 A contratação deve realizar suporte nas caixas postais Standard Edition que são caixas que não oferecem suporte a dispositivos móveis sendo ilimitada e dimensionada de acordo com a necessidade.
- 2.1.4 A contratação deve suportar as 137.000 mil caixas Standard Edition e 13.700 caixas Professional Edition tendo em vista que essa quantidade é justificada diante da quantidade do efetivo da Força Aérea que utilizam os serviços de e-mail.
- 2.1.5 A contratação deve proporcionar manutenção corretiva, sem custo adicional para a Contratante, durante o período de vigência contratual;
- 2.1.6 A solução deve proporcionar a abertura ilimitada de chamados de suporte técnico via WEB, durante o período de vigência contratual;
- 2.1.7 Os serviços de atualização e suporte técnico serão prestados pela CONTRATADA através de telefone, VPN ou WEB (internet). Por atualização do produto, entenda-se os serviços inerentes a cada produto, que contempla o acesso imediato às informações, patches, services packs e utilitários para resolução de problemas ou falhas;
- 2.1.8 A CONTRATADA deverá garantir acesso aos canais de suporte técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, através de número de telefone de discagem gratuita (0800 ou similar) e/ou Internet, para abertura de chamados técnicos, objetivando a resolução de problemas e dúvidas quanto ao funcionamento dos softwares adquiridos;
- 2.1.9 O tempo para início de atendimento a um chamado deverá ser de até 1 (uma) hora para incidentes envolvendo interrupção ou lentidão demasiada no serviço de correio eletrônico e de até 48 (quarenta e oito) horas para os demais casos;
- 2.1.10 O tempo para finalização de um chamado deverá ser de até 24 (vinte e quatro) horas para as situações envolvendo interrupção de serviço de correio eletrônico e de até 48 (quarenta e oito) horas para os demais incidentes;
- 2.1.11 Em todo atendimento técnico deverá ser fornecido o número do chamado na sua abertura, bem como, o responsável pela abertura e os motivos ou problemas referentes ao chamado pela CONTRATADA;
- 2.1.12 Ao final do atendimento, o técnico da CONTRATADA deverá enviar ao gestor do contrato, da Força Aérea, sob demanda, um relatório do atendimento mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, data e hora do primeiro atendimento, os problemas verificados, as providências adotadas, as recomendações e orientações técnicas e demais datas e horários necessários ao acompanhamento dos trabalhos executados. Caso os prazos previstos nos itens 2.1.6 e 2.1.7 não sejam cumpridos, deve constar também no relatório a justificativa, a qual será analisada pelo gestor do contrato

- 2.1.13 Na atualização dos softwares, a CONTRATADA deverá fornecer upgrades para novas versões, bem como releases e patches de manutenção desenvolvidos das licenças de uso dos softwares, não implicando em custos adicionais para a contratação;
- 2.1.14 Todos os manuais e softwares deverão ser entregues ou disponibilizados via internet (sem impressão ou envio de mídia ótica) com fornecimento de usuário e senha de acesso ao site do fabricante, caso necessário, para download da imagem de instalação original;
- 2.1.15 A CONTRATADA deverá prestar o suporte técnico completo da solução, incluindo mão de obra especializada, suporte do fabricante, execução de reinstalações de ambiente, execução de atualizações de versão, uso de recursos dos produtos, solução de problemas e aplicação de correções. O prazo e a aplicação das atualizações deverão ser sempre acordados com a equipe técnica da Força Aérea e o descumprimento dos prazos acordados podem acarretar sanções contra a CONTRATADA;
- 2.1.16 É necessária a autorização formal da Força Aérea para instalação ou desinstalação de quaisquer softwares, equipamentos ou componentes;
- 2.1.17 Ainda poderão ser executadas as seguintes tarefas em relação à prestação de suporte:
 - 2.1.17.1 Resolução de dúvidas sobre o produto;
 - 2.1.17.2 Discussão de melhorias na configuração;
 - 2.1.17.3 Resolução de pequenos problemas e ajustes na solução;
 - 2.1.17.4 Atuação em problemas decorrentes de integração entre o Zimbra e outras soluções de mercado;
 - 2.1.17.5 Para os fins de suporte técnico e gerenciamento, a CONTRATADA deverá disponibilizar acesso total ao conteúdo, presente em área restrita de suporte no endereço eletrônico (website) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configurações atualizadas, lista com questões recorrentes ou FAQ's, com pesquisa efetuada por meio de ferramentas de busca) e atualizações;
- 2.1.18 Em casos de incidentes ou paralisações, emendar todos seus esforços para o restabelecimento do ambiente e em seguida proceder com análise de causa raiz para mitigar problemas futuros.
- 2.1.19 Gerenciamento do Serviço.
 - 2.1.19.1 O prazo de suporte técnico da solução ofertada deverá ser de, no mínimo, 24 (vinte e quatro) meses, contados a partir da data de assinatura do contrato.
 - 2.1.19.2 A CONTRATADA deve garantir para a CONTRATANTE o fornecimento de acesso irrestrito (24 horas x 7 dias da semana) à área de suporte do fabricante, especialmente ao endereço eletrônico (web site), a toda a documentação técnica pertinente (guias de instalação/configurações atualizadas, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).
 - 2.1.19.3 As respostas do suporte técnico contratado deverão ser efetuadas na língua portuguesa (português do Brasil), tanto por e-mail, quanto por contato telefônico.
 - 2.1.19.4 O suporte técnico deverá ser prestado em caso de falhas, necessidade de configuração de funcionalidades, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes aos appliances que compõem a solução.
 - 2.1.19.5 A abertura de chamados pelo CONTRATANTE será efetuada por correio eletrônico, por sistema de controle de chamados, com e-mail de resposta do chamado aberto apresentando o número do ticket aberto, para acompanhamento.
 - 2.1.19.6 A CONTRATADA deverá fornecer os níveis de atendimento conforme abaixo indicado:
 - 2.1.19.7 Os chamados de severidade Crítica (quando há indisponibilidade de uso da solução) deverão ser atendidos em até 1 (uma) hora após a abertura e deverão ser solucionados em até 12 (doze) horas, contados a partir da abertura do chamado.
 - 2.1.19.7.1 Os chamados de severidade ALTA (Quando há indisponibilidade de uso da solução) deverão ser atendidos em até 6 (seis) horas após a abertura e deverão ser solucionados em até 24 (vinte e quatro) horas, contados a partir da abertura do chamado.

- 2.1.19.7.2 Os chamados de severidade MÉDIA (Quando há falha, simultânea ou não, de uma ou mais funcionalidades que não cause indisponibilidade, mas apresente problemas de funcionamento e/ou performance da solução) deverão ser atendidos em até 12 (doze) horas após a abertura e deverão ser solucionados em até 48 (quarenta e oito) horas, contados a partir da abertura do chamado.
- 2.1.19.7.3 Os chamados de severidade BAIXA (Nível de severidade aplicado para instalação, configuração, atualização de versões e implementações de novas funcionalidades) deverão ser atendidos em até 24 (vinte e quatro) horas após a abertura e deverão ser solucionados em até 48 (quarenta e oito) horas, contados a partir da abertura do chamado.
- 2.1.19.7.4 Os chamados de severidade INFORMATIVO (Nível informacional ou dúvidas) deverão ser atendidos em até 16 (dezesesseis) horas após a abertura e deverão ser solucionados em até 48 (quarenta e oito) horas após a abertura.
- 2.1.19.8 A CONTRATADA deverá possuir técnicos especializados na solução, com no mínimo 1 (um) técnico certificado pelo fabricante e com certificação dentro da validade. Os serviços deverão ser executados com base nos parâmetros mínimos a seguir estabelecidos:

Ordem	Descrição do Evento	Nível de Criticidade	Tempo até primeiro atendimento	Tempo até finalização atendimento
1	Configurações Gerais do ambiente administrativo do Zimbra	Alto	6 h	24 h
2	Alteração de configuração do servidor ZIMBRA	Baixo	24 h	48 h
3	Atualização de versão do servidor ZIMBRA	Baixo	24 h	48 h
4	Atualizações do Sistema Operacional	Baixo	24 h	48 h
5	Implantação de regra no <i>antispam</i>	Alto	6 h	24 h
6	Erro de sistema operacional do servidor	Alto	6 h	24 h
7	Reinstalação do software Zimbra e/ou do sistema operacional	Alto	6 h	24 h
8	Sistema de Produção Zimbra Parado	Crítico (Emergencial)	1 h	12 h
9	Falha que não cause indisponibilidade	Médio	12 h	48 h
10	Dúvidas ou orientações	Informativo	16 h	48 h

- 2.1.19.9 A contratada deverá utilizar acesso remoto mediante acompanhamento das ações de suporte por técnico do Centro de Computação da Aeronáutica, permitindo à contratante a visualização do terminal remoto utilizado pela CONTRATADA.

- 2.1.19.10 Deverá ser possível atualizar os produtos automaticamente e sem custos adicionais, deverá ser possível o acesso ao conteúdo mais recente dos produtos, funcionalidades adicionais e correções de produtos disponibilizadas pelo fabricante.
- 2.1.19.11 Deve ser possível submeter pedidos para atualização de produtos.
- 2.1.19.12 Para que as atualizações de versões estejam disponíveis durante toda a vigência do contrato, a contratada deverá estar credenciada e autorizada pelo fabricante.
- 2.1.19.13 A Contratante reserva o direito de, a qualquer momento, solicitar tais comprovações que se fizerem necessárias.
- 2.1.19.14 A contratada deverá, sem ônus adicional para o Contratante, fornecer as atualizações ("patches") de segurança e de versão para os softwares, incluindo plugins, que compõem a solução.
- 2.1.19.15 A solução deverá manter a filtragem das mensagens em ambos os sentidos (inbound e outbound) mesmo após o término do licenciamento ou suporte.
- 2.1.19.16 Além da análise das informações fornecidas em documentação técnica pertinente, deverá ser realizado teste de homologação (Prova de Conceito) da solução nas instalações do contratante a fim de validar o atendimento aos requisitos básicos.
- 2.1.19.17 O teste de homologação será exigido da contratada apenas em caso de atualização de versão e de demais recursos computacionais necessários para o funcionamento da ferramenta durante a vigência do contrato(em tempo de contrato).
- 2.1.19.18 O teste de homologação será realizado remotamente e deverá comprovar que a atualização de versão não impactará no funcionamento da ferramenta.
- 2.1.19.19 O Teste de Homologação terá o prazo de até 10 (dez) dias úteis, contados da data da convocação, para entregar uma amostra completa da solução ofertada contendo equipamentos (quando couber) acompanhado dos softwares e licenças necessárias ao seu funcionamento pelo período de 30 (trinta) dias corridos.
- 2.1.19.20 O Teste de Homologação será realizado sem custo para a CONTRATANTE pelo período de 30 (trinta) dias corridos, contados da data da entrega.
- 2.1.19.21 Estão incluídos no prazo de 30 (trinta) dias corridos a instalação, a configuração e a demonstração de que os produtos atendem às especificações constantes no Item 6 do Termo de referência.
- 2.1.19.22 Além dos pontos acima, o adjudicatário deverá apresentar declaração de que tem pleno conhecimento das condições necessárias para a prestação do serviço como requisito para celebração do contrato.
- 2.1.19.23 Declaração do licitante de que tem pleno conhecimento das condições necessárias para a prestação do serviço.
- 2.1.19.24 A implantação consiste em entregar a solução em plenas condições de uso (configurada e integrada com a solução de correio eletrônico utilizada pela CONTRATANTE).
- 2.1.19.25 Todas as customizações presentes na solução atual, em operação, na CONTRATANTE devem ser mantidas e atualizadas pela CONTRATADA.
- 2.1.19.26 Também devem ser migradas todas as configurações presentes de forma nativa na solução atual pela CONTRATANTE.
- 2.1.19.27 A instalação em alta disponibilidade e testes dos produtos devem estar inclusos no custo do produto.
- 2.1.19.28 A alta disponibilidade é caracterizada pela instalação de 2 (dois) ou mais nós de processamento, configurados em cluster, para cada serviço disponibilizado pela solução, ou seja, cada funcionalidade (envio, recebimento ou edição de e-mails, etc) deve ter mecanismos que mantenha o funcionamento em alta disponibilidade.
- 2.1.19.29 Caberá à CONTRATADA enviar de forma prévia documento completo informando as regras de firewall necessárias para a implantação da solução, bem com a documentação clara e inequívoca acerca dos dados que serão trafegados por meio destas regras; havendo liberações para rede externa da contratante que não do próprio fluxo de e-mails, deve ser fornecido um documento onde a contratada detalha e responsabiliza-se única e exclusivamente pela segurança dos dados trafegados.

- 2.1.19.30 A implementação deverá ser realizada de tal forma que as interrupções no ambiente de produção sejam as mínimas possíveis e estritamente necessárias, e, ainda, não causem transtornos aos usuários finais do órgão.
- 2.1.19.30.1 Havendo necessidade de interrupções no ambiente de produção, a contratada deverá realizar as intervenções fora do horário comercial, podendo ser a noite ou durante o fim de semana, a critério da CONTRATANTE.
- 2.1.19.31 A CONTRATADA deverá executar uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente. Estes testes deverão ser realizados nos componentes de hardware e software envolvidos no projeto.
- 2.1.19.32 A CONTRATADA deverá realizar Testes de falhas, redundância, backup e restauração.
- 2.1.19.33 Durante a execução dos serviços, pelo menos um representante da CONTRATANTE participará e fará composição na equipe designada para as atividades.
- 2.1.19.34 Ao final do processo de implantação deve ser gerado um documento detalhando os passos realizados para instalação e configuração da solução.
- 2.1.19.35 Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas de qualidade, promovendo sua substituição quando necessário.
- 2.1.19.36 Além das funcionalidades básicas e comuns do software de e-mail Zimbra, a CONTRATADA deverá também implantar todas as funcionalidades disponíveis na ferramenta, mesmo que na forma de plugins e extras, incluindo chat corporativo, drive de arquivos e ferramenta office colaborativa integrada, a critério da CONTRATANTE.

2.2 Licenciamento de Filtro de Conteúdo de E-mail

- 2.2.1 A solução de filtro de conteúdo de e-mail deve suportar a totalidade de quantidade de caixas (13.700 caixas postais Professional Edition e 137.000 caixas postais Standard Edition) no e-mail corporativo da FAB, sem perda de desempenho e funcionalidade, mesmo que o licenciamento seja feito para uma fração do total de contas ativas.
- 2.2.2 A solução de filtro de e-mail deverá permanecer licenciada durante o período vigente do contrato.
- 2.2.3 A solução pode ser fornecida como appliance (hardware com software embarcado) ou somente software, a ser disponibilizado em máquina virtual pronta ou, ainda, somente o software a ser instalado e configurado em máquina virtual a ser disponibilizada.
- 2.2.4 Solução deverá analisar mensagens eletrônicas suspeitas de serem maliciosas, spam (e-mail não solicitado), vírus (e-mails com anexos infectados), Phishing (e-mails de fraude) ou, estarem fora da política de segurança e uso da Força Aérea e, tomar ações sobre elas (quando se tratar de vírus: tentar excluir os vírus, na falha deste, excluir o e-mail suspeito; quando se tratar de Spam: permitir ao usuário optar pela exclusão ou recebimento da mensagem).
- 2.2.5 A solução deverá identificar spam, fraude e vírus, independentemente do idioma do e-mail.
- 2.2.6 Permitir a criação de exceções do anti-spam Whitelist (Listas brancas), garantindo que certos remetentes nunca serão marcados como spam.
- 2.2.7 A solução deverá possuir ferramenta ou serviço de verificação para controle de tráfego de e-mail baseado em reputação do remetente externo de mensagem eletrônica. A rede de reputação não deve ser baseada somente em informações de fluxo da própria base instalada, mas sim em informações provenientes de gaiolas de spam, listas de URL, listas de equipamentos comprometidos, composição da mensagem, endereços IP em Blacklist (lista negra), volume global de tráfego, Whitelist e composição da mensagem.
- 2.2.8 O usuário deve poder identificar e-mails como spam ou não, se foram classificados incorretamente.
- 2.2.9 A atualização de todos os componentes e mecanismos de identificação e bloqueio de spam e antivírus deverá ser feita de forma automática com intervalos de checagem nos servidores do fabricante de antispam.

- 2.2.10 A solução deverá possuir integração com serviço de diretórios LDAP do serviço de e-mail para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas.
- 2.2.11 A solução deverá analisar mensagens através de, no mínimo, os seguintes métodos:
 - 2.2.11.1 Reputação do endereço IP do remetente;
 - 2.2.11.2 Deverá identificar e associar reputação de endereços IPs que estão emitindo spam, manifestando comportamento de zombies ou botnets, phishing;
 - 2.2.11.3 Análise de URL no corpo da mensagem;
 - 2.2.11.4 Análise de padrões no corpo da mensagem;
 - 2.2.11.5 Análise de Anexos.
- 2.2.12 A solução ofertada deverá ter a capacidade de analisar e tomar, no mínimo, as seguintes ações sobre as mensagens
 - 2.2.12.1 Entregar a mensagem ao destinatário;
 - 2.2.12.2 Adicionar TAGs no campo assunto e encaminhar ao destinatário;
 - 2.2.12.3 Descartar a mensagem sem notificação; e
 - 2.2.12.4 Descartar a mensagem notificando o remetente.
- 2.2.13 A solução deve ser capaz de bloquear mensagens com URLs que levem a sites fraudulentos ou que possibilitem o phishing scam (roubo de dados). Essa habilidade deve estar presente sem a necessidade de configuração e/ou pré-conhecimento dos sites de fraude por parte dos administradores da plataforma;
- 2.2.14 O software deve possuir mecanismos Antiphishing (antifraude) para verificação de URLs contidas em e-mails e correlação com o conteúdo.
- 2.2.15 A solução deve permitir a marcação de mensagens consideradas spam através de modificação no cabeçalho.
- 2.2.16 A ferramenta deve possuir administração por interface Web utilizando os protocolos HTTP e HTTPS.
- 2.2.17 O software deve suportar a manipulação de múltiplos domínios. Cada domínio deverá poder ter um login independente.
- 2.2.18 O software deve suportar configuração de vários domínios e roteamento de e-mails de forma independente para cada domínio utilizado.
- 2.2.19 A solução deve oferecer a possibilidade da criação de filtros que permitem controle tanto de entrada quanto a saída de e-mails;
 - 2.2.19.1 Filtrar, no mesmo equipamento, o tráfego de e-mails de entrada e saída;
 - 2.2.19.2 Permitir a criação de filtros de bloqueio para todos os usuários, grupos ou indivíduos;
 - 2.2.19.3 Permitir o bloqueio de anexos perigosos baseado na extensão (ex.: exe), tipo MIME (ex.: imagem), ou nome (ex.: vírus.bat); e
 - 2.2.19.4 Suportar alias de domínio.
- 2.2.20 A ferramenta adquirida deve mostrar gráficos em tempo real de:
 - 2.2.20.1 Fluxo e e-mails entrando e saindo por volume de dados e número de e-mails;
 - 2.2.20.2 Número de e-mails spam;
 - 2.2.20.3 Número de e-mails com vírus;
 - 2.2.20.4 Fluxo de e-mails em quantidade e com assunto;
- 2.2.21 A ferramenta de filtro de e-mail deve oferecer no mínimo relatórios:
 - 2.2.21.1 Sobre todos os appliances de um cluster de forma centralizada através de uma única interface web no console de gerenciamento;
 - 2.2.21.2 De forma gráfica, com a possibilidade de agendar o envio dos mesmos aos administradores via e-mail;
 - 2.2.21.3 Que permitam a seleção de dados por data ou por um intervalo de tempo específico;
 - 2.2.21.4 Que permitam a configuração de um período para a retenção de dados;
 - 2.2.21.5 Globais ou por domínio contendo no mínimo as seguintes informações:

- 2.2.21.5.1 Sumário de mensagens;
- 2.2.21.5.2 Quantidade de mensagens processadas;
- 2.2.21.5.3 Principais origens de spam por domínio, endereço de e-mail;
- 2.2.21.5.4 Principais destinos de spam por domínio, endereço de e-mail;
- 2.2.21.5.5 Relatórios de Vírus mais incidentes;
- 2.2.21.5.6 Principais fontes de ataque;
- 2.2.21.5.7 Estatísticas da quarentena;
- 2.2.21.5.8 Conexões completadas x bloqueadas;
- 2.2.21.5.9 Relatório de tráfego;
- 2.2.21.5.10 Principais destinatários de Spam;
- 2.2.21.5.11 Principais destinatários de e-mail;
- 2.2.21.5.12 TOP Attachments;
- 2.2.21.5.13 TOP SPF Violations; e
- 2.2.21.5.14 TOP Ataques por fraude de e-mail / tentativa de spoof.
- 2.2.21.6 Que permitam a seleção com definição de origem e destinos específicos;
- 2.2.21.7 Estatísticos de conexões, ameaças, quarentena, SPAM;
- 2.2.21.8 Que apresentem estatísticas e monitoramento em tempo real (online) de e-mails com base em gráficos;
- 2.2.21.9 Capacidade de remoção automática das mensagens em quarentena de acordo com as configurações definidas pelo administrador do sistema.
- 2.2.22 Os relatórios no mínimo devem poder ser filtrados por período, ponto de filtragem que o e-mail passou, remetente e destinatário.
- 2.2.23 Os relatórios devem possuir uma forma de gerar relatórios que mostre qual a classificação que a mensagem atingiu, dentre eles no mínimo:
 - 2.2.23.1 Provável SPAM;
 - 2.2.23.2 SPAM;
 - 2.2.23.3 VÍRUS;
 - 2.2.23.4 Conteúdo Bloqueado;
 - 2.2.23.5 Whitelist;
 - 2.2.23.6 Blacklist;
 - 2.2.23.7 Tamanho Excedido; e
 - 2.2.23.8 Phishing.
- 2.2.24 Possuir, no mínimo, os seguintes tipos de relatório:
 - 2.2.24.1 Relatório para um único usuário ou Domínio;
 - 2.2.24.2 Relatório de Volume de Mensagens por Data;
 - 2.2.24.3 Relatório dos Principais Destinatários de SPAM;
 - 2.2.24.4 Relatório dos Principais Remetentes de SPAM;
 - 2.2.24.5 Relatório de Top E-mail Relays;
 - 2.2.24.6 Relatório de Top Remetentes por Quantidade;
 - 2.2.24.7 Relatório de Top Remetentes por Volume;
 - 2.2.24.8 Relatório de Top Destinatário por Quantidade;
 - 2.2.24.9 Relatório de Top Destinatário por Volume;
 - 2.2.24.10 Relatório de Vírus; e
 - 2.2.24.11 Relatório de Estatísticas da Quarentena.
- 2.2.25 O Filtro de e-mail adquirido deve possuir possibilidade de rastreamento, independente de qual equipamento do cluster processou, de forma centralizada e por meio da interface de gerenciamento HTTPS (não será aceito pesquisa via linha de comando);
- 2.2.26 O rastreamento da mensagem deve ser possível através de qualquer um dos seguintes campos:
 - 2.2.26.1 ID da mensagem;
 - 2.2.26.2 E-mail do Remente;
 - 2.2.26.3 E-mail do Destinatário;
 - 2.2.26.4 Domínio do Remetente;
 - 2.2.26.5 Domínio do Destinatário;
 - 2.2.26.6 Assunto da mensagem;
 - 2.2.26.7 Nome do anexo;

- 2.2.26.8 Palavra contida no conteúdo do corpo da mensagem;
- 2.2.26.9 IP de Origem da mensagem;
- 2.2.26.10 Tamanho da mensagem;
- 2.2.26.11 Regra de SPAM;
- 2.2.26.12 Se a mensagem foi entregue ou não;
- 2.2.26.13 Regras personalizadas aplicadas na mensagem;
- 2.2.26.14 Nome da ameaça encontrada; e
- 2.2.26.15 Rastreamento completo de mensagens aceitas, retidas e rejeitadas, desde o recebimento da mensagem pelo IP cliente até a entrega para o IP destino, usando com o filtro o assunto, o remetente, o destinatário, regra de bloqueio, conteúdo do corpo da mensagem, data, status, hora de entrega da mensagem permitindo a concatenação dos filtros através dos operadores lógicos “e” e “ou”.
- 2.2.27 A console deve apresentar ainda as seguintes características de rastreamento de mensagens:
 - 2.2.27.1 O rastreamento deve ser a partir de uma única interface de gerenciamento independente de qual *appliance* filtrou a mensagem, não sendo aceito pesquisa via linha de comando;
 - 2.2.27.2 O rastreamento deverá ter a opção de ser efetuado de todos os pontos de filtragem, sem a obrigatoriedade de separação de um único ponto de filtragem por vez.
- 2.2.28 Deve apresentar como resultado as seguintes informações:
 - 2.2.28.1 Remetente da mensagem;
 - 2.2.28.2 Destinatários da mensagem;
 - 2.2.28.3 Servidor de origem;
 - 2.2.28.4 Se foi armazenada em quarentena;
 - 2.2.28.5 Se continha vírus;
 - 2.2.28.6 A regra que atuou;
 - 2.2.28.7 O servidor de origem;
 - 2.2.28.8 O tamanho da mensagem;
 - 2.2.28.9 Se foi entregue ou não; e
 - 2.2.28.10 Qual ponto de filtragem utilizado (qual *appliance* processou a mensagem).
- 2.2.29 No caso de a mensagem ter sido entregue, deve ser possível a apresentação do log de entrega da mesma e para qual endereço IP a mensagem foi entregue.
- 2.2.30 Se o e-mail tiver sido bloqueado por ser considerado spam ou possível spam, deve apresentar os filtros aplicados, bem como a pontuação apresentada por cada filtro e explicação do que representa o filtro aplicado (para facilidade do entendimento do administrador).
- 2.2.31 Deve ser capaz de visualizar a fila de e-mails em tempo real, bem como o sentido do e-mail na fila (se é fila de entrada de e-mail ou saída de e-mail), indicando total de e-mails na fila de saída, total de e-mails na fila de entrada e total de e-mails com erros na entrega.
- 2.2.32 Rastrear e-mails a partir de uma determinada ameaça.
- 2.2.33 Apresentar na interface gráfica as fontes de ataque e através delas, apresentar quais os e-mails foram recebidos, originários dessa fonte de ataque.
- 2.2.34 A solução deve ser capaz de bloquear ataques de negação de serviço (Denial of Service)
- 2.2.35 Deve ser uma solução MTA (Mail Transfer Agent) completa suportando o protocolo SMTP, e com Suporte a envio e recebimento de e-mails criptografados utilizando o protocolo TLS/SSL, permitindo configurar domínios onde o TLS é mandatório;
- 2.2.36 A solução deverá possuir a capacidade de executar as seguintes ações:
 - 2.2.36.1 Limitar o número de conexões TCP permitidas através de um valor configurável; e
 - 2.2.36.2 Rejeitar a conexão SMTP que se caracterize como "flooding".
- 2.2.37 Deve ser capaz de efetuar a filtragem do tráfego de correio eletrônico bloqueando a entrada de:
 - 2.2.37.1 Vírus;
 - 2.2.37.2 Spyware;
 - 2.2.37.3 Worms;
 - 2.2.37.4 Trojans;
 - 2.2.37.5 Spam;
 - 2.2.37.6 Phishing; e
 - 2.2.37.7 E-mail Marketing, ou qualquer outra forma de ameaça virtual.

- 2.2.38 Deve possuir controle total da comunicação permitindo restringir:
 - 2.2.38.1 IP reverso mal configurado;
 - 2.2.38.2 Domínios inexistentes;
 - 2.2.38.3 Permitir identificar e bloquear e-mails vindos de domínios recentemente cadastrados; e
 - 2.2.38.4 Enforce RFC821.
- 2.2.39 Deve permitir ao administrador criar filtros e assinaturas, bem como realizar atualização automática das mesmas, em frequência de consulta configurada pelo administrador. A frequência de atualização desta consulta deve ser de no mínimo 15 minutos, sem necessidade de interrupção do serviço.
- 2.2.40 A solução deve ser capaz de filtrar contra vírus as mensagens tanto de entrada quanto de saída de e-mails.
- 2.2.41 Permitir criação de políticas diferenciadas para tratamento de spam, vírus e filtragem de conteúdo, de acordo com o destinatário da mensagem.
- 2.2.42 Permitir configurar ações diferenciadas sobre as mensagens suspeitas incluindo (obrigatoriamente de forma gráfica e simplificada):
 - 2.2.42.1 Aceitar;
 - 2.2.42.2 Colocar em quarentena;
 - 2.2.42.3 Inserir tag personalizado no assunto;
 - 2.2.42.4 Marcar o cabeçalho;
 - 2.2.42.5 A solução deve ser capaz de tomar as seguintes ações sobre as mensagens;
 - 2.2.42.6 Alterar o assunto da mensagem;
 - 2.2.42.7 Adicionar cabeçalhos para rastreamento;
 - 2.2.42.8 Descartar a mensagem; e
 - 2.2.42.9 Colocar em uma determinada área de quarentena definida pelo administrador.
- 2.2.43 Deve permitir também a criação de regras baseadas no idioma que as mensagens foram escritas, com capacidade de identificar no mínimo, português, e Inglês, ou a aplicação de regras por país.
- 2.2.44 A ferramenta deve possuir a capacidade de criar filtros personalizados usando expressões regulares.
- 2.2.45 Permitir criação de listas negras e listas brancas, com opção por domínio, subdomínio, endereço de e-mail e endereço IP.
- 2.2.46 Deve prover um mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente (relay).
- 2.2.47 Capacidade de limitar o número máximo de mensagens enviadas por remetente a cada hora, com opção de bloqueio automático do remetente, caso esse limite seja excedido.
- 2.2.48 Permite criar regras customizáveis contra *spammers*, possibilitando um controle avançado em todo conteúdo do e-mail efetuando buscas por Expressões Regulares presentes em todo conteúdo do e-mail (SMTP HEADER, BODY, URL, ANEXOS), sendo possível criar regras compostas utilizando os operadores lógicos “E” e “OU”.
- 2.2.49 O parceiro da solução Zimbra deve possuir seu próprio sistema de reputação (RBL), integrado à solução, com a possibilidade de o administrador reportar um possível *spammer*. Esta consulta deve retornar os dados do remetente, com informações referentes à:
 - 2.2.49.1 Infraestrutura de rede;
 - 2.2.49.2 Registro em blacklists mundiais; e
 - 2.2.49.3 Configuração de serviço de notificação de envio e autenticidade de mensagens como SPF e DKIM.
- 2.2.50 Deve oferecer a capacidade de efetuar consultas externas para análise de endereço IP do remetente quanto a sua reputação, bem como verificação de Spams e phishings recebidos e outros tipos de ameaças.
- 2.2.51 Deve ser capaz de realizar Reverse DNS LookUp (rDNS), para validação de fontes de e-mail.
- 2.2.52 Deve possuir suporte ao bloqueio de conexões de e-mails nocivos antes do diálogo SMTP, permitindo a economia de banda, armazenamento e otimização de processamento do appliance, em especial baseado em lista local de bloqueio, RBLs e SPF.
- 2.2.53 Deve permitir que o administrador do sistema cadastre novas RBLs para serem utilizadas em nível de conexão SMTP.
- 2.2.54 Deve oferecer a possibilidade de restringir o processamento de mensagens (relay) endereço IP.

- 2.2.55 Deve ter capacidade de proteção a spoofing de e-mail (tanto Spoofing de e-mails na entrada – quando o hacker utiliza o domínio do órgão como remetente, como Spoofing de e-mails na saída – quando tem algum e-mail de saída que não esteja com o domínio do órgão como remetente), já incrementado na solução, bastando o administrador ativar a regra, sem necessidade de customizar uma regra para isso.
- 2.2.56 Deve possuir capacidade de criar cotas de envio e recebimento de e-mails em um prazo determinado de tempo, limitando o fluxo e prevenindo ataque do tipo DOS ou distribuição de spam através de um computador infectado na rede interna.
- 2.2.57 Deve ser capaz de limitar o fluxo de mensagens, de acordo com o volume de mensagens indevidas recebidas de um determinado IP de origem;
- 2.2.58 Deve possuir funcionalidade de verificação de DMARC (Domain-based Message Authentication Reporting & Conformance);
- 2.2.59 Deve possuir controle de surtos, penalizando o remetente por um tempo configurável pelo administrador ao detectar:
 - 2.2.59.1 Número excessivo de spams (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;
 - 2.2.59.2 Número excessivo de vírus (configurado pelo administrador) oriundos de uma mesma fonte de e-mail; e
 - 2.2.59.3 Número excessivo de ataques de dicionário (configurado pelo administrador) oriundos de uma mesma fonte de e-mail.
- 2.2.60 Deve possuir apresentação de ameaças detectadas em tempo real. Nesse sistema de detecção de ameaças em tempo real, deve ser possível identificar:
 - 2.2.60.1 Fontes de ataque;
 - 2.2.60.2 Ameaças encontradas; e
 - 2.2.60.3 Ameaças identificadas.
- 2.2.61 Deve possuir filtro de AntiSpam para detecção de spams usando no mínimo as seguintes tecnologias:
 - 2.2.61.1 *FingerPrint*: Filtro por assinatura de spam;
 - 2.2.61.2 Análise Heurística: Análise completa de toda mensagem contra spam, de acordo com as características da mensagem;
 - 2.2.61.3 Análise de Documentos: Análise de documentos anexados na mensagem (PDF, DOC, DOCX e TXT);
 - 2.2.61.4 Análise de Imagens: Filtragem de spam em imagens;
 - 2.2.61.5 Filtro de URL: Filtragem por URL mal-intencionada contidas no corpo da mensagem, dessa forma combatendo possível e-mail Phishing;
 - 2.2.61.6 Filtro de URL com Categorização – Permitir ao administrador definir através de categorias, com no mínimo 10 categorias, divididas por assunto, possibilitando ao administrador definir uma pontuação. Categorias mínimas contidas na solução:
 - 2.2.61.6.1 Conteúdo pornográfico;
 - 2.2.61.6.2 Abuso infantil;
 - 2.2.61.6.3 Redes sociais;
 - 2.2.61.6.4 Racismo e ódio;
 - 2.2.61.6.5 Esportes;
 - 2.2.61.6.6 Notícias; e
 - 2.2.61.6.7 Compras *online*.
- 2.2.62 Deve possuir no mínimo as seguintes tecnologias para prevenção e bloqueio de spam:
 - 2.2.62.1 recurso de Grey List;
 - 2.2.62.2 Deve possuir recurso de checagem por SPF (Sender Policy Framework) permitindo a criação de regras individuais e customizadas para usuários ou grupos, permitindo criar ações específicas para “fail” e “soft fail”, conforme descrito pelo Comitê Gestor da Internet no Brasil em seu website oficial ([HTTP://www.antispam.br/admin/spf](http://www.antispam.br/admin/spf)); Recurso de checagem por Sender ID;
 - 2.2.62.3 Recurso de checagem por assinatura DKIM;
 - 2.2.62.4 Recurso de checagem de DNS Reverso;
 - 2.2.62.5 Checagem de validade de domínio através de verificação da configuração da zona do DNS do remetente;
 - 2.2.62.6 Análise de reputação de IP;
 - 2.2.62.7 Filtros de URL;

- 2.2.62.8 Filtro de anti-phishing;
- 2.2.62.9 Consulta de RBL's (real-time blackhole list);
- 2.2.62.10 Filtro bayesiano utilizando tecnologia Bayes Databases; e
- 2.2.62.11 Classificar a reputação de novas origens de spam com tecnologia de classificação dinâmica. O sistema de reputação deve utilizar dados de redes globais de monitoramento de tráfego web e de e-mail, não restringindo ao fluxo de mensagens do ambiente instalado.
- 2.2.63 Deve possuir a possibilidade de criação de regras personalizadas de filtragem baseadas em:
 - 2.2.63.1 Origens das mensagens;
 - 2.2.63.2 Destino das mensagens;
 - 2.2.63.3 Domínios;
 - 2.2.63.4 Endereços de e-mails;
 - 2.2.63.5 Expressões regulares (dicionário de palavras);
 - 2.2.63.6 Fluxo;
 - 2.2.63.7 Quantidade de mensagens;
 - 2.2.63.8 Tamanho de anexo;
 - 2.2.63.9 Número máximo de destinatários em uma única mensagem;
 - 2.2.63.10 Tipo de arquivos em anexo;
 - 2.2.63.11 Extensões de arquivos em anexo, identificados por Mime-Type;
 - 2.2.63.12 Anexos criptografados;
 - 2.2.63.13 Anexos compactados;
 - 2.2.63.14 Níveis de compactação dos arquivos anexos;
 - 2.2.63.15 Quantidade de anexos na mensagem; e
 - 2.2.63.16 Conteúdo HTML no corpo da mensagem.
- 2.2.64 Deve possuir mecanismo de análise de conteúdo HTML no corpo da mensagem mensagens, permitindo ao administrador desarmar as tags HTML e bloquear as mensagens, possuindo no mínimo a identificação das Tags "<form>", "<script>" e "<iframe>" em uma mensagem.
- 2.2.65 Deve oferecer a possibilidade de criar regras para ações a serem tomadas pela ferramenta, quando as mensagens forem consideradas Confiáveis e Spams permitindo ao administrador configurar nesses casos as seguintes ações:
 - 2.2.65.1 Entregar direto o e-mail;
 - 2.2.65.2 Colocar em quarentena;
 - 2.2.65.3 Remover mensagem;
 - 2.2.65.4 Auditar mensagem;
 - 2.2.65.5 Encaminhar mensagens;
 - 2.2.65.6 Notificar o destinatário; e
 - 2.2.65.7 Adicionar header na mensagem.
- 2.2.66 Deve possuir um sistema de detecção de ataque de diretórios (DHA – Directory HarvestAttack), capaz de recusar novas conexões SMTP de uma fonte emissora, caso ela tenha enviado, em um período de tempo, mensagens a usuários inválidos/inexistentes no domínio.
- 2.2.67 Deve permitir regras internas para aumentar ou diminuir a probabilidade de ser SPAM com base em critérios internos da contratante, permitindo definir no mínimo: país de origem, endereço de domínio e IP do remetente.
- 2.2.68 A solução deve permitir a utilização de quarentena por usuário, possibilitando que cada usuário cadastrado em um controlador de diretório, como por exemplo Microsoft Active Directory ou LDAP, esteja integrado com a solução e administre suas próprias mensagens categorizadas como spam.
- 2.2.69 Deve permitir a aplicação de políticas de SPAM diferentes por nome de domínio, destinatário, grupo de destinatários e por destinatário específico, integrado aos sistemas de diretório LDAP e MS Active Directory.
- 2.2.70 Deve ter a capacidade de rejeitar mensagens para destinatários inválidos durante o dialogo SMTP (tratar Non-Delivery Report Attack);
- 2.2.71 Deve possuir proteção contra bounce email attack através "Bounce Address Tag Verification".
- 2.2.72 Deve permitir a inclusão de múltiplas listas de remetentes bloqueados, permitindo regras

- de bloqueio se o IP estiver presente nestas listas.
- 2.2.73 Deve permitir que mensagens de Falso Negativo sejam reportadas através da interface gráfica para o laboratório do fabricante ou oferecer um caminho para que mensagens de falso negativo sejam reportadas diretamente ao laboratório do fabricante.
 - 2.2.74 Deve possuir algum mecanismo que permita a adição de Cabeçalho de identificação da classificação das mensagens como SPAM, a fim de integrar com sistemas de correio eletrônicos baseados em Zimbra Collaboration Suite.
 - 2.2.75 Deve ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de e-mail).
 - 2.2.76 Deverá possuir módulo de detecção “Hora Zero” para a identificação de novas ameaças desconhecidas pelo antivírus, colocando em determinada área da quarentena por período, até nova verificação pelo antivírus.
 - 2.2.77 Fazer varredura em arquivos compactados recursivamente, no mínimo, 5 (cinco) camadas, contemplando no mínimo, os seguintes compactadores: .rar, .zip, .tar, .arj, .cab, .lha, .exe, .lzh, .tgz e .gzip.
 - 2.2.78 A solução deve possuir um motor antivírus e Antimalware do próprio fabricante da solução, ou um motor Antivírus e Anti Malware de terceiro já integrado à solução sem custo adicional.
 - 2.2.79 Oferecer proteção contra Vírus, no mínimo com as tecnologias já licenciadas sem a necessidade de módulo adicional.
 - 2.2.80 Deverá oferecer proteção contra: Dia-zero (zero-day), Vírus outbreak, Hora-zero (Zero-hour) e Targeted Attack protection.
 - 2.2.81 Oferecer a possibilidade de o administrador tomar no mínimo as seguintes ações:
 - 2.2.81.1 Alterar o assunto da mensagem;
 - 2.2.81.2 Adicionar cabeçalhos para rastreamento;
 - 2.2.81.3 Descartar a mensagem;
 - 2.2.81.4 Colocar em uma determinada área da quarentena definida pelo administrador; e
 - 2.2.81.5 Notificar o remetente e/ou destinatário com uma mensagem customizável, informando o nome do vírus.
 - 2.2.82 Permitir quarentena automática de anexos criptografados;
 - 2.2.83 Permitir criação de rota customizada para permitir entrada de anexos criptografados para entrega a determinados grupos de e-mails.
 - 2.2.84 A solução deverá permitir ao administrador agendar o envio do resumo das mensagens na quarentena individual do usuário (Digest) em períodos de tempo pré-configurável por horário e dia, possibilitando ações do usuário diretamente através dos comandos definidos neste Digest, dispensando a instalação de agentes e acesso à quarentena individual do usuário.
 - 2.2.85 O digest deve ser enviado em Língua portuguesa do Brasil, mas com a possibilidade de customização do texto, para todos os usuários ou para um determinado grupo de usuários.
 - 2.2.86 Deve ser possível a customização do digest com as seguintes características alteráveis:
 - 2.2.86.1 E-mail de origem;
 - 2.2.86.2 Título/Assunto do e-mail;
 - 2.2.86.3 Mensagem do digest, com possibilidade de inclusão de imagens e links, bem como mudança de fonte, alinhamento e cor; e
 - 2.2.86.4 Logomarca do digest.
 - 2.2.87 O digest deve permitir ao usuário final tomar no mínimo as ações de:
 - 2.2.87.1 Liberar uma mensagem bloqueada.
 - 2.2.87.2 Bloquear o remetente da mensagem (blacklist), para que as futuras mensagens do mesmo já sejam barradas.
 - 2.2.87.3 Marcar o remetente como confiável (whitelist), para que as futuras mensagens do mesmo não sejam pontuadas como spam.
 - 2.2.87.4 Reportar o bloqueio indevido.
 - 2.2.87.5 Solicitar envio de novo resumo.
 - 2.2.87.6 Acessar sua área de quarentena.
 - 2.2.88 Deverá prover proteção contra-ataques dirigidos como Spear-phishing, Ataques Zero-Day e Ameaças avançadas persistentes (APTs).
 - 2.2.89 Deve possuir no mínimo 3 (três) camadas de proteção sendo elas:
 - 2.2.89.1 Verificação da lista de códigos maliciosos;
 - 2.2.89.2 Verificação de campanhas de e-mails emergentes e conhecimento de novos sites maliciosos; e

- 2.2.89.3 Análise de código: Verificação de comportamento suspeito, scripts escondidos, partes de códigos maliciosos e redirecionamento a outros sites maliciosos.
- 2.2.90 Possuir acesso ao Dashboard do módulo de Segurança contra-ataques dirigidos.
- 2.2.91 O sistema de proteção contra-ataques dirigidos deve executar no mínimo 3 (três) etapas:
 - 2.2.91.1 Detecção - A análise de e-mail deve verificar variáveis em tempo real incluindo as propriedades da mensagem, bem como, o histórico de e-mail do destinatário para identificar anomalias que indiquem uma ameaça potencial;
 - 2.2.91.2 Proteção - Deve assegurar que links para URLs suspeitas são dinamicamente reescritas antes que o e-mail seja entregue ao destinatário. Cada vez que um usuário clica em um destes links esteja ele na empresa ou em um local remoto o serviço verifica se o destino é seguro; e
 - 2.2.91.3 Ação - Deve demonstrar aos administradores e gestores de segurança em tempo real e de forma interativa uma visão dos ataques sofridos e das ameaças que possam sofrer, passando para usuários específicos, dispondo de ferramentas para ajudar a remediar danos, tudo baseado em um painel de controle on-line.
- 2.2.92 Não será aceita solução baseada apenas em reputação de URL.
- 2.2.93 A solução deve ser proativa e ter capacidade de detecção por heurística, utilizando técnicas de análise de grande volume de dados, desta forma definindo um modelo de padrão de mensagens da corporação, levando em conta remetentes, destinatários, volume de mensagens e vários outros fatores, dessa forma modelando os e-mails "Normais" da corporação e barrando "Anomalias",fazendo essa análise e definição de padrão por caixa postal.
- 2.2.94 O sistema deverá ser capaz analisar anexos no mínimo nas extensões PDF, Microsoft Office, arquivos em Flash para payloads maliciosos, Microsoft Office com as seguintes extensões a serem verificadas:
 - 2.2.94.1 .swf;
 - 2.2.94.2 .pdf;
 - 2.2.94.3 .doc;
 - 2.2.94.4 .xls;
 - 2.2.94.5 .xlsx;
 - 2.2.94.6 .ppt;
 - 2.2.94.7 .pps;
 - 2.2.94.8 .pptx;
 - 2.2.94.9 .rtf.
- 2.2.95 O Dashboard deverá exibir *timeline* (do inglês, linha do tempo) das ameaças, exibindo quando foi recebida, identificada e quando foi clicada ou liberada.
- 2.2.96 No Dashboard deverá ser possível filtrar um endereço IP em um campo de busca para analisar todas as ocorrências com aquele endereço IP, bem como verificar o status atual dele e preview da página web.
- 2.2.97 O Dashboard deverá possuir ferramenta para bloqueio ou liberação do endereço IP pelo administrador da ferramenta.
- 2.2.98 O Dashboard deverá possuir ferramenta para bloqueio ou liberação do arquivo pelo administrador da ferramenta.
- 2.2.99 A ferramenta de segurança contra-ataques dirigidos, deve possuir o sistema colaborativo, ao qual o administrador poderá configurar que o usuário final possa indicar liberação e bloqueio de URL's, mesmo analisados pelo sistema e dessa forma reportando falsos positivos e falsos negativos. Deve prover também um Dashboard onde o Administrador poderá verificar todos os reportes enviados pelos usuários, ficando a cargo do administrador decidir pelo bloqueio ou a liberação de tal URL e/ou Arquivo.
- 2.2.100 A solução deve possuir capacidade de detecção de Spoofing de e-mails externos, isto é, ter a capacidade de comparar o domínio do cabeçalho do e-mail (Header do E-mail/Envelope SMTP), com o domínio apresentado como remetente para o usuário final (Cabeçalho From) e indicar o que deve ser feito se forem diferentes:
 - 2.2.100.1 Pontuar
 - 2.2.100.2 Ignorar;
 - 2.2.100.3 Bloquear.
- 2.2.101 O sistema deve possuir a opção de configurar regras para detectar e-mails que estejam utilizando ataques do tipo Look-A-Like Domain, isto é, detectar e-mails com domínios similares aos domínios utilizados pelo órgão.

- 2.2.102 Deve possuir sistema de detecção de e-mails oriundos de servidores de e-mails gratuitos (*free emails*), tais como Google, Yahoo, Hotmail etc.
- 2.2.103 Nativamente deve possuir sistema de detecção de e-mails externos (e-mails de entrada) que tentem utilizar o(s) domínio(s) da própria empresa como remetente, sem necessidade de criação de regra específica para este tipo de fraude.

2.3 Treinamento

- 2.3.1 A capacitação deverá ser fornecida em turma de 07 (sete) colaboradores da área de tecnologia da CONTRATANTE.
- 2.3.2 O treinamento deverá ser realizado presencialmente, em infraestrutura disponibilizada pela CONTRATANTE e deverá possuir carga horária mínima de 24 (vinte e quatro) horas de cada módulo tendo em vista no total de 96 (noventa e seis) horas no total.
- 2.3.3 O treinamento será realizado no seguinte endereço: Centro de Computação da Aeronáutica(CCA-RJ) Av. Brg. Trompowski, 68 – Galeão, Rio de Janeiro – RJ, 21044-020, Rio de Janeiro / RJ – CEP 21941-520 Telefone: (21) 2101-7800
- 2.3.4 A capacitação poderá ser realizada em turma única ou em duas turmas, a critério da CONTRATADA
 - 2.3.4.1 Se em turma única, o treinamento será de 7 (sete) participantes, terá carga horária máxima, por dia, de 4 (quatro) horas. Será realizado em horário comercial, no modelo de treinamento presencial.
 - 2.3.4.2 Se em duas turmas, o treinamento terá uma turma de 4 (quatro) alunos e outra turma de 3 (três) alunos com carga horária máxima, por dia, de 8 (oito) horas. Será realizado em horário comercial, no modelo de treinamento presencial.
- 2.3.5 A capacitação deverá consistir em treinamento oficial em acordo com as políticas do fabricante da solução fornecida.
- 2.3.6 Deverá ser ministrado por instrutor certificado na solução.
- 2.3.7 Os softwares, materiais, apostilas, profissionais, instrutores e todos os requisitos necessários à realização adequada do treinamento são de responsabilidade exclusiva da CONTRATADA.
- 2.3.8 Uma cópia do material do treinamento deverá ser enviada com antecedência mínima de 15 (quinze) dias da data de início do treinamento à CONTRATANTE, para análise e aprovação.
- 2.3.9 O material não aprovado pelo Contratante deverá ser refeito pela CONTRATADA e novamente aprovado.
- 2.3.10 O treinamento deverá ser ministrado em português e é composto de aulas teóricas e práticas (Hands On).
- 2.3.11 O treinamento deverá abordar as funcionalidades:
 - 2.3.11.1 Solução de gateway de segurança de e-mail ofertada, bem como a instalação, configuração, administração, operação, otimização, automatização de tarefas, metodologia de diagnóstico e resolução de problemas (troubleshooting), geração de relatórios, cópia de segurança (backup) e restauração, controle de acesso, auditoria e gerenciamento de logs;
 - 2.3.11.2 Plataforma de Sistema de Colaboração bem como a instalação, configuração, administração, operação, otimização, automatização de tarefas, metodologia de diagnóstico e resolução de problemas;
 - 2.3.11.3 Linux para utilização na implantação do sistema bem como a configuração, administração, operação, otimização, automatização de tarefas (shell script), metodologia de diagnóstico e resolução de problemas; e
 - 2.3.11.4 Postfix para utilização na implantação do sistema bem como a configuração, administração, operação, otimização, metodologia de diagnóstico e resolução de problemas
- 2.3.12 Todas as despesas com passagens, hospedagens e alimentação dos seus instrutores no período do treinamento ficarão a cargo da CONTRATADA.
- 2.3.13 Para a realização da capacitação, a empresa deverá fornecer certificado de conclusão para cada participante.
- 2.3.14 O cronograma para realização dos eventos será definido pela CONTRATANTE em conjunto com a contratada.
- 2.3.15 Ao final do treinamento, deverá ser realizada junto aos participantes uma avaliação do curso por meio de formulário da CONTRATADA.

- 2.3.16 Caso o curso seja avaliado como insatisfatório pelos participantes da turma, à CONTRATANTE, deverá informar formalmente por escrito o ocorrido e justificar o fato.
- 2.3.17 O cálculo para avaliação insatisfatória dar-se-á da seguinte forma: A média da avaliação do curso entre os participantes for ruim ou regular.
- 2.3.18 Os critérios da avaliação são medidos como segue: Ruim (1); Regular (2); Bom (3); Ótimo (4 ou 5).
- 2.3.19 A CONTRATADA deverá assegurar-se que os participantes do treinamento assinem ou confirmem diariamente lista de presença. A lista deverá ser entregue à CONTRATANTE.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação.

3.2. A Justificativa e objetivo da contratação encontram-se pormenorizados em Tópico específico dos apêndices deste Termo de Referência.

3.2.1. A Lei Geral de Proteção de Dados Pessoais (LGPD) - LEI Nº 13.709, DE 14 de Agosto de 2018, já em vigor em todo Brasil, torna obrigatório a definição de mecanismos formais que visem auxiliar no controle sobre o tratamento de dados nas instituições.

3.2.2. Esta contratação tem por objetivo a contratação de suporte técnico especializado, atualização e gerenciamento do licenciamento Zimbra Network Edition e aquisição de solução de segurança do tipo Anti-spam para promover o aumento dos níveis de segurança no ambiente de e-mail institucional. Refere-se ao objetivo de identificar e bloquear, em tempo real, ataques, invasões ou abusos direcionados ao ambiente de e-mail, de forma a reduzir os riscos relacionados à imagem institucional, perda de informações e descumprimento de normas e regulamentos. Visa também atender a necessidade de possuir uma infraestrutura mais robusta, necessária para atender às demandas de envio e recebimento de mensagens institucionais internas e externas, através da implementação de recursos de segurança da informação. Visa atender as áreas finalísticas com melhor qualidade, em menor espaço de tempo, diminuindo o período de inatividade dos usuários, causados por incidentes de segurança, aumentando assim a produtividade; prover melhores serviços aos usuários finais, oferecendo maior qualidade, ampliando a eficiência e a segurança das atividades executadas.

3.2.3. Em decorrência disso, é fundamental a definição de estratégias que unifiquem os propósitos desses pilares da Segurança da Informação. Dentre as medidas de segurança que garantem a proteção e a preservação das informações da Instituição, destaca-se a utilização de uma ferramenta de detecção e de prevenção de contaminações ou ataques de programas maliciosos, como vírus e Malware em geral, que possam vir a comprometer os dados e informações do negócio.

3.2.4. Correio eletrônico é atualmente o canal mais usado para ataques oportunistas e direcionados, além de um ponto importante de saída para conteúdo confidencial, sendo assim, uma solução integrada de anti-spam e mecanismo de prevenção de perda de dados se mostra um componente crítico da estratégia de segurança em um ambiente de correio eletrônico onde ameaças estão sempre em evolução.

3.2.5. A contratação mostra-se imprescindível em razão da necessidade de manutenção dos serviços de segurança da informação e de correio eletrônico, sendo de suma importância a adoção da solução de segurança para tratamento de mensagens não solicitadas (SPAM e PHISHING), de modo a evitar a disseminação de softwares maliciosos.

3.3. Em atenção ao parágrafo único do art. 1º do decreto nº 10.947/2022, o objeto da contratação está previsto no Planejamento Anual de Aquisições e Contratações (PAAC) de 2023, disposto no portal da força aérea brasileira (FAB), <https://www2.fab.mil.br/paac/>, conforme detalhamento a seguir:

3.3.1. Região/unidade: 120128

3.3.2. Data de publicação no portal da FAB: 10 DE ABRIL DE 2023

3.3.3. Código de planejamento do objeto no PAAC: CELOG23SER013

3.4. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2023 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) <2021-2024> do COMAER, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS			
ID	Objetivos Estratégicos		
1	Aperfeiçoar o planejamento, a governança, a execução orçamentária e os processos de aquisição em TI administrativa.		
ALINHAMENTO AO PDTIC <2021-2024>(PCA 11-320)			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
1.1	Padronizar o portfólio de ativos de TI do COMAER por meio da centralização das aquisições de TI.	1.1.1	Adquirir licença de software para manutenção das atividades das OM

4. REQUISITOS DA CONTRATAÇÃO

Sustentabilidade

4.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.1.1. Por se tratar de contratação de suporte de software, de forma remota, sem a utilização de componentes mecânicos, tóxicos ou biodegradáveis, esta contratação não possui requisitos de sustentabilidade ambiental.

Da vedação de utilização de marca/produto na execução do serviço

4.2. Diante das conclusões extraídas do Estudo Técnico Preliminar, a Administração não aceitará o fornecimento da solução que não seja proveniente de parceiros Zimbra.

Da exigência de carta de solidariedade

4.3. Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

Subcontratação

4.4. Não é admitida a subcontratação do objeto contratual.

4.5. Será realizada verificação de amostra do objeto para averiguar se a Solução de TIC apresentada pela Licitante detém os requisitos mínimos necessários para realização dos serviços a serem contratados, de acordo com as funcionalidades, procedimentos e critérios objetivos descritos no Termo de Referência.

4.6. Serão exigidas amostras referentes aos seguintes itens:

4.6.1. O Teste de Homologação terá o prazo de até 10 (dez) dias úteis, contados da data da convocação, para entregar uma amostra completa da solução ofertada contendo equipamentos (quando couber) acompanhado dos softwares e licenças necessárias ao seu funcionamento pelo período de 30 (trinta) dias corridos.

4.6.2. O Teste de Homologação será realizado sem custo para a CONTRATANTE pelo período de 30 (trinta) dias corridos, contados da data da entrega.

4.6.3. Estão incluídos no prazo de 30 (trinta) dias corridos a instalação, a configuração e a demonstração de que os produtos atendem às especificações constantes no Item 7 do Termo de referência.

Garantia da Contratação

4.7. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% do valor contratual, conforme regras previstas no contrato.

4.7.1. A garantia nas modalidades caução e fiança bancárias deverá prestada em até 90 dias após a assinatura do contrato.

4.7.2. No caso de seguro-garantia sua apresentação deverá ocorrer, no máximo, até a data de assinatura do contrato.

4.8. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

4.9. O Contratado deverá realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução dos serviços.

4.10. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento)

4.11. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

4.11.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

4.11.2. Prejuízos diretos causados à Administração decorrente de culpa ou dolo durante a execução do contrato;

4.11.3. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

4.11.4. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

4.12. A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

4.13. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

4.14. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

4.15. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

4.16. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 5 dias úteis, contados da data em que for notificada.

4.17. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

4.18. Será considerada extinta a garantia:

4.18.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

4.18.2. No prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2" do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017; e

4.18.3. O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

Requisitos de Negócio

4.19. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.19.1. É fundamental a definição de estratégias que unifiquem os propósitos da Segurança da Informação. Dentre as medidas de segurança que garantem a proteção e a preservação das informações da Instituição, destaca-se a utilização de uma ferramenta de detecção e de prevenção de contaminações ou ataques de programas maliciosos, como vírus e Malware em geral, que possam vir a comprometer os dados e informações do negócio.

Requisitos de Capacitação

4.20. A capacitação deverá ser fornecida em turma de 07 (sete) colaboradores da área de tecnologia da CONTRATANTE

4.21. O treinamento deverá ser realizado no seguinte endereço: Centro de Computação da Aeronáutica(CCA-RJ) Av. Brg. Trompowski, 68 – Galeão, Rio de Janeiro – RJ, 21044-020, Rio de Janeiro / RJ – CEP 21941-520 Telefone: (21) 2101-7800

4.22. A capacitação poderá ser realizada em turma única ou em duas turmas, a critério da CONTRANTE:

4.22.1. Se em turma única, o curso terá carga horária máxima, por dia, de 4 (quatro) horas.

4.22.2. Se em duas turmas, o curso terá carga horária máxima, por dia, de 8 (oito) horas.

4.23. A capacitação deverá consistir em treinamento oficial em acordo com as políticas do fabricante da solução fornecida.

4.24. Deverá ser ministrado por instrutor certificado na solução.

4.25. Os softwares, materiais, apostilas, profissionais, instrutores e todos os requisitos necessários à realização adequada do treinamento são de responsabilidade exclusiva da CONTRATADA.

4.26. Uma cópia do material do treinamento deverá ser enviada com antecedência mínima de 15 (quinze) dias da data de início do treinamento à CONTRATANTE, para análise e aprovação.

4.27. O material não aprovado pelo Contratante deverá ser refeito pela CONTRATADA e novamente aprovado.

4.28. O treinamento deverá ser ministrado em português e é composto de aulas teóricas e práticas (Hands On).

4.29. O treinamento deverá abordar as funcionalidades:

4.29.1. Solução de gateway de segurança de e-mail ofertada, bem como a instalação, configuração, administração, operação, otimização, automatização de tarefas, metodologia de diagnóstico e resolução de problemas (troubleshooting), geração de relatórios, cópia de segurança (backup) e restauração, controle de acesso, auditoria e gerenciamento de logs;

4.29.2. Plataforma de Sistema de Colaboração bem como a instalação, configuração, administração, operação, otimização, automatização de tarefas, metodologia de diagnóstico e resolução de problemas;

4.29.3. Linux para utilização na implantação do sistema bem como a configuração, administração, operação, otimização, automatização de tarefas (shell script), metodologia de diagnóstico e resolução de problemas; e

4.29.4. Postfix para utilização na implantação do sistema bem como a configuração, administração, operação, otimização, metodologia de diagnóstico e resolução de problemas.

4.30. Todas as despesas com passagens, hospedagens e alimentação dos seus instrutores no período do treinamento ficarão a cargo da CONTRATADA.

4.31. Para a realização da capacitação, a empresa deverá fornecer certificado de conclusão para cada participante.

4.32. Após a realização da capacitação, a empresa deverá fornecer certificado de conclusão para cada participante, em cada módulo distinto.

4.33. O cronograma para realização dos eventos será definido pela CONTRATANTE em conjunto com a contratada.

4.34. Ao final do treinamento, deverá ser realizada junto aos participantes uma avaliação do curso por meio de formulário da CONTRATADA.

4.35. Caso o curso seja avaliado como insatisfatório pelos participantes da turma, o treinamento deverá ser refeito, sem ônus adicional à CONTRATANTE, respeitando as condições elencadas neste Termo de Referência.

4.36. O cálculo para avaliação insatisfatória dar-se-á da seguinte forma: A média da avaliação do curso entre os participantes for ruim ou regular.

4.37. Os critérios da avaliação são medidos como segue: Ruim (1); Regular (2); Bom (3); Ótimo (4 ou 5).

4.38. A CONTRATADA deverá assegurar-se que os participantes do treinamento assinem ou confirmem diariamente lista de presença. A lista deverá ser entregue à CONTRATANTE.

Requisitos Legais

1.1. O presente processo de contratação deve estar aderente à [Constituição Federal](#), à [Lei nº 14.133/2021](#), à [Instrução Normativa SGD/ME nº 94, de 2022](#), [Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021](#), [Lei nº 13.709, de 14 de agosto de 2018](#) (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

4.39. Cumprir os requisitos legais, quando a contratada houver se beneficiado da preferência estabelecida pelo art. 26º, da Lei nº 14.133, de 2021.

4.40. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante.

Requisitos de Manutenção

4.41. Devido às características da solução, há necessidade de realização de manutenções (corretivas/preventivas/adaptativa/evolutiva) pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades;

4.42. A Contratada apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, em valor correspondente a 5 % (cinco por cento) do valor total do contrato, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, devendo ser renovada a cada prorrogação.

4.43. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

4.44. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

4.44.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

4.44.2. Prejuízos diretos causados à Administração decorrente de culpa ou dolo durante a execução do contrato;

4.44.3. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

4.44.4. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

4.45. A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

4.46. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

4.47. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

4.48. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

4.49. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 5 dias úteis, contados da data em que for notificada.

4.50. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

4.51. Será considerada extinta a garantia:

4.51.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

4.51.2. No prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2" do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

4.51.3. O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

Requisitos Temporais

4.52. Os itens do Lote 01 são serviços continuados e serão entregues mensalmente ao longo do contrato.

4.52.1. Especificamente o Item 02 do Lote 01 deverá ser instalado e configurado e posto em homologação em, no máximo, 30 dias a contar da assinatura do contrato.

4.52.1.1. filtro de anti-spam deverá dentro do prazo acima ser disponibilizado em ambiente de homologação, integrado ao ambiente principal, entretanto sem afetar a circulação das mensagens, apenas em caráter informativo, até a homologação pela equipe técnica da CONTRATANTE.

4.52.1.2. A CONTRATANTE terá 30 dias corridos para homologar o ambiente de filtro anti-spam.

4.52.1.3. Para atender o disposto na lei nº 14.133/2021 em seu Art. 41, inciso II a exigência de amostra será feita em ambiente de homologação durante 30 dias a contar da assinatura do contrato e caso a solução venha a ser reprovada nessa fase a contratada deverá enviar por escrito de forma detalhada os motivos da reprovação e desenhar uma possível solução de contorno.

4.52.1.4. Após a homologação a CONTRATADA tem 10 dias corridos para configurar o ambiente do filtro anti-spam no ambiente de produção do correio corporativo da CONTRATANTE.

4.53. O item 01 do Lote 02, treinamento, deverá ser iniciado em até 90 dias da assinatura do contrato.

4.54. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.55. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

Requisitos de Segurança e Privacidade

4.56. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante.

4.57. Solução deverá analisar mensagens eletrônicas suspeitas de serem maliciosas, spam, vírus e Phishing ou estarem fora da política de segurança e uso da Força Aérea.

4.58. A solução deverá possuir integração com serviço de diretórios LDAP do serviço de e-mail para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas.

4.59. Permitir criação de políticas diferenciadas para tratamento de spam, vírus e filtragem de conteúdo, de acordo com o destinatário da mensagem.

4.60. Deve permitir a aplicação de políticas de SPAM diferentes por nome de domínio, destinatário, grupo de destinatários e por destinatário específico, integrado aos sistemas de diretório LDAP e MS Active Directory.

4.61. O treinamento deverá consistir em treinamento oficial em acordo com as políticas do fabricante da solução fornecida.

Requisitos Sociais, Ambientais e Culturais

4.62. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

4.62.1. Os profissionais da CONTRATADA deverão trajar-se de maneira adequada, quando no ambiente da CONTRATANTE, e usar linguagem respeitosa e formal no trato com a Gestão e/ou Fiscalização Contratual, os dirigentes da CONTRATANTE e usuários, em consonância com as regras e normas internas do órgão.

4.62.2. Os serviços prestados pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de modo a evitar e prevenir o desperdício de insumos e materiais.

4.62.3. A CONTRATADA deverá instruir os seus empregados quanto à necessidade de racionalização de recursos no desempenho de suas atribuições, bem como das diretrizes de responsabilidade ambiental adotadas pelo CONTRATANTE.

4.62.4. A CONTRATADA deverá assumir a responsabilidade por todos os encargos e obrigações sociais previstas na legislação social e trabalhista em vigor, obrigando-se a saldá-las na época própria, vez que seus profissionais e prepostos não manterão qualquer vínculo empregatício com a CONTRATANTE.

Requisitos da Arquitetura Tecnológica

4.63. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

4.64. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

4.65. A implementação deverá ser realizada de tal forma que as interrupções no ambiente de produção sejam as mínimas possíveis e estritamente necessárias, e, ainda, não causem transtornos aos usuários finais do órgão.

4.65.1. Havendo necessidade de interrupções no ambiente de produção, a contratada deverá realizar as intervenções fora do horário comercial, podendo ser a noite ou durante o fim de semana, a critério da CONTRATANTE.

Requisitos de Projeto e de Implementação

4.66. Os serviços deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

4.66.1. A implementação deverá ser realizada de tal forma que as interrupções no ambiente de produção sejam as mínimas possíveis e estritamente necessárias, e, ainda, não causem transtornos aos usuários finais do órgão.

4.66.2. Havendo necessidade de interrupções no ambiente de produção, a contratada deverá realizar as intervenções fora do horário comercial, podendo ser a noite ou durante o fim de semana, a critério da CONTRATANTE.

Requisitos de Implantação

4.67. Os serviços deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

4.68. Implementação do Correio Corporativo em nuvem privada em nosso Datacenter, garantindo segurança dos dados em territorialidade;

4.69. Possibilidade de implementação de mecanismos de sistema e de segurança contemplados nas próximas versões.

Requisitos de Garantia e Manutenção

4.70. O prazo de suporte técnico da solução ofertada deverá ser de, no mínimo, 24 (vinte e quatro) meses, contados a partir da data do aceite definitivo.

4.71. A CONTRATADA deve garantir para a CONTRATANTE o fornecimento de acesso irrestrito (24 horas x 7 dias da semana) à área de suporte do fabricante, especialmente ao endereço eletrônico (web site), a toda a documentação técnica pertinente (guias de instalação/configurações atualizadas, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

4.72. As respostas do suporte técnico contratado deverão ser efetuadas na língua portuguesa (português do Brasil), tanto por e-mail, quanto por contato telefônico.

4.73. O suporte técnico deverá ser prestado em caso de falhas, necessidade de configuração de funcionalidades, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes aos appliances que compõem a solução.

4.74. A abertura de chamados pelo CONTRATANTE será efetuada por correio eletrônico, por sistema de controle de chamados, com e-mail de resposta do chamado aberto apresentando o número do ticket aberto, para acompanhamento.

4.75. A CONTRATADA deverá fornecer os níveis de atendimento conforme abaixo indicado:

4.75.1. Os chamados de severidade Crítica (quando há indisponibilidade de uso da solução) deverão ser atendidos em até 1 (uma) hora após a abertura e deverão ser solucionados em até 12 (doze) horas, contados a partir da abertura do chamado;

4.75.2. Os chamados de severidade ALTA (Quando há indisponibilidade de uso da solução) deverão ser atendidos em até 6 (seis) horas após a abertura e deverão ser solucionado em até 24 (vinte e quatro) horas, contados a partir da abertura do chamado;

4.75.3. Os chamados de severidade MÉDIA (Quando há falha, simultânea ou não, de uma ou mais funcionalidades que não cause indisponibilidade, mas apresente problemas de funcionamento e/ou performance da solução) deverão ser atendidos em até 12 (doze) horas após a abertura e deverão ser solucionados em até 48 (quarenta e oito) horas, contados a partir da abertura do chamado;

4.75.4. Os chamados de severidade BAIXA (Nível de severidade aplicado para instalação, configuração, atualização de versões e implementações de novas funcionalidades) deverão ser atendidos em até 16 (dezesesseis) horas após a abertura e deverão ser solucionados em até 48 (quarenta e oito) horas, contados a partir da abertura do chamado;

4.75.5. Os chamados de severidade INFORMATIVO (Nível informacional ou dúvidas) deverão ser atendidos em até 16 (dezesesseis) horas após a abertura.

4.76. A CONTRATADA deverá possuir técnico especializado na solução, com no mínimo 1 (um) técnico certificado pelo fabricante e com certificação dentro da validade.

Requisitos de Experiência Profissional

4.77. Os serviços de assistência técnica, suporte e garantia deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

4.78. O preposto do contrato, responsável técnico com especialidade em Tecnologia da Informação, deverá garantir a correta gestão administrativa do contrato, bem como a execução dos serviços contratados e atendimento dos níveis mínimos de serviço e, também:

4.78.1. O preposto do contrato e seu substituto eventual, deverão ser indicados pela CONTRATADA;

4.78.2. O preposto, e seu substituto, devem responder pela fiel execução do contrato; e

4.78.3. A comprovação da qualificação mínima será exigida a todos os profissionais alocados na realização dos serviços correlatos ao objeto mediante a apresentação de diplomas, certificados e currículos profissionais.

Requisitos de Formação da Equipe

4.79. A CONTRATADA deverá adequar o conhecimento e perfis de seus profissionais, para o atendimento e suporte técnico.

4.80. A qualificação profissional mínima exigida para algumas tarefas vinculará à prestação dos respectivos serviços por profissionais que possuam qualificação adequada para a prestação dos serviços.

4.81. Caso alguma certificação exigida tenha sido atualizada ou substituída será aceita a nova versão ou certificação.

4.82. A comprovação de certificação dos profissionais poderá ser exigida pela CONTRATANTE a qualquer tempo. A não apresentação da documentação comprobatória da certificação, quando solicitada, ensejará a aplicação de penalidades, conforme termos contratuais.

4.83. Os diplomas de curso superior e pós-graduação devem ser devidamente registrados e fornecidos por instituição de ensino superior, reconhecida pelo Ministério da Educação (MEC).

4.84. Após a seleção da equipe pela CONTRATADA e apresentação formal, a qualificação técnica dos profissionais será verificada pelos Gestores e Fiscais de Contrato.

Requisitos de Metodologia de Trabalho

4.85. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

4.86. A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

4.87. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e 24 horas por dia e 7 dias por semana por via telefônica.

4.88. A execução do serviço deve ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

4.89. Na execução das demandas a CONTRATADA deve zelar pela observância às políticas, diretrizes, procedimentos, padrões e modelos para as atividades de gestão e fiscalização de contratos e planejamento de contratações.

Requisitos de Segurança da Informação e Privacidade

4.90. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

4.91. As soluções oferecidas pela consultoria devem garantir o atendimento ao disposto na LGPD – Lei Geral de Proteção de Dados.

Outros Requisitos Aplicáveis

4.92. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto nº 9.507, de 21 de setembro de 2018, não se constituindo em quaisquer das atividades, previstas no art.3º do aludido decreto, cuja execução indireta é vedada.

5. INFORMAÇÕES RELEVANTES PARA O [DIMENSIONAMENTO E/OU APRESENTAÇÃO] DA PROPOSTA

- 5.1.** A demanda do órgão tem como base as seguintes características:
- 5.2.** Atingir índice de 99,9% de disponibilidade e manutenção de ambiente, mantendo o mesmo estável;
- 5.3.** Integração com uma base de dados única (LDAP Central), atendendo a determinação de autenticação pelo Portal do Militar;
- 5.4.** Implementação do Correio Corporativo em nuvem privada em nosso Datacenter, garantindo segurança dos dados e territorialidade;
- 5.5.** Criação de um site de redundância/contingência;
- 5.6.** Manutenção do Correio Corporativo Zimbra, agilidade na resolução dos chamados; e
- 5.7.** A implantação em ambiente de produção deverá ser realizada após planejamento com equipe do Centro de Computação da Aeronáutica do Rio de Janeiro, em dias não úteis de modo a causar o menor impacto para os usuários finais.

Vistoria

- 5.8.** Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

6. PAPÉIS E RESPONSABILIDADES

- 6.1.** São obrigações da CONTRATANTE:
- 6.2.** nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- 6.3.** encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
- 6.4.** receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 6.5.** aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- 6.6.** liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- 6.7.** comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- 6.8.** definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;
- 6.9.** prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

6.10. São obrigações do CONTRATADO

6.11. indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

6.12. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

6.13. reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

6.14. propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

6.15. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

6.16. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

6.17. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

6.18. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

6.19. fazer a transição contratual, quando for o caso;

6.20. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

6.20.1.1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

6.20.1.2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e

6.20.1.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

7. MODELO DE EXECUÇÃO DO CONTRATO

Condições de execução

7.1. A execução do objeto seguirá a seguinte dinâmica:

7.1.1. Os itens do Lote 01 são serviços continuados e serão entregues mensalmente ao longo do contrato.

7.1.2. Especificamente o Item 02 do Lote 01 deverá ser instalado e configurado e posto em homologação em, no máximo, 30 dias a contar da assinatura do contrato, sobe pena de desconto do valor no contrato e eventual multa por atraso.

7.1.3. O filtro de anti-spam deverá dentro do prazo acima ser disponibilizado em ambiente de homologação, integrado ao ambiente principal, entretanto sem afetar a circulação das mensagens, apenas em caráter informativo, até a homologação pela equipe técnica da CONTRATANTE.

7.1.4. A CONTRATANTE terá 30 dias corridos para homologar o ambiente de filtro anti-spam.

7.1.5. Após a homologação a CONTRATADA tem 10 dias corridos para configurar o ambiente do filtro anti-spam no ambiente de produção do correio corporativo da CONTRATANTE.

7.1.6. O item 01 do Lote 02, treinamento, deverá ser iniciado em até 90 (noventa) dias da assinatura do contrato.

Local da prestação dos serviços

7.2. Os serviços serão prestados no seguinte endereço Centro de Computação da Aeronáutica(CCA-RJ) Av. Brg. Trompowski, 68 – Galeão, Rio de Janeiro – RJ, 21044-020, Rio de Janeiro / RJ – CEP 21941-520 Telefone: (21) 2101-7800

Materiais a serem disponibilizados

7.3. Não serão fornecidos materiais por se tratar de suporte de software.

8. INFORMAÇÕES RELEVANTES PARA O DIMENSIONAMENTO DA PROPOSTA

8.1. A demanda do órgão tem como base as seguintes características:

8.1.1. Atingir índice de 99,9% de disponibilidade e manutenção de ambiente, mantendo o mesmo estável;

8.1.2. Integração com uma base de dados única (LDAP Central), atendendo a determinação de autenticação pelo Portal do Militar;;

8.1.3. Implementação do Correio Corporativo em nuvem privada em nosso Datacenter, garantindo segurança dos dados e territorialidade;

8.1.4. Criação de um site de redundância/contingência;

8.1.5. Manutenção do Correio Corporativo Zimbra, agilidade na resolução dos chamados;

8.1.6. A implantação em ambiente de produção deverá ser realizada após planejamento com equipe do Centro de Computação da Aeronáutica do Rio de Janeiro, em dias não úteis de modo a causar o menor impacto para os usuários finais.

Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

8.2. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

Formas de transferência de conhecimento

8.3. Não será necessária transferência de conhecimento devido às características do objeto.

Procedimentos de transição e finalização do contrato

8.4. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

Quantidade mínima de bens ou serviços para comparação e controle

8.5. Modelo descrito no *Item 1.1 deste Termo de Referência*.

Mecanismos formais de comunicação

8.6. *São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:*

- 8.6.1. Ordem de Serviço;
- 8.6.2. Ata de Reunião;
- 8.6.3. Ofício;
- 8.6.4. Sistema de abertura de chamados;
- 8.6.5. E-mails e Cartas;

8.7. A troca de informações por outros meios não previstos neste Termo de Referência terá caráter não oficial e não poderá produzir efeitos que gerem ônus para qualquer das partes.

Formas de Pagamento

8.8. Os critérios de medição e pagamento dos serviços prestados serão tratados no item 9.9. deste Termo de Referência.

8.9. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicadas pelo contratado.

8.10. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.11. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.12. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.13. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Manutenção de Sigilo e Normas de Segurança

8.14. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos os e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

8.15. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contra-

tado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos Anexo B

9. MODELO DE GESTÃO DO CONTRATO

9.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da [Lei nº 14.133, de 2021](#), e cada parte responderá pelas consequências de sua inexecução total ou parcial.

9.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

9.3. As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

9.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

9.5. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

9.6. A reunião será realizada em conformidade com o previsto no [inciso I do Art. 31 da IN SGD/ME nº 94, de 2022](#), e ocorrerá em até **90** dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

9.7. A pauta desta reunião observará, pelo menos:

9.7.1. Presença do representante legal da contratada, que apresentará o seu preposto;

9.7.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

9.7.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

9.7.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

9.7.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

9.8. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos ([Lei nº 14.133, de 2021, art. 117, caput](#)), nos termos do [art. 33 da IN SGD nº 94, de 2022](#), observando-se, em especial, as rotinas a seguir.

9.8.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no [art. 33, II, da IN SGD nº 94, de 2022](#), acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. ([Decreto nº 11.246, de 2022, art. 22, VI](#));

9.8.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. ([Lei nº 14.133, de 2021, art. 117, §1º](#), e [Decreto nº 11.246, de 2022, art. 22, II](#));

- 9.8.3. Identificada qualquer inexactidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. ([Decreto nº 11.246, de 2022, art. 22, III](#));
- 9.8.4. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. ([Decreto nº 11.246, de 2022, art. 22, IV](#)).
- 9.8.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. ([Decreto nº 11.246, de 2022, art. 22, V](#)).
- 9.8.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual ([Decreto nº 11.246, de 2022, art. 22, VII](#)).
- 9.8.7. O fiscal administrativo do contrato, além de exercer as atribuições previstas no [art. 33, IV, da IN SGD nº 94, de 2022](#), verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamentos e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário ([Art. 23, I e II, do Decreto nº 11.246, de 2022](#)).
- 9.8.8. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; ([Decreto nº 11.246, de 2022, art. 23, IV](#)).
- 9.8.9. O gestor do contrato, além de exercer as atribuições previstas no [art. 33, I, da IN SGD nº 94, de 2022](#), coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. ([Decreto nº 11.246, de 2022, art. 21, IV](#)).
- 9.8.10. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. ([Decreto nº 11.246, de 2022, art. 21, III](#)).
- 9.8.11. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. ([Decreto nº 11.246, de 2022, art. 21, II](#)).
- 9.8.12. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. ([Decreto nº 11.246, de 2022, art. 21, VIII](#)).
- 9.8.13. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata [o art. 158 da Lei nº 14.133, de 2021](#), ou pelo agente ou pelo setor com competência para tal, conforme o caso. ([Decreto nº 11.246, de 2022, art. 21, X](#)).
- 9.8.14. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. ([Decreto nº 11.246, de 2022, art. 22, VII](#)).

9.8.15. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. ([Decreto nº 11.246, de 2022, art. 21, VI](#)).

9.8.16. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

9.8.17. O contratado deverá manter preposto aceito pela Administração no local do serviço para representá-lo na execução do contrato.

9.8.18. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

Critérios de medição e pagamento

9.9. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), conforme previsto no **Anexo A**.

9.10. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

- 9.10.1. não produzir os resultados acordados;
- 9.10.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
- 9.10.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

9.11. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

9.12. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

- 9.12.1. Pronto atendimento, em até 24 horas após solicitação da prestação de serviço.
- 9.12.2. Verificação do serviço realizado por técnico devidamente designado pela CONTRATANTE; e
- 9.12.3. Garantia do serviço prestado.

9.13. Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

- 9.13.1. Não produziu os resultados acordados;
- 9.13.2. Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida; e
- 9.13.3. Deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

Do recebimento

9.14. Os itens do lote 1 serão serviços continuados e serão entregues mensalmente e o item 1 do Lote 2 será entregue em até 90 dias após a assinatura do contrato, pelos fiscais técnico e administrativo, mediante

termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. ([Art. 140, I, a, da Lei nº 14.133](#) e [Arts. 22, X e 23, X do Decreto nº 11.246, de 2022](#)).

9.15. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

9.16. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. ([Art. 22, X, Decreto nº 11.246, de 2022](#)).

9.17. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. ([Art. 23, X, Decreto nº 11.246, de 2022](#))

9.18. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

9.19. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

9.20. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

9.21. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. ([Art. 119 c/c art. 140 da Lei nº 14133, de 2021](#))

9.22. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

9.23. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

9.24. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

9.25. Os serviços serão recebidos definitivamente no prazo de 90 dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

9.26. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento ([art. 21, VIII, Decreto nº 11.246, de 2022](#)).

9.27. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

9.28. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

9.29. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

9.30. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

9.31. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do [art. 143 da Lei nº 14.133, de 2021](#), comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

9.32. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

9.33. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Procedimentos de Teste e Inspeção

9.34. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

9.34.1. O modelo utilizado para atestar a prestação de serviços será o atingimento do Instrumento de Medição de Resultado (IMR) e manutenção da disponibilidade do ambiente.

9.34.2. A mensuração consistirá no confronto das informações constantes do Relatório de execução dos serviços, no mês de referência, com as bases de dados em planilhas ou painéis de acompanhamentos e outros, a fim de verificar se as informações estão de acordo com o serviço efetivamente prestado.

Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

9.35. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Pela inexecução total ou parcial do objeto deste contrato	Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado Multa de: a) 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar,

	nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença; b) 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida; c) 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida; d) 0,2% a 3,2% por dia sobre o valor mensal do contrato; e e) 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;
--	--

9.36. Nos termos do [art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022](#), será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

9.36.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

9.36.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

Liquidação

9.37. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do [art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022](#).

9.37.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o [inciso II do art. 75 da Lei nº 14.133, de 2021](#).

9.38. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

9.38.1. o prazo de validade;

9.38.2. a data da emissão;

9.38.3. os dados do contrato e do órgão contratante;

9.38.4. o período respectivo de execução do contrato;

9.38.5. o valor a pagar; e

9.38.6. eventual destaque do valor de retenções tributárias cabíveis.

9.39. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

9.40. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no [art. 68 da Lei nº 14.133, de 2021.](#)

9.41. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

9.42. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

9.43. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

9.44. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

9.45. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

9.46. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da [Instrução Normativa SEGES/ME nº 77, de 2022.](#)

9.47. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice **ICTI** de correção monetária.

Forma de pagamento

9.48. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

9.49. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.50. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

9.51. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

9.52. O contratado regularmente optante pelo Simples Nacional, nos termos da [Lei Complementar nº 123, de 2006](#), não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Cessão de crédito

9.53. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na [Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020](#), conforme as regras deste presente tópico.

9.54. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

9.55. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme [o art. 12 da Lei nº 8.429, de 1992](#), tudo nos termos do [Parecer JL-01, de 18 de maio de 2020](#).

9.56. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

9.57. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

10. DO REAJUSTE

10.1. Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação – ICTI.

11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Forma de seleção e critério de julgamento da proposta

11.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço

11.2. O regime de execução do contrato será por Empreitada por Preço Unitário, por Lote.

Da Aplicação da Margem de Preferência

11.3. Não será aplicada margem de preferência na presente contratação.

Exigências de habilitação

11.4. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

11.5. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

11.6. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.7. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

11.8. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

11.9. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução [Normativa DREI/ME n.º 77, de 18 de março de 2020](#).

11.10. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

11.11. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

11.12. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o [art. 107 da Lei nº 5.764, de 16 de dezembro 1971](#).

11.13. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

11.14. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

11.15. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

11.16. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

11.17. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do [Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943](#);

11.18. Prova de inscrição no cadastro de contribuintes Estadual/ Distrital ou Municipal/ Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

11.19. Prova de regularidade com a Fazenda Estadual/ Distrital ou Municipal/ Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

11.20. Caso o fornecedor seja considerado isento dos tributos Estadual/ Distrital ou Municipal/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

11.21. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na [Lei Complementar n. 123, de 2006](#), estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

11.22. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação ([art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021](#)), ou de sociedade simples;

11.23. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - [Lei nº 14.133, de 2021, art. 69, caput, inciso II](#));

11.24. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I - Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);

II - Solvência Geral (SG) = (Ativo Total) / (Passivo Circulante + Passivo não Circulante); e

III - Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).

11.25. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimonial líquido mínimo de até 10% do valor total estimado da contratação

11.26. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. ([Lei nº 14.133, de 2021, art. 65, §1º](#)).

11.27. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. ([Lei nº 14.133, de 2021, art. 69, §6º](#))

Qualificação Técnica

11.28. Registro ou inscrição da empresa na entidade profissional em plena validade;

11.29. Apresentação de profissional, devidamente registrado no conselho profissional competente caso existir, quando for o caso, detentor de atestado de responsabilidade técnica por execução do serviço de características semelhantes, para fins de contratação por meio de declaração formal emitida pelo fabricante da solução de e-mail e colaboração, informando que a empresa licitante é uma revenda autorizada e que está apta pelo fabricante de comercializar, prestar os serviços, suporte e treinamentos oficiais para os softwares contratados.

11.30. Comprovar por meio de declaração formal, certidões ou atestados, regularmente emitidos pelo conselho profissional competente caso existir, quando for o caso, que demonstrem capacidade operacional na execução de serviços similares de complexidade tecnológica e operacional equivalente ou superior, bem como documentos comprobatórios emitidos na forma do § 3º do art. 88 da Lei 14.133/2021 emitida pelo fabricante da solução de e-mail e colaboração, informando que a empresa licitante é um centro de treinamentos autorizado capacitado para ministrar treinamentos oficiais para os itens contratados.

11.31. Indicação do pessoal técnico, das instalações e do aparelhamento adequado e disponíveis para a realização do objeto da licitação, bem como da qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos. Possuindo em seu quadro profissional, profissionais com certificação nível avançado pelo fabricante e comprovado através de cópias autenticadas dos certificados emitidos em nome do colaborador.

11.32. Declaração emitida pelo fabricante de que a contratada possui instrutor certificado e habilitado a ministrar cursos oficiais de administração da ferramenta em sua última versão.

11.33. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

11.34. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

11.34.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

11.34.1.1. Estrutura de alta disponibilidade;

11.34.1.2. Mínimo de 10% do total de contas da estrutura (aproximadamente 15.000 contas de usuários);

11.34.1.3. Declaração de pessoas jurídicas de direito público ou privado atestando a execução de operação, manutenção e suporte no software Zimbra de forma satisfatória;

11.34.2. Será aceito o somatório de atestados que comprovem que o licitante gerencia ou gerenciou serviços de terceirização compatíveis com o objeto licitado por período não inferior a 3 (três) anos, referentes a períodos sucessivos não contínuos, não havendo obrigatoriedade de os três anos serem ininterruptos.

11.34.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MP n. 5, de 2017.

11.34.4. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MP n. 5/2017.

11.34.5. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MP n. 5/2017.

11.34.6. A CONTRATADA também deverá apresentar, os Certificados e comprovação de experiência dos seus profissionais para a prestação dos serviços.

11.34.7. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

11.35. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

11.35.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos [arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971](#);

11.35.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

11.35.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

11.35.4. O registro previsto na [Lei n. 5.764, de 1971, art. 107](#);

11.35.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

11.35.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

11.35.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o [art. 112 da Lei n. 5.764, de 1971](#), ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

12.1. O custo estimado total da contratação por 24 (vinte e quatro) meses é de **R\$ 1.603.278,87 (um milhão, seiscentos e três mil, duzentos e setenta e oito reais e oitenta e sete centavos)**, conforme custos unitários apostos no 1.1.

13. ADEQUAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

13.1. A contratação será atendida pela seguinte dotação:

13.1.1. Gestão/Unidade: 00001/120128;

13.1.2. Fonte de Recursos: Ação 20SA;

13.1.3. Elemento de Despesa: 33.90.40;

13.1.4. Plano Interno: SDT126ICD02;

13.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

Cronograma Físico Financeiro

TERMO DE REFERÊNCIA - SERVIÇOS DE TIC - LICITAÇÃO

Lote	Item	Descrição	QTD	Valor Total	Valor Anual	Valor Mensal	Pagamento	Prazo para execução	Prazo para pagamento
1	1	Serviço de suporte e atualização das caixas postais	1	R\$ 3.055.968,00	R\$ 611.193,60	R\$ 50.932,80	mensal	24 meses	20 dias úteis
	2	Licenciamento de filtro de conteúdo de e-mail	1	R\$ 864.000,00	R\$ 172.800,00	R\$ 14.400,00	mensal	24 meses	20 dias úteis
2	3	Treinamento	1	R\$ 35.291,67	R\$ 35.291,67	-	único		20 dias úteis

Integrante Requisitante Érico Asano de Mello Ten Cel Eng Chefe da Divisão Técnica Matrícula: 388008-7	Integrante Técnico Rodrigo Cezar de Albuquerque 2T QOCON ANS Chefe da Seção de Correio Corporativo Matrícula: 743159-7	Integrante Administrativo Vanessa da Costa Câmara 1º Ten QOEA SVA Chefe da Subdivisão de Intendência Matrícula: 337238-3
--	---	---

Autoridade Máxima da Área de TIC
Paulo Henrique de Oliveira Leite Cel Av Chefe do CCA-RJ Matrícula: 304758-0

Rio de Janeiro, *data conforme assinatura eletrônica*

Aprovo,

Autoridade Competente
Paulo Henrique de Oliveira Leite Cel Av Chefe do CCA-RJ Matrícula: 304758-0



MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

CONTROLE DE ASSINATURAS ELETRÔNICAS DO DOCUMENTO

Documento:	Termo de referencia pos CJU
Data/Hora de Criação:	19/06/2023 18:38:36
Páginas do Documento:	44
Páginas Totais (Doc. + Ass.)	45
Hash MD5:	5a7f3bbfb89c9e2e2b2ec1cf0d7dad1e
Verificação de Autenticidade:	https://autenticidade-documento.sti.fab.mil.br/assinatura

Este documento foi assinado e conferido eletronicamente com fundamento no artigo 6º, do Decreto nº 8.539 de 08/10/2015 da Presidência da República pelos assinantes abaixo:

Assinado via ASSINATURA CADASTRAL por 2º Ten RODRIGO CEZAR DE ALBUQUERQUE no dia 21/06/2023 às 10:56:18 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Ten Cel Eng ÉRICO ASANO DE MELLO no dia 21/06/2023 às 13:37:44 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por 1º Ten VANESSA DA COSTA CAMARA no dia 21/06/2023 às 13:46:34 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Ten Cel QOEFOT ASSUÉSIO MENDONÇA DA ROCHA no dia 21/06/2023 às 15:45:38 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Cel PAULO HENRIQUE DE OLIVEIRA LEITE no dia 21/06/2023 às 15:53:07 no horário oficial de Brasília.

CONTROLE DE ASSINATURAS ELETRÔNICAS DO DOCUMENTO