PODER JUDICIÁRIO
JUSTIÇA FEDERAL DA 2ª REGIÃO

ANEXO I – TERMO DE REFERÊNCIA

Solicitação Eletrônica de Compra Nº JFES-SEC-2024/00067

1. DA DEFINIÇÃO DO OBJETO

1.1. Contratação da renovação da solução de segurança de filtragem de conteúdo e-mail (antispam), contemplando licenciamento de *appliances* virtuais, suporte técnico e garantia pelo período mínimo de 3 (três) anos, serviços de instalação e capacitação, conforme o caso.
   1.1.1. As condições estabelecidas no Termo de Referência prevalecem sobre as apresentadas no CATSER.
1.2. O objeto dessa licitação é uno e indivisível e será adjudicado a uma única licitante.

2. DO MODELO DE PLANILHA DE FORMAÇÃO DE PREÇOS DISCRIMINADOS

2.1. A licitante deverá apresentar proposta de preços conforme modelo constante no anexo "MODELO DE PLANILHA DE FORMAÇÃO DE PREÇOS DISCRIMINADOS", contendo discriminação detalhada dos produtos/serviços ofertados, valor unitário e total, em moeda nacional brasileira.
2.2. Juntamente com a proposta, a licitante deverá comprovar o atendimento a cada item do anexo "REQUISITOS TÉCNICOS ESPECÍFICOS", que trata dos requisitos técnicos específicos da licença, que poderá ser feita pela entrega dos manuais, sites, catálogos e/ou publicações originais do fabricante, com indicação das páginas/folhas/textos da informação desejada, conforme o modelo da tabela:

Comprovação de atendimento ao anexo "REQUISITOS TÉCNICOS ESPECÍFICOS"		
Item do ANEXO	**Documento de Comprovação**	
< Número do item/subitem>	*< Informar o documento (manual do fabricante, site, catálogo e/ou publicação original) que que comprove o atendimento à especificação >*	*< Indicação da página, folha, texto ou outro meio para localizar a informação desejada >*
...	...	...

2.3. Na cotação de preços deverão estar inclusos todos os itens de custo e despesas, tais como materiais, serviços, transportes, embalagens, seguro, mão-de-obra, salários dos profissionais, impostos, encargos sociais, encargos tributários, taxas, fretes e as demais despesas que incidam direta ou indiretamente sobre os produtos, mesmo que não estejam relacionadas na proposta, não sendo admitido nenhum ônus adicional à contratante durante a prestação dos serviços.
2.4. As descrições apresentadas na definição do objeto e na planilha de formação de preços correspondem às características mínimas desejadas, nada impedindo o fornecimento de produto com características superiores às especificadas.
2.5. As licitantes deverão apresentar em suas propostas informações detalhadas dos componentes da solução ofertada, apresentando fabricante/marca, modelo, *part numbers*, descrição técnica, quantidade e preço unitário dos produtos ofertados, consoante o Acórdão 1432/2024 do Plenário do Tribunal de Contas da União.
2.6. A solução atual em operação do órgão é do fabricante HSC – *High Security Center* , sendo composta pelos seguintes elementos:
   2.6.1. Dois *appliances* virtuais atuando como agentes de filtragem em *cluster* ativo-ativo, garantindo performance e alta disponibilidade, sem perda de informação.

2.6.2. Um a*ppliance* virtual atuando como console de gerenciamento centralizado da solução.
2.6.3. Subscrições dos mecanismos de proteção e suporte com data de **expiração em 01 de dezembro de 2024**.

2.7. O período de validade das subscrições dos mecanismos de proteção e do suporte será de no mínimo 3 (três) anos, contados a partir de **01 de dezembro de 2024** ou da data de emissão do TERMO DE RECEBIMENTO DEFINITIVO, caso ocorra em data posterior a 01 de dezembro de 2024.

2.8. Visita técnica facultativa para balizamento da elaboração das propostas de preços.
2.8.1. Será facultado às licitantes realizarem visita técnica nas instalações da contratante com objetivo de conhecerem os locais e condições físicas das localidades onde o serviço será prestado, de forma a obterem informações, esclarecerem dúvidas, verificarem eventuais dificuldades na execução do objeto do certame, viabilizando a elaboração mais precisa das suas propostas de preço.
2.8.2. A visita técnica deverá ser previamente agendada pelos meios indicados no item 18.4, com antecedência mínima de 3 (três) dias e no prazo máximo de até uma semana antes da data agendada para a licitação.
2.8.3. As visitas técnicas serão acompanhadas pela equipe técnica da contratante, que poderá impedir o registro de fotos e vídeos das suas instalações.
2.8.4. Não serão aceitos questionamentos técnicos finalizada a fase de licitação, bem como alegações posteriores de desconhecimento de quaisquer condições como justificativa para o não cumprimento do objeto ou para gerar ônus adicional à contratante.

3. DA JUSTIFICATIVA E MOTIVAÇÃO DA CONTRATAÇÃO

3.1. A solução de filtragem de e-mails é um dos componentes essenciais do ambiente de TIC, cuja função principal é garantir a segurança e eficiência no tráfego das mensagens eletrônicas recebidas e enviadas pelos usuários do órgão, procurando bloquear comunicações indesejadas, tais como, *spams*, propagandas, *phishings*, bem como mensagens com conteúdo impróprio ou com anexos contendo *malwares* dos mais diversos tipos.

3.2. A presente contratação tem por objetivo a renovação da solução de filtragem de e-mails existente no órgão, assegurando a continuidade das atualizações dos mecanismos de segurança e do suporte, essenciais para se manter a segurança adequada ao ambiente de rede corporativo.

3.3. Assim, o ganho alcançado com a informatização dos processos de negócio gerou, por outro lado, uma alta dependência sobre a infraestrutura tecnológica, sistemas de informação e serviços de TI, e dada a criticidade dessa solução para prover segurança ao ambiente de rede corporativo, essa aquisição é essencial para a continuidade do negócio, garantindo a disponibilidade e a adequação às novas demandas dos serviços de TI oferecidos pelo órgão.

4. DOS RESULTADOS/BENEFÍCIOS A SEREM ALCANÇADOS

4.1. Segurança da comunicação eletrônica dos usuários da rede corporativa.
4.2. Alta disponibilidade dos serviços e sistemas de TI.
4.3. Maior celeridade na solução de eventuais problemas na solução de segurança objeto da contratação.

4.4. Ambiente operacional atualizado e menos suscetível a falhas de funcionamento e de segurança.

5. FUNDAMENTAÇÃO DA CONTRATAÇÃO - REFERÊNCIA AOS ESTUDOS PRELIMINARES DA CONTRATAÇÃO

5.1. Foram utilizados como base o Documento de Oficialização da Demanda n° JFES-DOD-2024/00007 e o Estudo Técnico Preliminar juntados à Solicitação Eletrônica de Compra que deu origem à presente contratação.

6. DO ALINHAMENTO DA CONTRATAÇÃO E O PLANEJAMENTO ESTRATÉGICO DA JF

6.1. A solução está alinhada aos planos estratégico e diretor de tecnologia da informação e comunicação, respectivamente PETI e PDTIC, conforme apresentado nos quadros a seguir.

6.2. O objeto da contratação também está previsto no Plano de Contratações Anual – PAC da Seção Judiciária do Espírito Santo.

ALINHAMENTO AO PLANO ESTRATÉGICO – PETI / ENTIC-JUD
Objetivo Estratégico
OE7 - Aprimorar a Segurança da Informação e a Gestão de Dados

ALINHAMENTO AO PLANO DIRETOR - PDTIC	
Id	**Necessidade/Iniciativa**
4	Segurança da Informação no âmbito da TI

7. DA RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE BENS E/OU SERVIÇOS A SEREM CONTRATADOS

7.1. Atualmente o órgão possui instalados no datacenter a solução de segurança de filtragem de e-mail *Mail Inspector* da empresa HSC – *High Security Center*, composta por 2 (dois) *appliances* virtuais atuando como agentes de filtragem em cluster ativo-ativo, garantindo performance e alta disponibilidade, sem perda de informação, e 1 (um) *appliance* virtual atuando como console de gerenciamento centralizado da solução, com mecanismos de proteção ativos para 1.500 (mil e quinhentas) caixas postais, sendo que o contrato de suporte da solução é válido até 01/12/2024.

7.2. Assim, o quantitativo de bens e serviços foi dimensionado de forma a manter as funcionalidades atuais de operação da solução de segurança, mantendo sua implementação em *appliances* virtuais e ajustando o quantitativo de caixas postais às necessidades do órgão.

8. DA DESCRIÇÃO DA SOLUÇÃO DE TIC

8.1. Essa solução de TIC compreende a renovação dos serviços de subscrição dos mecanismos de proteção, garantia, suporte técnico da solução de segurança de filtragem de conteúdo de e-mail (*antispam*) existente no órgão, pelo período mínimo de 3 (três) anos, contemplando os serviços de instalação, configuração e capacitação, no caso de substituição da solução atual em operação.

8.2. No contexto dessa contratação, entende-se como "renovação da solução de segurança" o pleno funcionamento dos mecanismos de proteção e análise de conteúdo de e-mail, bem

como serviço de suporte vigente fornecido pelo fabricante da solução. Dessa forma, haverá duas possibilidades de fornecimento que atendam às necessidades do órgão:

8.2.1. Atualização do licenciamento e do suporte da solução de segurança em operação, fabricante HSC. Nesse caso, não será necessário serviço de instalação e treinamento oficial, haja vista ser uma solução já em funcionamento e com a equipe técnica do órgão capacitada para operá-la.

8.2.2. Substituição da solução de segurança em operação por nova solução de segurança de filtragem de conteúdo de e-mail de outro fabricante. Nesse caso, a licitante deverá contemplar adicionalmente os serviços de instalação da nova solução e o treinamento oficial do fabricante para a devida capacitação da equipe técnica do órgão

9. LEVANTAMENTO DAS ALTERNATIVAS E ANÁLISE DE MERCADO DE TIC

9.1. As alternativas foram lançadas no Estudo Técnico Preliminar

10. DA JUSTIFICATIVA DA ALTERNATIVA ESCOLHIDA

10.1. A justificativa foi descrita no Estudo Técnico Preliminar

11. DA NATUREZA DO OBJETO

11.1. Os serviços objeto desta contratação podem ser caracterizados como comuns, nos termos do art. 6°, XIII da Lei 14.133/2020, considerando que os padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

11.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

12. DO PARCELAMENTO E ADJUDICAÇÃO DO OBJETO

12.1. Os bens e serviços previstos nessa contratação possuem relação de interdependência, pois compõem uma solução de segurança integrada, com utilização de tecnologia proprietária do fabricante, não sendo possível o parcelamento da contratação.

12.2. Assim, consideramos o objeto da licitação indivisível devendo ser adjudicado a uma única licitante.

13. DA MODALIDADE E TIPO DE LICITAÇÃO – FORMAS E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

13.1. O fornecedor será selecionado por meio da realização de procedimento de **Licitação**, na modalidade **Pregão**, na sua forma eletrônica, por se tratar de bens e serviços comuns, nos termos do art. 28 c/c 29 da Lei 14.133/2021.

13.2. O critério de julgamento da licitação é o **menor preço** para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática, nos termos do inciso XLI do art.6° da Lei 14.133/2021.

13.3. O regime de execução do contrato é por preço global.

13.4. Exigências de **habilitação**:

13.4.1. Para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, as exigências e demais condições são aquelas estabelecidas no edital.

14. DO IMPACTO AMBIENTAL DECORRENTE DA CONTRATAÇÃO E DA SUSTENTABILIDADE

14.1. O conceito de TI verde é definido como um conjunto de práticas que torna mais sustentável e menos prejudicial o uso da tecnologia e está ligado aos processos de fabricação dos componentes, a administração e a utilização dos ativos de TI, bem como o descarte do "lixo eletrônico".

14.2. A partir de tal premissa a SJES vem priorizando a adoção de processos na forma eletrônica, inclusive os administrativos, utilizando softwares aplicativos. Os documentos deverão ser gerados e mantidos em sua forma digital e, com o objetivo de garantir a integridade deles, nestes poderão ser utilizados recursos tecnológicos de segurança da informação. O objetivo da referida adoção é reduzir o número de cópias e impressões em papel, o que também se aplica aos documentos utilizados na gestão e fiscalização dos contratos.

14.3. A abertura de chamados técnicos e encaminhamentos de demandas deverão ser realizados, preferencialmente, sob a forma eletrônica, evitando-se a impressão de papel.

15. DA CONFORMIDADE TÉCNICA E LEGAL

15.1. Os itens fornecidos e a prestação dos serviços, pela contratada, deverão apresentar a qualificação técnica e seguir os ditames legais aplicáveis à contratação, necessários ao fiel cumprimento dos serviços contidos neste Termo de Referência e seus anexos, no Edital do Pregão Eletrônico, na Proposta da contratada aceita, no Contrato Administrativo assinado, bem como nas disposições contidas na Lei nº 14.133/21 e suas alterações posteriores, demais regulamentos e normas administrativas federais.

16. DA QUALIFICAÇÃO TÉCNICA – CRITÉRIOS TÉCNICOS DE SELEÇÃO DO FORNECEDOR

16.1. Como qualificação técnica a Licitante deverá apresentar, juntamente com os documentos de habilitação, pelo menos 01 (um) atestado ou certidão de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove o fornecimento de pelo menos 100 (cem) licenças de solução de segurança de filtragem de conteúdo de e-mail (*antispam*), pelo período mínimo de 12 (doze) meses, devendo conter nome do atestante, endereço e telefone da pessoa jurídica, ou qualquer outra forma que permita à contratante contatar a empresa declarante.

16.1.1. O quantitativo de licenças solicitado poderá ser contabilizado em mais de um atestado ou certidão de capacidade técnica.

16.2. Justifica-se a exigência do atestado ou certidão de capacidade técnica como forma de comprovar a experiência e competência da Licitante para a prestação de um serviço essencial às atividades do órgão, minimizando o risco de eventuais prejuízos à Administração durante a execução contratual.

17. DOS REQUISITOS DA CONTRATAÇÃO

17.1. **CARACTERÍSTICAS GERAIS**

17.1.1. As especificações devem ser consideradas como requisitos mínimos, sendo aceitas especificações idênticas ou superiores.

17.2. **ENDEREÇOS DE INSTALAÇÃO E PRESTAÇÃO DOS SERVIÇOS**

17.2.1. **Sede da Justiça Federal do Espírito Santo (JFES):** Av. Marechal Mascarenhas de Moraes, 1877, Monte Belo, Vitória – ES, CEP: 29.053-245.

17.3. **DA LICENÇA DE *APPLIANCE* VIRTUAL (ITEM 1)**

17.3.1. A contratada deverá fornecer as licenças de *software* de solução de segurança de filtragem de conteúdo de e-mail atendendo aos **requisitos técnicos descritos no anexo "REQUISITOS TÉCNICOS ESPECÍFICOS"** e abrangendo as demais exigências dessa especificação.

17.3.2. Deverá ser fornecido certificado do fabricante da solução de segurança que comprove o registro no seu *site* oficial do quantitativo das licenças e do suporte técnico pelo período mínimo de 3 (três) anos, conforme item 2.7.

17.3.3. Os produtos deverão ser entregues em sua versão mais atual, compatível com a instalação local na infraestrutura da contratante (*on premises*).

17.3.4. A contratada deve apresentar o manual de administração da solução ofertada, no idioma português do Brasil e/ou inglês, caso seja distinta da existente em operação na contratante.

17.4. **DO SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO (ITEM 2)**

17.4.1. Esse serviço somente será prestado caso a solução fornecida seja distinta da existente em operação na contratante.

17.4.2. Os serviços de instalação serão executados preferencialmente via acesso remoto, a ser disponibilizado pela contratante.

17.4.3. A contratada será responsável pela execução de todas as atividades necessárias para substituição da solução atual pela nova fornecida, devendo contemplar:

17.4.3.1. Instalação da solução fornecida no ambiente virtual da contratante.

17.4.3.2. Migração ou adaptação das regras e configurações da solução atual para a nova solução fornecida.

17.4.3.3. Elaboração e execução de procedimentos, scripts, políticas e/ou quaisquer outras aplicações necessárias para o funcionamento pleno da solução fornecida, inclusive eventuais ajustes necessários no ambiente virtual e servidores da contratante, tais como, Exchange, DNS, AD, entre outros.

17.4.3.4. Desativação da solução atual.

17.4.4. Caso seja necessário qualquer tipo de intervenção presencial nos equipamentos onde serão instalados a solução fornecida, caberá à contratada orientar os técnicos da contratante de todos os procedimentos a serem executados.

17.4.5. Os serviços de instalação e configuração devem ser realizados com licença de avaliação e somente após sua conclusão as licenças fornecidas devem ser ativadas, considerando o prazo de vigência estabelecido no item 2.7.

17.4.6. Os serviços de instalação não terão qualquer ônus adicional para a contratante, e a seu critério, poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados, visando minimizar os transtornos aos usuários pela eventual indisponibilidade dos serviços de TI.

17.4.7. Ao final dos serviços de instalação a contratada deverá entregar documentação, compreendendo as seguintes atividades e condições:

17.4.7.1. Deverá ser entregue em meio digital, formato compatível com o MS-Office 2013 e editável pela contratante.

17.4.7.2. Se houver documentos que não possam ser elaborados com o MS-Office, deverá ser fornecido o arquivo digital no formato original.

17.4.7.3. A Contratante poderá solicitar a conversão da documentação para formato PDF.

17.4.7.4. Deverá ser gerada a documentação *as-built*, contemplando todas as características do ambiente da contratante após a implementação da solução de segurança, além de um relatório final contendo todas as atividades realizadas durante o projeto.

17.4.7.5. A documentação deverá contemplar os procedimentos básicos para a operação diária da solução, incluindo as rotinas de manutenção necessárias e os procedimentos a serem adotados em caso de recuperação de desastres.

17.4.8. Ao final dos serviços de instalação a contratada deverá realizar a transferência de conhecimento tecnológico na modalidade *hands-on* para capacitar a equipe técnica da contratante na solução implantada, compreendendo as seguintes atividades e condições:

17.4.8.1. A atividade realizada será *online* na modalidade de ensino à distância e/ou videoconferência.

17.4.8.2. A contratada deverá prover a plataforma para o acesso *online*.

17.4.8.3. A programação das atividades de repasse de conhecimento tecnológico deverá ser estabelecida pela contratada, com a anuência da contratante.

17.4.8.4. Deverá ocorrer em horário de expediente da contratante.

17.4.8.5. Capacitação para até 3 (três) participantes da equipe técnica da contratante.

17.4.8.6. Carga horária mínima de 4 (quatro) horas.

17.4.8.7. Deverá ser realizada em língua portuguesa.

17.4.8.8. Deverá enfatizar e apresentar as características específicas da implantação da solução na contratante

17.4.8.9. O material didático deverá ser entregue a todos os participantes, preferencialmente em meio digital e em língua portuguesa ou, na sua impossibilidade, em língua inglesa.

17.4.8.10. O profissional que irá repassar o conhecimento deverá possuir certificação oficial do desenvolvedor da solução.

17.4.8.11. O conteúdo programático deverá abranger no mínimo os seguintes tópicos:

17.4.8.11.1. Instalação, configuração e utilização da solução de segurança.

17.4.8.11.2. Criação de regras para filtragem de conteúdo das mensagens.

17.4.8.11.3. Gerenciamento da quarentena.

17.4.8.11.4. Configuração do *backup* e mecanismos para recuperação de desastres.

17.4.8.11.5. Análise e criação de relatórios.

17.4.8.11.6. Outros recursos existentes, além dos mencionados nos itens anteriores, que sejam úteis à administração da solução.

17.4.8.12. Ao final da capacitação a contratada deverá emitir certificado e/ou declaração de participação para os alunos que alcançarem no mínimo 75% (setenta e cinco por cento) de presença, contendo no mínimo as seguintes informações:

17.4.8.12.1. Título e/ou descrição da capacitação.

17.4.8.12.2. Período de realização.

17.4.8.12.3. Carga horária.
17.4.8.12.4. Ementa (conteúdo programático).
17.4.8.12.5. Nome do(s) instrutor(es).
17.4.8.12.6. Nome do(s) participante(s).
17.4.8.12.7. Razão social e CNPJ da Contratada.
17.4.8.13. A transferência de conhecimento tecnológico não terá qualquer ônus adicional para a CONTRATANTE.

17.5. **DO TREINAMENTO OFICIAL DO FABRICANTE (ITEM 3)**

17.5.1. Esse serviço somente será prestado caso a solução fornecida seja distinta da existente em operação na contratante.
17.5.2. Deverá ser fornecido o treinamento oficial do fabricante da solução fornecida.
17.5.3. O treinamento deverá ser ministrado por instituição autorizada, na modalidade *online* de ensino a distância - EAD, contemplando conteúdos que abranjam instalação, configuração, operação e administração da solução fornecida.
17.5.3.1. O ambiente de treinamento remoto deve ser fornecido pela contratada, com todos os *softwares*, recursos e materiais didáticos necessários para o adequado aprendizado pelos participantes.
17.5.4. O **conteúdo do treinamento e sua carga horária deverão ser apresentados na proposta** de preço das empresas licitantes.
17.5.5. O treinamento deverá ser ministrado em língua portuguesa, em dias úteis e em horário comercial.
17.5.6. A data do início do treinamento deverá ser agendada junto à contratante com antecedência mínima de 10 (dez) dias.
17.5.6.1. Se o treinamento for distribuído em módulos, cada módulo deverá ser agendado com antecedência mínima de 10 (dez) dias.
17.5.7. O material didático oficial do fabricante da solução ofertada deverá ser entregue a todos os participantes, preferencialmente em meio digital e em língua portuguesa ou, na sua impossibilidade, em língua inglesa.
17.5.8. Eventual alteração no conteúdo do treinamento apresentado pela contratada em sua proposta deverá ser submetida previamente para aprovação do gestor técnico do contrato.
17.5.9. Será exigido o controle de frequência dos participantes e uma cópia deverá ser encaminhada à contratante ao final do treinamento.
17.5.10. Ao final do treinamento, deverá ser emitido certificado e/ou declaração de participação para os alunos que alcançarem no mínimo 75% (setenta e cinco por cento) de presença, contendo no mínimo as seguintes informações:
17.5.10.1.1. Título e/ou descrição da capacitação.
17.5.10.1.2. Período de realização.
17.5.10.1.3. Carga horária.
17.5.10.1.4. Ementa (conteúdo programático).
17.5.10.1.5. Nome do(s) instrutor(es).
17.5.10.1.6. Nome do(s) participante(s).
17.5.10.1.7. Razão social e CNPJ da Instituição

17.6. **DO SUPORTE TÉCNICO**

17.6.1. O suporte técnico e garantia deve contemplar:
17.6.1.1. Disponibilização para a contratante, via Internet, de todas as versões (*upgrades*), atualizações (*releases*) e correções (*updates*), de forma a

manter a solução permanentemente atualizada, bem como, das assinaturas dos mecanismos de proteção.

17.6.1.2. Acesso à documentação dos produtos e à base de conhecimento da do fabricante.

17.6.1.3. Identificação e correção de problemas de *software* ou em sua configuração.

17.6.1.4. Esclarecimento de dúvidas e orientação sobre os produtos, suas funcionalidades e procedimentos de instalação, configuração, manutenção e operação da solução.

17.6.2. Os serviços de suporte à solução deverão compreender, sem limites de incidentes, o atendimento em horário comercial **8x5**.

17.6.3. O suporte técnico deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes aos componentes da solução.

17.6.4. O suporte técnico compreende os procedimentos descritos abaixo, não limitados a eles, bem como a configuração e utilização de qualquer funcionalidade disponível na solução:

17.6.4.1. Alteração de qualquer configuração de topologia que a contratante julgue necessário.

17.6.4.2. Administração e configuração do gerenciamento da solução de segurança.

17.6.4.3. Suporte em caso de indisponibilidade do *cluster* da solução de segurança.

17.6.4.4. Resolução de problemas de comunicação da solução de segurança com outros sistemas de correio eletrônico.

17.6.4.5. Suporte à configuração das funcionalidades e regras disponíveis.

17.6.4.6. Suporte técnico para identificação e resolução de problemas no funcionamento da solução de segurança.

17.6.4.7. Suporte nas atualizações do sistema operacional e assinaturas dos mecanismos de proteção da solução de segurança.

17.6.4.8. Auxílio na customização de relatórios disponíveis na solução de segurança.

17.6.4.9. Realizar otimização de performance (*tunning*) da solução de segurança.

17.6.4.10. Apoio técnico em configurações de alta disponibilidade, redundância e gerência da solução de segurança.

17.6.4.11. Suporte, administração e monitoramento das políticas e tarefas de *backup*.

17.6.4.12. Apoio técnico para tarefas de auditoria e análise de logs.

17.6.5. A contratada deverá disponibilizar acesso a Central de Atendimento para abertura de chamados de resolução de problemas, suporte técnico ou assistência técnica relacionados ao funcionamento apropriado da solução objeto dessa especificação.

17.6.6. A abertura de chamados e o suporte junto à Central de Atendimento deverão ser feitos em português do Brasil, durante todo o prazo de vigência do contrato.

17.6.6.1. Na impossibilidade de atendimento em português do Brasil, a contratante poderá solicitar contratada que realize os procedimentos de abertura e acompanhamento dos chamados, conforme item 17.6.13

17.6.7. Cada chamado técnico, independentemente de sua criticidade e forma de abertura, deverá ser registrado no sistema de informação utilizado pela Central de Atendimento, contendo ao menos as seguintes informações:

17.6.7.1. Número único de identificação.

17.6.7.2. Data e hora da abertura do chamado.

17.6.7.3. Severidade atribuída ao problema.

17.6.7.4. Descrição do problema.

17.6.7.5. Histórico de atendimento e solução.
17.6.7.6. Data e hora do encerramento.

17.6.8. Uma notificação da abertura dos chamados abertos no sistema de gestão de chamados provido pela contratada será encaminhada para endereço eletrônico indicado pela contratante, que fará uso deste sistema para atualizar as informações relacionadas ao atendimento de cada chamado.

17.6.9. Ao abrir um chamado a contratante poderá agendar data e hora para início do atendimento.

17.6.10. As solicitações junto à Central de Atendimento poderão ser realizadas, cumulativamente, das seguintes maneiras:

17.6.10.1. Ligações telefônicas locais pertencentes à área tarifária 27 ou discagem direta gratuita (0800).
17.6.10.2. Website.
17.6.10.3. E-mail.

17.6.11. A contratada deverá informar os meios disponíveis e os procedimentos necessários para abertura de chamados junto à Central de Atendimento própria e/ou do fabricante da solução.

17.6.12. A contratada deverá realizar abertura e escalonamento de chamados junto ao fabricante sempre que necessário.

17.6.13. Caso julgue necessário, a contratante poderá solicitar à contratada que realize os procedimentos de abertura e acompanhamento dos chamados técnicos de suporte à solução junto ao fabricante.

17.6.14. Os serviços de suporte técnico não terão qualquer ônus adicional para a contratante.

17.6.15. O histórico completo dos chamados deverá estar disponível para consulta pela contratante durante a vigência contratual.

17.6.16. Nos casos em que as manutenções necessitarem de interrupção dos serviços, a contratante deverá ser notificada para que se proceda com a aprovação da manutenção ou para que seja agendada nova data mais adequada.

17.6.17. O prazo máximo para atendimento e solução de chamados referentes ao suporte técnico dependerá da severidade do incidente e está definido conforme tabela abaixo.

Prazo para solução de chamados		
Severidade	**Descrição**	**Tempo de Solução**
Alta	Solução de segurança inoperante com falha de todos os componentes.	Até 04 (quatro) horas
Média	Solução de segurança parada em um dos seus componentes, com uma funcionalidade inoperante ou com serviço degradado (desempenho inadequado ou intermitente)	Até 48 (quarenta e oito) horas
Baixa	Solução de segurança funcionando com pequenos problemas sem impacto direto na operação não causando quebra de funcionalidade ou de operação	Até 72 (setenta e duas) horas
Informacional	Esclarecimentos e informações em geral	Até 96 (noventa e seis) horas

17.6.18. Os prazos de atendimento começam a ser contados a partir do horário de abertura do chamado junto à Central de Atendimento da contratada.

17.6.19. Entende-se por tempo de solução o prazo necessário para restabelecimento do serviço em plena condição de funcionamento ou em condição de ser escalonado para um nível menor de severidade, conforme a ordem decrescente (média ou baixa).

17.6.20. O nível de severidade poderá ser definido pela contratante no momento da abertura de cada chamado.

17.6.21. O nível de severidade poderá ser reclassificado a critério da contratante. Caso isso ocorra, haverá o início de nova contagem de prazo, conforme o novo nível de severidade.

17.6.22. Este prazo poderá ser prorrogado desde que a contratante aceite as justificativas apresentadas pela CONTRATADA que revelem a necessidade de dilação de prazo.

17.6.23. Não se encaixam nos prazos de atendimento estabelecidos acima, problemas cuja solução dependa de correção de falhas (*bugs*) ou da liberação de novas versões ou correções de *software* (*patches*).

17.6.23.1. Nesses casos, a contratada deverá restabelecer o ambiente através de uma solução de contorno, considerando os prazos conforme a severidade, e informar à contratante quando a solução definitiva será disponibilizada.

18. DAS CONDIÇÕES E PRAZOS DE ENTREGA

18.1. A contratada terá o prazo máximo estabelecidos abaixo para a entrega do objeto, contados a partir do recebimento da **Ordem de Início de Serviço** emitida pelo gestor do contrato.

18.1.1. Licenças e serviços de instalação e configuração - Itens 1 e 2: o prazo para entrega será até o vencimento da solução de segurança atual da contratante, conforme estabelecido no item 2.6.3, ou seja, **01 de dezembro de 2024**.

18.1.2. Treinamento oficial - Item 3: o prazo para entrega do item será até **15 de dezembro de 2024**.

18.2. Eventual pedido de prorrogação do prazo poderá ser realizado até o terceiro dia útil anterior à data final para a entrega do bem/serviço, devendo ser instruído com os fundamentos e documentos necessários à comprovação do alegado.

18.3. Caso a contratante julgue necessário, poderá solicitar à contratada que informe os procedimentos necessários para acesso direto ao site do fabricante que permitam confirmar o fornecimento realizado.

18.4. Agendamentos de serviços, entrega de equipamentos e outras questões técnicas relativas ao objeto contratado deverão ser direcionados ao Supervisor da Seção de Rede de Computadores (SERED) da JFES, tel: (27) 3183-5045, sered@jfes.jus.br, no horário de 12:00 as 19:00 horas.

18.5. Questões administrativas da contratação, tais como, encaminhamento de documentos fiscais, de termos assinados, entre outras, deverão ser direcionadas à Seção de Projetos, Aquisições e Acompanhamento de Contratos (SEPRAC) da SJES, tel.: (27) 3183-5164, seprac@jfes.jus.br, no horário de 12:00 as 19:00 horas.

19. DO CRONOGRAMA DE EXECUÇÃO

19.1. A execução do objeto resume-se à entrega da comprovação dos serviços de subscrição e suporte e, adicionalmente no caso de substituição da solução existente, da instalação e

treinamento oficial e no prazo e condições definidos nesse Termo de Referência, resumindo as atividades no quadro abaixo.

Atividade	Responsável	Prazo
Emissão da Ordem de Início	Gestor	Até 5 dias da assinatura do contrato
Entrega das licenças e serviços de instalação	Contratada	Até 01/12/2024
Treinamento oficial	Contratada	Até 15/12/2024

19.2. O pagamento ocorrerá de forma integral na entrega do objeto, não sendo prevista a contratação como serviço como serviço continuado e pagamentos periódicos.

20. DAS OBRIGAÇÕES DO CONTRATANTE

20.1. Nomear Gestor e Fiscais Técnico, Administrativo e Demandante do contrato para acompanhar e fiscalizar a execução do contrato.
20.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens.
20.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.
20.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao Órgão gerenciador da Ata de Registro de Preços, quando aplicável.
20.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato e em observância à forma estipulada pela Administração.
20.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.
20.7. Disponibilizar o acesso lógico e físico necessário para a realização dos serviços.
20.8. Efetuar o pagamento em observância à forma estipulada pela Administração.

21. DAS OBRIGAÇÕES DA CONTRATADA

21.1. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato.
21.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.
21.3. 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.
21.4. Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas por lei e nesse Termo de Referência.
21.5. Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do contrato.
21.6. Manter atualizadas as informações fornecidas à contratante, especialmente as referentes ao seu Preposto e aos meios de aberturas de chamados, quando o caso.
21.7. Respeitar as normas e procedimentos de controle interno, inclusive de acesso às dependências e sistemas da contratante.

21.8. Fornecer os itens solicitados dentro dos prazos estipulados e de acordo com as especificações definidas.

21.9. Prover suporte para a resolução de quaisquer problemas ou dúvidas referentes ao fornecimento, através de telefone ou e-mail.

21.11. 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, sempre que considerar a medida necessária.

22. DOS PAPÉIS A SEREM DESEMPENHADOS PELOS PRINCIPAIS ATORES DO ÓRGÃO E DA EMPRESA ENVOLVIDOS NA CONTRATAÇÃO

22.1. Gestor do Contrato: servidor com atribuições gerenciais, preferencialmente da Área Requisitante da solução, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;

22.2. Fiscal Demandante do Contrato: servidor representante da Área Requisitante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos funcionais da solução;

22.3. Fiscal Técnico do Contrato: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos técnicos da solução;

22.4. Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais;

22.5. Preposto: funcionário representante da contratada, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

23. DOS INSTRUMENTOS FORMAIS DE SOLICITAÇÃO DE FORNECIMENTO DOS BENS E/OU PRESTAÇÃO DE SERVIÇOS

23.1. A comunicação poderá ocorrer por e-mail, ofícios ou ordens de serviços.

23.2. A solicitação de serviços de suporte se dará por meio da central de atendimento, conforme estabelecido no item 17.6.10 e subitens.

24. DAS CONDIÇÕES DE RECEBIMENTO PROVISÓRIO E DEFINITIVO

24.1. Os bens e/ou serviços serão recebidos provisoriamente, de forma sumária, no ato da entrega, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

24.2. Após a verificação da qualidade e quantidade e consequente aceitação mediante termo detalhado, o recebimento definitivo ocorrerá, a contar do recebimento provisório, no prazo de:

24.2.1. **10 dias úteis:** para as contratações decorrentes de despesas cujos valores **ultrapassem** o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

24.2.2. **5 dias úteis:** para as 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.

24.3. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

24.4. Os bens e/ou serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

24.5. A cada nova entrega, inicia-se a contagem de novo prazo para recebimento definitivo.

24.6. 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 pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

24.7. O prazo para a solução, pela contratada, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

24.8. 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.

25. DAS CONDIÇÕES DE PAGAMENTO

Da liquidação e do pagamento

25.1. A nota fiscal/fatura deverá ser encaminhada à contratante no seguinte endereço: Av. Marechal Mascarenhas de Moraes, 1877, Monte Belo, Vitória - ES, CEP 29.053-245, à SEPRAC – Seção de Projetos, Aquisições e Acompanhamento de Contratos. Em caso de nota fiscal eletrônica, poderá ser enviada para o e-mail seprac@jfes.jus.br.

25.2. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de **LIQUIDAÇÃO**:

25.2.1. 10 dias úteis: para as contratações decorrentes de despesas cujos valores ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021

25.2.2. 5 dias úteis: para as 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

25.2.3. Os prazos acima poderão ser prorrogados, por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022

25.3. 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:

25.3.1. O nome, endereço e CNPJ da Justiça Federal (Justiça Federal de 1º Grau, Seção Judiciária do ES, Av. Marechal Mascarenhas de Moraes, 1877, Monte Belo, Vitória-ES, CEP: 29.053-245, CNPJ: 05.424.467/0001-82).

25.3.2. O nome, Inscrição Estadual e CNPJ da contratada.

25.3.3. Prazo de validade;

25.3.4. Data de emissão

25.3.5. Dados do contrato;

25.3.6. Período respectivo de execução do contrato;

25.3.7. Valor a pagar;

25.3.8. Eventual destaque do valor de retenções tributárias cabíveis.

25.4. 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

25.5. 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.

25.6. 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.

25.7. 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.

25.8. 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.

25.9. 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.

25.10. 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

25.11. O **PAGAMENTO** será efetuado, a contar da finalização da liquidação da despesa, no prazo de:

25.11.1. 10 dias úteis: para as contratações decorrentes de despesas cujos valores ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021

25.11.2. 5 dias úteis: para as 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

25.11.3. Os prazos acima poderão ser prorrogados, por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022

25.12. 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 IPCA.

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

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

25.15. 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.

25.16. 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.

26. DA FISCALIZAÇÃO E ACOMPANHAMENTO DA EXECUÇÃO CONTRATUAL

26.1. Compete à Fiscalização, entre outras atribuições:

26.1.1. Verificar a conformidade da execução contratual com as normas específicas e se os procedimentos e materiais empregados são adequados para garantir a qualidade desejada dos serviços.

26.1.2. Ordenar à contratada que corrija, refaça ou reconstrua as partes dos serviços executados com erros, imperfeições ou em desacordo com as especificações.

26.1.3. Acompanhar e aprovar os serviços executados.

26.2. A ação da fiscalização não exonera a contratada de suas responsabilidades contratuais e legais.

26.3. A contratada se submeterá a mais ampla e irrestrita fiscalização por parte da contratante, quanto à execução dos serviços prestando todos os esclarecimentos solicitados.

26.4. As irregularidades detectadas pela fiscalização da contratante serão comunicadas por escrito à contratada, para sua pronta correção ou adequação.

27. DA TRANSFERÊNCIA DE CONHECIMENTO

27.1. Conforme itens 17.4.8 e 17.5 do Termo de Referência.

28. DAS PENALIDADES E SANÇÕES ADMINISTRATIVAS

28.1. Para as sanções administrativas serão levadas em conta a legislação federal que rege a matéria concernente às licitações e contratos administrativos e as disciplinas normativas no âmbito da Seção Judiciária do Espirito Santo.

29. DO PRAZO DE VIGÊNCIA CONTRATUAL

29.1. O prazo de vigência da contratação inicia na assinatura do termo contratual até o final da validade das subscrições dos mecanismos de proteção e do suporte, sendo de no mínimo 3 (três) anos contatos a partir de **01 de dezembro de 2024** ou da data de emissão do Termo de Recebimento Definitivo, caso ocorra em data posterior, conforme apresentado no item 2.7.

30. DA GARANTIA CONTRATUAL

30.1. Para segurança da contratante, quanto ao cumprimento das obrigações contratuais, a contratada deverá apresentar garantia contratual, no percentual de **5% (cinco por cento)** do valor global do contrato, mediante a opção por uma das modalidades previstas no § 1º do art. 96 da Lei n°14.133/2021.

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

31. DAS CONDIÇÕES PARA A ASSINATURA DO CONTRATO

31.1. A contratada deverá indicar funcionário de seu quadro para atuar como preposto junto à contratante, fornecendo o nome completo, números de telefones, e-mail e endereço para correspondência.

31.2. A contratada deverá assinar os termos de sigilo conforme item 34.

31.3. A contratada deverá informar no momento da assinatura do contrato os contatos da central de atendimento para abertura de chamado para atendimento, conforme descrito nessa especificação.

31.4. A contratada deverá apresentar assinada declaração de cumprimento da Lei Geral de Proteção de Dados Pessoais - Lei n.13.709/2018, conforme anexo "MODELO DE DECLARAÇÃO DE CUMPRIMENTO DA LGPD".

31.1. A Contratada deverá comprovar que é assistência técnica autorizada ou parceiro autorizado do fabricante da solução e está apta a comercializar seus produtos e serviços, sendo que a comprovação se dará por meio de consulta ao site oficial do fabricante, a ser informado pela empresa; ou por meio de documento assinado por representante do fabricante da solução, cuja aceitação ficará condicionada à validação pela área técnica.

32. DAS ESTIMATIVAS DE PREÇOS DA CONTRATAÇÃO

32.1. A estimativa de preços, conforme as normas vigentes do Órgão, é elaborada por área específica e apresentada em documento próprio anexo ao Edital da licitação.

33. DA ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

33.1. A execução financeira se dará integralmente com a entrega de cada item objeto da contratação, conforme descrito nesse Termo de Referência, não havendo necessidade de cronograma ou maiores detalhamentos da execução física.

33.2. Essa contratação terá o programa "SEG0" como fonte de recursos.

34. DA CONFIDENCIALIDADE E SIGILO DAS INFORMAÇÕES

34.1. A contratada deverá assinar o Termo de Compromisso, bem como preencher e assinar o Termo de Ciência, conforme modelos anexos.

35. APROVAÇÃO E ASSINATURA

A Equipe de Planejamento foi instituída pelo despacho JFES-DES-2024/08697.

Seguem as assinaturas dos integrantes da equipe de planejamento, bem como a aprovação da autoridade máxima da área de TIC, em atenção às orientações do Guia de Contratações de TIC do Poder Judiciário do Conselho Nacional de Justiça – CNJ.

Equipe de Planejamento da Contratação		
Integrante Requisitante	**Integrante Técnico**	**Integrante Administrativo**
Rodrigo Queiroga Barros Supervisor da SERED[1] Matrícula: 10726	**Rodrigo Queiroga Barros** Supervisor da SERED[1] Matrícula: 10726	**Lourenia Moreira Rocha** Supervisora da SEPRAC[2] Matrícula: 10525

Aprovado,

Autoridade Máxima da Área de TIC / Autoridade Competente
Fabrício Vasconcelos Costa Diretor da Divisão de Tecnologia da Informação Matrícula: 10365

[1] Seção de Rede de Computadores
[2] Seção de Projetos, Aquisições e Acompanhamento de Contratos

Item	Descrição Geral	Unid.	Qtd.	Valor Unit.	Valor Total
1	Licença de a*ppliance* virtual de solução de filtragem de conteúdo de e-mail, com subscrição dos mecanismos de proteção, garantia e suporte pelo período de, no mínimo, 3 (três) anos. CATSER: 27502	Licença	1100		
2[3]	Serviço de instalação e configuração. CATSER: 26972	Unidade	1		
3[4]	Treinamento oficial do fabricante CATSER: 3840	Unidade	3		
Valor Total					

Detalhamento dos itens da proposta				
Fabricante/Marca da solução: *<nome do fabricante/marca>*				
Item	**Part-Number[5]**	**Descrição detalhada do fabricante**	**Quant.**	**Valor Unit.**
1	*<part number 1.1>*	*<descrição part number 1.1>*		
	…	…		
	<part number 1.n>	*<descrição part number 1.n>*		
3	*<part number 3.1>*	*<descrição part number 3.1>*		
	…	…		
	<part number 3.x>	*<descrição part number 3.x>*		

Nota: o Item 2 não necessita de detalhamento, pois corresponde a atividade específica a ser executada pela contratada.

[3] Esse item só precisa ser entregue e ter cotação caso a solução ofertada seja diferente da solução atual em operação na contratante, *MailInspector Enterprise Virtual* da empresa *HSC - High Security Center*. Caso contrário, será zero.
[4] Idem nota de rodapé 3
[5] Onde couber, devem ser discriminados detalhadamente todos os part numbers que compõe o item da solução, com suas respectivas descrições, quantidades e cotações unitárias.

TERMO DE COMPROMISSO

Ref. Contrato [ ]

JUSTIÇA FEDERAL DE PRIMEIRO GRAU NO ESPIRITO SANTO, sediada à av. Marechal Mascarenhas de Moraes 1877, Bairro Monte Belo, Vitória-ES, CEP: 29053-245, CNPJ n.º 05.424.467/0001-82 doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.° <CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N. º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto n. 7.845/2012- Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pelo CONTRATANTE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômicos, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

DE ACORDO	
CONTRATANTE	**CONTRATADA**
_____ Justiça Federal de 1º Grau – SJES Juiz Federal Diretor do Foro Dr.	_____ XXXXX Representante legal
Testemunha 1	**Testemunha 2**
_____	_____

PODER JUDICIÁRIO
JUSTIÇA FEDERAL DA 2ª REGIÃO

ANEXO IV – MODELO DE TERMO DE CIÊNCIA

TERMO DE CIÊNCIA

Nº PROCESSO:	**JFES-EOF-**	**Nº CONTRATO:**	

1 – IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Gestor do Contrato:		**Matr.**	
Contratante:	Justiça Federal de Primeiro Grau – SJES		
Contratada:		**CNPJ:**	
Preposto da Contratada:		**CPF:**	

Por este instrumento, os funcionários abaixo-assinados declaram, sob as penas da lei, terem ciência e conhecerem o Termo de Compromisso de Manutenção de Sigilo (TCMS) emitido por ocasião da assinatura do Contrato XX/20XX, e se comprometem a seguir, naquilo que lhe couber, todas as disposições do referido Termo.

Vitória, ES, XX de XXXXXXXX de 20XX

CIÊNCIA			
CONTRATADA			
Funcionários			
Nome	Identidade	CPF	Assinatura

DECLARAÇÃO DE CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LEI N. 13.709/2018

1. É vedada às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

2. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassadas em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento contratual.

3. As partes responderão administrativa e judicialmente, caso causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância à LGPD.

4. Em atendimento ao disposto na Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), a CONTRATANTE, para a execução do serviço objeto deste edital, terá acesso aos dados pessoais dos/as representantes da LICITANTE/CONTRATADA, tais como: número do CPF e do RG, endereços eletrônico e residencial e cópia do documento de identificação.

5. A LICITANTE/CONTRATADA declara que tem ciência da existência da Lei Geral de Proteção de Dados Pessoais (LGPD) e, se compromete a adequar todos os procedimentos internos ao disposto na legislação, com intuito de proteção dos dados pessoais repassados pela CONTRATANTE.

6. A LICITANTE/CONTRATADA fica obrigada a comunicar à CONTRATANTE, em até 24 (vinte e quatro) horas, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que possa vir causar risco ou dano relevante aos Titulares de Dados Pessoais, apresentando as informações descritas nos incisos do § 1º do art. 48 da LGPD, cabendo à CONTRATANTE as demais obrigações de comunicação previstas no referido artigo.

Vitória/ES, _____ de _____ de 20____

CONTRATADA	
_____ *<Nome>* *<Qualificação>*	
Testemunha 1	**Testemunha 2**
_____ *<Nome>* *<Qualificação>*	_____ *<Nome>* *<Qualificação>*

1. ASPECTOS GERAIS DA SOLUÇÃO

1.1. A solução deve ser entre em *appliance* virtual compatível com o ambiente VMWare ESXi 7 e superiores, e Open Shift na versão mais atual disponível quando da entrega da proposta.
1.2. Deve permitir a expansão da solução a qualquer tempo, sem cobrança adicional de licença ou limitação de *appliance* virtual.
1.3. A solução *anti-spam* deve possuir controle de caixas postais e fluxo de análise de mensagens/dia ilimitadas, de acordo com os recursos de *hardware* disponíveis.
1.4. Deve ser uma solução MTA (*Mail Transfer Agent*) completa com suporte ao protocolo SMTP, que controla o envio e o recebimento de todas as mensagens da empresa, com registro de logs das atividades do MTA.
1.5. A licença de uso deve atingir um número de no mínimo 1.100 (mil e cem) caixas postais.
1.6. O sistema operacional deve ser para uso próprio em sistema de proteção e-mail, não sendo aceito sistema onde simplesmente é instalado um programa de filtragem de e-mail rodando sobre sistema operacional "genérico" ou de distribuição livre.
1.7. O sistema operacional deverá ser do próprio fabricante e específico para a solução de filtragem de e-mail.
1.8. Deve ser capaz de filtrar o tráfego de correio, bloqueando a entrada de vírus, *spyware*, *worms*, *trojans*, *spam*, *phishing*, e-mail *marketing*, e-mail adulto ou outras formas de ameaças virtuais.
1.9. A solução deve suportar o processamento de no mínimo 20.000 (vinte mil) conexões simultâneas e 150.000 (cento e cinquenta mil) mensagens por hora.
1.10. A licença de uso do *software* deve possuir 3 (três) anos de atualização do fabricante compreendendo os seguintes módulos:
    1.10.1. Atualização das assinaturas de segurança disponibilizadas automaticamente, por exemplo: assinaturas de vírus, malwares e outras ameaças, serviços de reputação de websites, IPs e assinaturas de websites e aplicativos web.
    1.10.2. Direito de uso da versão mais atual do produto licenciado caso esta esteja disponível pelo fabricante, bem como atualizações de recursos e melhorias dentro da mesma versão.
    1.10.3. Acesso a base de inteligência global do fabricante para análise online de ameaças.
1.11. Analisar mensagens, no mínimo, por meio dos seguintes métodos:
    1.11.1. Proteção dinâmica por reputação.
    1.11.2. Assinaturas de spam.
    1.11.3. Filtros de vírus.
    1.11.4. Filtros de anexos.
    1.11.5. Filtros de phishing.
    1.11.6. Análise heurística.
    1.11.7. Análise do cabeçalho, corpo e anexo das mensagens.
    1.11.8. E-mail bounce.
    1.11.9. Dicionários pré-definidos e customizados com palavras e expressões regulares.
1.12. Deve possuir mecanismo de backup e recuperação da configuração da solução.
1.13. Deve possuir capacidade de envio de backup via FTP ou SFTP, sendo configurado diretamente na interface gráfica da solução, sem necessidade de qualquer configuração em linha de comando.
1.14. Os manuais de instalação e administração da solução devem ser disponibilizados no idioma português do Brasil ou inglês.
1.15. Deve possuir banco de dados para armazenamento dos registros de acesso, logs de sistema e configurações.

1.15.1. Caso a solução necessite de banco de dados específico e proprietário, as licenças deste deverão ser fornecidas pela CONTRATADA junto com a solução ofertada sem ônus para a CONTRATANTE.

1.15.2. Não serão aceitas soluções baseadas em armazenamento de logs em formato texto.

1.16. Deve possuir capacidade de configuração de roteamento de mensagens para múltiplos domínios de destino.

1.17. Deve permitir a configuração de múltiplos domínios, com aplicação de regras de forma independente para cada um dos domínios.

1.18. Ter a capacidade de processar o tráfego de entrada e de saída de mensagens no mesmo equipamento, com base no IP e domínio de origem da mensagem, permitindo criar filtros e ações diferenciadas para cada sentido.

1.19. A solução deve ser capaz de efetuar a saída de e-mails indicando um IP específico para a saída de mensagens, isto é, possuir a capacidade de redirecionar as mensagens de saída por IP's diferentes para cada domínio cadastrado no sistema se o administrador assim desejar.

1.20. A solução deve permitir criação de regras por:

1.20.1. Grupos de usuários.

1.20.2. Domínios.

1.20.3. Range de IP.

1.20.4. IP/Rede.

1.20.5. Remetentes específicos.

1.20.6. Destinatários específicos.

1.20.7. Grupos de LDAP.

1.21. Tratar e analisar mensagens originadas e recebidas possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sentido de tráfego.

1.22. Deve possuir ferramenta de auditoria de e-mail, com facilidade de pesquisa por origem, destino, assunto e conteúdo da mensagem permitindo a concatenação dos filtros através dos operadores lógicos "e" e "ou".

1.23. Suporte à assinatura e validação de autenticidade de mensagens através de Domains Keys, DKIM e SPF.

1.24. Permitir efetuar controle profundo dos anexos das mensagens, podendo tomar ações diferenciadas para:

1.24.1. Conteúdo do anexo.

1.24.2. Mime-Type do anexo.

1.24.3. Extensão do anexo.

1.24.4. Nome completo do anexo.

1.24.5. Nome parcial do anexo.

1.24.6. Expressão regular.

1.24.7. Tamanho do anexo.

1.24.8. Anexos compactados com senha.

1.24.9. Quantidade de níveis de compactação no mesmo anexo.

1.25. Deve possuir um sistema de disaster/recover ao qual é efetuado o upload de um arquivo de backup e restauração do mesmo automaticamente.

1.26. Deve possuir sistema de diagnóstico via interface web, com no mínimo a execução dos seguintes testes:

1.26.1. Teste de conectividade ICMP, informando o host a ser testado.

1.26.2. Teste de DNS, informando o host ou o domínio a serem testados.

1.26.3. Teste de envio de e-mail.

1.26.4. Teste de TRACEROUTE.

1.26.5. Teste de DNS reverso.
1.26.6. Teste de SPF, para checar se tem registro para um determinado domínio.
1.26.7. Teste de DKIM, para checar se tem registro para um domínio.
1.26.8. Teste de DMARC, para checar se tem registro para um domínio.
1.26.9. Teste de portas de saída utilizadas pelo sistema.

1.27. Deve ter a capacidade de controle sobre os serviços executados no sistema, com a ação de: parar, inicializar ou reinicializar. O controle dos serviços devem ser sobre no mínimo os seguintes itens:
1.27.1. Serviço de antivírus.
1.27.2. Serviço de MTA.
1.27.3. Serviço de Banco de Dados.
1.27.4. Serviço de SMNP.

1.28. Para maior segurança e conformidade, deve possuir controle de acesso a solução, restringido a liberação do seu uso, associando o perfil de acesso com IP e/ou rede liberada.

1.29. Deve possuir analisador de relatórios DMARC integrado, com no mínimo as seguintes funcionalidades e/ou características:
1.29.1. Importação de relatórios em formato XML.
1.29.2. Apresentação dos principais indicadores de desempenho:
1.29.2.1. Pass rate.
1.29.2.2. Fail rate.
1.29.2.3. Quarantine rate.
1.29.2.4. Discard rate.
1.29.3. Análise granular dos resultados para cada domínio, incluindo:
1.29.3.1. Gráficos de tendências (pass rate ao longo do tempo).
1.29.3.2. Tabela com os principais alinhamentos e desalinhamentos.
1.29.3.3. Identificação de padrões e anomalias.
1.29.4. Filtragem dos resultados por data, domínio, tipo de falha (SPF, DKIM, DMARC).
1.29.5. Configuração de alertas para eventos como:
1.29.5.1. Diminuição significativa do pass rate.
1.29.5.2. Aumento do volume de e-mails falsificados.
1.29.5.3. Novas fontes de e-mails não autorizados.
1.29.6. Notificações por e-mail.
1.29.7. Geração de relatórios em formato PDF ou CSV.

2. ALTA DISPONIBILIDADE

2.1. Suportar cluster de alta disponibilidade na forma de cluster ativo-ativo ou load balance através do registro MX e/ou sistemas de balanceamento proprietário, assegurando as funções de filtragem e que o serviço de recebimento, processamento e entrega das mensagens não pare por falha na solução.

2.2. O sistema deve permitir o gerenciamento de múltiplos clusters da solução em um único ambiente, sem necessidade de abertura de novas telas e/ou instalação de novos softwares ou recursos para tal finalidade.

2.3. Administração centralizada de múltiplos nós de filtragem em uma única interface web, independente se estiver em modo cluster ativo-ativo ou load balance de forma que o gerenciamento e a replicação de políticas do cluster também seja feita de forma centralizada.

2.4. A administração de todo cluster deve ser feita através de um único IP de destino, não sendo

permitido a gestão de regras de forma descentralizada.

2.5. Possuir capacidade de replicação automática das configurações e balanceamento de carga através um único IP virtual.

2.6. O cluster funcionando no modo ativo-ativo, quando ocorrer a queda de um dos equipamentos, a solução deve garantir a idoneidade das informações sem perda.

2.7. A inclusão de novos nodes no cluster deve ser efetuada através da interface gráfica de gerenciamento (GUI), sem necessidade de utilização de linhas de comando.

3. GERENCIAMENTO

3.1. A interface de gerenciamento do sistema deve ter suporte ao idioma português do Brasil ou inglês.

3.2. A console de gerenciamento deve acessada através de protocolo seguro (HTTPS – HyperText Transfer Protocol Secure) com no mínimo as seguintes funcionalidades:

3.3. Administração centralizada de todas as regras e filtros integrantes da solução.

3.4. Status da versão das assinaturas do antivírus em uso.

3.5. Controle de acesso de usuários, com diferentes privilégios de configuração.

3.6. Criação de relatórios, gráficos e estatísticas, com suporte a múltiplos domínios.

3.7. Gerência das áreas de quarentena pelo administrador e possibilidade do usuário gerenciar sua área de quarentena.

3.8. Deve possuir administração via console, através de SSH para CLI (command line interface), para execução de comandos de administração e suporte.

3.9. Deve ser capaz de utilizar os protocolos de transferência de arquivos SCP e FTP.

3.10. O acesso à interface de administração deve possuir diferentes níveis de permissionamento, de forma granular, permitindo que sejam configurados perfis diferentes, por endereços de e-mail e domínio permitidos.

3.11. O sistema deve possuir ainda, no mínimo, os perfis pré-definidos:

3.11.1. Administrador: Com acesso total às configurações da solução.

3.11.2. Administrador: Com acesso total às configurações da solução sem acesso à leitura dos e-mails armazenados tanto na quarentena como mensagens auditadas.

3.11.3. Auditor: Com acesso a visualização dos e-mails armazenados para auditoria.

3.11.4. Operador: Com acesso à administração da quarentena e gerenciamento da “Black e White List”.

3.11.5. Usuário: Possui a capacidade de administrar sua “Black e White List”, individualmente, bem como sua área de quarentena individual.

3.12. Permitir a criação de grupos, para posterior aplicação de regras. Os grupos poderão ser criados através das seguintes métricas:

35.1.1. E-mails.

35.1.2. Domínios.

35.1.3. IP’s.

35.1.4. Range de IP.

35.1.5. Expressão Regular.

35.1.6. Usuários.

35.1.7. Listas de distribuição.

35.1.8. Grupos de LDAP.

4. ALERTAS E LOGS

4.1. Deve enviar notificações por e-mail ao administrador, caso as atualizações não tenham sido realizadas com sucesso.

4.2. A solução deve ser capaz de gerar notificações a remetente e/ou destinatário com mensagem de alerta customizável.
4.3. Possuir registro de log das ações executadas na interface de administração para fins de auditoria. Esse log deve ser de fácil acesso, não sendo necessário acionamento da fabricante da solução.
4.4. Possuir mecanismo de alerta por e-mail quando houver nova atualização do sistema e sobre o status do processo de atualizações.
4.5. Deve possuir capacidade de envio dos logs de um nó específico ou de todo o cluster para um servidor de syslog ou de SIEM. Também deve ser possível selecionar os logs a serem enviados, no mínimo, para as opções abaixo:
    4.5.1. Critical.
    4.5.2. Warning.
    4.5.3. Informational.
    4.5.4. Debug.
4.6. Deve ser possível enviar alertas por e-mail e pelo protocolo SNMP caso ocorra consumo excessivo de algum recurso do sistema. Os sistemas monitorados para envio dos alertas devem ser, no mínimo:
    4.6.1. Espeço em disco.
    4.6.2. Filas de e-mail.
    4.6.3. Memória.
    4.6.4. Processador.
    4.6.5. Serviço de filtragem.
    4.6.6. Atualização da solução de segurança.
    4.6.7. Antivírus e *anti-spam*.
4.7. Deve ter a capacidade de envio de estatísticas de performance para detecção e prevenção de excesso de consumo de disco, processamento e memória, prevenindo dessa forma interrupções e falhas por falta de recursos.

5. QUARENTENA

5.1. Permitir ao administrador da solução executar pesquisa nas áreas de quarentena de todos os usuários através de interface web segura (HTTPS), acessando o próprio sistema de gerenciamento.
5.2. Deve possibilitar a gestão de quarentena pelos administrados de forma que o mesmo possa visualizar a razão de um determinado bloqueio, remetente, destinatário, data, assunto, IP do host destinatário, a mensagem original, tamanho da mensagem original e permitindo no mínimo as ações liberar e/ou excluir.
5.3. Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais regra foram ativadas.
5.4. A interface deve permitir identificar quais regras do módulo de anti-spam foram ativadas a fim de permitir ao administrador a elaboração de regras granulares, sem necessidade de efetuar busca de histórico em logs.
5.5. A solução deve suportar a criação de áreas de quarentena personalizadas para usuários específicos.
5.6. Deve permitir que o tempo de armazenamento da quarentena seja individual por cada área de quarentena.
5.7. Deve permitir a visualização do resumo de todas as áreas de quarentena e volume de mensagens.
5.8. O sistema de quarentena de e-mails deve criptografar automaticamente as mensagens armazenadas, evitando o acesso não autorizado aos arquivos e ao conteúdo dos e-mails

armazenados em quarentena, assim aumentando a confiabilidade e segurança da solução.

5.9. Possibilitar ao administrador selecionar o período de expiração das mensagens na quarentena, por exemplo: manter as mensagens das últimas 72 horas, dessa forma ao ultrapassar esse limite, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos.

5.10. O tempo de armazenamento da quarentena deve ser individual por área de quarentena, devendo também permitir armazenamento por tempo "indeterminado".

5.11. Possibilitar ao administrador selecionar o rotacionamento das mensagens em quarentena por tamanho da quarentena, por exemplo limitar uma quarentena a 100GB, sendo que ao ultrapassar o limite deste tamanho, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos.

5.12. O administrador ao criar uma quarentena customizada, deverá ter a capacidade de selecionar quais usuários poderão ter acesso a ela.

5.13. Pelo sigilo da informação, permitir que seja selecionada quais quarentenas customizadas somente sejam acessíveis a determinados administradores, permitindo a granularidade de acesso destas quarentenas.

6. NOTIFICAÇÕES DE QUARENTENA INDIVIDUAL DO USUÁRIO

6.1. A solução deverá permitir ao administrador agendar o envio do resumo das mensagens na quarentena individual do usuário (digest) em períodos de tempo pré-configuráveis por horário e dia, possibilitando ações do usuário diretamente através dos comandos definidos neste digest, dispensando a instalação de agentes e acesso a quarentena individual do usuário.

6.2. Grupos diferentes de usuários devem poder receber a notificação em horários diferentes.

6.3. O digest deve ser enviado em português do Brasil, mas com a possibilidade de customização do texto, para todos os usuários ou para um determinado grupo de usuários.

6.4. Deve ser possível a customização do digest com as seguintes características alteráveis:

- 6.4.1. E-mail de origem.
- 6.4.2. Título/Assunto do e-mail.
- 6.4.3. Mensagem do *digest*, com possibilidade de inclusão de imagens e links, bem como mudança de fonte, alinhamento e cor.
- 6.4.4. Logomarca do *digest*.

6.5. O digest deve permitir ao usuário final tomar no mínimo as ações de:

- 6.5.1. Liberar uma mensagem bloqueada.
- 6.5.2. Bloquear o remetente da mensagem (*blacklist*), para que as futuras mensagens do mesmo já sejam barradas.
- 6.5.3. Marcar o remetente como confiável (*whitelist*), para que as futuras mensagens do mesmo não sejam pontuadas como spam.
- 6.5.4. Reportar o bloqueio indevido.
- 6.5.5. Solicitar envio de novo resumo.
- 6.5.6. Acessar sua área de quarentena.

6.6. Deve permitir que o administrador escolha qual quarentena a ser incluída no digest do usuário final, por exemplo incluir no digest os e-mails quarentenados que foram considerados conteúdos maliciosos (vírus).

6.7. A solução deverá permitir ao administrador selecionar quais ações serão liberadas para o usuário final selecionar, no mínimo:

- 6.7.1. Liberar e-mail.
- 6.7.2. Reportar Falso Positivo.

6.7.3. Incluir o remetente do e-mail em *blacklist* individual (do próprio usuário).
6.7.4. Incluir o remetente do e-mail em *whitelist* individual (do próprio usuário).
6.7.5. Visualizar o e-mail.

7. FUNCIONALIDADES PARA O USUÁRIO FINAL

7.1. Possuir interface web de administração segura HTTPS para que cada usuário final possa administrar suas opções pessoais e sua quarentena, sem que estas opções interfiram na filtragem dos demais usuários.
7.2. A interface de quarentena do usuário deve estar no idioma português do Brasil.
7.3. O usuário final deve ser capaz de incluir e remover endereços em sua lista pessoal de bloqueio ou de liberação de e-mails.
7.4. O usuário final deve ser capaz de visualizar as mensagens bloqueadas e liberá-las, a seu critério, desde que as mesmas sejam consideradas somente como “possível spam” ou “spam”.
7.5. O usuário final deve ser capaz de solicitar liberação de uma mensagem ao administrador, caso a mensagem contenha conteúdo considerado malicioso ou bloqueado por outro critério qualquer, o qual não permita que o usuário final a libere.

8. USUÁRIOS E GRUPOS

8.1. Possuir integração com serviço de diretórios LDAP e Microsoft Active Directory para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas, bem como impedir ataques de dicionário (Directory Harvest Attack).
8.2. Permitir criação de conectores para múltiplos serviços de diretório, por exemplo conector para servidor LDAP e outro conector para Microsoft Active Directory.
8.3. Possuir a funcionalidade de filtrar individualmente, baseado em políticas definidas por domínio, subdomínio, grupo de usuários e usuário individual, de forma integrada com ferramentas de LDAP, mesmo que a mensagem seja destinada a múltiplos destinatários, em categorias distintas.
8.4. Permitir a utilização de mais de um servidor de LDAP ou Microsoft Active Directory ao mesmo tempo. Caso ocorra indisponibilidade do servidor primário a autenticação dos usuários deverá ocorrer normalmente no outro servidor configurado.
8.5. Integração nativa com o Microsoft Exchange 2010 e superiores.
8.6. Possibilitar a customização de regras e políticas por usuários ou grupos.
8.7. A solução deverá permitir a configuração do intervalo de sincronismo com o serviço de diretório.
8.8. Permitir atrelar grupos a regras específicas de rotas, por exemplo: não aplicar determinada regra do módulo de antivírus para os e-mails que vierem de um determinado domínio, sendo que esta regra somente será aplicada a um grupo específico de usuários.

9. RELATÓRIOS

9.1. Deve permitir a geração de relatórios de todos os nodes do cluster de forma centralizada através de uma única interface web no console de gerenciamento.
9.2. Deve ser capaz de gerar relatórios gráficos e agendar o envio dos mesmos a usuários específicos via e-mail.
9.3. Deve ser capaz de gerar relatórios por data ou por um intervalo de tempo específico.
9.4. Deve ser possível configurar um período para a retenção dos dados utilizados para geração dos relatórios.

9.5. Capacidade de criar relatórios contendo no mínimo as seguintes informações:
- 9.5.1. Sumário de mensagens.
- 9.5.2. Quantidade de mensagens processadas.
- 9.5.3. Relatório de Volume de Mensagens por Data.
- 9.5.4. Principais origens de *spam* por domínio, endereço de e-mail.
- 9.5.5. Principais destinos de *spam* por domínio, endereço de e-mail.
- 9.5.6. Principais origens de vírus.
- 9.5.7. Principais fontes de ataque.
- 9.5.8. Relatório de *top* e-mail *relays*.
- 9.5.9. Relatório de *top* remetentes por quantidade.
- 9.5.10. Relatório de *top* remetentes por volume.
- 9.5.11. Relatório de *top* destinatário por quantidade.
- 9.5.12. Relatório de *top* destinatário por volume.
- 9.5.13. Estatísticas da quarentena.
- 9.5.14. Conexões completadas X bloqueadas.
- 9.5.15. Relatório de tráfego.
- 9.5.16. Principais destinatários de *spam*.
- 9.5.17. Principais destinatários de e-mail.
- 9.5.18. Top Ataques por fraude de e-mail / tentativa de *spoof*.

9.6. Permitir filtros de relatórios com definição de origem e destinos específico.

9.7. Possuir relatórios estatísticos de conexões, ameaças, quarentena e spam.

9.8. Deve apresentar estatísticas e monitoramento em tempo real (online) de e-mails com base em gráficos.

9.9. Os relatórios, no mínimo, devem poder ser filtrados por:
- 9.9.1. Período de tempo.
- 9.9.2. Ponto de filtragem que o e-mail passou.
- 9.9.3. De (remetente).
- 9.9.4. Para (destinatário).
- 9.9.5. Qual a classificação que a mensagem atingiu, dentre eles no mínimo:
  - 9.9.5.1. Provável spam.
  - 9.9.5.2. Spam.
  - 9.9.5.3. Vírus.
  - 9.9.5.4. Conteúdo bloqueado.
  - 9.9.5.5. Whitelist.
  - 9.9.5.6. Blacklist.
  - 9.9.5.7. Tamanho excedido.
  - 9.9.5.8. Phishing.
- 9.9.6. Relatório para um único usuário ou domínio.

10. RASTREAMENTO DAS MENSAGENS

10.1. Permitir o rastreamento de mensagens, independente de qual equipamento do cluster processou, de forma centralizada e por meio da interface de gerenciamento web, não sendo aceita pesquisa exclusivamente via linha de comando.

10.2. O rastreamento deve ser possível através de qualquer um dos seguintes campos:
- 10.2.1. ID da mensagem.
- 10.2.2. E-mail do remente.
- 10.2.3. E-mail do destinatário.
- 10.2.4. Domínio do remetente.

10.2.5. Domínio do destinatário.
10.2.6. Assunto da mensagem.
10.2.7. Nome do anexo.
10.2.8. Palavra contida no conteúdo do corpo da mensagem.
10.2.9. IP de origem da mensagem.
10.2.10. Tamanho da mensagem.
10.2.11. Regra de *spam*.
10.2.12. Se a mensagem foi entregue ou não.
10.2.13. Regras personalizadas aplicadas na mensagem.
10.2.14. Nome da ameaça encontrada.

10.3. A console deve apresentar ainda as seguintes características de rastreamento de mensagens:
10.3.1. Rastreamento completo de mensagens aceitas, retidas e rejeitadas, desde o recebimento da mensagem pelo IP cliente até a entrega para o IP destino, usando como 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”.
10.3.2. 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.
10.3.3. Deve apresentar como resultado as seguintes informações:
10.3.3.1. Remetente da mensagem.
10.3.3.2. Destinatários da mensagem.
10.3.3.3. Servidor de origem.
10.3.3.4. Se foi armazenada em quarentena.
10.3.3.5. Se continha vírus.
10.3.3.6. A regra que atuou.
10.3.3.7. O servidor de origem.
10.3.3.8. O tamanho da mensagem.
10.3.3.9. Se foi entregue ou não.
10.3.3.10. Qual ponto de filtragem utilizado (por qual equipamento processou a mensagem).
10.3.4. No caso de a mensagem ter sido entregue, deve ser possível a apresentação do log de entrega da mesma e para qual IP entregue.
10.3.5. Se o e-mail tiver sido bloqueado por ser considerado spam ou possível spam, o log deve apresentar os filtros aplicados, bem como os critérios utilizados por cada filtro (pontuação).
10.3.6. 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 ou saída), 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.
10.3.7. Rastrear e-mails a partir de uma determinada ameaça.
10.3.8. Apresentar na interface gráfica as fontes de ataque e, através delas, apresentar quais e-mails foram recebidos, originários dessa fonte de ataque.

11. PROTEÇÃO CONTRA ATAQUES DIRECIONADOS

11.1. A solução deve ser capaz de bloquear ataques de negação de serviço (Denial of Service).
11.2. 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.

11.3. A solução deverá possuir a capacidade de executar as seguintes ações:
- 11.3.1. Limitar o número de conexões TCP permitidas através de um valor configurável.
- 11.3.2. Rejeitar a conexão SMTP que se caracterize como flooding.
- 11.3.3. Deve ser capaz de efetuar a filtragem do trafego de correio eletrônico bloqueando a entrada e saída de:
  - 11.3.3.1. Vírus.
  - 11.3.3.2. Spyware.
  - 11.3.3.3. Worms.
  - 11.3.3.4. Trojans.
  - 11.3.3.5. Spam.
  - 11.3.3.6. Phishing.
  - 11.3.3.7. E-mail Marketing, ou qualquer outra forma de ameaça virtual.

11.4. Deve possuir controle total da comunicação permitindo restringir:
- 11.4.1. IP reverso mal configurado.
- 11.4.2. Domínios inexistentes.
- 11.4.3. Permitir identificar e bloquear e-mails vindos de domínios recentemente cadastrados.

11.5. Deve permitir ao administrador criar filtros e assinaturas, bem como realizar sua atualização automática, em frequência de consulta configurável.

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

11.7. Permitir configurar ações diferenciadas sobre as mensagens suspeitas, incluindo:
- 11.7.1. Aceitar.
- 11.7.2. Colocar em quarentena.
- 11.7.3. Inserir tag personalizada no assunto.
- 11.7.4. Marcar o cabeçalho.

11.8. A solução deve ser capaz de tomar as seguintes ações sobre as mensagens:
- 11.8.1. Alterar o assunto da mensagem.
- 11.8.2. Adicionar cabeçalhos para rastreamento.
- 11.8.3. Descartar a mensagem.
- 11.8.4. Colocar em uma determinada área de quarentena definida pelo administrador.

11.9. Deve permitir a criação de regras baseadas no idioma que as mensagens foram escritas, com capacidade de identificar no mínimo, português, inglês e espanhol.

11.10. Deve permitir a criação de regras baseadas por país.

11.11. Possuir a capacidade de criar filtros personalizados usando expressões regulares.

11.12. Permitir criação de blacklists e whitelists, com opção por domínio, subdomínio, endereço de e-mail e endereço IP.

11.13. Deve prover um mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente (relay).

11.14. 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.

11.15. 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”.

11.16. O fabricante da solução deve possuir consulta de reputação de IP de remetentes de e-

mail. Esta consulta deve retornar os dados do remetente, com informações referentes à:

11.16.1. IP reverso e localização.

11.16.2. Registro em blacklists mundiais.

11.16.3. Configuração de serviço de notificação de envio e autenticidade de mensagens de mensagens como SPF e DKIM.

11.17. Capacidade de efetuar consultas externas ou internas na própria console da solução, para análise de endereço IP do remetente quanto a sua reputação, bem como verificação de spams e phishings recebidos e outros tipos de ameaças.

11.18. Deve ser capaz de realizar Reverse DNS LookUp (rDNS), para validação de fontes de e-mail.

11.19. Deve possuir suporte ao bloqueio de conexões de e-mails nocivos durante o diálogo SMTP, permitindo a economia de banda, armazenamento e otimização de processamento da solução, em especial baseado em lista local de bloqueio de conexão por:

11.19.1. IP.

11.19.2. E-mail.

11.19.3. Domínio.

11.19.4. RBL's – Realtime Blackhole Lists.

11.20. Deve permitir que o administrador do sistema cadastre novas RBL's para serem utilizadas a nível de conexão SMTP.

11.21. 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).

11.22. 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.

11.23. Possuir mecanismo de Spam Throttling permitindo ao administrador limitar o fluxo de mensagens recebidas de origens com baixa reputação.

11.24. Deve ser capaz de limitar o fluxo de mensagens automaticamente, de acordo com o volume de mensagens indevidas recebidas de um determinado IP de origem.

11.25. Possuir funcionalidade de verificação de DMARC (Domain-based Message Authentication Reporting & Conformance).

11.26. Possuir controle de Outbreak, penalizando o remetente por um tempo configurável pelo administrador ao detectar:

11.26.1. Número excessivo de spams (configurado pelo administrador) oriundos de uma mesma fonte de e-mail.

11.26.2. Número excessivo de vírus (configurado pelo administrador) oriundos de uma mesma fonte de e-mail.

11.26.3. Número excessivo de ataques de dicionário (configurado pelo administrador) oriundos de uma mesma fonte de e-mail.

11.27. Deve possuir apresentação de ameaças detectadas em tempo real. Nesse sistema de detecção de ameaças em tempo real, deve ser possível identificar:

11.27.1. Fontes de ataques.

11.27.2. Ameaças encontradas.

12. PROTEÇÃO CONTRA SPAM E PHISHING

12.1. Possuir filtro de anti-spam para detecção de spams usando no mínimo as seguintes tecnologias:

12.1.1. FingerPrint: filtro por assinatura de spam.

12.1.2. Análise heurística: análise completa de toda mensagem contra spam, de acordo com as características da mensagem.
12.1.3. Análise de documentos: análise de documentos anexados na mensagem (PDF, DOC, DOCX e TXT).
12.1.4. Análise de imagens: filtragem de spam em imagens.
12.1.5. Filtro de URL: filtragem por URL mal-intencionada contidas no corpo da mensagem, dessa forma combatendo possível e-mail phishing.

12.2. Permitir ao administrador definir filtros por URL através de categorias, divididas por assunto, sendo possível definir uma pontuação. Categorias mínimas contidas na solução:
12.2.1. Conteúdo pornográfico.
12.2.2. Abuso infantil.
12.2.3. Redes sociais.
12.2.4. Racismo e ódio.
12.2.5. Pesquisa de empregos.
12.2.6. Streaming de áudio.
12.2.7. Streaming de vídeo.
12.2.8. Esportes.
12.2.9. Notícias.
12.2.10. Compras online.

12.3. Deve possuir tecnologia capaz de avaliar um link recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se nesta página apontada pelo link há algum formulário de solicitação de senha, usuário e outras ameaças, efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing.

12.4. Deve possuir tecnologia capaz de avaliar um link URL recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se este link encaminha para um sistema que efetua um redirecionamento automático para download de um arquivos (Tipo Zip, EXE, RAR, etc), na tentativa de enganar o usuário, efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing.

12.5. Deve permitir que o administrador cadastre novas RBL's, devendo ser possível selecionar quais RBL's serão utilizadas a nível de conexão SMTP e quais serão utilizadas a nível de filtro de spam.

12.6. Possuir no mínimo as seguintes tecnologias para prevenção e bloqueio de spam:
12.6.1. Recurso de greylist.
12.6.2. 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".
12.6.3. Recurso de checagem por DMARC.
12.6.4. Recurso de checagem por assinatura DKIM.
12.6.5. Recurso de checagem de DNS Reverso.
12.6.6. Checagem de validade de domínio através de verificação da configuração da zona do DNS do remetente.
12.6.7. Análise de reputação de IP.
12.6.8. Reputação de mensagens.
12.6.9. Filtros de URL.
12.6.10. Filtro de anti-phishing.
12.6.11. Consulta de RBL´s (Realtime Blackhole List).

12.6.12. Machine learning.

12.7. 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.

12.8. Possuir a possibilidade de criação de regras personalizadas de filtragem baseadas em:
- 12.8.1. Origens das mensagens.
- 12.8.2. Destino das mensagens.
- 12.8.3. Domínios.
- 12.8.4. Endereços de e-mails.
- 12.8.5. Expressões regulares (dicionário de palavras).
- 12.8.6. Fluxo.
- 12.8.7. Quantidade de mensagens.
- 12.8.8. Tamanho de anexo.
- 12.8.9. Número máximo de destinatários em uma única mensagem.
- 12.8.10. Tipo de arquivos em anexo.
- 12.8.11. Extensões de arquivos em anexo, identificados por Mime-Type.
- 12.8.12. Anexos criptografados.
- 12.8.13. Anexos compactados.
- 12.8.14. Níveis de compactação dos arquivos anexos.
- 12.8.15. Conteúdo HTML no corpo da mensagem.

12.9. Possuir mecanismo de análise de conteúdo HTML no corpo da mensagem, permitindo ao administrador desarmar as tags HTML possivelmente perigosas e bloquear as mensagens, possuindo no mínimo a identificação das seguintes tags:
- 12.9.1. “<form>”.
- 12.9.2. “<script>”.
- 12.9.3. “<iframe>”.

12.10. Possibilidade de criar regras para ações a serem tomadas pela ferramenta, quando as mensagens forem consideradas confiáveis e/ou spams, permitindo ao administrador configurar nesses casos as seguintes ações:
- 12.10.1. Entregar direto o e-mail.
- 12.10.2. Colocar em quarentena.
- 12.10.3. Remover mensagem.
- 12.10.4. Auditar mensagem.
- 12.10.5. Encaminhar a mensagem.
- 12.10.6. Notificar o destinatário.
- 12.10.7. Adicionar header na mensagem.
- 12.10.8. Transformar HTML em texto simples.

12.11. Possuir sistema de detecção de ataque de diretórios (DHA – Directory Harvest Attack), 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.

12.12. Deve permitir a criação de regras 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, IP do remetente, campo header da mensagem, conteúdo no corpo da mensagem e URL contidas no e-mail.

12.13. 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 Microsoft Active Directory.

12.14. Deve ter a capacidade de rejeitar mensagens para destinatários inválidos durante o dialogo SMTP (tratar Non-Delivery Report Attack).

12.15. Possuir proteção contra bounce e-mail attack através do método Bounce Address Tag Verification.
12.16. Deve permitir a inclusão de múltiplas listas de remetentes bloqueados, permitindo regras de bloqueio se o IP estiver presente nestas listas.
12.17. Deve permitir que mensagens de falso negativo sejam reportadas através da interface gráfica para o laboratório de pesquisa do fabricante ou oferecer um caminho para que mensagens de falso negativo sejam reportadas diretamente ao laboratório do fabricante.
12.18. Deve possuir mecanismo que permita a adição de cabeçalho de identificação da classificação das mensagens como spam, a fim de integrar com sistemas de correio eletrônicos tais como Microsoft Exchange 2010 e superiores.

13. PROTEÇÃO CONTRA VÍRUS E MALWARES

13.1. Possuir módulo de verificação de antivírus.
13.2. Deverá ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de e-mail).
13.3. Scan de arquivos compactados recursivamente, no mínimo, 5 (cinco) camadas, contemplando no mínimo, os seguintes compactadores: .rar, .zip, .tar, .arj, .cab, .lha, .exe, .lzh, .tgz, .gzip, .bzip.
13.4. Deve possuir sistema de detecção a técnicas de mascaramento de ameaças:
13.4.1. Stealth.
13.4.2. Ameaças polimórficas.
13.5. Proteção contra vírus, no mínimo com as tecnologias já licenciadas sem a necessidade de módulo adicional:
13.5.1. Dia-zero (“zero-day”).
13.5.2. “Virus outbreak”.
13.5.3. “Targeted attack protection”.
13.5.4. “APT - advanced persistent threat”.

14. AVISO LEGAL - DISCLAIMER

14.1. Capacidade de incluir disclaimers nas mensagens enviadas.
14.2. A solução deverá suportar aplicação de disclaimers diferenciados para usuários e grupos diferentes através da integração com o serviço de diretório LDAP ou Microsoft Active Directoy.
14.3. A solução deverá suportar a configuração dos disclaimers em formato HTML e texto.

15. REGRAS DE CONFORMIDADE - COMPLIANCE

15.1. Deve permitir criar regras de compliance “Auditoria/Aderência” através de filtros avançados de análise da mensagem, permitindo identificar através de dicionários (conjunto de palavras e expressões regulares) personalizados pelo administrador ou já existentes na ferramenta.
15.2. As regras de conformidade podem ser criadas utilizando os termos dos dicionários definidos e que estejam nos seguintes campos da mensagem, podendo ser definido o número de ocorrências mínimas para execução da regra:
15.2.1. Cabeçalho.
15.2.2. URL (contidas no e-mail).
15.2.3. Corpo do e-mail.
15.2.4. Anexos e documentos no mínimo: .doc, .docx, .xls, .xlsx, .pdf, .ppt, .pptx e .txt.
15.3. Permitir ao administrador criar regras de compliance para arquivos criptografados, possibilitando ao administrador configurar a ação a ser tomada quando um anexo

criptografado é identificado. A solução deve ter no mínimo três algoritmos de detecção:
15.3.1. Mecanismo heurístico.
15.3.2. Myme-Type.
15.3.3. Extensão.

16. CRIPTOGRAFIA DE E-MAIL

16.1. Deve possuir módulo de criptografia integrado na solução, licenciado com a mesma quantidade de caixas postais da solução de proteção de e-mail.
16.2. A criptografia deve atuar na saída de e-mails trabalhando de maneira transparente ao usuário final, sem a necessidade de plugins, agentes ou outro tipo de software, com uma interface para o destinatário das mensagens customizável pelo administrador.
16.3. A console de gerenciamento do módulo de criptografia deve ser a mesma para toda a solução, não exigindo console de administração adicional.
16.4. Deve possibilitar ao administrador, definir quais mensagens serão criptografadas com base no mínimo em:
16.4.1. Assunto.
16.4.2. Destinatário.
16.4.3. E-mail do Remetente.
16.4.4. Nome do Anexo.
16.5. A criptografia das mensagens deve utilizar sistema de chaves gerada de forma independente.
16.6. Deve impossibilitar o uso de Cache de Browser para acesso as mensagens criptografadas.
16.7. Deve possibilitar ao administrador a indicação do tempo de expiração da mensagem criptografada.
16.8. Deve possibilitar ao administrador indicar se o destinatário poderá responder o e-mail.
16.9. Deve possibilitar ao administrador indicar se o destinatário poderá encaminhar o e-mail.
16.10. A solução de criptografia de emails deve ser responsivo, permitindo aos usuários lerem emails criptografados na solução tanto em tablets, como em celulares smartphones.

17. SISTEMA DE PROTEÇÃO CONTRA ATAQUES DIRIGIDOS (TARGETED ATTACK PROTECTION - TAP)

17.1. Deverá prover proteção contra ataques dirigidos tais como:
17.1.1. Spear-phishing.
17.1.2. Ataques Zero-Day.
17.1.3. Ameaças avançadas persistentes (APTs).
17.2. Deve possuir no mínimo 3 (três) camadas de proteção sendo elas:
17.2.1. Verificação da lista de códigos maliciosos: verificação de campanhas de e-mails emergentes e conhecimento de novos sites maliciosos.
17.2.2. Análise estática (análise de código): verificação de comportamento suspeito, scripts escondidos, partes de códigos maliciosos e redirecionamento a outros sites maliciosos.
17.2.3. Análise dinâmica: utilização de sandbox para simular a máquina de um usuário real e observar as alterações efetuadas no sistema.
17.3. Possuir, dentro da solução, um dashboard do módulo de segurança contra-ataques dirigidos.
17.4. O sistema de proteção contra-ataques dirigidos deve executar no mínimo 3 (três)

etapas:

17.4.1. 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.

17.4.2. Proteção - deve assegurar que links para URLs sejam 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.

17.4.3. 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 online.

17.5. Não será aceita solução baseada apenas em reputação de URL.

17.6. A solução deve conter engine para detecção de anomalias, não podendo se limitar a analise com definições baseadas em ataques já conhecidos.

17.7. Deve ser possível habilitar ou desabilitar a proteção URL baseada em rotas especificas configuradas no mínimo pelas seguintes condições:

17.7.1. E-mail do destinatário.
17.7.2. E-mail do remetente.
17.7.3. Domínio de origem.
17.7.4. Domínio de destino.
17.7.5. IP/Rede.
17.7.6. Range de IP.
17.7.7. Expressão regular.
17.7.8. Usuários.
17.7.9. Listas de distribuição.
17.7.10. Grupo de LDAP.

17.8. A proteção de URL deverá reescrever os links do e-mail e a cada clique o sistema deverá analisar a URL e somente depois de passar por todos os testes, sendo constatado que não é malicioso, deve redirecionar para a URL original. Se após a análise for constatado site malicioso, o sistema deverá exibir mensagem de alerta e o site deverá ser bloqueado para acesso.

17.9. O sistema deverá ser capaz de varrer anexos, no mínimo dos tipos pdf, arquivos em flash para payloads maliciosos e Microsoft Office.

17.10. Ao detectar arquivos maliciosos, deverá ser capaz de configurar regras para descartar e salvar uma cópia na quarentena.

17.11. Deve possuir tecnologia sandbox local do mesmo fabricante ou em nuvem do próprio fabricante, desde que esteja em conformidade com todas as regras da legislação vigente brasileira (Lei Geral de Proteção de Dados Pessoais).

17.12. Deverá ser capaz de efetuar a verificação da reputação de anexos e caso a reputação do anexo não conste no banco de dados, a solução deverá ter a opção de enviar automaticamente o anexo para a nuvem do fabricante para análise em tempo real em sistema de sandbox do próprio fabricante, caso o administrador opte por este serviço. Este sistema de sandbox deve conter tecnologia de detecção usando “analise comportamental” do arquivo identificando assim malwares e variantes sem a necessidade de assinaturas.

17.13. A proteção URL deverá acompanhar o destinatário na URL reescrita. Quando uma mensagem for dirigida a vários destinatários, o envelope será dividido de modo que existam apenas um receptor associado com uma URL reescrita para permitir que administradores possam controlar quais usuários clicaram na URL reescrita e os usuários que ignoraram

através do dashboard.

17.14. A proteção URL deverá reescrever links para os protocolos HTTP, HTTPS, FTP e URL's que comecem com "www" independente do protocolo.

17.15. A solução deverá permitir que o administrador configure o sistema de proteção URL para que reescreva todas as mensagens que contiverem URL e envie ao sandbox para testes garantindo um alto nível de segurança.

17.16. A solução deverá prover lista de exceções de URL para que não sejam reescritas.

17.17. O dashboard deverá exibir o número de cliques em cada ameaça.

17.18. O dashboard deverá exibir qual usuário clicou na URL detectada como ameaça.

17.19. O dashboard deverá exibir informações atualizadas sobre as ameaças detectadas, deverá exibir a classificação da mensagem e deverá exibir status atualizado e detalhado sobre as ameaças no mínimo com as seguintes informações:

17.19.1. Clicado – número de vezes que uma URL reescrita foi clicada por um usuário, inclusive se a mensagem for encaminhada para outro usuário e também for clicada.

17.19.2. Bloqueado - número de vezes que o modulo de Proteção URL impediu o usuário de acessar o site malicioso.

17.19.3. Permitida – número de vezes que o modulo de proteção URL permitiu ao usuário acessar o site original da URL reescrita e que não foi detectada como maliciosa.

17.20. O dashboard deverá exibir timeline das ameaças, exibindo quando foi recebida, identificada e quando foi clicada ou liberada.

17.21. No dashboard deverá ser possível filtrar uma URL em um campo de busca para analisar todas as ocorrências com aquela URL, bem como verificar o status atual dela e preview da página web.

17.22. O dashboard deverá possuir ferramenta para bloqueio ou liberação de URL pelo administrador da ferramenta.

17.23. No dashboard deverá ser possível filtrar um IP em um campo de busca para analisar todas as ocorrências com aquele IP, bem como verificar o status atual dele e preview da página web.

17.24. O dashboard deverá disponibilizar sistema de coleta (report) de amostra do IP para análise da engenharia do fabricante.

17.25. O dashboard deverá possuir ferramenta para bloqueio ou liberação do IP pelo administrador da ferramenta.

17.26. No dashboard deverá ser possível ao administrador enviar uma amostra de um arquivo para análise e visualizar o retorno de todas as ocorrências encontradas para esse arquivo.

17.27. O dashboard deverá possuir ferramenta para bloqueio ou liberação do arquivo pelo administrador da ferramenta.

17.28. 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 reports enviados pelos usuários, ficando a cargo do administrador decidir pelo bloqueio ou a liberação de tal URL e/ou arquivo.

17.29. Deve possuir módulo de CDR "Content Disarm and Reconstruction", que quando ativado irá remover conteúdos possivelmente perigosos, em no mínimo para os seguintes tipos:

17.29.1. JavaScript.

17.29.2. Links.

17.29.3. Executáveis.

17.29.4. VB Script.

17.29.5. De dentro de documentos, em no mínimo para os seguintes tipos:

17.29.5.1. pdf.
17.29.5.2. doc.
17.29.5.3. docx.
17.29.5.4. ppt.
17.29.5.5. pptx.
17.29.5.6. xls.
17.29.5.7. xlsx.

17.30. Deve possuir capacidade de ignorar reescrita de algumas URL's e não envio de arquivos para análise no sandbox do fabricante.

17.31. O sandbox do fabricante deve ter a capacidade de analisar arquivos, mesmo que estejam inseridos em arquivos compactados, do tipo:
17.31.1. .swf.
17.31.2. .pdf.
17.31.3. .doc.
17.31.4. .xls.
17.31.5. .xlsx.
17.31.6. .ppt.
17.31.7. .ppt.
17.31.8. .pptx.
17.31.9. .rtf.

17.32. Deve ter a opção de não fazer reescrita de URL's em casos de mensagens oriundas de determinados países.

17.33. Deve poder desativar a reescrita de URL's se a mensagem atingir uma pontuação mínima de spam definida pelo administrador.

17.34. Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista de bloqueio (Blacklist) no sistema de detecção.

17.35. Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista segura (Whitelist) no sistema de detecção.

18. SISTEMA DE PROTEÇÃO A FRAUDES DE E-MAIL

18.1. A solução deverá ter a capacidade de detectar domínios recém registrados (tempo considerado como recém adquirido deverá ser configurável pelo administrador) e indicar o que deve ser feito neste caso:
18.1.1. Pontuar.
18.1.2. Ignorar.
18.1.3. Bloquear.

18.2. 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:
18.2.1. Pontuar.
18.2.2. Ignorar.
18.2.3. Bloquear.

18.3. 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.

18.4. Deve possuir sistema de detecção de e-mails oriundos de servidores de e-mails gratuitos tais como Google, Yahoo, Hotmail, etc, para serem usados em regras personalizadas de

filtragem.

18.5. Nativamente deve possuir sistema de detecção de e-mails externos (e-mails de entrada) que tentem utilizar o domínio da própria empresa como remetente, sem necessidade de criação de regra específica para este tipo de fraude.