JUSTIÇA FEDERAL
CONSELHO DA JUSTIÇA FEDERAL

TERMO DE REFERÊNCIA N. 0540915/CJF

1 Definição do objeto (art. 6º, XXIII, "a", lei n. 14.133/2021)

1.1 Contratação de solução de segurança para proteção de estações de trabalho, *Data Center*, *e-mail* corporativo e aplicativos Microsoft 365, contemplando instalação e configuração, transferência de conhecimento e, suporte técnico com garantia do fabricante do Conselho da Justiça Federal, pelo prazo de 36 meses.

1.2 A contratação será realizada em 1 grupo com 9 itens, conforme tabela apresentada a seguir:

GRUPO	ITEM	DESCRIÇÃO	QTDE	UNIDADE
1	1.1	Proteção para estações de trabalho	580	Dispositivo
	1.2	Proteção para Serviço de *E-mail*	1300	Usuário
	1.3	Proteção para Microsoft 365	550	Usuário
	1.4	Proteção para *Data Center*	60	*Socket*
	1.5	Proteção para *Storage*	2	Servidor
	1.6	Inspeção de Tráfego de Rede (NDR) para 4Gbytes	1	Solução
	1.7	Instalação e Configuração	1	Serviço
	1.8	Suporte Técnico Mensal	36	Mês
	1.9	Repasse de conhecimento para até 5 participantes	1	Turma

1.3 Compõem este Termo de Referência os seguintes anexos:

1.3.1 Anexo I – Detalhamento dos Requisitos Técnicos do Objeto;

1.3.2 Anexo II – Cronograma de Implantação dos Serviços;

1.3.3 Anexo III – Planilha de Composição de Custos;

1.3.4 Anexo IV – Termo de Confidencialidade e Sigilo da Contratada;

1.3.5 Anexo V – Termo de Vistoria.

1.4 Requisitos da contratação (art. 6º, XXIII, "d" c/c art. 18, §1º, III, lei n. 14.133/2021)

Os requisitos técnicos são apresentados no Anexo I deste Termo de Referência.

1.5 Descrever solução de TIC de forma detalhada, motivada e justificada

Trata-se de contratação de solução de segurança de TI para proteção estações de trabalho, *Data Center*, *e-mail* corporativo e aplicativos Microsoft 365 para os ambientes computacionais do Conselho da Justiça Federal – CJF e da NUJFE, contemplando serviço de instalação e configuração, transferência de conhecimento e suporte técnico com garantia do fabricante para 36 (trinta e seis) meses,

Os serviços a serem contratados se enquadram como de natureza contínua nos termos do art. 5º, inciso XXIII, alínea *k*, da Instrução Normativa n. 12/2022-CJF. Os serviços deverão ser prestados em

conformidade com os padrões técnicos de desempenho e qualidade estabelecidos pelo CONTRATANTE.

As soluções a serem contratadas e os seus respectivos quantitativos estão descritas no item 1.2 deste Termo de Referência e os requisitos técnicos estão descritos no Anexo I.

1.6 Ciclo de vida do objeto

Em relação ao ciclo de vida do objeto pretendido, sua avaliação pode ser realizada em conformidade com os quesitos descritos a seguir:

1.6.1 Ciclo de vida dos *softwares*:

Produção:

Esta fase engloba o desenvolvimento do software e a atualização regular para fornecer novos recursos e corrigir problemas de segurança.

Nesta fase, dois indicadores parecem úteis ao gestor do contrato para verificar essa fase do ciclo de vida:

- Número de atualizações lançadas por ano, refletindo a capacidade da empresa contratada de responder às necessidades dos usuários e corrigir falhas de segurança. Medir o número dessas atualizações pode dar uma ideia da proatividade da empresa em manter o software seguro;
- Tempo de resposta para correção de bugs: quando um bug é identificado no software, é crucial que ele seja corrigido rapidamente para minimizar qualquer interrupção potencial no trabalho do usuário. Este indicador pode ser medido pelo tempo decorrido entre a identificação do bug e a sua correção.

Distribuição:

Não fica claro pelo DOD apresentado (id. 0464636) se a distribuição será ou não digital, todavia, um ponto merece destaque:

- Tempo de ativação da licença: este indicador pode ser medido desde o momento em que o pedido de licença é feito até quando ele é ativado e pronto para uso. Idealmente, isso deve ser um processo rápido e sem problemas.

Armazenamento:

Não fica claro pelo DOD apresentado (id. 0464636) se o software adquirido requer armazenamento no dispositivo do usuário ou se será armazenado em nuvem para certos recursos. Contudo, um indicador parece importante no ciclo de vida da contratação, qual seja:

- Proteção dos dados usuários: este indicador é fundamental, pois se refere à proteção dos dados dos usuários armazenados na nuvem. Pode ser medido através do número de incidentes de segurança ou vazamento de dados que ocorreram ao longo do contrato. Idealmente, esse número deveria ser zero.

Utilização:

Esta fase é extremamente crítica, ao envolver a efetividade do software para os usuários do Conselho da Justiça Federal. Indicadores úteis aqui poderiam ser:

- Satisfação do usuário com o software: este indicador pode ser medido por meio de pesquisas de satisfação do usuário, com perguntas que avaliam aspectos como a facilidade de uso, a funcionalidade do software e a qualidade do suporte ao cliente;
- Tempo de inatividade do sistema: este é um indicador crítico que mede a quantidade de tempo em que o software não está disponível para uso devido a problemas técnicos, manutenções ou falhas. É importante porque a inatividade do sistema pode interromper as operações, impactando a produtividade, prazos, mas principalmente a segurança, como

destacado no DOD da SUGOV (id. 0464636). Este indicador pode ser quantificado registrando a duração e a frequência das interrupções do serviço.

Descarte:

Como o software é uma solução digital, a etapa de descarte é um pouco diferente da de produtos físicos. Ao invés de ser fisicamente descartado, o software é "descartado" quando as licenças expiram ou são descontinuadas. Indicadores úteis nesta fase poderiam ser:

Requisitos para desinstalação: este indicador se refere à facilidade de desinstalação do software dos sistemas da organização. Este indicador pode ser quantificado observando o tempo necessário para concluir o processo de desinstalação e o número de etapas necessárias;

Preservação de dados: quando um contrato de licença de software é encerrado, é importante considerar o que acontece com os dados gerados ou armazenados nos dispositivos dos usuários. Este indicador avalia se os dados podem ser facilmente exportados e preservados após o término do contrato. Ele pode ser mensurado observando a facilidade de exportação de dados e se os dados permanecem acessíveis e utilizáveis após a exportação.

1.6.2 Ciclo de vida dos serviços

As considerações nesta fase se referem aos serviços de instalação e configuração, transferência de conhecimento e suporte técnico.

Planejamento:

Este é o estágio inicial do ciclo de vida, onde a necessidade de serviços, incluindo suporte técnico é identificada e um plano de licitação é elaborado. As especificações dos serviços devem ser claramente definidas e os requisitos técnicos são cuidadosamente articulados para garantir que os possíveis licitantes tenham uma compreensão clara do escopo do contrato. A análise de mercado pode ser realizada para avaliar as opções disponíveis e determinar uma estimativa de custo.

Para o todo o ciclo de vida dos serviços de instalação e configuração, transferência de conhecimento e suporte técnico, é crucial identificar indicadores para avaliação qualitativa e quantitativa da contração. Alguns indicadores usados pelo gestor podem ser:

- Dimensionamento de necessidades: esta métrica se refere à precisão com que a unidade demandante avalia as necessidades de suporte do software, considerando tanto o presente quanto o futuro. Isso pode ser medido em termos de uma análise de lacunas entre as capacidades atuais e futuras desejadas.
- Equipamentos de segurança: como a empresa contratada será responsável por fornecer os equipamentos de segurança necessários para a execução dos serviços, é importante incluir no edital de licitação detalhes claros sobre as expectativas em relação a esses equipamentos. O indicador poderia ser a adequação e a conformidade desses equipamentos com as normas de segurança vigentes.
- Preparação para possíveis riscos e contingências: avaliar a preparação do plano de licitação para possíveis riscos e contingências. Isso poderia ser medido considerando a inclusão de cláusulas de gestão de riscos e contingências no edital.

Processo de licitação:

A licitação é publicada e os licitantes potenciais são convidados a apresentar suas propostas. As propostas são então avaliadas com base nos critérios estabelecidos no plano de licitação, tais como a experiência do licitante no fornecimento de suporte técnico para o software em questão, a qualidade do serviço proposto e o preço.

Embora para o todo o ciclo de vida seja crucial identificar indicadores para avaliação qualitativa e quantitativa da contração, aqui não há sugestão de indicadores porque este processo está a cargo da SAD, a qual observa parâmetros legais (já estabelecidos) e um fluxo claro para o prosseguimento correto do certame em comento.

Execução do Contrato:

Uma vez que a licitação é concedida a um fornecedor, o contrato entra em sua fase de execução. Durante este estágio, a empresa fornece o suporte técnico conforme especificado no contrato e seus desempenho deve ser monitorado e avaliado regularmente para garantir a conformidade com os termos do contrato e a qualidade do suporte técnico fornecido.

Para o todo o ciclo de vida, é crucial identificar indicadores para avaliação qualitativa e quantitativa da contração. Alguns indicadores usados pelo gestor podem ser:

- Tempo de resposta: este indicador mede o tempo necessário para que a equipe de suporte técnico da empresa contratada responda a uma solicitação de serviço. Este é um aspecto crítico da execução do serviço de suporte técnico.
- Taxa de resolução na primeira chamada: esta métrica se refere ao percentual de chamadas de suporte ou *tickets* resolvidos na primeira interação com a equipe de suporte técnico.
- Tempo de resolução: este indicador mede o tempo médio que a equipe de suporte leva para resolver um problema depois que ele foi relatado.
- Escalabilidade do suporte: este indicador avalia a capacidade do serviço de suporte de lidar com um aumento no volume de solicitações ou complexidade dos problemas sem comprometer a qualidade do serviço.
- Manutenção preventiva: este indicador se refere à quantidade e efetividade das ações de manutenção preventiva realizadas para evitar problemas futuros.

Revisão e Encerramento:

No final do contrato, é necessário realizar uma revisão para avaliar a eficácia dos serviços fornecidos e determinar se os objetivos do contrato foram alcançados. Nesta fase, alguns indicadores usados pelo gestor podem ser:

Satisfação do usuário: a avaliação da satisfação dos usuários é fundamental para entender a efetividade dos serviços prestados. Isso pode ser medido por meio de pesquisas de satisfação, avaliando itens como a rapidez na resolução de problemas, a facilidade de comunicação com o suporte e a clareza das informações fornecidas.

Tempo de resolução de problemas: medir o tempo médio que leva para um problema reportado ser resolvido é um indicador crucial da eficiência do serviço de suporte. Este indicador pode ser quebrado em várias etapas, como tempo para o primeiro contato, tempo para diagnóstico e tempo para resolução.

Taxa de recorrência de problemas: este indicador mede quantos problemas resolvidos reaparecem. Uma alta taxa de recorrência pode indicar uma abordagem de "correção de sintomas" ao invés de "correção de causas raiz", o que é insustentável a longo prazo.

Melhorias contínuas: um bom fornecedor não só atenderá às necessidades atuais, mas também buscará melhorias contínuas nos serviços prestados. Este indicador mede a quantidade e a efetividade das melhorias propostas e implementadas durante o período do contrato.

Transferência de conhecimento: ao final do contrato, o fornecedor deve ter transferido conhecimento suficiente para a equipe de TI, de forma que eles possam manter o funcionamento básico do software sem a necessidade de suporte externo constante. Este indicador pode ser medido pela competência da equipe interna no final do contrato.

2 Fundamentação da contratação (art. 6º, XXIII, "b" c/c art. 18, §1º, I e II, lei n. 14.133/2021)

2.1 Motivação da contratação

O Conselho da Justiça Federal possui vigente o Contrato CJF n. 31/2018, firmado com a empresa ALLTECH Soluções em tecnologia Ltda, cujo objeto é a contratação de solução de segurança para proteção de *endpoints*, dos servidores do *Data Center* e do serviço de *e-mail*, com garantia de 60 (sessenta) meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico.

Com o fim da vigência deste contrato, assim como da vigência do direito de atualização das licenças d e *antimalware* de *endpoints* e servidores e da solução de proteção do serviço de *e-mail*, em 26/12/2023, se faz necessária uma nova contratação para dar continuidade ao atendimento da demanda, além da possibilidade de aprimoramento nos serviços prestados.

Apesar da qualidade já demonstrada da solução contratada em 2018, a equipe técnica de segurança da informação do CJF vislumbra a possibilidade de implementação de melhorias, que poderão se dar por meio da adição de novas funcionalidades ou ferramentas voltadas para a detecção e resposta de ameaças de segurança.

Os serviços de proteção de *endpoint* mais atuais dispõem de funcionalidades que vão além da simples proteção contra ocorrências pontuais de *malwares* ou *ransomwares* nos dispositivos, mas também fornecem informações mais aprofundadas, que podem ser cruciais para identificação de ataques cibernéticos de maior magnitude contra o ambiente tecnológico deste Conselho.

Ante ao exposto, faz-se necessária uma nova contratação visando atender à necessidade de prover segurança aos dispositivos e *e-mails* corporativos do CJF. Trata-se de contratação de licenciamento de software de soluções de segurança visando a prevenção de ataques cibernéticos em servidores de rede, estações de trabalho (*endpoints*), serviço de *e-mail* e Microsoft 365 voltada para o ambiente corporativo do CJF.

2.2 Objetivos a serem alcançados

2.2.1 Assegurar que os níveis de proteção e detecção de ameaças referentes à Segurança da Informação sejam mantidos e aprimorados, garantindo a continuidade da segurança dos sistemas e dados da organização;

2.2.2 Garantir que a solução de segurança esteja atualizada com as mais recentes tecnologias, assinaturas de ameaças e inteligência de segurança para lidar com as ameaças cibernéticas em constante evolução;

2.2.3 Assegurar que a solução esteja equipada para lidar com novas variantes de *malware*, táticas de ataque e vetores de ataque que possam surgir desde a implementação inicial;

2.2.4 Reforçar a capacidade de resposta a incidentes, incluindo a automação de ações de contenção e remediação, reduzindo o tempo necessário para lidar com ameaças ativas;

2.2.5 Manter e aprimorar a detecção de ameaças presentes em *e-mails*, como *phishing* e ataques de engenharia social, para evitar comprometimentos por meio dessa superfície de ataque;

2.2.6 Aumentar o grau de satisfação dos usuários com os produtos e serviços fornecidos pela área de Segurança da Informação;

2.2.7 Redução do tempo de restauração da operação normal dos serviços com o mínimo de impacto nos processos de negócios da CONTRATANTE, dentro dos Níveis Mínimos de Serviço (NMS) e prioridades acordados;

2.2.8 Aprimorar a percepção do adequado gerenciamento de segurança de Segurança da Informação por parte da alta administração e dos usuários internos e externos, deixando transparente que há efetivo gerenciamento dos incidentes de segurança de tecnologia da informação;

2.2.9 Aprimorar o tratamento de vulnerabilidades de segurança do ambiente de TI;

2.2.10 Desenvolver resiliência e melhorar a capacidade da TI de enfrentar eventos adversos relacionados a cibersegurança.

2.3 Benefícios diretos e indiretos

2.3.1 Identificação e resposta rápida à ameaças cibernéticas, incluindo *malware*, *ransomware* e ameaças de dia zero, em *endpoints*, servidores, *e-mails* e aplicativos Microsoft 365 através de recursos e serviços de detecção e resposta avançada de ameaças.

2.3.2 Monitoramento do tráfego de rede visando identificar atividades suspeitas, ataques de intrusão

e comportamentos anômalos que possam indicar comprometimento.

2.3.3 Possibilidade de automatização de ações de resposta a incidentes, como isolamento de *endpoints* comprometidos, bloqueio de comunicações maliciosas e remediação rápida de sistemas afetados.

2.3.4 Capacidade de visibilidade abrangente de diversas camadas da infraestrutura de TI, permitindo uma compreensão clara da postura de segurança da organização e a detecção proativa de ameaças.

2.3.5 Detecção e bloqueio de ameaças avançadas presentes em *e-mails*, como *phishing* e outros tipos de ataques de engenharia social, reduzindo o risco de comprometimento por meio de comunicações eletrônicas.

2.3.6 Aprimoramento da segurança das ferramentas e aplicativos Microsoft 365, como o Microsoft Teams e o OneDrive, protegendo os dados armazenados e compartilhados nessas plataformas.

2.3.7 Redução do tempo necessário para identificar, investigar e responder a incidentes de segurança, minimizando assim o impacto financeiro e operacional decorrente de violações de segurança.

2.4 Alinhamento entre a contratação e o Plano Estratégico Institucional e/ou de TIC e o Plano Anual de Contratações

A contratação está alinhada com as seguintes diretrizes estratégicas aplicáveis ao Conselho da Justiça Federal:

Estratégia Nacional do Poder Judiciário 2021-2026 – Resolução CNJ n. 325, de 30 de junho de 2020:

- Macro desafio do Poder Judiciário: fortalecimento da estratégia nacional de TIC e de proteção de dados.

Estratégia Nacional de Segurança da Informação do Poder Judiciário – Resolução CNJ n. 396, de 7 de junho de 2021:

- Objetivos estratégicos: aumentar a resiliência às ameaças cibernéticas, permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário 2021 – 2026 – Resolução CNJ n. 370 de 28 de janeiro de 2021:

- Objetivo estratégico: aprimorar a Segurança da Informação a Gestão de Dados.

Estratégia do Conselho da Justiça Federal – Portaria CJF n. 576, de 24 de junho de 2020:

- Objetivo estratégico: fortalecer a segurança da informação - promover ações que objetivam viabilizar e assegurar a disponibilidade, a integridade e a confidencialidade das informações, assim como a transparência e a proteção aos dados pessoais, desde a sua coleta até o seu processamento e o compartilhamento.

Plano Estratégico de Tecnologia da Informação da Justiça Federal – Resolução CJF n. 685, de 15 de dezembro de 2020:

- Objetivo estratégico: promover e fortalecer a segurança da informação digital na Justiça Federal.

Plano Diretor de Tecnologia da Informação 2021 – 2023 - Portaria CJF n. 600, de 11 de fevereiro de 2021:

- Iniciativa 4: Aprimorar serviços de TI do CJF.
- Iniciativa 6: Manter serviços de TI em operação.
- Iniciativa 13: Aperfeiçoar a infraestrutura de TI do CJF.
- Iniciativa 15: Aprimorar a Segurança da Informação do CJF e da JF.

Macrodesafio do Poder Judiciário:

- Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados;

Objetivo(s) estratégico(s) da Justiça Federal:

- Aperfeiçoar e Assegurar a efetividade dos serviços de TI para a Justiça Federal;
- Assegurar a atuação sistêmica da TI na Justiça Federal;
- Promover e fortalecer a segurança da informação digital na Justiça Federal;

2.5 Referência aos Estudos Preliminares de STIC

Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda – DOD (id. 0464636) e os Estudos Técnicos Preliminares - ETP (id. 0497062) acostados ao processo SEI n. 0001703-88.2023.4.90.8000.

2.6 Relação entre a demanda prevista e a quantidade de bens e/ou serviços a serem contratados

A solução abrange licenças e agentes para todo o parque computacional do CJF e da NUJUFE.

Para o licenciamento das estações de trabalho e servidores de armazenamento foram consideradas as quantidades cobertas pelo contrato CJF 031/2018 e que já atendem ao quantitativo contabilizado em julho/23.

O licenciamento de caixas de correio considerou o total de caixas postais gerenciadas pelo serviço de *e-mail* corporativo MS Exchange, tanto de usuários e quanto de unidades (caixas corporativas).

O quantitativo de usuários Microsoft 365 foi baseado no total de licenças Microsoft 365 padrão E1 e Microsoft 365 padrão E3 constante no id. 0465117 do processo SEI n. 0003441-13.2022.4.90.8000.

O quantitativo de licenças para proteção de *Data Center* está incluído tanto o ambiente de *Data Center* do CJF quanto da NUJUFE. Para o ambiente do CJF, são necessárias 20 (vinte) licenças de *sockets*, das quais, atualmente, 18 (dezoito) estão cobertas pelo Contrato CJF n. 031/2018, com validade até 26/12/23. Para o ambiente da NUJUFE, são necessárias 40 (quarenta) licenças de *sockets*, as quais estão cobertas pelo Contrato CJF n. 013/2021, com validade até 08/08/24. Desta maneira, para este último, a demanda somente será realizada em 2024 mediante emissão de Ordem de Serviço para a Contratada.

O serviço de instalação e configuração está previsto para ocorrer em uma única atividade assim que as licenças e agentes da solução estejam disponíveis conforme cronograma de entrega.

O serviço de suporte técnico mensal está dimensionado para atendimento durante toda a vigência do contrato estipulado para 36 meses.

O repasse de conhecimento está dimensionado para a equipe de administração de soluções de segurança do CJF e eventuais servidores relacionados com a administração da solução em uma turma de até 5 participantes.

2.7 Análise de mercado de Tecnologia da Informação e Comunicação com o levantamento das soluções disponíveis e/ou contratadas por órgãos ou entidades da Administração Pública, seus respectivos valores, bem como a definição e a justificativa da escolha da solução

Inicialmente foram levantadas as necessidades de negócio para esta contratação no artefato Estudos Técnicos Preliminares (id. 0497062), a partir da motivação/justificativa descrita no Documento de Oficialização da Demanda - DOD (id. 0464636).

Dentre as possibilidades de atendimento da demanda, considerados os riscos da contratação, restaram duas alternativas viáveis tecnicamente:

1. Contratação de solução de proteção de *endpoints*, *Data Center*, *antispam* e Microsoft 365 atualmente em uso pelo CJF com expansão de novas funcionalidades de detecção e resposta

avançada de incidentes. Expansão da solução de gestão de acesso privilegiado atualmente utilizada no CJF e TRFs.

2. Contratação de solução de proteção de *endpoints*, *Data Center*, *antispam* e Microsoft 365 com expansão de novas funcionalidades de detecção e resposta avançada de incidentes em ampla concorrência.

Sendo assim, dentre as opções que atendem ao escopo pretendido e considerando as características, riscos, vantagens e desvantagens técnicas identificadas, a alternativa que se apresenta como adequada nos termos fundamentados nos estudos técnicos preliminares é a contratação de solução de proteção de endpoints, *Data Center*, antispam e Microsoft 365 com expansão de novas funcionalidades de detecção e resposta avançada de incidentes em ampla concorrência.

2.8 Custo total estimado para a contratação (art. 6º, XXIII, "i", lei n. 14.133/2021)

Para realização da estimativa de custo, a equipe de contratação levou em consideração os principais fornecedores de soluções de segurança do mercado que poderiam atender aos requisitos definidos para esta contratação. Entre elas estão TrendMicro, Trellix, Karspesky, Sophos, Checkpoint, Crowdstrike e PaloAlto. Contudo, apenas a empresa Alltech, revenda autorizada da TrendMicro, respondeu à solicitação de cotação de preços, enviando a Proposta acostada ao id. 0497067, fls. 59-64.

Com objetivo de dar publicidade ao processo, dar conhecimento das condições de contratação e receber propostas contendo estimativas de preços, a minuta do Termo de Referência, com suas especificações técnicas, foi enviado por *e-mail* (id. 0520143) às revendas dos diversos fabricantes que poderiam atender ao objeto a ser contratado.

Os integrantes técnicos também realizaram pesquisa para obtenção de contratos vigentes com vários órgãos da administração pública para este mesmo objeto. Dentre os órgãos pesquisados foram identificados contratos firmados na Polícia Rodoviária Federal (PRF), Ministério do Desenvolvimento Regional (MDR), Agência de Tecnologia da Informação do Estado do Piauí (ATI-PI), Escola Superior do Ministério Público da União (ESMPU), DETRAN-PA e Tribunal de Justiça da Bahia.

Assim, com base nas propostas recebidas e nos contratos com objeto e condições similares, foi elaborado o Mapa Comparativo de Preços para esta contratação, acostado ao id. 0520113. Foram seguidas as diretrizes da Instrução Normativa SEGES/ME n. 65, de 7 de julho de 2021, art. 5º, utilizando-se, de forma combinada, os parâmetros constantes dos incisos II e IV. Destaca-se que as informações detalhadas sobre a metodologia estão descritas na própria planilha do Mapa Comparativo.

A estimativa dos valores em reais obtidos de cada item está indicada na tabela abaixo:

ITEM	DESCRIÇÃO	UNIDADE	QTD	PREÇO UNITÀRIO	PREÇO TOTAL
1	Proteção para estações de trabalho	Dispositivo	580	R$ 411,23	R$ 238.515,72
2	Proteção para Serviço de *E-mail*	Usuário	1300	R$ 176,92	R$ 230.000,00
3	Proteção para Microsoft 365	Usuário	550	R$ 272,73	R$ 150.000,00
4	Proteção para *Data Center*	Socket	60	R$ 20.731,71	R$ 1.243.902,60
5	Proteção para Storage	Servidor	2	R$ 30.000,00	R$ 60.000,00
6	Inspeção de Tráfego de Rede (NDR) para 4Gbytes	Solução	1	R$ 1.450.000,00	R$ 1.450.000,00
7	Instalação e Configuração	Serviço	1	R$ 25.000,00	R$ 25.000,00
8	Suporte Técnico Mensal	Meses	36	R$ 6.500,00	R$ 234.000,00
9	Repasse de conhecimento para até 5 participantes	Turma	1	R$ 14.476,33	R$ 14.476,33
	TOTAL:				**R$ 3.645.894,65**

2.9 Natureza do objeto a ser contratado

2.9.1 O objeto da presente contratação pode ser precisamente especificado por meio de padrões usuais de mercado. Desta forma, entende-se que o objeto desta contratação é classificado como serviço comum para fins do disposto no art. 6º, inciso XIII, da Lei n 14.133/2021, podendo, portanto, ser contratado por meio de processo licitatório na modalidade Pregão, preferencialmente na forma eletrônica.

2.10 Conformidade técnica e legal do objeto

2.10.1 O presente Termo de Referência foi elaborado em conformidade com as seguintes normas:

2.10.1.1 Lei 14.133/2021, que regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos administrativos;

2.10.1.2 Resolução CJF n. 6/2008, alterada pela Resolução CF n. 687, de 15 de dezembro de 2020, que dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2º graus;

2.10.1.3 Portaria CJF n. 303/2018, que define as normas a serem seguidas no CJF, relativas à utilização de recursos de tecnologia da informação, de forma a minimizar os riscos à segurança da informação na instituição;

2.10.1.4 Portaria CNJ n. 162/2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); e

2.10.1.5 Portaria CJF n. 413/ 2014, que dispõe sobre a aprovação da Política de Controle Acesso Lógico, que veda a utilização de identificação genérica e de uso compartilhado para acesso aos recursos de rede.

2.11 Justificativa para o parcelamento ou não da solução de TIC

O objeto do certame não será parcelado, uma vez que os serviços técnicos especializados que compõe o objeto formam um conjunto indissociável, composto pela interligação dos serviços que funcionam harmonicamente.

As melhores práticas de implementação da solução se baseiam na integração dos serviços, que são indissociáveis e apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.

Somente a execução de forma integrada dos serviços garante a qualidade das entregas, evitando transferência de responsabilidades, nos casos de eventuais problemas causados por serviços prestados por mais de uma empresa contratada.

É importante, também, se observar o posicionamento do Egrégio Tribunal de Contas da União, nos autos do Acórdão n. 1916/2009 – Plenário, sobre a matéria:

15. Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 23, § 1º, da Lei n. 8.666/1993, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente viável. A respeito da matéria, esta Corte de Contas já editou a Súmula n. 247/2004, in verbis: "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das

licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes...” (grifos não constam do original).

Nesse toar, mencionamos o Acórdão TCU n. 5134/2014 – 2ª Câmara, de modo que a interpretação da Súmula 247 TCU e do art. 23, §1º da Lei n. 8.666/1993nãodeve ser feita de modo literal, já que itens de mesma natureza devem compor um único lote, não havendo restrição ao caráter competitivo do certame.

Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e econômica para a sua adoção.

Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: “O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória.” (Comentários à Lei de Licitações e Contratos Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209).

Ainda, de acordo com a Lei 14.133/2021 em seu art. 40 § 3°, as licitações de serviços atenderão ao princípio do parcelamento, quando for tecnicamente viável e economicamente vantajoso.

Portanto, em virtude da especificidade do objeto, pode-se afirmar ser tecnicamente inadequado o seu desmembramento, sob pena de não se atender o objetivo buscado, que é proporcionar maior celeridade e qualidade na implementação da solução de segurança da informação. Sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adoção do parcelamento do objeto, seria, no caso concreto, mais vantajosa para o CJF.

Tendo em vista que uma das necessidades de negócio definida para esta contratação consiste na interoperabilidade da solução de detecção e resposta avançada de incidentes e automação de respostas decorrente do correlacionamento dos dados recebidos pelos demais itens que compõem o objeto, não é possível contratar tais itens em separado. Neste caso, o parcelamento provocaria restrições de funcionalidade na interoperabilidade pretendida.

2.12 Permissão consórcio ou subcontratação da solução de TIC, justificando-se a decisão.

Fica vedado à CONTRATADA subcontratar, no todo ou em parte, os serviços de suporte técnico, objeto deste Termo de Referência. De maneira análoga, fica vedado a participação de consórcios, visto que a participação em consórcio não amplia o leque de concorrentes, apenas aumenta a complexidade administrativa da gestão contratual.

3 Forma e critério de seleção de fornecedor (art. 6º, XXIII, "h", lei n. 14.133/2021)

3.1 Modalidade e critério de julgamento

O objeto da licitação tem a natureza de serviço comum continuado, pois existe a necessidade de pleno funcionamento da solução visto a essencialidade dos serviços e atividades a serem executadas pelo CONTRATANTE, nos termos do art. 6º, inciso XV, da Lei n. 14.133/2021.

Caracteriza-se também como comum, pois os padrões de desempenho e de qualidade podem ser objetivamente definidos com base em especificações usuais no mercado, conforme Acórdão nº 2.471/2008-TCU-Plenário.

Entende-se que a presente contratação deverá ser processada na modalidade licitatória de **PREGÃO ELETRÔNICO**, com critério de julgamento por **MENOR PREÇO GLOBAL**.

3.2 Critérios de seleção do fornecedor (art. 6º, XXIII, "h", lei n. 14.133/2021)

3.2.1 O licitante que apresentar documentação em desacordo com este edital será inabilitado.

3.2.2 Quando da formulação de sua proposta, a licitante deverá especificar de forma clara, completa e minuciosa, todos os itens ofertados na Planilha de Preços.

3.2.3 Observar, quando da formulação de sua proposta, as especificações e características obrigatórias, não sendo permitida a oferta de preços alternativos ou a inclusão de condições que impeçam o julgamento objetivo da licitação.

3.2.4 A proposta deverá indicar, em qual página e item da documentação apresentada, está a comprovação do atendimento dos requisitos técnicos descritos no ANEXO I deste Termo de Referência. Não será aceita proposta sem a indicação na documentação técnica apresentada.

3.2.5 A proposta deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados, com descrição detalhada de cada item.

3.2.6 O valor total de cada item não poderá ser superior ao valor estimado no Edital, mesmo a licitante tendo proposto o menor preço global.

3.2.7 A LICITANTE vencedora deverá apresentar atestado(s) de capacidade técnica, que comprove(m) que a empresa LICITANTE tenha fornecido a contento, para órgãos ou entidades públicas ou privadas, solução de segurança abarcando os seguintes quantitativos:

i) 30 (trinta) licenças de proteção para *Data Center*;

ii) 290 (duzentos e noventa) licenças para proteção de estações de trabalho;

iii) 650 (seiscentos e cinquenta) licenças para proteção de serviço de *E-mail*; e

iv) 275 (duzentos e setenta e cinco) licenças para proteção de Microsoft 365.

3.2.7.1 Configura-se como parcela de maior relevância da presente contratação, em consonância com o que determina o §1º do art. 67 da Lei 14.133/2021, os itens 1.1, 1.2, 1.3 e 1.4 da tabela constante do item 1 deste Instrumento (Definição do objeto), por se tratarem do núcleo principal da solução desejada e estarem cotados com valor acima de 4% (quatro por cento) do valor total estimado da contratação em tela.

3.2.8 Não será aceito o somatório de atestados de capacidade técnica para fins de comprovação técnico-operacional dos licitantes, tendo em vista que é do interesse do Conselho da Justiça Federal que a Contratada seja capaz de atender a um ambiente com dimensões proporcionais ao atualmente em operação.

3.2.9 Deverão constar do(s) atestado(s) de capacidade técnica em destaque, os seguintes dados: identificação do emitente, especificação completa do fornecimento/serviço executado, prazo de vigência do contrato, local e data de expedição, data de início e término do contrato.

3.3 Margem de preferência

3.3.1 **Lei 8.248/1991 e Decreto 7.174/2010**: Não se aplica a Lei 8.248/1991, pois não há previsão em seu art. 16-A de serviços relacionados à contratação de solução de segurança de TI para proteção de servidores de rede, estações de trabalho, serviço de *e-mail* e Microsoft 365. Consequentemente, afasta-se a aplicação do Decreto 7.174/2010, o qual regulamenta a lei supracitada.

3.3.2 **Decreto 8.538/2015**: Não se aplica o referido decreto pois o tratamento diferenciado e simplificado para as microempresas e as empresas de pequeno porte não é vantajoso para a Administração Pública e pode representar prejuízo ao conjunto ou ao complexo do objeto a ser contratado, conforme mencionado no item 2.5 (Justificativa para o parcelamento ou não do objeto), uma vez que os serviços técnicos especializados que compõe o objeto formam um conjunto indissociável, composto pela interligação dos serviços que funcionam harmonicamente. Assim preconizado no Art. 10, inciso II, do normativo mencionado.

3.4 Vistoria

3.4.1 Caso a licitante deseje realizar vistoria, esta deverá ser realizada no Conselho da Justiça Federal (CJF), no Setor de Clubes Esportivos Sul - SCES - Trecho III - Polo 8 - Lote 9 - CEP 70200-003 - Brasília/DF;

3.4.2 A licitante poderá vistoriar o local onde serão executados os serviços até o último dia útil anterior à data fixada para a abertura da sessão pública, com o objetivo de inteirar-se das condições e grau de dificuldade existentes, mediante prévio agendamento de horário, com antecedência mínima de 48 (quarenta e oito) horas, junto a Secretaria de Tecnologia da Informação (STI) do CJF, pelos telefones (61) 3022-7400 e (61) 3022-7403, de 14 às 18 horas, limitada a realização da vistoria a um interessado por dia;

3.4.3 A vistoria poderá ser substituída por uma declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação. Não serão admitidas, em hipótese alguma, alegações posteriores de desconhecimento da complexidade dos serviços e de dificuldades técnicas não previstas;

3.4.4 Detalhes sobre o ambiente tecnológico do CJF serão apresentados durante a vistoria somente mediante assinatura de Termo de Confidencialidade e Sigilo da Contratada (Anexo IV), a ser preenchido e assinado pelo representante legal da empresa.

4 Modelo de execução e de gestão do contrato (art. 6º, XXIII, "f", lei n. 14.133/2021)

4.1 Vigência

03 (três) meses, contados da assinatura do contrato, para a execução, mediante a emissão da Ordem de Serviço, da entrega, instalação, configuração, transferência de conhecimento e recebimento definitivo dos itens que compõem a solução.

36 (trinta e seis) meses, prorrogáveis sucessivamente, até o limite de 10 (dez) anos, nos termos do art. 107 da Lei 14.133/2021, a partir do Recebimento Definitivo referente aos serviços de garantia e suporte técnico da solução de segurança, devido à natureza de serviços contínuos desta contratação.

4.1.1 Justificativa:

O período de vigência de 36 (trinta e seis) meses contínuos para execução dos serviços se dá, sobretudo para que a contratação seja atrativa pelo mercado, favorecendo a Administração em termos de economicidade e ampliação da competitividade. Deve-se considerar ainda que os serviços contínuos são imprescindíveis para garantir a segurança cibernética de estações de trabalho, *Data Center*, *e-mail* corporativo e aplicativos Microsoft 365 utilizados no ambiente computacional do CJF. Caso o serviço de proteção seja descontinuado, coloca-se em risco todos os dados armazenados e serviços utilizados pelo Conselho, podendo comprometer de forma severa a continuidade das atividades da Justiça Federal como um todo. Portanto, um período maior de vigência contratual também implica na mitigação de riscos para o CONTRATANTE.

Considerando que a vida útil dos componentes da solução é superior a 12 meses, pretende-se adquirir o suporte técnico pelo período de 36 meses, visando manter a continuidade e a operacionalidade da solução. É fortemente recomendável que os ativos de TI estejam cobertos por garantia e suporte técnico durante toda sua vida útil, de modo a garantir o máximo aproveitamento do investimento e manter sua disponibilidade tecnicamente assegurada.

Impende, ainda, assinalar que os ativos que integram solução de segurança cibernética são comumente contratados no setor privado com cobertura de serviços em caráter plurianual, considerando o tempo de vida útil da tecnologia empregada. Em âmbito governamental, esta prática é igualmente adotada, conforme se verifica nos excertos das Boas Práticas, Orientações e Vedações para Contratação de Ativos de TIC – Versão 4 do Ministério do Planejamento, Desenvolvimento e Gestão (disponível em https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf).

Ademais, cumpre mencionar que a solução de proteção para estações de trabalho, *Data Center*, *e-mail* corporativo e aplicativos Microsoft 365 se traduz em uma solução de missão crítica, a qual possui uma alta complexidade de instalação, a qual, na presente contratação, levará aproximadamente 3 meses, conforme Cronograma constante do Anexo II deste Termo de Referência. Isso reforça a característica plurianual de sua contratação, de modo que sua futura substituição, ao término de seu ciclo de vida útil, seja adequadamente planejada e operacionalizada por parte da Secretaria de tecnologia da Informação - STI.

Por fim, cabe destacar que a celebração ora proposta de 36 meses para a avença encontra-se aderente ao disposto no inciso I do art. 40 da Lei n. 14.133/2021, o qual estabelece que o planejamento de compras deverá observar as condições de aquisição e pagamentos semelhante às do setor privado.

4.2 Do reajuste

4.2.1 Após o interregno de um ano, contado da data do orçamento estimado pela administração, os preços iniciais do suporte técnico mensal poderão ser reajustados, mediante negociação entre as partes, tendo como referência o limite máximo a variação acumulada do Índice Nacional de Preços ao Consumidor Amplo/IPCA, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística/IBGE.

4.2.2 No primeiro reajuste, as PARTES atentarão para que o percentual a ser aplicado não seja superior à variação acumulada no período compreendido entre o mês do orçamento estimado, que foi realizado em agosto de 2023 e aquela em que se verificar no mês anterior ao aniversário deste orçamento.

4.2.3 Os reajustes seguintes serão calculados considerando-se a variação acumulada dos 12 (doze) últimos meses anteriores ao aniversário do orçamento.

4.2.4 Caso o índice estabelecido para delimitar o reajustamento dos preços seja extinto ou, de qualquer forma, não possa mais ser utilizado para esse fim, as partes desde já concordam que em substituição seja adotado o que vier a ser determinado pela legislação então em vigor.

4.2.5 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice para delimitar o reajustamento dos preços.

4.2.6 Incumbe à CONTRATADA a apresentação do pedido de reajuste acompanhado da respectiva memória de cálculo, a qual, após análise e aprovação pelo CONTRATANTE, redundará na emissão do instrumento pertinente ao reajuste contratual.

4.3 Obrigações contratuais da contratante e da contratada

4.3.1 Deveres e responsabilidades do CONTRATANTE

4.3.1.1 Acompanhar e fiscalizar a execução do objeto contratual.

4.3.1.2 Determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual.

4.3.1.3 Informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados.

4.3.1.4 Comunicar oficialmente quaisquer falhas e/ou anormalidades verificadas no cumprimento das obrigações contratuais à CONTRATADA.

4.3.1.5 Avaliar todos os serviços prestados pela CONTRATADA.

4.3.1.6 Responsabilizar-se pelos pagamentos dos serviços prestados pela CONTRATADA mediante a apresentação de Nota Fiscal.

4.3.1.7 Indicar os seus representantes para fins de contato e demais providências inerentes à execução do contrato.

4.3.1.8 Para os serviços inclusos no período de garantia do objeto e para a realização de suporte técnico, o CONTRATANTE permitirá o acesso dos técnicos habilitados e identificados da CONTRATADA às instalações onde se encontrarem os equipamentos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive àqueles referentes à identificação, trânsito e permanência em suas dependências.

4.3.2 Deveres e responsabilidades da CONTRATADA

4.3.2.1 Fornecer os softwares e equipamentos da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional do CONTRATANTE, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração.

4.3.2.2 Acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços objeto deste Termo de Referência.

4.3.2.3 Submeter à prévia aprovação do CONTRATANTE toda e qualquer alteração pretendida na prestação dos serviços.

4.3.2.4 Manter, durante a execução do contrato a ser firmado, as condições de habilitação e qualificação exigidas na licitação.

4.3.2.5 Sujeitar-se à fiscalização do CONTRATANTE, no tocante ao fornecimento e a prestação dos serviços, prestando todos os esclarecimentos solicitados e atendendo de imediato às reclamações fundamentadas, caso venham a ocorrer.

4.3.2.6 Prestar as atividades objeto da licitação, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos softwares e equipamentos da solução.

4.3.2.7 Indicar profissional que atuará, desde o início da execução do contrato até a conclusão da implantação, como Gerente de Projeto.

4.3.2.8 Propor os ajustes necessários à adequação, segurança e racionalização dos serviços prestados, respeitando o objeto deste Termo de Referência.

4.3.2.9 Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício da atividade objeto deste Termo de Referência.

4.3.2.10 Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação das penalidades previstas, caso os prazos e condições não sejam cumpridos.

4.3.2.11 Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de pagamentos adicionais ao CONTRATANTE ou a não prestação satisfatória dos serviços.

4.3.2.12 Guardar inteiro sigilo dos dados que tiver acesso, reconhecendo serem estes de propriedade exclusiva do CONTRATANTE.

4.3.2.13 Substituir imediatamente, a critério do CONTRATANTE, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado devidamente justificado.

4.3.2.14 A CONTRATADA será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato.

4.3.2.15 Sujeitar-se a mais ampla e irrestrita fiscalização, por parte da Equipe de Fiscalização e/ou Recebimento indicada pelo CONTRATANTE para acompanhamento da execução do contrato, prestando todos os esclarecimentos que lhes forem solicitados e atendendo às reclamações formuladas.

4.3.2.16 Comunicar a Equipe de Fiscalização e/ou Recebimento, por escrito, qualquer anormalidade que ponha em risco o fornecimento ou a execução dos serviços.

4.3.2.17 Corrigir as falhas detectadas pela Equipe de Fiscalização e/ou Recebimento indicada pelo CONTRATANTE.

4.3.2.18 Executar as atividades previstas no contrato em estrito cumprimento aos prazos previstos no ANEXO II – CRONOGRAMA DE IMPLANTAÇÃO, após a emissão de Ordem de Serviço pelo CONTRATANTE.

4.3.2.19 Cumprir as exigências de reserva de cargos previstas em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

4.4 Papéis a serem desempenhados durante a execução contratual

4.4.1 Pelo CONTRATANTE:

4.4.1.1 **Equipe de Fiscalização do Contrato**: os produtos e serviços objetos desta contratação serão fiscalizados por servidor ou comissão de servidores do Contratante, doravante denominados Fiscalização, que terá autoridade para exercer toda e qualquer ação de orientação geral, controle e fiscalização da execução contratual.

4.4.1.1.1 À Equipe de Fiscalização compete, dentre outras atribuições:

a) Solicitar à Contratada e seus prepostos, ou obter da Administração, tempestivamente, todas as providências necessárias ao bom andamento do contrato e anexar aos autos do processo correspondente cópia dos documentos escritos que comprovem essas solicitações de providências.

b) Manter organizado e atualizado um sistema de controle em que se registrem as

ocorrências ou os serviços descritos de forma analítica.

c) Acompanhar e atestar a prestação dos serviços contratados e indicar a ocorrência de inconformidade desses serviços ou não cumprimento do contrato.

d) Encaminhar à Secretaria de Administração os documentos para exame e deliberação sobre a possível aplicação de sanções administrativas.

4.4.1.1.2 A ação da Fiscalização não exonera a Contratada de suas responsabilidades contratuais.

4.4.2 Pela CONTRATADA:

4.4.2.1 Representante legal: pessoa formalmente designada e devidamente autorizada a firmar contrato em nome da Contratada.

4.4.2.2 Preposto: nomeado pelo representante legal no início da execução contratual, nos termos do art. 118 da Lei nº 14.133/21, que atuará como representante da Contratada durante a execução contratual. Deve ser apresentado, por ocasião da primeira reunião de planejamento, conforme Cronograma constante do Anexo II.

4.4.2.3 Gerente de Projetos: líder e responsável pela entrega dos serviços de planejamento e implantação da solução, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados no Edital. Deve ser apresentado, por ocasião da primeira reunião de planejamento, conforme Cronograma constante do Anexo II.

4.4.2.4 Responsável Técnico: funcionário da empresa responsável pela prospecção, elaboração e implantação da solução além de responder por questões técnicas atinentes à solução durante a execução contratual. Deve ser apresentado, por ocasião da primeira reunião de planejamento, conforme Cronograma constante do Anexo II.

4.5 Qualificação técnica dos profissionais da contratada

4.5.1 O Gerente de Projetos deve atender no mínimo aos seguintes requisitos:

4.5.1.1 Deve possuir escolaridade de nível superior completo;

4.5.1.2 Deve possuir certificação PMP – Project Management Professional do PMI – Project Management Institute ou possuir MBA – Master of Business Administration em Gerência de Projetos.

4.6 Dinâmica de execução contratual

4.6.1 Execução contratual:

4.6.1.1 A CONTRATADA deverá iniciar a execução das atividades de entrega, instalação e configuração dos softwares e equipamentos da solução a partir da emissão da Ordem de Serviço pelo CONTRATANTE, conforme ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.6.1.2 A CONTRATADA e o CONTRATANTE deverão realizar, **em até 3 (três) dias corridos** após a emissão da Ordem de Serviço, reunião de planejamento presencial na sede do CONTRATANTE ou por meio de reunião à distância, a ser acordado com o CONTRATANTE, com o objetivo de apresentar a metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução CONTRATADA, conforme ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.6.1.3 A CONTRATADA deverá apresentar o Plano de Implantação, em até 10 (dez) dias corridos da emissão da Ordem de Serviço, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos softwares e equipamentos da solução, conforme ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.6.1.4 A CONTRATADA deverá entregar todos os equipamentos, softwares e acessórios da solução no prazo máximo de até 45 (quarenta e cinco) dias corridos, a contar da data de emissão da Ordem de Serviço, conforme ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.6.1.5 Não será permitida a entrega parcial dos *softwares* e equipamentos, devendo a CONTRATADA entregar em sua totalidade o quantitativo solicitado na Ordem de Serviço emitida pelo CONTRATANTE, podendo a CONTRATADA incorrer em sanção contratual.

4.6.2 Plano de implantação:

4.6.2.1 A CONTRATADA deverá elaborar Plano de Implantação da solução contendo cronograma de execução das atividades, previsão de recursos, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação, contendo também os seguintes itens:

4.6.2.2 Descrição e detalhamento dos procedimentos para entrega, retirada das embalagens e conferência dos equipamentos, softwares e acessórios entregues.

4.6.2.3 Descrição e detalhamento das informações sobre as etapas de instalação física dos equipamentos incluindo distribuição dos equipamentos pelos racks, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e de endereçamento de gerência IP.

4.6.2.4 Proposta de interconexão física e lógica dos componentes da solução aos ativos rede do CONTRATANTE, observando as melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução.

4.6.2.5 Planejamento da engenharia de tráfego da solução com base nas melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução.

4.6.2.6 Descrição e detalhamento das condições de rollback de cada mudança no ambiente do CONTRATANTE para a instalação da solução.

4.6.2.7 Descrição e detalhamento das atividades de teste de operação da solução e planos de testes para os diversos componentes da solução que comprovem o funcionamento das regras e configurações aplicadas, bem como dos recursos de tolerância a falhas dos softwares e equipamentos da solução.

4.6.2.8 Descrição e detalhamento da transferência de conhecimento nos termos do item 4.6.6.

4.6.3 Serviço de instalação e configuração

4.6.3.1 As atividades de entrega, instalação e configuração dos softwares e equipamentos da solução deverão ocorrer na sede do CONTRATANTE. A entrega de produtos deverá ocorrer em dias úteis no período de 8:00 às 16:00 horas e os serviços de implantação ou quaisquer outros que possam causar instabilidade no ambiente de produção devem ser realizados em horários fora do expediente do órgão e previamente agendados com a Equipe de Fiscalização do Contrato;

4.6.3.2 O CONTRATANTE poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento dos serviços e sistemas em produção;

4.6.3.3 O processo de entrega, instalação e configuração dos componentes da solução deverá ser

acompanhado e supervisionado pela equipe técnica indicada pelo CONTRATANTE;

4.6.3.4 Entregar os equipamentos novos e 1º uso juntamente com todos os itens acessórios de hardware e de software necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interface, suportes, drivers de controle, programas de configuração, conforme especificações constantes no ANEXO I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO deste Termo de Referência;

4.6.3.5 Entregar os equipamentos devidamente protegidos e embalados, originais lacrados, sem danos de transporte e manuseio;

4.6.3.6 Entregar os equipamentos e softwares, às suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos;

4.6.3.7 Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização;

4.6.3.8 Caso a implantação de qualquer elemento da solução cause interferência na correta operação da rede de dados do CONTRATANTE, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar ao ambiente à condição anterior à implantação;

4.6.3.9 A execução dos serviços de entrega, instalação e configuração dos softwares e equipamentos da solução deverá contemplar, no mínimo, os seguintes itens:

4.6.3.9.1 Instalação física e ativação dos componentes da solução;

4.6.3.9.2 Integração à rede do CONTRATANTE, sem interrupção no funcionamento normal dos serviços de TI. Caso exista a necessidade de interrupção de qualquer equipamento ou serviço em produção para a integração da solução, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o CONTRATANTE;

4.6.3.9.3 Instalação e configuração dos softwares e funcionalidades exigidas na especificação técnica dos elementos que compõem a solução fornecida, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução mediante solicitação da equipe do CONTRATANTE;

4.6.3.9.4 Realização de testes de operação da solução que comprovem o funcionamento dos recursos de tolerância a falhas dos diversos componentes da solução, quando aplicável;

4.6.3.9.5 Atualização do Plano de Implantação com todas as informações que representem a topologia física e lógica e a configuração final aplicadas.

4.6.3.10 Os serviços e entregas serão executados no Conselho da Justiça Federal (CJF), no Setor de Clubes Esportivos Sul - SCES - Trecho III - Polo 8 - Lote 9 - CEP 70200-003 - Brasília/DF.

4.6.4 Serviço de suporte técnico

4.6.4.1 O serviço de suporte técnico para os softwares e equipamentos da solução deverá ser executado pela CONTRATADA, durante o prazo de 36 (trinta e seis) meses, contados a partir da data de emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos softwares e equipamentos da solução.

4.6.4.2 O serviço de suporte técnico da solução consiste em:

4.6.4.2.1 Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de

suporte, no local de instalação da solução, visando a solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução, permitindo o retorno à condição normal de operação.

4.6.4.2.2 Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, por meio de contato telefônico ou outro recurso de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução.

4.6.4.2.3 Realizar visitas técnicas preventivas no local de instalação da solução (on-site), com frequência mensal, e com duração de pelo menos 1 (uma) hora a cada visita, visando assegurar o melhor desempenho da solução.

4.6.4.2.4 Substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas.

4.6.4.3 O CONTRATANTE realizará a abertura de chamados técnicos de suporte por ligação telefônica, por *e-mail* ou via Internet, em período integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

4.6.4.4 A CONTRATADA deverá informar o procedimento para abertura de chamado técnico de suporte no documento Plano de Implantação.

4.6.4.5 Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em endereço eletrônico (WEB site) deverá estar disponível, também, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

4.6.4.6 Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, a CONTRATADA deverá informar o número do chamado, para fins de controle.

4.6.4.7 A CONTRATADA deverá enviar mensalmente, ou disponibilizar acesso por meio de portal internet, relação consolidada dos chamados abertos no mês, mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, problemas verificados, técnico responsável pelo atendimento.

4.6.4.8 A CONTRATADA deverá disponibilizar acesso a base de conhecimento do fabricante dos componentes da solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ’s, com pesquisa efetuada através de ferramentas de busca) e atualizações.

4.6.4.9 A CONTRATADA deverá realizar a cada ocorrência, como escopo das atividades de visitas técnicas preventivas, as tarefas de coleta e análise de logs dos produtos, realizar o levantamento de configurações aplicadas nos softwares e equipamentos da solução, buscando compará-las às melhores práticas e recomendações dos fabricantes, avaliar aspectos de segurança e desempenho da solução, finalizando com a elaboração de relatório técnico com as informações coletadas e as recomendações a serem aplicadas à solução.

4.6.4.10 As visitas técnicas preventivas deverão ser realizadas por técnico(s) plenamente qualificado(s), com certificação emitida pelos fabricantes dos softwares e equipamentos da solução ofertada, e deverão ser prestadas com acompanhamento da equipe técnica do CONTRATANTE.

4.6.4.11 A contagem de prazo para a realização das visitas técnicas preventivas será iniciada após emissão do Termo de Recebimento Definitivo, devendo ocorrer automaticamente em dia e hora previamente agendada com o CONTRATANTE e serão consideradas concluídas após o entrega do relatório técnico de atendimento e aceite pelo CONTRATANTE. A cada visita deverá ser gerado relatório técnico com sugestões e ajustes para a melhoria de desempenho,

funcionalidade e segurança.

4.6.4.12 A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CONTRATANTE, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações.

4.6.5 Níveis mínimos do serviço de suporte técnico

4.6.5.1 Quando da abertura de chamado técnico de suporte, os chamados deverão ser categorizados em 3 (três) níveis, da seguinte forma:

Criticidade	Descrição	Prazo máximo para início de atendimento (contados a partir da abertura do chamado)	Prazo máximo para restauração de serviço (contados a partir da abertura do chamado)
Severidade 1 (Alta)	Atuação ON-SITE em ocorrências que causem indisponibilidade ou restrição de funcionalidade da solução prejudicando a operação normal e que gerem impacto ao negócio.	Em até 1 (uma) hora deve ter um técnico da CONTRATADA ON-SITE.	Em até 3 (três) horas
Severidade 2 (Média)	Atuação REMOTA visando sanar problemas que criem restrições a operação normal da solução não gerando impacto ao negócio.	Em até 6 (seis) horas um técnico da CONTRATADA entra em contato.	Em até 12 doze) horas
Severidade 3 (Baixa)	Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução ou dúvidas de operação e configuração.	Em até 12 (doze) horas um técnico da CONTRATADA entra em contato.	Em até 36 (trinta e seis horas)

4.6.6 Transferência de conhecimento

4.6.6.1 A CONTRATADA deverá realizar a transferência de conhecimento, preferencialmente de forma remota, para a equipe técnica do CONTRATANTE por meio de treinamento nas tecnologias da solução com carga horária total de no mínimo 20 (vinte) horas.

4.6.6.2 O serviço de transferência de conhecimento será solicitado sob demanda, mediante de emissão de ordem de serviço específica para este serviço conforme ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.6.6.3 A transferência de conhecimento deverá iniciar no prazo máximo de 15 (quinze) dias corridos após a emissão da ordem de serviço específica para esta etapa conforme ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.6.6.4 O programa para a transferência de conhecimento deverá abordar as principais funcionalidades de administração e operação da solução e ser previamente aprovado pelo CONTRATANTE, e eventuais mudanças de conteúdo solicitadas deverão constar no material didático.

4.6.6.5 O material didático da transferência de conhecimento deverá ser disponibilizado em formato eletrônico, sem custo adicional para o CONTRATANTE, devendo ainda estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês),

tendo em vista que é comum soluções de Tecnologia da Informação serem desenvolvidas por empresas estrangeiras e material bilíngue.

4.6.6.6 Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária.

4.6.6.7 O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a emissão da Ordem de Serviço na primeira reunião de planejamento.

4.6.6.8 Caso a transferência de conhecimento não seja satisfatória com relação à profundidade do conteúdo apresentado ou domínio dos temas por parte do instrutor, a CONTRATADA deverá complementar, sem ônus adicional, o repasse dos pontos considerados pelo CONTRATANTE como insatisfatórios.

4.6.6.9 A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos softwares e equipamentos da solução ofertada.

4.7 Recebimento do objeto

4.7.1 Em conformidade com o artigo 140 da Lei n.º 14.133/21, o objeto deste contrato será aceito:

4.7.1.1 **Provisoriamente**, pelo responsável por seu acompanhamento e fiscalização, com verificação da conformidade dos equipamentos e serviços com as exigências contratuais, nos prazos estipulados no Anexo II;

4.7.1.2 **Definitivamente**, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais, conforme prazos estipulados no Anexo II.

4.7.2 A Equipe de Fiscalização do CONTRATANTE fará a emissão do Termo de Recebimento Provisório (TRP1) da etapa da entrega dos softwares e equipamentos da solução, em até 5 (cinco) dias corridos da comunicação da CONTRATADA, conforme descrito no cronograma do ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.3 A CONTRATADA deverá realizar a instalação e configuração dos softwares e equipamentos da solução e entrega das licenças de uso no prazo máximo de 15 (quinze) dias corridos, contados a partir da data de emissão do Termo de Recebimento Provisório (TRP1), conforme ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.4 A conclusão das etapas de instalação e configuração dos softwares e equipamentos da solução e entrega das licenças de uso deverá ser formalizada mediante comunicado escrito da CONTRATADA ao CONTRATANTE.

4.7.5 A Equipe de Fiscalização do CONTRATANTE fará a emissão do Termo de Recebimento Provisório (TRP2) da etapa de instalação e configuração dos softwares e equipamentos da solução em até 5 (cinco) dias corridos da comunicação da CONTRATADA, conforme descrito no cronograma do ANEXO II- CRONOGRAMA DE IMPLANTAÇÃO.

4.7.6 A Equipe de Fiscalização do CONTRATANTE fará a emissão do Termo de Recebimento Definitivo (TRD) da entrega, instalação, configuração e licenciamento da solução em até 10 (dez) dias corridos da emissão do Termo de Recebimento Provisório (TRP2), conforme descrito no cronograma do ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.7 A Equipe de Fiscalização do CONTRATANTE fará a emissão do Termo de Recebimento Provisório, mediante relatório detalhado, da etapa de prestação de serviços de suporte técnico em até 5 (cinco) dias corridos da ciência da relação consolidada dos chamados abertos no mês (item 4.6.4.7).

4.7.8 A Equipe de Fiscalização fará a emissão do Termo de Recebimento Definitivo, mediante Termo Circunstanciado, da etapa de prestação dos serviços de suporte técnico em até 10 (dez) dias corridos após a emissão do Termo de Recebimento Provisório aludido no item 4.7.7.

4.7.9 Na hipótese de ser verificada a impropriedade do objeto no ato da entrega/execução, a equipe de fiscalização rejeita-lo-á imediatamente, no todo ou em parte, sendo a Contratada notificada a proceder à regularização no prazo máximo de 20 (vinte) dias corridos após a verificação.

4.7.10 Havendo reincidência quanto à impropriedade do objeto no momento da entrega/execução retificadora, poderão ser aplicadas as sanções previstas contratualmente.

4.7.11 Após o recebimento provisório, a fiscalização avaliará as características do objeto, identificando eventuais problemas.

4.7.12 Estando em conformidade, será efetuado o Recebimento Definitivo.

4.7.13 Se, após o aceite provisório, constatar-se que o objeto foi entregue em desacordo com o contrato ou com a proposta, com incorreção, ou incompleto, serão interrompidos os prazos de recebimento e suspenso o pagamento após a notificação à Contratada, condição que será mantida até o saneamento da situação.

4.7.14 Quando houver entrega de bem ou material em desacordo com o especificado neste Termo de Referência, no Instrumento Convocatório, no Contrato ou com defeito, será rejeitado parcial ou totalmente, conforme o caso, e a Contratada será obrigada a substituí-los dentro do prazo contratual, sob pena de se considerar atraso na entrega.

4.7.15 A Contratada ficará obrigada a trocar, a suas expensas, o bem ou material que vier a ser recusado.

4.7.16 A Contratada deverá retirar o bem ou material recusado no momento da entrega do bem ou material correto. O Conselho da Justiça Federal não se responsabilizará por qualquer dano ou prejuízo que venha a ocorrer após esse prazo.

4.7.17 Será considerado abandonado o bem ou material que não for recolhido pela Contratada em até 30 dias após a comunicação do CONTRATANTE.

4.7.18 A Administração poderá dar a destinação que julgar conveniente ao bem ou material abandonado em suas dependências.

4.7.19 A Contratada deverá entregar todo o bem ou material discriminado no contrato, não havendo pagamento em caso de entrega parcial até que ocorra o adimplemento da obrigação.

4.7.20 Independentemente da aceitação, a CONTRATADA garantirá a qualidade do serviço ou bem fornecido pelo prazo estabelecido contratualmente, obrigando-se a reparar aquele que apresentar incorreções ou defeito no prazo estabelecido pelo CONTRATANTE.

4.7.21 O aceite provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança d o serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos por lei ou pelo contrato.

4.7.22 A entrega do objeto pela CONTRATADA e seu recebimento pelo CJF não implicam sua aceitação definitiva, que será caracterizada pelo ateste da nota fiscal/fatura correspondente;

4.8 **Critérios de medição e pagamento** (art. 6º, XXIII, "g", lei n. 14.133/2021)

4.8.1 A CONTRATADA deverá emitir Notas Fiscais/Faturas relativas aos valores dos *softwares* e equipamentos da solução e garantia por 36 (trinta e seis) meses, serviços de instalação e configuração

e serviço de transferência de conhecimento após receber cópia do Termo de Recebimento Definitivo previsto no ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO.

4.8.2 O pagamento do serviço de suporte técnico será efetuado mensalmente, sendo iniciado somente após o Recebimento Definitivo da solução, mediante envio da Nota Fiscal/Fatura pela CONTRATADA.

4.8.3 O pagamento será efetuado, por ordem bancária, mediante a apresentação de nota fiscal correspondente ao fornecimento do bem/execução do serviço, devidamente atestada pela equipe de fiscalização do contrato, devendo ser emitida, obrigatoriamente, pelo CNPJ da Contratada.

4.8.4 As notas fiscais deverão ser encaminhadas aos *e-mails* indicados pelo gestor do contrato ou peticionadas no sistema SEI.

4.8.5 No corpo da nota fiscal deverá ser especificado o objeto contratado, o período faturado no formato dia/mês/ano, os quantitativos dos itens, quando couber, e a identificação da respectiva nota de empenho.

4.8.6 Recebida a nota fiscal, o gestor do contrato deverá atestá-la em até 5 (cinco) dias úteis e encaminhá-la à área financeira para:

a) liquidação da despesa, a contar do recebimento da nota fiscal, no prazo de:

a.1) **5 (cinco) dias úteis**, nos casos dos valores que não ultrapassem o limite de que trata o inciso II do art. 75 da Lei n. 14.133/2021;

a.2) **10 (dez) dias úteis**, nos demais casos.

b) pagamento da despesa, a contar da liquidação da despesa, no prazo de:

b.1) **5 (cinco) dias úteis**, nos casos dos valores que não ultrapassem o limite de que trata o inciso II do art. 75 da Lei n. 14.133/2021;

b.2) **10 (dez) dias úteis**, nos demais casos.

4.8.7 Os prazos de que trata o item 4.8.6 “a”, poderão ser excepcionalmente prorrogados, justificadamente, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

4.8.8 O prazo para a solução, pela CONTRATADA, de inconsistências na execução do objeto ou de saneamento da nota fiscal, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins de que trata o item 4.8.6, “a”.

4.8.9 Na hipótese de caso fortuito ou força maior que impeça a liquidação ou o pagamento da despesa, o prazo para o pagamento será suspenso até a sua regularização, devendo ser mantida a posição da ordem cronológica em que a despesa originalmente estava inscrita.

4.8.10 A fim de que o CONTRATANTE possa efetuar o pagamento, a CONTRATADA deverá apresentar nota fiscal constando a indicação do banco, da agência e do número da conta corrente onde deverá ser efetuado o crédito;

4.8.11 O CONTRATANTE, no momento do pagamento, providenciará as devidas retenções tributárias, nos termos da legislação vigente, exceto nos casos em que a CONTRATADA comprovar, na forma prevista em lei, não lhe serem aplicáveis tais retenções.

4.8.12 Em caso de eventual atraso de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, o valor faturado será atualizado monetariamente pelo percentual “*pro rata temporis*” do Índice de Preço ao Consumidor Amplo - IPCA conhecido quando do faturamento, compreendido entre a data limite estipulado para pagamento e aquela em que se der o efetivo

pagamento.

4.9 Adequação orçamentária (art. 6º, XXIII, "j", lei n. 14.133/2021)

A despesa em questão está prevista no Plano Anual de Contratações de 2023 do Conselho da Justiça Federal (item 71) e no Plano Orçamentário Ações de Informática 2023, sob a natureza de despesa detalhada 3.3.90.40.07 (Manutenção Corretiva/Adaptativa e Sustentação Softwares).

4.10 Glosas

4.10.1 O não cumprimento dos níveis de qualidade do Serviço de Suporte Técnico por ocorrência, independentemente das Sanções Administrativas previstas no Contrato, implicará em redutor sobre o valor mensal do serviço de suporte técnico (glosa), nos seguintes casos:

4.10.1.1 **Glosa de 10% (dez por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela não resolução dos chamados com severidade alta, limitada até 06 (seis) horas de atraso.

4.10.1.2 **Glosa de 5% (cinco por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela não resolução dos chamados com severidade média, limitada até 10 (dez) horas de atraso.

4.10.1.3 **Glosa de 1% (um por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela não resolução dos chamados com severidade baixa, limitada até 30 (trinta) horas de atraso.

4.10.1.4 **Glosa de 10% (dez por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, no início do atendimento dos chamados com severidade alta, limitada até 02 (duas) horas de atraso, a partir desse prazo será aplicada a glosa por atraso na resolução do chamado.

4.10.1.5 **Glosa de 5% (cinco por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, no início do atendimento dos chamados com severidade média, limitada até 06 (cinco) horas de atraso, a partir desse prazo será aplicada a glosa por atraso na resolução do chamado.

4.10.1.6 **Glosa de 1% (um por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, no início do atendimento dos chamados com severidade baixa, limitada até 24 (vinte e quatro) horas de atraso, a partir desse prazo será aplicada a glosa por atraso na resolução do chamado.

4.10.2 Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação das glosas previstas, a cada nova ocorrência a CONTRATADA sofrerá primeiramente a Sanção Administrativa de advertência citada no item 4.11.1.1.

4.10.3 No caso de reincidência, aplicar-se-á a respectiva penalidade de mora prevista no item 4.11, a depender do caso.

4.10.4 A aplicação da glosa servirá ainda como indicador de desempenho da CONTRATADA na execução dos serviços

4.10.5 O faturamento do serviço de suporte técnico deverá ser mensal, mediante apresentação de nota de cobrança consolidada para todos os softwares e equipamentos da solução, já descontadas as glosas eventualmente aplicadas em função do não atendimento dos níveis de qualidade definidos no contrato,

determinando o valor total do serviço para o mês.

4.10.6 No caso de aplicação de glosa referente à demora na conclusão de chamados do mesmo nível de severidade, para qualquer componente da solução, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses, serão aplicadas as sanções administrativas previstas no contrato.

4.10.7 No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela Área Administrativa.

4.10.8 Se a decisão da Administração for favorável ao recurso da CONTRATADA, a mesma emitirá a nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado.

4.10.9 A nota de cobrança emitida pela CONTRATADA deverá ser atestada pelo Gestor do Contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas.

4.11 Sanções

4.11.1 No caso de atraso injustificado ou inexecução total ou parcial do compromisso assumido com o CJF, as sanções administrativas aplicadas à Contratada serão:

4.11.1.1 **Advertência**;

4.11.1.2 **Multa de mora**, nos seguintes termos:

4.11.1.2.1 Multa moratória no percentual correspondente a **0,05% (cinco centésimos por cento)**, calculada sobre o valor total da contratação, por dia de atraso na entrega do plano de implantação e da apresentação do preposto, gerente de projetos e responsável técnico, além do prazo máximo definido no ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO, até o limite de 30 (trinta) dias corridos, a partir do qual poderá ficar caracterizada a inexecução total ou parcial do contrato.

4.11.1.2.2 Multa moratória no percentual correspondente a **0,1% (um décimo por cento)**, calculada sobre o valor total da contratação, por dia de atraso na entrega de todos os equipamentos e *softwares* que compõem a solução, além do prazo máximo definido no ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO, até o limite de 30 (trinta) dias corridos, a partir do qual poderá ficar caracterizada a inexecução total ou parcial do contrato.

4.11.1.2.3 Multa moratória no percentual correspondente a **0,1% (um décimo por cento)**, calculada sobre o valor total da contratação, por dia de atraso na conclusão da etapa de instalação e configuração da solução, além dos prazos máximos definidos no ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO até o limite de 30 (trinta) dias corridos, a partir do qual poderá ficar caracterizada a inexecução total ou parcial do contrato.

4.11.1.2.4 Multa moratória no percentual correspondente a **2% (dois por cento)**, calculada sobre o valor total do serviço de transferência de conhecimento, por dia de atraso na conclusão do serviço de transferência de conhecimento além do prazo estipulado no cronograma do ANEXO II - CRONOGRAMA DE IMPLANTAÇÃO, até o limite de 30 (trinta) dias corridos. Após o limite estabelecido, incidirá mais 20 (vinte) vezes o valor da sanção prevista na cláusula 4.11.1.2.7.

4.11.1.2.5 Multa moratória no percentual correspondente a **1% (um por cento)**, por dia de atraso, até o limite de 30 (trinta) dias corridos, calculada sobre o valor da garantia

contratual, no caso de atraso injustificado na sua entrega, nos termos do item 4.14 (Garantia Contratual). Após o limite estabelecido, incidirá mais 100 (cem) vezes o valor da sanção prevista na cláusula 4.11.1.2.7.

4.11.1.2.6 Multa moratória no percentual correspondente a **0,1% (um décimo por cento)**, calculada sobre o valor total da contratação, por dia de atraso, no caso de descumprimento das obrigações referentes a reparação de falhas de funcionamento dos componentes da solução previstas no serviço de garantia da solução, até o limite de 30 (trinta) dias corridos. Após o limite estabelecido, incidirá mais 150 (cento e cinquenta) vezes o valor da sanção prevista na cláusula 4.11.1.2.7

4.11.1.2.7 Multa por mora no percentual correspondente a **0,006% (seis milésimos por cento)**, calculada sobre o valor total da contratação, por dia/hora de atraso no cumprimento de quaisquer obrigações previstas em contrato e não arroladas acima, até o limite de 30 (trinta) dia/horas corridas(os).

4.11.1.3 **Multa compensatória** de:

4.11.1.3.1 **20% (vinte por cento)**, calculada sobre o custo mensal fixo da contratação, por ocorrência, no caso de aplicação de glosa referente ao mesmo indicador de Nível Mínimo de Serviço, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intercalados durante um período de 12 (doze) meses. Após a 5ª (quinta) aplicação desta sanção ao longo da execução contratual, poderá ser considerado inexecução parcial do contrato;

4.11.1.3.2 **30% (trinta por cento)** sobre o valor da contratação, em caso de inexecução total das obrigações contratuais;

4.11.1.3.3 **10% (dez por cento)** sobre o valor da contratação, em caso de inexecução parcial das obrigações contratuais.

4.11.1.3.4 O valor da multa compensatória não poderá ser inferior a 0,5% do valor total do contrato, conforme previsto no art. 156, § 3º, da Lei 14.133/2021.

4.11.1.4 **Impedimento de licitar e contratar com a Administração** pelo prazo de até 3 (três) anos;

4.11.1.5 **Declaração de inidoneidade** para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

4.11.2 A inexecução total ou parcial do contrato poderá acarretar a sua rescisão, conforme previsto neste instrumento e no art. 115 da Lei nº 14.133/2021, bem como a incidência das consequências legais cabíveis, inclusive indenização por perdas e danos, eventualmente causados ao CONTRATANTE.

4.11.3 A não manutenção das condições de habilitação da CONTRATADA ao longo da execução do contrato poderá ensejar a RESCISÃO CONTRATUAL UNILATERAL pelo Conselho da Justiça Federal após regular procedimento administrativo, resguardado à CONTRATADA o direito ao contraditório e à ampla defesa, e ainda a aplicação de **multa de 10% (dez por cento)** sobre o valor da contratação.

4.11.4 O valor da multa, aplicada após regular processo administrativo, seguirá a seguinte ordem de execução:

a) Descontado dos pagamentos devidos pelo CONTRATANTE à CONTRATADA; ou

b) Executado da Garantia Contratual; ou

c) Recolhido pela contratada mediante pagamento de GRU; ou

d) Cobrado Judicialmente.

4.11.5 O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a CONTRATADA, nos termos da Lei n. 14.133/2021.

4.11.6 As penalidades serão obrigatoriamente registradas no SICAF e sua aplicação será precedida da concessão da oportunidade de ampla defesa para o adjudicatário, na forma da lei.

4.11.7 Eventual pedido de prorrogação deverá ser encaminhado ao CJF preferencialmente na forma eletrônica.

4.11.8 **Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério do CONTRATANTE.**

4.12 Local da execução contratual

4.12.1 A entrega do objeto constante da Ordem de Serviço será realizada nas dependências do respectivo CONTRATANTE, em dias úteis em que houver expediente, das 8:00 às 16:00 horas.

4.12.2 Os serviços de implantação ou quaisquer outros que venham a causar instabilidade no ambiente de produção deverão ser previamente agendados com a Equipe de Fiscalização do Contrato e deverão ser executados, preferencialmente, fora do horário de expediente do órgão.

4.12.3 A entrega dos equipamentos, softwares e qualquer acessório que componha o objeto, bem como a realização dos serviços de garantia e suporte previstos neste contrato deverão ser realizados na sede do CONTRATANTE, conforme relação abaixo:

4.12.4 Conselho da Justiça Federal: Setor de Almoxarifado, localizado no Setor de Clubes Esportivos Sul Trecho 3 – Polo 8 – Lote 9 - Brasília / DF, CEP 70200-003 – Telefone 3022-7000;

4.13 Informações acerca da análise/ impacto ambiental decorrente da contratação

4.13.1 A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao CJF por ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas ao software e ainda aos serviços elencados no presente Termo de Referência;

4.13.2 A CONTRATADA deverá, para a execução do contrato, fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços, conforme disposto no art. 6°, inciso IV, da Instrução Normativa SLTI/MPOG n. 01, de 19 de janeiro de 2010;

4.13.3 A CONTRATADA deverá se atentar às normas em vigor atinentes à sustentabilidade expressas na 2ª edição do Manual de Sustentabilidade de compras e contratos do Conselho da Justiça Federal, instituído pela Portaria CJF n. 96, de 10 de fevereiro de 2023;

4.13.4 A CONTRATADA deverá respeitar a legislação vigente e as normas técnicas, elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade e acessibilidade do software e ainda dos serviços elencados neste Termo de Referência.

4.14 Garantia contratual

4.14.1 A CONTRATADA deverá apresentar garantia de execução em uma das modalidades previstas no art. 96 da Lei no 14.133/2021, em valor correspondente a 5% (cinco por cento) do valor

inicial/anual do contrato, em até 20 (vinte) dias úteis, contados da XXXX.

4.14.2 Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a execução do contrato e por 90 dias após o término da vigência contratual, e permanecerá em vigor mesmo que a CONTRATADA não pague o prêmio nas datas convencionadas.

4.14.2.1 Caso não seja apresentada a apólice de seguro-garantia no prazo estabelecido em Edital, será aplicada a penalidade prevista no item 4.11.1.2.5 deste termo.

4.14.2.2 A apólice do seguro garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

4.14.2.3 Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto art. 96, § 2o, da Lei 14.133/2021.

4.14.3 Caso utilizada outra modalidade de garantia, somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

4.14.4 Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, a CONTRATADA ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

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

a) prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

b) prejuízos causados à Administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

c) multas moratórias e punitivas aplicadas pela Administração à CONTRATADA;

d) obrigações e ações trabalhistas, previdenciárias e para com o FGTS e sua respectiva multa, não adimplidas pela CONTRATADA, quando couber.

4.14.6 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

4.14.7 A garantia em dinheiro deverá ser efetuada em favor do CONTRATANTE, em conta específica na Caixa Econômica Federal, com correção monetária, conforme disposto no Decreto- Lei 1.737, de 20 de dezembro de 1979.

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

4.14.9 No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

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

4.14.11 Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 20 (vinte)

dias úteis, contados da data em que for notificada.

4.14.12 O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

4.14.13 Será considerada extinta a garantia com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

4.14.14 O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

4.14.15 A CONTRATADA autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no contrato.

4.14.16 Os emitentes das garantias previstas nesta cláusula deverão ser notificados pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais, nos termos do §4o do art. 137 da Lei n. 14.133/2021.

4.14.17 Para efeitos da execução da garantia, os inadimplementos contratuais deverão ser comunicados pelo CONTRATANTE à CONTRATADA e/ou à Instituição Garantidora, no prazo máximo de 90 (noventa) dias após o término de vigência do contrato.

4.15 **Confidencialidade de informações** (art. 32, § 2º, lei n. 14.133/2021)

4.15.1 A CONTRATADA compromete-se a manter em caráter confidencial, mesmo após a eventual rescisão do contrato, todas as informações a seguir especificadas:

4.15.2 Política de segurança adotada pelo CJF e pelos órgãos da Justiça Federal e as configurações de hardware e software relacionadas.

4.15.3 Processo de instalação, configuração e customizações de produtos, ferramentas e os itens constantes do(s) objeto(s).

4.15.4 Qualquer informação do CONTRATANTE que venha tomar conhecimento em razão da execução dos serviços.

4.15.5 A CONTRATADA deverá concordar e assinar Termo de Confidencialidade especificado no Anexo IV.

Autenticado eletronicamente por **Nelio Alves da Silva**, **Chefe - Seção de Segurança de Rede** , em 15/01/2024, às 17:12, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

Autenticado eletronicamente por **Ricardo Rodrigues Loiola**, **Subsecretário(a) - Subsecretaria de Segurança da Tecnologia da Informação**, em 15/01/2024, às 17:35, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

Autenticado eletronicamente por **Michael da Silva Placido**, **Diretor(a) - Divisão de Governança das Contratações**, em 15/01/2024, às 17:46, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

ANEXO I

DETALHAMENTO DOS REQUISITOS TÉCNICOS DO OBJETO

1. Funcionalidades gerais

1.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução.

1.2. Deve permitir atualização incremental da lista de definições de vírus.

1.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável.

1.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines.

1.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas.

1.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento.

1.7. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pelo console de administração da solução completa.

1.8. Deve possibilitar instalação "silenciosa".

1.9. Deve permitir o bloqueio por nome de arquivo.

1.10. Deve permitir o rastreamento e bloqueio de infecções.

1.11. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks.

1.12. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho.

1.13. Deve desinstalar automática e remotamente a solução de anti-*malware* atual, sem requerer outro

software ou agente.

1.14. Deve permitir a desinstalação através do servidor ou console de gerenciamento da solução.

1.15. Deve possuir a possibilidade de exportar e importar configurações da solução.

1.16. Deve permitir a geração de backup ou snapshots da base de dados e dos demais componentes (Chaves Criptográficas) através do console de gerenciamento.

1.17. Deve possuir a possibilidade de determinar a capacidade ou prazo de armazenamento da área de quarentena.

1.18. Deve permitir a deleção dos arquivos quarentenados.

1.19. Deve permitir remoção automática de clientes inativos por determinado período.

1.20. Deve permitir integração com Active Directory para acesso ao console de administração.

1.21. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-*malware* instalada.

1.22. Deve permitir criação de diversos perfis e usuários para acesso ao console de administração.

1.23. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de anti-*malware*, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante.

1.24. Deve permitir agrupamento automático de estações de trabalho e notebooks no console de gerenciamento baseando-se no escopo do Active Directory ou IP.

1.25. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento.

1.26. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento do console de anti-*malware*.

1.27. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento do console de anti-*malware* não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias.

1.28. Deve prover segurança através de SSL para as comunicações entre o servidor e o console de gerenciamento web ou console MMC.

1.29. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção.

1.30. Deve permitir o logon integrado ao Active Directory, mesmo que existam múltiplas florestas ou relações de confiança entre os domínios.

1.31. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de anti-*malware* e o controlador de domínio.

1.32. Deve permitir a criação de usuários locais de administração no console de anti-*malware*.

1.33. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração do console de anti-*malware*.

1.34. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e

customizados a diferentes partes do console de gerenciamento.

1.35. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador.

1.36. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks.

1.37. Deve permitir a gerência de domínios separados para usuários previamente definidos.

1.38. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido no console de administração.

1.39. Deve possuir capacidade de habilitar automaticamente uma política de defesa caso ocorra uma epidemia na rede (baseado em quantidade de ataques encontrados em determinado intervalo de tempo), em uma arquitetura considerando agente único.

1.40. O administrador do sistema de segurança deve possuir a possibilidade de aplicar a proteção para as vulnerabilidades, escolhendo o perfil ou o host.

1.41. Será permitida a composição de soluções para atendimento das funcionalidades previstas nestas especificações.

2. Proteção antimalware para estações de trabalho Microsoft Windows

2.1. A solução deve atender a 550 (quinhentos e cinquenta) estações de trabalho e 60 (sessenta) estações de trabalho VMware Horizon VDI com sistema operacional Windows.

2.2. Deve ser capaz de realizar a proteção a códigos maliciosos nos sistemas operacionais:

2.2.1. Microsoft Windows 10 e versões superiores.

2.3. Suportar as seguintes plataformas virtuais:

2.3.1. VMware Horizon 8 e versões superiores;

2.3.2. VMware Vsphere ESXi 7 e versões superiores.

2.4. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

2.4.1. Processos em execução em memória principal (RAM);

2.4.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

2.4.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

2.4.4. Arquivos recebidos por meio de programas de comunicação instantânea tais como Whatsapp, Telegram, Facebook Messenger, Microsoft Teams, Zoom, Google Meet;

2.4.5. Arquivos recebidos a partir de sites Web;

2.4.6. Arquivos acessados ou recebidos por *e-mail*.

2.5. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

2.5.1. Em tempo real de arquivos acessados pelo usuário;

2.5.2. Em tempo real dos processos em memória, para a captura de programas maliciosos

executados em memória, sem a necessidade de escrita de arquivo;

2.5.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

2.5.4. Por linha-de-comando parametrizável;

2.5.5. Automáticos do sistema com as seguintes opções:

a) Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
b) Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
c) Frequência: horária, diária, semanal e mensal;
d) Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

2.6. Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).

2.7. Deve ser compatível com o Centro de Alertas e Segurança (Windows Security Center ou Action Center), possibilitando que o serviço identifique a presença de todos os módulos da solução instalada no endpoint.

2.8. Deve permitir a Integração com o *Antimalware Scan Interface* da Microsoft (AMSI).

2.9. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais.

2.10. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, *spyware*, *worms*, cavalos de tróia, *key loggers*, programas de propaganda, *rootkits*, *phishing*, dentre outros.

2.11. Deve utilizar mecanismos de proteção específicos contra ataques *ransonware*.

2.12. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex.

2.13. Deve possuir detecção heurística de vírus desconhecidos.

2.14. Deve permitir a configuração de otimização de verificação visando reduzir o consumo de CPU utilizada na varredura.

2.15. Deve possuir mecanismo de cache de informações dos arquivos já escaneados.

2.16. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada.

2.17. Deve permitir a utilização de Centro de Inteligência de reputação para análise de arquivos, de modo a prover, rápida detecção de novas ameaças.

2.18. Em caso de problemas com a conectividade com o Centro de Inteligência, ele deve manter uma base local para consulta de no mínimo hash de arquivos.

2.19. Deve ser capaz de detectar variantes de *malwares* que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça.

2.20. Deve ser capaz de bloquear o acesso a categorias maliciosas de sites web, inclusive as que não foram previamente categorizadas pelo fabricante.

2.21. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança.

2.22. Deve permitir a adição às listas de exclusão/arquivos conhecidos de modo a evitar novas detecções dos arquivos no ambiente de gestão da solução de endpoint.

2.23. Deve possuir capacidade nativa de envio de artefatos suspeitos ou de baixa reputação para análise de ameaças avançadas apresentando como resultado as seguintes informações:

2.23.1. Processos executados;

2.23.2. Modificações de Arquivos de Sistema;

2.23.3. Serviços criados e modificados;

2.23.4. Atividade de Rede Suspeita;

2.23.5. Modificações de Registros.

2.24. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total.

2.25. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão.

2.26. Deve permitir habilitar ou desabilitar o funcionamento dos seguintes dispositivos externos, no mínimo:

2.26.1. Discos de armazenamento locais;

2.26.2. Armazenamento removível;

2.26.3. Impressoras;

2.26.4. Modems;

2.26.5. Dispositivos de fita;

2.26.6. Dispositivos multifuncionais;

2.26.7. Leitores de smart card;

2.26.8. Wi-Fi;

2.26.9. Adaptadores de rede externos;

2.26.10. Dispositivos MP3 ou smartphones;

2.26.11. Dispositivos Bluetooth;

2.26.12. Câmeras e Scanners.

2.27. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB), mesmo que não haja permissão de escrita no dispositivo.

2.28. Deve possuir funcionalidade de “Machine Learning” utilizando como fonte de aprendizado a rede de inteligência do fabricante, identificando os aspectos maliciosos, características de boa pontuação e correlacionando, no mínimo, com as seguintes técnicas de proteção a vetores de

ataque:

2.28.1. Reputação de URL para exploração de navegadores, websites infectados e Office Exploits;

2.28.2. Reputação de arquivos para downloads de arquivos e anexos de e-mail.

2.28.3. Execução do instalador de software com classificação comportamental do instalador;

2.28.4. Execução do *malware* de software com classificação comportamental do instalador.

2.29. A funcionalidade de "Machine Learning" deve trabalhar baseado no mínimo nas seguintes premissas:

2.29.1. Office Exploits com reputação de URL;

2.29.2. Atualização da base de reputação das URLs com a periodicidade mínima de 1 hora;

2.29.3. Bloqueio de URLs de má reputação;

2.29.4. Bloqueio das instruções de Command & Control;

2.29.5. Atualização da base de reputação de Arquivos com a periodicidade mínima de 1 hora;

2.29.6. Bloqueio de ameaças polimorfas mesmo em arquivos desconhecidos;

2.29.7. Prevenção de Falso Positivos;

2.29.8. Bloqueio de *malwares* desconhecidos e suas variantes;

2.29.9. Implementar a classificação comportamental dos arquivos;

2.29.10. Aprendizado a partir dos indicadores de compromisso (IoC).

2.30. A funcionalidade de "Machine Learning" deve possuir a capacidade de implementar uma análise em tempo real correlacionando entre:

2.30.1. Veredicto das análises entre usuários da plataforma de segurança do mesmo fabricante;

2.30.2. Arquivos de softwares mundialmente espalhados na rede mundial de computadores;

2.30.3. Sites Web mundialmente espalhados pela rede mundial de computadores.

2.31. Deve ser capaz de correlacionar eventos entre computadores na rede (IoC Scanning).

2.32. Deve ser capaz de identificar e sinalizar ocorrências de elevação de privilégios.

2.33. Deve oferecer suporte ao envio de até 100 objetos diariamente para análise no ambiente de sandbox.

2.34. Deve ter a capacidade de coletar informações forenses do endpoint, abrangendo:

2.34.1.1.Dados;

2.34.1.2.Estado do sistema operacional;

2.34.1.3.Processos iniciados;

2.34.1.4.Conexões estabelecidas;

2.34.1.5.Arquivos criados;

2.34.1.6.Registro modificado;

2.34.1.7.Tentativas de conexão com um host remoto.

2.35. Deve ser capaz de executar tarefas para todo o ambiente e para dispositivos específicos, contendo, no mínimo, as capacidades abaixo:

2.35.1.1.Parar um processo;

2.35.1.2.Excluir um objeto;

2.35.1.3.Quarentenar um arquivo;

2.35.1.4.Recuperar um arquivo;

2.35.1.5.Prevenir a execução de um arquivo;

2.35.1.6.Executar um script ou investigar ameaças em memória;

2.35.1.7.Isolar o host;

2.35.1.8.Gerar Dump de memória;

2.35.1.9.Executar análise forense do disco;

2.35.1.10. Buscar chaves de registros;

2.35.1.11. Coletar informações de NTFS;

2.35.1.12. Criar Imagem do disco.

2.36. Deve disponibilizar visibilidade sobre o controle de aplicativos acessados pelos usuários nos endpoints.

3. Proteção antimalware para estações de trabalho Linux

3.1. A solução deve atender a 30 estações de trabalho Linux.

3.2. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais, no mínimo:

3.2.1. Ubuntu Linux 20.04 e versões superiores;

3.2.2. Suse Linux Enterprise;

3.3. Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).

3.4. O console de gerenciamento deve ser on-premises, permitindo o gerenciamento das políticas de segurança através da Internet.

3.5. A solução de proteção deve ser integrada ao sistema operacional através de módulos existentes do sistema operacional (Kernel Hook ou Fanotify).

3.6. Varredura manual, personalizável, com opção de limpeza dos *malwares* encontrados.

3.7. Varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais.

3.8. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, *spyware*, *worms*, cavalos de tróia, *key loggers*, programas de propaganda, *rootkits*, *phishing*, dentre outros.

3.9. O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço IP do cliente e ação realizada.

3.10. Geração de cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve

ser permitido somente pela solução de segurança ou o administrador.

3.11. A desinstalação do cliente nas estações de trabalho deve ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados.

3.12. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 06 (seis) níveis recursivos de compactação.

4. Solução de segurança para proteção para *Data Center*

4.1. A solução de deve atender a um ambiente de 60 (sessenta) *sockets* ou 30 (trinta) hosts, os quais são equivalentes.

4.2. Deve ser compatível com pelo menos os seguintes sistemas operacionais nas versões indicadas e versões superiores:

4.2.1. Suse Linux Enterprise 12;

4.2.2. CentOS 7;

4.2.3. Windows Server 2008;

4.2.4. Ubuntu 18;

4.2.5. Debian GNU/Linux 9;

4.2.6. Red Hat Enterprise Linux Server 7.3.

4.3. Suportar as seguintes plataformas virtuais:

4.3.1. VMware Vsphere ESXi 7 e versões superiores.

4.4. O console de gerenciamento deve ser on-premises, permitindo o gerenciamento das políticas de segurança através da Internet.

4.5. Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).

4.6. Deve ser gerenciada por console Web, compatível com pelo menos os browsers Microsoft Edge, Firefox e Google Chrome.

4.7. Deve suportar certificado digital para gerenciamento.

4.8. O console de administração deve permitir o envio de notificações via SMTP.

4.9. Todos os eventos e ações realizadas no console de gerenciamento precisam ser gravados, visando a auditoria.

4.10. Deve permitir a criação de widgets para facilitar a administração e visualização dos eventos.

4.11. Deve permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente, diminuindo o tráfego de internet.

4.12. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deve ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações.

4.13. Deve permitir a criação de relatórios. Tanto a criação e envio destes relatórios deve ocorrer: sob demanda, ou agendado com o envio automático do relatório via *e-mail*.

4.14. Deve fornecer pelo menos relatórios em dois dos seguintes formatos PDF, CSV, XLS e RTF.

4.15. Deve ser capaz de identificar ataques direcionados a componentes hospedados em ambiente RedHat Openshift.

4.16. Os usuários administradores devem possuir privilégios para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial".

4.17. Toda comunicação entre o console de gerenciamento e os agentes deve ser criptografada.

4.18. O console de gerenciamento deve possuir dashboards para facilitar a monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração.

4.19. Os agentes para plataforma Microsoft, quando aplicável, deverão ser instalados por pacote MSI e posteriormente ativados pelo console de gerenciamento, de forma a proporcionar maior segurança ao ambiente, ou podendo ser automatizados através de script PowerShell.

4.20. Os agentes para plataforma Linux deverão ser instalados por pacote .RPM ou .DEB e posteriormente ativados pelo console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou podendo ser automatizados através de bash script.

4.21. Em servidores Windows e Linux, deve permitir a atualização automática dos agentes após sua ativação.

4.22. Para efeito de administração, deve avisar quando um agente se encontra não conectado a seu console de gerenciamento.

4.23. Deve permitir a remoção automática de agentes inativos, com a possibilidade de definir o período por pelo menos 1 semana, 1 mês e 12 meses.

4.24. Deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host protegido.

4.25. Cada perfil poderá ser atribuído para um host ou conjunto de hosts.

4.26. Deve dispor de perfis pré-definidos e aptos a funcionarem de acordo com sua denominação.

4.27. Deve mostrar de forma simples quais máquinas estão usando determinada política.

4.28. Os agentes deverão possuir a capacidade de executar rastreamento nas máquinas onde estão instalados e fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional.

4.29. Esses rastreamentos devem ocorrer de forma agendada a ser definida pelo administrador.

4.30. Deve permitir a configuração de componentes de integração com o vCenter, a fim de permitir uma sincronização das máquinas virtuais conectadas a ele.

4.31. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente.

4.32. Deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador.

4.33. Deve ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor.

4.34. Deve possuir a capacidade de envio de logs para softwares de SIEM e SYSLOG servers em

formato CEF e LEEF.

4.35. Solução deve permitir criar relatórios customizados de todas as suas funcionalidades.

4.36. Deve permitir enviar os relatórios para uma lista de contatos independente de login no console de administração.

4.37. As atualizações de assinaturas deverão ocorrer de forma agendada e automática podendo ser até mesmo de hora em hora.

4.38. Deve ser possível baixar as assinaturas no console de gerenciamento, com opção de não as distribuir aos clientes.

4.39. O console de gerenciamento deve apresentar a capacidade de gerar rollback de suas atualizações de regras.

4.40. Deve possuir capacidade de gerar pacote de auto diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto.

4.41. Deve possuir a capacidade de colocar etiquetas para a ocorrência de determinados eventos ou dispositivos de modo a facilitar o gerenciamento, relatórios e visualização.

4.42. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes.

4.43. Solução deve possuir mecanismo de procura em seu console de gerenciamento de modo que seja facilitada a busca de regras.

4.44. Deve possuir a capacidade de classificação de eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos.

4.45. O fabricante deve participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante.

4.46. O console de gerenciamento deve se integrar com o Vmware vSphere, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para o console de gerenciamento da solução.

4.47. O fabricante da solução deve manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos.

4.48. Deve possuir REST API documentada para integração em esteira de automação.

4.49. A documentação da REST API deve conter exemplos prontos para implementação de determinadas funcionalidades.

4.50. Deve possuir a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador por meio de assinatura ou comportamento.

4.51. Deve possuir a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador assinatura ou comportamento.

4.52. Deve permitir desabilitar os módulos individualmente.

4.53. A funcionalidade de Antimalware deve possuir as seguintes características:

4.53.1. Deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e agendamento, com possibilidade de tomada de ações distintas para cada tipo de ameaça;

4.53.2. Deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura em determinados diretórios ou arquivos do sistema operacional;

4.53.3. Deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

4.53.4. Em plataforma Windows, deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

4.53.5. Deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

4.53.6. O scan de arquivos comprimidos deve ser de no mínimo 6 camadas de compressão;

4.53.7. O scan de arquivos comprimidos do tipo OLE deve ser de no mínimo 20 camadas de compressão;

4.53.8. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

4.53.9. Deve possuir a funcionalidade de monitoramento de comportamento para detectar mudanças e atividades suspeitas não autorizadas;

4.53.10. Deve oferecer a opção de escanear processos em memória em busca de Malware;

4.53.11. Para servidores Windows, deve permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline no console de gerenciamento;

4.53.12. Deve possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

4.53.13. Em servidores Windows, deve integrar-se com interface AMSI (Antimalware Scan Interface);

4.53.14. Deve mostrar informação da data sobre o último scan agendado ou manual executado;

4.53.15. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por *Ransomware*;

4.53.16. Deve possuir cache dos arquivos verificados de modo a evitar redundância da varredura;

4.53.17. Deve possibilitar otimização do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho nos servidores;

4.53.18. Deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

4.53.19. Em servidores Windows, deve possuir capacidade de detectar ameaças por

comportamento;

4.53.20. Deve possuir a possibilidade de escanear drivers de rede mapeados nos servidores.

4.54. A funcionalidade de Proteção Contra URLs Maliciosas deve possuir as seguintes características:

4.54.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

4.54.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

4.54.3. Deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, Médio e Baixo ou equivalente;

4.54.4. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

4.54.5. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

4.54.6. Deve possuir capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

4.54.7. Deve permitir que o administrador reclassifique uma URL através do site do fabricante ou outro canal de comunicação formal com objetivo de corrigir falsos positivos.

4.55. O módulo de Firewall deve possuir as seguintes características:

4.55.1. Operar como firewall de host, através da instalação de agente nos servidores protegidos;

4.55.2. Deve possuir a capacidade de controlar o tráfego baseado nos tipos de protocolos, endereços IP e intervalo de portas;

4.55.3. Deve possuir a capacidade de definir regras distintas para rede distintas;

4.55.4. Deve ser capaz de reconhecer e possibilitar o bloqueio de endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS Fingerprint;

4.55.5. Precisa possuir a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

4.55.6. Precisa possuir a capacidade de definição de regras para aplicações específicas;

4.55.7. Para facilitar a criação e administração de regras de firewall, deve trabalhar com objetos que podem ser lista de IPs e lista de portas;

4.55.8. Deve permitir personalizar políticas de acordo com o perfil das máquinas (por exemplo, se está no domínio ou não, versão de SO, de rede);

4.55.9. O firewall deve ser stateful bidirecional;

4.55.10. O firewall deve permitir liberar ou apenas logar eventos;

4.55.11. O firewall deve ser passível de criação de regras através do protocolo, origem do tráfego, destino e direção;

4.55.12. As regras de Firewall deverão possuir as seguintes ações, ou equivalentes: Allow, log only, deny ou application;

4.55.13. A solução, para facilidade de administração, deve utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

4.55.14. Deve realizar monitoramento de tráfego UDP;

4.55.15. Deve logar a atividade stateful;

4.55.16. Deve proteger contra ataques de negação de serviços, tais como SYN Flood e ack storm entre outros;

4.55.17. Devem existir regras padrão da solução que possam ser utilizadas como modelo para a criação e adição de novas regras;

4.55.18. Deve identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período configurado pelo administrador;

4.55.19. Deve permitir criar listas de exceções para identificar os IPs autorizados a realizar varreduras de portas ou da rede.

5. Solução de segurança para proteção de *E-mail*

5.1. A solução deve atender a 1300 mailboxes e pode ser entregue on-premises ou em nuvem.

5.2. Em caso de solução on-premises, deve ser entregue e instalada em um formato de "servidor/appliance virtual" (ambiente virtualizado), compatível com VMware Vsphere ESXi 7, nas instalações da contratante.

5.3. Em caso de solução on-premises, deve ser entregue e instalada em no mínimo dois servidores/appliances, para garantia de disponibilidade, sem custos adicionais para a CONTRATANTE.

5.4. Em caso de a solução entregue em nuvem deve atender os seguintes níveis de serviço mínimos:

5.4.1. Disponibilidade do serviço mínimo de 98% de uptime;

5.4.2. Efetividade no bloqueio de SPAM mínima de 99%;

5.4.3. Ocorrência de Falsos-positivos até 0,0004%;

5.4.4. Latência máxima na entrega de mensagens até 60 segundos.

5.5. Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).

5.6. Deve realizar proteção contra ameaças de *e-mail* e outras mensagens indesejadas (*spam*, *phishing*, *malware* e *e-mails* em massa), em praticamente qualquer idioma (análise multilíngue).

5.7. Todos os recursos e funcionalidades especificadas da solução deverão ser do mesmo fabricante.

5.8. Deve possuir um console único de gerenciamento da solução, que permita a administração completa de todas as regras de segurança.

5.9. O console deve ser acessado via WEB (HTTPS ou MMC), sem a necessidade de instalação de plugins adicionais.

5.10. Todas as funcionalidades devem ser parametrizáveis e configuráveis pelo console da solução

através de uma interface gráfica. Não será aceito a configuração por scripts ou execução de linha de comandos para atendimentos aos requisitos especificados.

5.10.1. De forma exemplificativa, as parametrizações e configurações deverão ser realizadas por "caixas de seleção", "opções (Flag)", "caixas de texto" ou "botões".

5.11. Caso a solução seja fornecida on-premises, deve disponibilizar painel (dashboard) nativo da própria solução, contendo pelo menos, as seguintes informações: consumo de CPU ou espaço ocupado da solução ou espaço livre em disco, tráfego de mensagens (inbound/outbound) por hora, top remetentes, quantidade de spams detectados, vírus detectados, mensagens em quarentena e políticas/regras mais utilizadas.

5.12. Deve possuir a capacidade de arquivar qualquer mensagem que viole as políticas corporativas, enviando para a estrutura de arquivamento do servidor de AntiSpam (Quarentena).

5.13. Deve possuir a capacidade de rejeitar conexões que tentem ser abertas pelos comandos "HELO" e "EHLO", sem que existam gravados seus endereços de "MX" e "A" nos servidores de DNS.

5.14. Caso a solução seja fornecida on-premises, todas as funcionalidades da solução devem continuar ativas mesmo após o término do contrato, sendo que apenas as atualizações deixarão de ser realizadas.

5.15. Deve contemplar atualizações automáticas das bases de assinaturas de vírus, spams e listas de Blacklist.

5.16. Deve possibilitar a atuação como cliente NTP (Network Time Protocol), em caso de instalação on-premises.

5.17. Deve permitir a inspeção de tráfego SMTP (inbound/outbound).

5.18. Deve possuir capacidade de gerar traps SNMP ou sylog para monitoramento de eventos, em caso de instalação on-premises.

5.19. Deve possuir capacidade de salvar/exportar relatórios para um dos seguintes tipos de arquivos: CSV, PDF ou HTML.

5.20. Deve possuir capacidade nativa de prevenção atualizada de ameaças avançadas ou 0-day, para URLs e anexos, sem custo ou franquia de consumo por análise, sem requerer integrações com terceiros para obtenção da capacidade..

5.21. Deve possuir capacidade de bloqueio de arquivos anexados por tipo.

5.22. Deve suportar tráfego de entrada e saída de *e-mails* de aproximadamente 3.300 mensagens por dia. E volume médio mensal em torno de 100.000 mensagens.

5.23. Deve possuir filtros de reputação.

5.24. Deve executar varredura de conteúdo (na entrada e na saída do correio eletrônico).

5.25. Deve ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego.

5.26. Deve possuir a detecção de Spam utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta.

5.27. Deve permitir a verificação do tipo real do arquivo, mesmo que ele tenha sido renomeado.

5.28. Deve permitir o escaneamento de arquivos executáveis comprimidos em tempo real.

5.29. Deve possuir proteção contra Spywares, sem a necessidade de um software ou agente adicional.

5.30. Deve permitir a criação de Whitelists e Blacklists para um melhor ajuste na detecção de Spam.

5.31. Deve permitir verificar a reputação de links que estejam dentro do corpo das mensagens.

5.32. Deve possuir possibilidade de Whitelist para a checagem de reputação em URLs dentro de mensagens.

5.33. Deve possibilitar a verificação do hash de arquivos anexados em tempo real para proteção contra Spam.

5.34. Deve possuir o módulo de quarentena de usuário integrado na solução e ser capaz de enviar notificação periódica para os usuários, informando as mensagens consideradas como Spam que foram inseridas na quarentena, em língua portuguesa.

5.35. Deve permitir a personalização do conteúdo das mensagens de notificação ao usuário.

5.36. Deve executar a remoção automática das mensagens armazenadas em quarentena.

5.37. Deve possuir módulo de consulta customizada e impressão de relatórios estatísticos.

5.38. Deve possuir a funcionalidade de verificação de SPF, DKIM e DMARC.

5.39. Deve possuir interface única de gerência de todos os produtos instalados na solução.

5.40. Deve possuir a capacidade de criação e gerenciamento de múltiplos grupos de usuários e a definição de regras e políticas diferenciadas para cada um destes grupos.

5.41. Deve suportar filtros que deverão ser executados à nível de MTA. Esses filtros deverão possuir a capacidade de classificar diferentes tipos de comportamento (como whitelist e blacklist).

5.42. Deve permitir a utilização de SSL/TLS para conexão.

5.43. Deve suportar SSL/TLS para conexões de entrada e saída.

5.44. Deve possuir capacidade de utilizar DNS reverso nas conexões de entrada.

5.45. Deve suportar vários domínios (registros MX), e suportar roteamento de mensagens baseado em cada um desses domínios.

5.46. Deve possibilitar que as filas de entrega do MTA possuam tamanho suficiente para suportar sobrecarga de mensagens no evento de uma falha ou de um problema em outros pontos de infraestrutura de messageria eletrônica, caso a solução seja fornecida on-premises.

5.47. Deve permitir a visualização e o gerenciamento das filas de mensagens (queues), com as opções de parar e retomar as filas e de excluir (flush) mensagens, caso a solução seja fornecida on-premises.

5.48. Deve suportar perfis únicos que tratam do comportamento de mensagens de volta (bounce) baseados nos domínios ou endereços IP de destino.

5.49. Deve possuir “Message Tracking” no próprio console gráfico para uma visualização detalhada do status da mensagem.

5.50. Deve suportar várias quarentenas residentes no próprio Servidor AntiSpam, onde as mensagens

deverão ser armazenadas pelo período especificado pelo administrador.

5.51. Possibilitar que o módulo de quarentena seja capaz de enviar uma notificação periódica aos usuários, informando as mensagens consideradas como Spam que foram inseridas na quarentena.

5.52. Deve permitir a criação de políticas de AntiSpam, filtros de conteúdo para cada um dos grupos criados.

5.53. Permitir a criação de políticas, por usuários ou grupos, baseadas no tamanho ou tipo de anexo das mensagens.

5.54. Deve possuir quarentena por usuário, proprietária do mesmo fabricante desenvolvedor da tecnologia da solução fornecida, com as seguintes características:

5.54.1. Possuir console web para que os usuários possam verificar as mensagens que estejam em quarentena por motivo de spam.

5.54.2. Permitir que o próprio usuário crie whitelists pessoais, independente do administrador, e de forma que estas whitelists não interfiram nos filtros de outros usuários.

5.55. Deve possuir mecanismo que estabeleça um sistema de reputações, pontuando os endereços IP quanto ao seu histórico de comportamento.

5.55.1. O sistema de verificação de reputação não deve basear-se somente em RBLs públicas.

5.55.2. O sistema de reputação deve utilizar uma conexão com base web nacional ou mundial, constantemente abastecida, de dados de várias fontes (blacklists, outros hardwares ou softwares do mesmo fabricante implementados em outras organizações etc.) com objetivo de aumentar a precisão da pontuação fornecida.

5.55.3. O administrador deve possuir a possibilidade de aplicar políticas por meio dessa pontuação, podendo no mínimo, varrer por spam ou definir um tipo de proteção contra ameaças.

5.56. Deve possuir capacidade de identificar e proteger o MTA contra ataques de Negação de Serviços (DoS).

5.57. Deve possuir proteção contra ataques de coleta de usuário/senha.

5.58. Deve possuir recurso de firewall de *e-mail*, protegendo o servidor de correio contra ataques de diretório (Directory Harvest Attack).

5.59. Deve ser capaz de bloquear a conexão SMTP caso a fonte emissora seja considerada como Spam e não atenda políticas básicas de segurança, tais como SPF, DMARC e BEC.

5.60. Os filtros de Conteúdo contra spam deverão varrer todas as partes das mensagens, incluindo:

5.60.1. Remetentes (comando SMTP MAIL FROM).

5.60.2. Destinatários (comando SMTP RCPT TO).

5.60.3. Cabeçalho do *e-mail*.

5.60.4. Corpo do *e-mail*.

5.60.5. Anexo(s) do *e-mail*.

5.61. O sistema de filtros deve suportar dicionários de palavras e expressões regulares e ser

personalizável.

5.62. O suporte de anexos deve possuir no mínimo:

5.62.1. Escaneamento por tipo MIME

5.62.2. Capacidade dê apagar automaticamente anexos.

5.63. Deve gerar relatórios, contendo, pelo menos:

5.63.1. Sumário de mensagens;

5.63.2. Principais remetentes de spam;

5.63.3. Principais destinatários de spam;

5.63.4. Estatísticas sobre a quarentena.

5.64. Deve possuir possibilidade de agendamento e envio dos relatórios por *e-mail*.

5.65. Deve possuir ferramenta para geração de relatórios DMARC.

5.66. Deve ser gerenciado de forma centralizada.

5.67. Deve permitir a criação de regras para entrada (inbound) e saída (outbound) de *e-mails*.

5.68. Deve possuir console de gerenciamento web.

5.69. Deve possuir console centralizado, incluindo:

5.69.1. Configurações de administração;

5.69.2. Objetos de política;

5.69.3. Objetos suspeitos;

5.69.4. Gerenciamento de usuário final;

5.69.5. Gerenciamento de diretório;

5.69.6. Informações sobre licenciamento;

5.69.7. Logs;

5.69.8. Relatórios;

5.69.9. Visualização de mensagens quarentenadas;

5.69.10. Gerenciamento de domínio;

5.69.11. Dashboard baseado em gráficos;

5.69.12. Rastreamento de *e-mails*, eventos e Logs.

5.70. Deve possuir métodos de autenticação como: Correspondência de IP do remetente, SPF (Sender Policy Framework); DKIM (DomainKeys Identified Mail) e DMARC (Authentication Message Reporting, Reporting & Conformity) baseado em domínio para proteger contra falsificação de *e-mail*.

5.71. Deve ser capaz de detectar conteúdos maliciosos encontrados em documentos anexos como Microsoft Word, Excel e PowerPoint e possuir a opção de limpar ou excluir o anexo.

5.72. Deve possuir a funcionalidade de restringir remetentes com base na validação de DNS reverso e com a capacidade de criação de listas de domínios permitidos em exceção (whitelist).

5.73. Deve ser capaz de permitir a filtragem baseada em reputação IP para no mínimo:

5.73.1. Remetentes permitidos com base no endereço IP e país;

5.73.2. Remetentes bloqueados com base no endereço IP e país.

5.74. Deve ser capaz de permitir a filtragem de remetente e destinatários para no mínimo: Remetentes aprovados por endereço de *e-mail* ou domínio, Remetentes bloqueados por endereço de *e-mail* ou domínio e validar destinatário de entrada de *e-mail*.

5.75. Deve possibilitar incluir X-Header no cabeçalho da mensagem para mensagens de *e-mail* correspondentes a remetentes aprovados.

5.76. A lista de remetentes aprovados e remetentes bloqueados deverão exibir no mínimo as seguintes informações:

5.76.1. Remetente;

5.76.2. Domínio do destinatário;

5.76.3. Data.

5.77. Deve detectar *malwares*, *worms*, e outras ameaças baseadas em assinatura e padrões.

5.78. Deve ser capaz de detectar spam baseado em assinatura e padrões.

5.79. Deve identificar *e-mails* marketing como redes sociais, fóruns e boletins de informações.

5.80. Deve permitir criar exceções para *e-mails* marketing.

5.81. Deve possuir configuração de classificação de spam com, no mínimo, três níveis: Alto, Médio e Baixo ou escala equivalente.

5.82. Deve detectar *phishing* e conteúdos suspeitos.

5.83. Deve detectar mensagens de graymail.

5.84. Deve realizar varreduras em arquivos JSE e VBE para identificar ameaças de macro.

5.85. Deve detectar ameaças desconhecidas utilizando machine learning.

5.86. Deve permitir visualizar relatório detalhado para cada detecção Machine Learning.

5.87. Deve possuir capacidade para detecção de explorações de documentos, ameaças de dia zero, vulnerabilidades conhecidas e outras ameaças usadas em ataques direcionados.

5.88. Deve possuir Proteção anti-ransomware.

5.89. Deve possuir análise de URLs no corpo do *e-mail*.

5.90. Deve possuir o recurso para analisar as URLs no momento do clique do usuário e as bloquear se forem maliciosas.

5.91. Deve possuir ações de bloqueio, liberação e alerta para as seguintes categorias ou equivalentes: perigoso, altamente suspeito, não testado e suspeito.

5.92. Deve possuir Proteção contra Comprometimento de *E-mail*.

5.93. Deve permitir adicionar usuários de alto perfil, possibilitando exportar a lista em CSV.

5.94. Deve possibilitar importar usuários de alto perfil através de arquivo CSV.

5.95. Deve fornecer informações detalhadas bem como razões para mensagens de e-mail detectadas como possíveis ataques analisados ou prováveis do Business Email Compromise (BEC).

5.96. Deve possuir Proteção contra-ataques de Engenharia Social.

5.97. Deve fornecer informações detalhadas bem como razões para mensagens de e-mail detectadas

como possíveis ataques de engenharia social.

5.98. Deve ser capaz utilizar no mínimo os seguintes bancos de dados de reputação que:

5.98.1. Tenham uma lista de endereços IP de servidores de correio que são conhecidos por serem fontes de spam;

5.98.2. Tenham uma lista de endereços IP identificados como envolvidos em *ransomware* ativos, *malware* ou outras campanhas de ameaças por *e-mail*;

5.98.3. Tenham uma lista de IPs atribuídos dinamicamente.

5.99. Deve possibilitar configurar exceções de varredura através de definições de condições, possibilitando execução das ações de bypass e deleção do e-mail, incluindo anexos, e quarentenar.

5.100. As ações de verificação configuradas para cada exceção devem ser aplicadas a todos os remetentes e destinatários.

5.101. Deve possuir regras de varredura avançadas que permitam especificar a análise das mensagens verificadas pela solução, considerando as seguintes condições:

5.101.1. Tamanho da mensagem;

5.101.2. Assunto;

5.101.3. Corpo do e-mail;

5.101.4. Cabeçalho;

5.101.5. Conteúdo do anexo;

5.101.6. Tamanho do anexo;

5.101.7. Extensão do anexo, incluindo .386, .ACM, .ASP, .AVP, .BAT, .CGI, .CHM, .CLA, .CLASS, .CMD, .CNV, .COM, .CS, .DLL, .DRV, .EXE, .HLP, .HTA, .HTM, .JS*, .LNK, .OCX, .OPO, .PHP, .PL. .SH, .SYS, .VBS, VBE, VXD, .WBS, .WIZ. WSH, .DOC, .DOCM, DOCX, .DOT, .DOTM, .DOTX, .DVB, .EML, .MD*, .PPA, .PPAM, .PPS, .PPSM, .PPSX, .PPT, .PPTM, .PPTX, XL,XLA, XLAM, .XLC, .XLK, XLL,.XLM, .XLR, .XLS, .XLSB, .XLSM, XLSX, .XLT, .XLTM, XLTX;

5.101.8. MIME content-type: video, audio, imagens, documentos e outros;

5.101.9. Anexo protegido por senha inclusive em arquivos compactados;

5.101.10. Quantidade de anexos;

5.101.11. Número de destinatários.

5.102. Deve possuir ações através das regras permitindo definir o que acontecerá com as mensagens que atendem às condições dos critérios da regra:

5.102.1. Monitorar, permitindo os administradores o monitoramento das mensagens. As ações de monitoramento incluem o envio de uma mensagem de notificação para outras pessoas ou o envio de uma cópia oculta (Cco) da mensagem para outras pessoas;

5.102.2. Bloquear, deve interceptar a mensagem, impedindo que ela atinja o destinatário original. As ações de bloqueio incluem excluir a mensagem inteira, colocar em quarentena e

enviar para um destinatário diferente;

5.102.3. Modificar, permitindo alterar a mensagem e/ou seus anexos. As ações de modificação incluem limpeza de vírus que podem ser limpos, exclusão de anexos de mensagens, inserção de um carimbo no corpo da mensagem ou TAG de assunto.

5.103. Deve ser possível criar políticas de *malwares*, spam e filtragem de conteúdo com:

5.103.1. Definição do destinatário, possibilitando selecionar domínios cadastrados, domínios específicos e grupos de usuários;

5.103.2. Especificação de endereços de remetente;

5.103.3. Exceções.

5.104. Deve possibilitar importar e exportar os destinatários, remetentes e listas de exceções.

5.105. Deve ser possível criar políticas que executem ações em mensagens que contêm *malware*, *worms* ou outros códigos maliciosos.

5.106. Deve ser possível realizar a limpeza de *malwares* ou códigos maliciosos, onde o *malware* pode ser removido com segurança do conteúdo do arquivo infectado, resultando em uma cópia não infectada da mensagem ou anexo original.

5.107. Deve possuir o serviço de banner para customização do portal com a logo.

5.108. Deve possuir integração com o Active Directory.

5.109. Deve permitir o gerenciamento de múltiplos domínios.

5.110. Deve ser capaz de criptografar *e-mails* baseado em políticas.

5.111. Deve assegurar a comunicação através da utilização do protocolo TLS.

5.112. Deve permitir a configuração da checagem do TLS.

5.113. Deve suportar: TLS 1.3, TLS 1.2, TLS 1.1 and TLS 1.0.

5.114. Deve permitir o rastreamento de mensagens de forma centralizada e por meio da interface de gerenciamento, não sendo aceito pesquisa via linha de comando.

5.115. Deve possuir permitir o rastreamento de mensagens enviadas e recebidas.

5.116. Deve possibilitar pesquisas de log de rastreamento de e-mail por até 30 dias.

5.117. Deve fornecer buscas para rastreamento de e-mail por: período, remetente, destinatário, tipo (bloqueado/liberado), ação, assunto, ID da mensagem e Hash do anexo SHA256.

5.118. Deve possuir permitir a consulta de eventos com os logs das políticas aplicadas por até 30 dias.

5.119. Deve fornecer consulta de eventos com os logs das políticas por: período, direção do tráfego, remetente, destinatário, nome da regra, tipo de ameaça, anexo, BEC, *Graymail*, *ransomware*, *phishing*, *spam*, *malware*, web reputation, ID da mensagem e ação.

5.120. Deve fornecer permitir rastrear os cliques de URL por: data, direção do tráfego, remetente, destinatário, ID da mensagem, URL, ação e a hora em que um URL foi clicada.

5.121. Deve ser possível consultar os logs de auditoria do console da solução por até 30 dias.

5.122. Deve ser possível encaminhar os logs para syslog.

5.123. Deve fornecer relatórios com base em uma programação diária, semanal, mensal e trimestral.

5.124. Os relatórios deverão ser, pelo menos, no formato PDF ou HTML.

5.125. Deve ser possível criar relatório agendados e manuais.

5.126. Deve ser possível obter relatório sobre com resumo do tráfego de e-mail de todos os domínios e por domínio, detecções de ameaças, detecções de arquivos da sandbox, detecções de URL da sandbox e os principais destinatários comprometidos por e-mail (BEC).

5.127. Deve suportar notificação via *e-mail*.

5.128. Deve possuir modelos de notificação pré-definidas para violação de políticas.

5.129. Deve possuir configuração de notificação quando:

5.129.1. o *e-mail* possuir um anexo compactado;

5.129.2. o tamanho da mensagem for excedido;

5.129.3. houver uma configuração de violação de segurança;

5.129.4. um vírus e spam for identificado.

5.130. Deve permitir visualizar as mensagens quarentenadas por data, remetente, destinatários e conteúdo.

5.131. Deve permitir a customização da notificação de quarentena pela menos semanal, uma vez ou mais vezes durante o dia.

5.132. A notificação de quarentena deve permitir a customização.

5.133. A notificação de quarentena deve ser, no mínimo, em inglês e português.

5.134. Deve possibilitar a gestão de quarentena de forma que seja possível que o administrador possa visualizar: a razão de um determinado bloqueio, o remetente, o destinatário, a data, o assunto, o IP do host de destino, a mensagem original, o tamanho da mensagem original.

5.135. Com base nos requisitos acima, deve ainda permitir as ações liberar e/ou excluir a mensagem.

5.136. Deve permitir realizar o download da mensagem quarentemada.

5.137. Caso uma mensagem seja bloqueada ou rejeitada, deve informar também a razão do bloqueio e quais as regras foram ativadas.

5.138. Deve possuir single sign-on (SSO) para a quarentena de usuário.

5.139. Deve possibilitar utilizar duplo fator de autenticação.

5.140. Deve possibilitar que usuário tome as seguintes ações ou similar em sua própria quarentena:

5.140.1. Excluir e bloquear o remetente: possibilitando excluir permanentemente a mensagem e adicionar o endereço aos remetentes bloqueados.

5.140.2. Excluir, possibilitando excluir permanentemente a mensagem.

5.140.3. Entregar e aprovar o remetente, permitindo liberar a mensagem da quarentena e adicionar o endereço aos remetentes aprovados, para que mensagens futuras de remetentes aprovados não sejam mantidas em quarentena.

5.140.4. Entregar, permitindo assim liberar a mensagem da quarentena.

5.141. Deve possibilitar que o usuário criar listas remetentes aprovados e remetentes bloqueados.

6. Proteção antimalware para armazenamento centralizado de dados (Storage)

6.1. A solução de deve atender a 2 repositórios de armazenamento de arquivos.

6.2. Deve possuir compatibilidade com NetApp Data Ontap 9.7, no mínimo.

6.3. A solução antimalware deve possuir a capacidade de limpar os arquivos contaminados e, na impossibilidade de realizar a limpeza, deve possuir a capacidade de incluir o arquivo em quarentena ou de exclui-los.

6.4. A solução antimalware em seu processo de escaneamento não deve comprometer o desempenho computacional do Sistema de Armazenamento e Gerenciamento de Dados (NAS).

6.5. Deve permitir configuração de ações para arquivos infectados com console de interface gráfica intuitiva para que o administrador configure qual ação a solução antimalware tomará para arquivos infectados.

6.6. Possibilidade de notificação de eventos e envio de alertas de forma automática para o administrador.

6.7. Armazenamento da ocorrência de vírus em log.

6.8. Possibilidade de funcionamento independente da ferramenta de gerenciamento.

6.9. Possibilidade de retorno de versão anterior das vacinas (rollback).

6.10. Deve detectar e remover vírus, worms, trojans, spywares e outros tipos de códigos maliciosos.

6.11. A solução antimalware deve permitir conexão de atualização em redes que possuam servidor proxy.

6.12. Permitir atualização automática e de forma incremental da base de dados de vacina.

6.13. Deve fornecer em tempo real o status atualizado da solução antimalware com no mínimo as seguintes informações: versão dos arquivos de vírus (update), dos mecanismos de verificação/correção (engine) e dos programas do sistema.

6.14. A solução antimalware deve permitir gerenciamento gráfico intuitivo portável ao console (gerenciamento remoto) e escaneamento centralizado.

6.15. A solução antimalware poderá ser executada em um servidor dedicado ou ser executada no próprio Sistema de Gerenciamento e Armazenamento de Dados (NAS).

6.16. Caso a solução antimalware necessite de um servidor dedicado, a mesma deve possuir no mínimo os seguintes requisitos:

6.16.1. Deve possuir arquitetura em cluster com 3 nós para melhoramento de desempenho e disponibilidade.

6.16.2. Deve permitir o balanceamento de carga entre os servidores da solução e operar em alta disponibilidade;

6.16.3. Uma vez um servidor configurado em um Sistema de Gerenciamento e Armazenamento de Dados, a conexão e reconexão entre eles devem ocorrer automaticamente.

6.17. A solução antimalware deve suportar, no mínimo, 4 (quatro) conexões de, no mínimo, 10 Gbps (dez gigabit por segundo) e o acesso simultâneo de, no mínimo, 50 usuários.

6.18. A solução antimalware deve permitir a configuração de escaneamento em pelo menos uma das seguintes modalidades:

6.18.1. Escaneamento manual;

6.18.2. Escaneamento em tempo real;

6.18.3. Escaneamento escalonado;

6.18.4. Escaneamento através de integração.

6.19. A solução antimalware deve permitir a configuração de uma lista de tipos de extensões predeterminadas pelo administrador do Sistema para os processos de escaneamento.

6.20. Deve acompanhar as requisições de escaneamento de arquivo e retornar o seu resultado.

6.21. A solução em seu processo de escaneamento não deve comprometer o desempenho computacional do Sistema de Armazenamento e Gerenciamento de Dados (NAS).

6.22. Para melhorar o desempenho, diminuir o tráfego e aumentar a velocidade, o Sistema antimalware deve permitir ao administrador do Sistema a configuração dos seguintes passos:

6.22.1. Configurar o Sistema de Armazenamento de Dados (STORAGE) para enviar ao Sistema antimalware somente arquivos com as extensões especificadas;

6.22.2. Os arquivos do Sistema de Armazenamento de Dados serão marcados como “limpos” se eles forem escaneados antes e solicitados sem nenhuma alteração.

6.23. Os arquivos marcados como “limpos” não deverão ser escaneados novamente pelo sistema antimalware.

6.24. Deve possuir rotinas bem definidas de escaneamento, atualizações e de logs.

6.25. Deve garantir a integridade dos dados e ser capaz de detectar e remover *malware* conhecidos e desconhecidos.

6.26. Deve utilizar escaneamento recursivo para arquivos compactados.

6.27. Deve permitir configuração de ações para arquivos infectados com console de interface gráfica intuitiva para que o administrador configure qual ação o Sistema tomará para arquivos infectados:

6.27.1. Deixar em quarentena arquivos infectados;

6.27.2. Limpar com backup;

6.27.3. Limpar sem backup;

6.27.4. Excluir arquivo infectado.

6.28. Notificação de eventos e envio de alertas de forma automática para o administrador como resguardo de situação séria, tal como epidemia de vírus ao Sistema de Armazenamento de Dados.

6.29. Armazenamento da ocorrência de *malware* em log centralizado.

6.30. Possibilidade de colocar arquivos e diretórios em listas de exclusões onde estes não serão verificados pela solução.

6.31. Possibilidade de funcionamento e administração independentes de ferramenta de gerenciamento centralizado.

6.32. Gerenciamento remoto e centralizado da solução.

6.33. Realizar ações específicas para cada tipo de código malicioso.

6.34. Fornecimento de vacina para novos vírus num prazo máximo de 24 (vinte e quatro) horas, a partir do acionamento ao fornecedor.

6.35. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo.

6.36. Permitir o reinício automático dos serviços do *malware*.

6.37. Proteção no mínimo contra códigos maliciosos classificados como vírus, *trojan horses*, *worms* entre outros.

6.38. Suporte compreensível com Help inteligente.

6.39. Da remoção:

6.39.1. Detecção e remoção de *malware* em tempo real;

6.39.2. Detecção e remoção de *malwares*, do tipo: Vírus, *worms*, *trojan horses* entre outros;

6.39.3. Proteção contra desinstalação e desativação não autorizada do produto.

6.40. Das Atualizações:

6.40.1. Permitir atualização automática e de forma incremental do cartório de vírus e da base de dados de vacina;

6.40.2. Permitir configuração de forma manual para atualizações referentes às mudanças no programa, erros resolvidos e melhorias;

6.40.3. Que a periodicidade e o horário das atualizações também possam ser configuráveis.

6.41. Deve fornecer em tempo real o status atualizado da solução antimalware com no mínimo as seguintes informações: Versão dos arquivos de vírus (update), dos mecanismos de verificação/correção (*engine*) e dos programas do sistema (upgrade).

6.42. Se uma nova atualização for disponibilizada à solução de antimalware, o administrador do sistema poderá apagar as informações no cache do sistema para forçar a aplicação de um novo escaneamento, inclusive aqueles arquivos que foram escaneados com a versão antiga.

7. Proteção para Microsoft 365

7.1. Aplicar proteções antimalware para a proteção dos serviços Exchange Online, SharePoint Online e OneDrive for Business da Microsoft.

7.2. Detectar ameaças, exploração de documentos em nuvem, reputação web e inteligência em nuvem.

7.3. Realizar análise dinâmica com tecnologia de inteligência para investigar o comportamento de arquivos suspeitos não apenas correspondência padrão estática e coloca em quarentena arquivos e *e-mails* prejudiciais.

7.4. Empregar detecção de *malware* por meio Machine Learning e comportamento, para diminuir seu risco de violação.

7.5. Detectar exploração de documentos para encontrar *malware* escondido dentro de formatos de arquivos comuns do Office, como Word, PowerPoint e Excel.

7.6. Realizar integração nuvem-a-nuvem, através de API da Microsoft ou autenticação no serviço de Office365, realizando a análise de *malware* utilizando tecnologia de *machine learning*. Integrar diretamente com a Microsoft dispensando o redirecionamento de tráfego de *e-mail*.

7.7. Tornar visível o uso de dados sensíveis no Exchange, SharePoint e OneDrive for Business.

7.8. Monitorar em tempo real para bloquear, colocar em quarentena, ou fazer relatórios de políticas de conformidade.

7.9. Deve realizar descobertas de dados no ambiente Microsoft Office 365.

7.10. Deve detectar dados confidenciais em texto e imagens dos seguintes tipos:

7.10.1. Números de cartão de crédito;

7.10.2. Número de CNH;

7.10.3. Número de identidade;

7.10.4. Número de CPF;

7.10.5. Número de Passaporte.

7.11. Deve permitir a identificação e proteção contra ameaças nas seguintes soluções em nuvem:

7.11.1. Microsoft 365 no mínimo Exchange Online, Sharepoint Online, Onedrive for Business e Microsoft Teams.

7.12. Deve bloquear caso o usuário tente fazer o upload de um determinado arquivo malicioso ou proibido nas plataformas Onedrive, Sharepoint e Microsoft Teams.

7.13. Bloquear upload de arquivos por tipo definido em política para as soluções supracitadas.

7.14. Identificar e bloquear URLs maliciosas e em arquivos, incluindo URLs inseridas em anexos.

7.15. Deve ser possível realizar escaneamento de forma manual para identificação de possíveis ameaças e arquivos maliciosos.

7.16. Deve ser possível configurar os destinatários para o recebimento dos resultados do escaneamento.

7.17. Deve fornecer informações detalhadas bem como razões para mensagens de *e-mail* detectadas como possíveis ataques analisados e prováveis do Business *E-mail* Compromise (BEC).

7.18. Deve possuir Proteção contra-ataques de Engenharia Social.

7.19. Deve ser capaz utilizar no mínimo os seguintes bancos de dados de reputação que:

7.20. Tenham uma lista de endereços IP de servidores de correio que são conhecidos por serem fontes de spam.

7.21. Tenham uma lista de endereços IP identificados como envolvidos em *ransomware* ativos, *malware* ou outras campanhas de ameaças por *e-mail*.

7.22. Deve permitir realizar escaneamento retroativo de ameaças sob demanda, isto é, em busca de ameaças já armazenadas.

7.23. Deve ser possível configurar o nível de sensibilidade das URLs maliciosas.

7.24. Deve ser possível cadastrar os usuários importantes com objetivo de analisar e identificar possíveis *e-mails* de fraude baseado em comportamento e padrão de escrita.

7.25. Deve permitir que os administradores configurem a periodicidade das notificações para, no

mínimo, URLs maliciosas identificadas, SPAMs maliciosos, *Phishing*, *Ransomware*, arquivos analisados na sandbox e identificados como alto e médio risco.

7.26. Deve permitir a visualização das estatísticas no dashboard por serviço integrado (Exchange Online, Teams, Onedrive, Sharepoint).

7.27. Deve ser possível ajustar o período dos logs para análise.

7.28. Deve possuir a capacidade de analisar arquivos e URLs em sandbox para identificação de ameaças desconhecidas (sem assinatura).

7.29. Deve utilizar mecanismos de proteção que contemplem, pelo menos, *malwares* conhecidos por assinatura, *malwares* desconhecidos por Machine Learning, bloqueio de conteúdo (por tipo de arquivo, por exemplo), reputação de URLs.

7.30. Deve permitir compartilhamento de informações através de SIEM via API ou através da gerência centralizada.

7.31. Deve prover relatórios que contemplem, pelo menos, riscos de segurança, ameaças, *ransomware*, arquivos analisados em *sandbox*, auditoria e API.

7.32. Os relatórios devem ser exportáveis para, pelo menos, PDF.

7.33. A verificação Antimalware deve permitir a customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.

7.34. Aplicar proteções antimalware, verificação de URLs maliciosas para a proteção dos serviços.

7.35. Aplicar proteções contra Comprometimento de *E-mail* utilizando análise de escrita.

7.36. Deve permitir a integração nuvem-a-nuvem, através de API com, no mínimo, a seguinte aplicação: Microsoft 365, realizando a análise de *malware* em sandbox.

7.37. Deve ser possível configurar o envio de notificação por *e-mail* para administradores, caso haja execução da regra e bloqueio ou quarentena como ação de resposta.

7.38. Os alertas enviados deverão permitir a customização tanto para o usuário quanto para o administrator.

7.39. Monitorar em tempo real para bloquear arquivos e, caso configurado, colocá-los em quarentena.

7.40. Empregar detecção de *malware* por meio de *sandbox* sem assinaturas, para diminuir seu risco de violação.

7.41. Monitorar o comportamento real de arquivos suspeitos em ambientes *sandbox* virtuais, usando múltiplas versões de sistemas operacionais e aplicações.

7.42. As políticas deverão possuir a capacidade de serem realizadas por usuário ou grupo.

7.43. Possuir um dashboard com as principais ameaças detectadas, a exemplo do tipo *Ransomware*, *Phishing* e Comprometimento de *E-mail*.

7.44. Deve ser capaz de implementar políticas para prevenção contra envio de informações sensíveis armazenados nas aplicações em nuvem.

7.45. A sandbox deve possuir a opção para funcionar em modo de monitoramento, não tomando nenhuma ação nos arquivos detectados.

7.46. Deve possui a funcionalidade de verificação de SPAM com níveis de detecções diferentes.

7.47. As ações realizadas pelo *antispam* deverão possuir as seguintes opções: quarentena, adicionar uma tag no assunto, deletar ou mover para a pasta de lixo.

7.48. Deve permitir o administrador adicionar ou bloquear um endereço na lista de remetentes.

7.49. Deve ser possível obter relatório sobre com resumo do tráfego de *e-mail* de todos os domínios e por domínio, detecções de ameaças, detecções de arquivos da *sandbox*, detecções de URL da *sandbox* e os principais destinatários comprometidos por *e-mail* (BEC).

8. Detecção e Resposta Avançada de Ataques (XDR)

8.1. Deve suportar a coleta de dados de diversas fontes, incluindo endpoints, rede, filtros da web e sensores de nuvem, para acelerar a detecção e resposta a incidentes e reduzir os tempos de resposta.

8.2. Deve permitir a integração com plataformas de segurança via API.

8.3. Deve ser capaz de ingerir diversas fontes de dados, entre elas Network Intrusion Detection Systems (NIDS), Endpoint Protection Platforms (EPP), Endpoint Detection and Response (EDR), com objetivo de aprimorar o processo de detecção de ameaças e tomar ágil processo de correlação e investigação de alertas.

8.4. Deve permitir a integração com a ferramenta de gerenciamento de tickets OTRS (Open-source Ticket Request System) possibilitando a gestão unificada de incidentes.

8.5. A quantidade de coletores necessários para a total ingestão de eventos do ambiente não deve onerar ou gerar custos adicionais de liecenciamento;

8.6. Deve fornecer ambiente gráfico para criação de fluxos de interação.

8.7. Deve permitir a automação das atividades de resposta a incidentes com base nas necessidades e processos mapeados.

8.8. Deve fornecer visibilidade de possíveis vazamentos de contas de usuário.

8.9. Deve fornecer informações de elevação de privilégio das contas nos dispositivos.

8.10. Deve ser compatível com a solução NSX da VMware para permitir integração com os ambientes virtualizados do CJF.

8.11. Deve realizar a coleta e análise dos dados de atividade de *endpoints* de desktop e servidor.

8.12. Deve realizar a coleta e análise dos dados de atividade de contas de *e-mail*.

8.13. Deve realizar a coleta e análise do tráfego de rede.

8.14. Deve fornecer insights sobre a postura de segurança baseado em um índice geral de risco, exposição de dispositivos, ataques em andamento e outros fatores relacionados.

8.15. Deve realizar a descoberta dos ativos organizacionais expostos a ataques, incluindo dispositivos e ativos voltados para a Internet, contas, aplicativos em nuvem e ativos em nuvem.

8.16. Deve realizar a avaliação das comunicações com destino a internet relacionadas a atividades ou endereços maliciosos ou vulneráveis, identificando os usuários e dispositivos envolvidos, fornecendo informações de mitigação do risco detectado.

8.17. Possuir console Web para gerenciamento e administração da ferramenta.

8.18. O recurso de detecção e resposta para *e-mails* deve ser integrado à solução da Microsoft Office 365 sem a necessidade de alterar configurações dos serviços de *e-mail* e configurações dos usuários.

8.19. O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines e possuir analista dedicado a desenvolvimento de defesas contra ameaças e *malwares*. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.

8.20. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente.

8.21. Deve permitir a ingestão de identidades do ambiente, através de integrações como SSO, IDPs via SAML, ou consumo de informações via LDAP ou API.

8.22. Deve prover diferentes níveis de administração e acesso a ferramenta para os usuários em pelo menos: Master Administrator, Administrator, Senior Analyst, Analyst e Auditor ou equivalentes.

8.23. Deve permitir configuração de duplo fator de autenticação para acesso dos usuários ao console de gerenciamento.

8.24. Deve registrar os logs de atividades realizados no console de gerenciamento para fins de auditoria.

8.25. Ter capacidade de enviar os eventos e detecções para aplicações de SIEM e Syslog terceiros;

8.26. Deve permitir configuração de notificações por *e-mail* (SMTP) para envio de alertas e notificações.

8.27. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nas contas de *e-mail*.

8.28. Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e maliciosas para identificação e categorização de ameaças no ambiente.

8.29. Deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente de segurança.

8.30. Deve possuir capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam.

8.31. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente.

8.32. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta.

8.33. Deve fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções.

8.34. Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação.

8.35. Deve monitorar os status dos produtos integrados à plataforma de resposta à incidentes através do console de gerenciamento.

8.36. Deve fornecer mecanismos de gestão e governança que permitam a identificação e avaliação de riscos sobre os ativos da organização, em conformidade com as recomendações do NIST (National Institute of Standards and Technology).

8.37. Deve fornecer um índice global de risco.

8.38. Deve deve fornecer sugestões sobre as ações de remediação mais importantes para reduzir o risco geral.

8.39. Deve fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos.

8.40. A gestão da superfície de ataque deve ser integrada na plataforma, fornecendo informações sobre Dispositivos Internos, Ativos Voltados para a Internet, Contas e Aplicações na Nuvem.

8.41. Deve ser fornecido um painel para exibir todos os usuários/dispositivos com Alto Risco para tomada de ações.

8.42. Deve ser possível realizar benchmarking em tempo real com comparação de nível de risco.

8.43. Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de identidade, como Azure AD, Office 365, AD local.

8.44. Deve detectar o comprometimento de contas de usuário.

8.45. Deve detectar vulnerabilidades exploráveis do sistema operacional nos *endpoints* e servidores.

8.46. Deve deve fornecer um guia para reduzir fatores de risco detectados.

8.47. Deve permitir definir um objetivo de redução de risco.

8.48. Visualizar um resumo dos eventos de risco que você deve remediar para alcançar o objetivo selecionado e alterar o status dos eventos de risco.

8.49. Visualizar informações sobre os ativos que foram mais impactados por cada evento de risco.

8.50. Deve permitir as seguintes ações para responder a riscos: Desativar/Ativar conta do usuário - Forçar logout - Redefinir senha - Isolar/Restaurar *Endpoint* - Monitorar tentativas de login - Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno - Bloquear/Desbloquear/Permitir Acesso a aplicativos ou URLs em nuvem.

8.51. Deve apresentar uma lista com todos os modelos de detecção pré-definidos que a solução possui.

8.52. Cada modelo deve possuir uma descrição e um score para auxiliar na identificação do risco e impacto de cada modelo.

8.53. Deve permitir ativar ou desativar qualquer modelo de detecção caso necessário.

8.54. Permitir criação de listas de exceção de objetos para redução de falso-positivo.

8.55. Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis:

8.55.1. Crítico;

8.55.2. Alto;

8.55.3. Médio;

8.55.4. Baixo.

8.56. Deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar sua organização a se defender proativamente contra ameaças.

8.57. Deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e terceiros para ajudar na identificação de ameaças.

8.58. Os relatórios de ameaças do fabricante deverão gerar alertas de detecção caso sejam identificadas atividades presentes nos relatórios dentro do ambiente.

8.59. Deve ser possível identificar individualmente cada relatório de ameaça.

8.60. Deve permitir adicionar bases de inteligência terceiras de forma manual, por API, importando arquivos com base CSV ou STIX através de assinatura de feeds de inteligência de ameaças terceiros.

8.61. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais.

8.62. O campo de busca deve permitir o uso de múltiplos operadores lógicos para no mínimo:

8.62.1. E;

8.62.2. Ou;

8.62.3. Não.

8.63. Deve permitir indexar múltiplas buscas utilizando operadores lógicos.

8.64. Deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas.

8.65. Deve permitir pesquisar por atividades de cada um dos contextos, mesmo que não tenham gerado qualquer tipo de detecção pelos modelos de detecção de ameaça.

8.66. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz.

8.67. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.

8.68. Deve somar as pontuações (score) de cada modelo durante a correlação das atividades para melhor categorização do incidente.

8.68.1. Deve exibir todos os detalhes do incidente em uma única página, contendo no mínimo:

8.68.2. Status do incidente;

8.68.3. Score;

8.68.4. Quantidade de contas de *e-mail* impactadas;

8.68.5. Data e hora da detecção;

8.68.6. Técnica do MITRE utilizada;

8.68.7. Modelo(s) de detecção acionado(s);

8.68.8. Objetos detectados dentro de cada modelo;

8.68.9. Deve permitir alterar o status de cada evento, para no mínimo Novo, Em progresso/análise e Fechado ou escala equivalente.

8.69. Permitir adicionar comentários e notas a cada evento pelos analistas da ferramenta.

8.70. Durante o processo de análise da cadeia de processos deve ser possível verificar todos os objetos relacionados à esta análise, as atividades executadas pelos objetos e sua reputação conforme categorização do fabricante.

8.71. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta.

8.72. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção.

8.73. Permitir adicionar um comentário junto a cada ação tomada para registro e contextualização das ações.

8.74. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores.

8.75. Permitir coletar e fazer o download de um arquivo para investigação local detalhada.

8.76. Permitir adicionar o remetente (sender) de um *e-mail* na lista de bloqueio, impedindo o mesmo de enviar novos *e-mails* os usuários da sua empresa.

8.77. Mover o *e-mail* selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este *e-mail* em suas caixas.

8.78. Deletar o *e-mail* selecionado das caixas selecionadas.

8.79. Deve permitir verificar todas as ações de respostas executadas no console ou por API.

8.80. Deve exibir os seguintes painéis de controle:

8.80.1. Índice de risco da empresa;

8.80.2. MITRE ATT&CK® Mapping for Enterprise;

8.80.3. Visão geral de alertas;

8.80.4. Top 10 vulnerabilidades em risco;

8.80.5. Top 10 usuários em risco;

8.80.6. Top 10 dispositivos em risco;

8.81. Deve permitir a geração e o download de relatórios únicos e/ou agendados.

8.82. Deve possuir a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado.

8.83. Deve permitir exportar sob demanda os logs em texto puro (CSV ou PDF).

8.84. Deve permitir investigação por palavras-chave customizadas para facilitar a busca de eventos.

8.85. Deve permitir recebimento e encaminhamento de logs via syslog.

8.86. Deve permitir receber logs de diferentes dispositivos.

9. Inspeção de Tráfego de Rede (NDR)

9.1. O modulo de análise e rede deve possuir a capacidade de analisar até 4 Gbps de throughput na rede.

9.2. O modulo deve ser integrado a rede através de port mirror.

9.3. Deve ser instalada a fim de detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados.

9.4. Deve atuar com a inspeção de rede da CONTRATANTE, estendendo visibilidade sob tráfego leste-oeste e norte-sul.

9.5. Deve aplicar técnicas de análise de tráfego avançadas baseadas em heurística.

9.6. Deve atuar com técnicas de detecção e resposta focadas em rede, de forma a identificar comportamentos maliciosos.

9.7. Deve permitir que seja implantada em linha com o tráfego de rede, e deve ser capaz de ser instalada em modo de espelhamento de rede.

9.8. Deve implementar características de NDR (Detecção e resposta à nível de rede) baseado em comportamento como complemento às soluções baseadas em assinatura.

9.9. Deve ser integrado nativamente com a solução de Detecção e Resposta Avançada de Ataques.

9.10. Caso seja implementada no modo em linha, deve permitir a criação de regras de by-pass para casos de falhas de interface.

9.11. Durante a inspeção do tráfego de rede em tempo real, deve ser capaz de identificar anomalias na rede e gerar alertas em casos de tráfego suspeito.

9.12. Deve identificar ameaças direcionadas avançadas e persistentes (APT).

9.13. Deve analisar possíveis fases de um ataque direcionado, identificando tentativas de coletas de informação, movimentação lateral, exfiltração de dados, descoberta de dispositivos e comunicações de comando e controle (C&C).

9.14. Deve identificar e mapear possíveis pontos de entrada na rede que possam ser exploradas por atacantes;

9.15. Deve prover orquestração para bloqueio de ameaças identificadas a partir da inspeção de rede.

9.16. Deve permitir análise de arquivos em sandbox, permitindo identificar ataques avançados (APT), Zero Days, códigos de exploração (exploits) embutidos, vulnerabilidades conhecidas e arquivos maliciosos no tráfego de rede, de forma automática e quando aplicável.

9.17. Quando implantada em linha com a rede da CONTRATANTE, deve possuir a capacidade de analisar tráfego TLS.

9.18. Para fins de dimensionamento, a solução de inspeção de rede e sandbox deve analisar, no mínimo, 4 Gbps, inspecionando e detectando comportamentos maliciosos nos protocolos HTTP, HTTPS, DNS, FTP, SMTP, POP3, SMB, Telnet, RDP, Kerberos, IRC, LDAP, VNC, SQL, MYSQL, WebSocket, ARP entre outros.

9.19. Para fins de dimensionamento, o appliance deverá estar licenciado para possibilitar a análise inline de até 4 Gbps de tráfego, devendo o appliance possuir ao menos 4 interfaces 10Gbps SR

SFP+ (com respectivos tranceivers inclusos) e 4 interfaces UTP RJ45 1Gbps.

9.20. Caso um único hardware não suporte a capacidade especificada, será permitido o agrupamento de até 2 (dois) dispositivos para tal, desde que o console permaneça centralizada na plataforma de detecção e resposta.

9.21. O hardware deve incluir interfaces de gerenciamento 1Gb base-T RJ45 e gerenciamento externo como iDrac Enterprise.

9.22. Deve possuir disco com capacidade mínima de armazenamento de 2TB, em RAID que garanta redundância e performance.

9.23. Não serão aceitos appliances de Unified Threat Management (UTM) e Next-Generation Firewall (NGFW) para monitoramento do tráfego, ainda que possua recurso e licenciamento específico para análise de ameaças em rede.

9.24. Deve ser capaz de analisar protocolos mascarados ou tunelados em ICMP, IP, UDP e TCP.

9.25. Deve fornecer proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos ou equivalentes:

9.25.1. Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança;

9.25.2. Detecção de ataques direcionados e persistentes;

9.25.3. Correlação de regras para detecção ações maliciosas;

9.25.4. Análise de todas as fases de uma sequência de ataques;

9.25.5. Plataforma de integração com outras soluções de segurança;

9.25.6. Analisador virtual de ameaças (sandbox);

9.25.7. Orquestração de bloqueio de ameaças na rede;

9.25.8. Serviço de Monitoração e Análise de Ameaças Digitais em rede;

9.25.9. Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;

9.25.10. Serviço que interpreta a ameaça digital como a representação de um software malicioso ou ação maliciosa tal como: *spyware*, *phishing*, *spear phishing*, *worms*, *bot*, trojan, *adware*, *network exploit*, *web Exploit*, *Cross-site scripting*, *information stealing malware* e outras ações que podem compor ataques a integridade e funcionamento do ambiente;

9.25.11. Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;

9.25.12. Análise e correlação de atividades maliciosas tais como: Detecção específica de *malwares* conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede; Detecção de *worm* advindos da rede e de *e-mail*; Detecção de programas de exploração de vulnerabilidades (Exploits) na rede; Detecção

de empacotamentos maliciosos no tráfego da rede;

9.25.13. Dados estatísticos de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas.

9.26. Permitir a identificação da relevância dos eventos de segurança, apontando a devida criticidade aos alertas gerados.

9.27. Permitir realizar pesquisas customizadas dos alertas de segurança por meio do console de gerenciamento.

9.28. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança.

9.29. Permitir a customização de alertas com base no tipo de incidente de segurança por meio do console de gerenciamento.

9.30. Permitir a integração com sistemas de serviço de diretório.

9.31. Capacidade de verificar em tempo real a reputação de endereços web (URLs) e servidores de correio SMTP.

9.32. A análise de SMTP poderá ser realizada em uma solução separada do sensor de HTTP e demais protocolos.

9.33. Deve possuir mecanismo de conhecimento de senhas para derivação de arquivos protegidos.

9.34. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança.

9.35. Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques.

9.36. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até a camada de aplicação em protocolo TCP/IP.

9.37. Capacidade de detectar ameaças web derivadas de vulnerabilidades e downloads de conteúdo malicioso.

9.38. Deve possuir capacidade de disponibilizar as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura.

9.39. Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos.

9.40. Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças.

9.41. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos executáveis (scripts), PDF´s, executáveis, PPTX, DOCX, XLSX, LNK, ELF, CHM, RTF, ODP, DLLs, JAR, ZIP e RAR.

9.42. Deve detectar ameaças do dia zero, vulnerabilidade, URLs maliciosas e spams dirigidos no protocolo SMTP.

9.43. A solução de análise em sandbox deve possuir a capacidade de analisar, de forma estática e

dinâmica, ameaças com características de auto inicialização ou alteração de arquivos de sistema, rootkits/cloakings, arquivos malformados, engenharia social, dentre outros.

9.44. A análise de sandbox deve identificar e analisar ameaças que tenham características de evitar a segurança e análise em ambiente simulado, autopreservação e roubo de dados.

9.45. Deve possuir recurso de prevenção de ameaças avançadas, com capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK MITRE Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução.

9.46. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho.

9.47. Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações.

9.48. Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança.

9.49. Deve permitir o rastreio por *malwares* utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados).

9.50. Deve analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística.

9.51. Deve possuir tecnologia de proteção contra ameaças desconhecidas, ataques dirigidos e ameaças de dia zero, sendo que este módulo majoritariamente deve pertencer ao mesmo fabricante.

9.52. Deve possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches.

9.53. Deve possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance.

9.54. Deve permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa.

9.55. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em único ponto.

9.56. Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via internet pelo fabricante da solução.

9.57. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução.

9.58. Deve ser capaz de identificar movimentos laterais em uma rede corporativa.

9.59. Deve possuir interface web para busca e investigação local de incidentes.

9.60. Caso a solução seja fornecida on-premises, o sensor deve suportar a análise em sandbox de, pelo menos, arquivos 15 simultaneamente. Caso um único hardware não tenha tal capacidade, é

permitido o empilhamento ou agrupamento.

9.61. Possibilitar a predefinição de políticas para determinar quais tipos de arquivos deverão ser enviados para análise.

9.62. Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web.

9.63. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e escaneamentos de porta.

9.64. Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado.

9.65. Deve possuir regras que identifiquem comunicações peer-to-peer, instant messengers e streaming de mídia.

9.66. Deve possuir capacidade de geração de relatórios consolidados e detalhados com as seguintes informações:

9.66.1. Visão Geral dos Incidentes de Segurança;

9.66.2. Discriminação dos Tipos de Incidentes;

9.66.3. Top Ameaças Analisadas;

9.66.4. Top Hosts Infectados;

9.66.5. Recomendações de Segurança;

9.66.6. Deve possuir detalhes técnicos dos incidentes detectados;

9.66.7. Deve possuir estatística do tráfego analisado;

9.66.8. Deve possuir indicadores de risco do ambiente;

9.66.9. Recomendações de Segurança.

9.67. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e atualizada dinamicamente, hosts com alto nível de risco, classificando os tipos de eventos detectados.

9.68. Deve possuir interface gráfica que apresente em tempo real estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URLs maliciosas acessadas etc..

9.69. Quando detectada uma ameaça, deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada.

9.70. As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação.

9.71. Deve permitir o upgrade e downgrade de versão de firmware.

9.72. O hardware deve possuir discos e fontes redundantes.

9.73. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de

portas comuns e tunelamento de protocolo.

9.74. Deve ser capaz de detectar tentativas de escaneamento de rede.

9.75. Deve ser capaz de detectar propagação de *malwares* na rede.

9.76. Deve ser capaz de detectar tentativas de força bruta em credenciais.

9.77. Deve ser capaz de detectar tentativas de roubo de informação.

9.78. Deve ser capaz de detectar ameaças que se replicam na rede.

9.79. Deve ser capaz de detectar Exploits na rede.

9.80. O Monitoramento de protocolos de comunicação deve ser feito através do hardware que compõe a solução.

9.81. Deve apresentar panorama de detecções de comunicações suspeitas e maliciosas baseado em geolocalização, onde são marcadas origens geográficas de ataques e eventos de segurança monitorados pela solução, por meio de dashboard.

9.82. Deve permitir busca por informações de destino e origem de comunicações, incluindo: endereço IP, endereço MAC, domínio, protocolo e grupo de rede.

9.83. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos.

9.84. Capacidade de salvar uma investigação antes de ser finalizada.

9.85. Capacidade de restaurar uma investigação para continuá-la ou consultá-la.

9.86. Capacidade de gerar relatórios baseados nas investigações.

9.87. Deve permitir apresentação dos dados gerados por meio de tabelas e gráficos.

9.88. Deve trabalhar com geolocalização para identificar a origem geográfica de um ataque.

9.89. Deve enviar alertas via *e-mail*.

9.90. Deve permitir a configuração de alarmes personalizados, com base em investigações.

9.91. A arquitetura da solução deve ser escalável horizontalmente, permitindo que haja um crescimento da arquitetura, sem requerer a troca do hardware em utilização, mas incrementando novas instâncias à topologia, de acordo com o tráfego excedente necessário.

9.92. O console de gerenciamento deve possuir dashboards para facilidade de monitoramento, possibilitando no mínimo:

9.92.1. As janelas poderão ser customizadas pelo administrador em quantidade e período de monitoração;

9.92.2. Deve permitir que, por meio de um único console, o administrador possa configurar as regras de inspeção e detecção, verificar status do sistema e gerar relatórios.

9.93. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização.

9.94. Deve permitir a identificação baseada em localização geográfica quanto a origem de ameaças.

9.95. Deve possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática.

9.96. O console de gerenciamento deve ser gerenciado por Microsoft Edge, Google Chrome ou

Firefox.

9.97. Solução deve possuir mecanismo de busca em seu console de gerenciamento de modo que seja facilitada a busca por detecções.

9.98. Deve permitir a integração com plataforma de detecção e resposta do próprio fabricante, com objetivo de correlacionar as detecções do NDR com as demais tecnologias de segurança implantadas nas camadas de *endpoint*, servidores e *e-mail*.

9.99. A integração com a solução de detecção e resposta deve permitir que as ameaças sejam rastreadas desde a entrada na rede até tentativas de roubo de dados, exibindo etapas gráficas da ação do atacante.

9.100. Deve exibir no formato de tabela, as transações identificadas contendo detalhes do ataque, bem como os Indicadores de Comprometimento (IOCs).

9.101. Deve ser capaz de identificar ameaças evasivas em tempo real atuando com análise profunda e inteligência para identificar e prevenir ataques.

9.102. Deve ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque.

9.103. A solução de inspeção de rede deve possuir a capacidade de integrar-se com a solução de Detecção e Resposta Avançada de Ataques, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente.

9.104. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações:

9.104.1. Uso de CPU;

9.104.2. Uso de Disco;

9.104.3. Uso de Memória;

9.104.4. Tráfego malicioso analisado;

9.104.5. Todo o tráfego analisado.

9.105. Deve possuir integração com ferramentas de SIEM.

9.106. Deve permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deve conter no mínimo:

9.106.1. Deve suportar ao menos a integração com dois servidores syslogs;

9.106.2. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

9.107. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa.

9.108. Deve possuir capacidade de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em trânsito através de logs de sensor.

9.108.1. Deve listar os 10 hosts mais críticos do ambiente da CONTRATANTE, de forma a categorizá-los de acordo com a severidade atual baseada em número e criticidade das detecções, segundo a escala de Crítico, Alto, Médio e Baixo ou escala equivalente.

9.109. Deve correlacionar cada host listado a um alerta de investigação, quando aplicável.

9.110. As detecções de cada host listado deverão ser apresentadas com detalhes para devida investigação.

9.111. Deve apresentar os logs de rede de maneira evidente e destaca por meio de rótulo e cor, a fim de diferenciar dos demais logs de outros sensores.

9.112. Solução deve apresentar relatórios customizados de todas as suas funcionalidades e deve conter no mínimo:

9.112.1. Computadores infectados;

9.112.2. Origem de infecções;

9.112.3. Estatísticas de ameaças;

9.112.4. Riscos potenciais de segurança;

9.112.5. Riscos de perda de informações;

9.112.6. Risco de sistema comprometido;

9.112.7. Risco de disseminação de ameaças;

9.112.8. Infecções de *malware;*

9.112.9. Eventos suspeitos.

9.113. Deve apresentar função de pesquisa por logs contendo no mínimo:

9.114. Critérios de pesquisa por dia, mês e ano.

9.115. Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos.

9.116. Possibilidade de pesquisa por ameaças, URLs maliciosas, análises virtuais, correlação de incidentes, nome de *malware*, protocolo e direção da detecção.

9.117. Os relatórios e logs deverão ser exportados nos formatos PDF, TXT ou CSV.

9.118. Deve compartilhar IOCs detectados com a solução de detecção e resposta por meio da integração nativa.

9.119. A partir da solução de detecção e resposta, os IOCs poderão ser compartilhados com outros sensores do fabricante e ferramentas de terceiros, sendo estas ao menos: MS Active Directory, Microsoft 365 e Fortinet.

10. Proteção Host IPS e Host Firewall

10.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

10.1.1. Microsoft Windows 10 e versões superiores;

10.1.2. Windows Server 2012 e versões superiores.

10.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e

host firewall.

10.3. O módulo deve ser integrado como solução do Endpoint e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.

10.4. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio).

10.5. Deve permitir ativar e desativar o produto sem a necessidade de remoção.

10.6. Deve possuir regras para controle do tráfego de pacotes de determinadas aplicações.

10.7. Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura contra ataques dia zero.

10.8. Deve ser capaz de identificar e bloquear ataques conhecidos através de assinaturas.

10.9. A atualização de assinaturas não deve exigir reinício do sistema operacional.

10.10. Deve efetuar proteção automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host IPS para proteger o endpoint contra a possível exploração da vulnerabilidade.

10.11. Deve prover proteção contra as vulnerabilidades de aplicações terceiras tais como oracle java, abobe pdf reader, adobe flash player, realnetworks real player, Microsoft office, apple itunes, apple quick time, apple safari, google chrome, mozilla firefox, opera browser, ms internet explorer, entre outras.

10.12. Deve fornecer proteção contra vulnerabilidades existentes nas estações de trabalho.

10.13. Deve proteger contra ataques locais iniciados por dispositivos periféricos de armazenamento conectados à estação de trabalho.

10.14. Deve proteger contra ataques que trafegam por fluxos criptografados, para o escopo de servidores.

10.15. Deve proteger contra ataques de negação de serviço.

10.16. Deve proteger contra tentativas de invasão.

10.17. Deve possuir proteção contra BOTs.

10.18. Deve permitir a criação de políticas de firewall diferenciadas em múltiplas placas de rede no mesmo sistema operacional, para o escopo de servidores.

10.19. Deve permitir a criação de políticas de segurança personalizadas.

10.20. Deve possuir capacidade de identificar e bloquear, no mínimo, os seguintes tipos de ataques:

10.20.1. Denial of Service (DOS);

10.20.2. Port scanning;

10.20.3. Network Flooding.

10.21. Deve permitir a emissão de alertas via smtp ou snmp.

10.22. Deve permitir criar regras com base nos seguintes parâmetros:

10.22.1. Descrição;

10.22.2. Ação;

10.22.3. Direção;

10.22.4. Protocolo de Rede;

10.22.5. Aplicação e Executáveis;

10.22.6. Tempo de aplicação da regra.

10.23. Deve possuir integração com o Centro de Inteligência do fabricante para verificar a reputação do endereço IP.

10.24. A reputação deve considerar os níveis: Mínimo, Médio, Alto e Não verificado ou escala equivalente.

10.25. Para evitar consumo de banda, deve manter cache para a consulta mencionada no item anterior.

10.26. Deve permitir a criação de grupos lógicos através de lista de IP, MAC ou portas.

10.27. Deve permitir a criação de contextos para a aplicação para criação de regras de firewall.

10.28. Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez.

10.29. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas.

10.30. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos.

10.31. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação.

11. Controle de aplicações de Endpoints

11.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

11.1.1. Microsoft Windows 10 e versões superiores;

11.1.2. Windows Server 2012 e versões superiores.

11.2. O módulo deve ser integrado como solução do Endpoint e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.

11.3. Deve permitir a criação de políticas de segurança personalizadas.

11.4. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

11.4.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

11.4.2. Range de endereços IPS;

11.4.3. Sistema operacional;

11.4.4. Grupos de máquinas espelhados do Active Directory;

11.4.5. Usuários ou grupos do Active Directory.

11.5. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política.

11.6. As políticas de segurança devem permitir o controle do intervalo de envio dos logs.

11.7. As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política.

11.8. As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deve comunicar-se.

11.9. As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário.

11.10. As políticas de segurança devem permitir o controle através de regras de aplicação.

11.11. As regras de controle de aplicação devem permitir as seguintes ações:

11.11.1. Permissão de execução;

11.11.2. Bloqueio de execução;

11.11.3. Bloqueio de novas instalações.

11.12. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra.

11.13. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

11.13.1. Hash do executável;

11.13.2. Atributos do certificado utilizado para assinatura digital do executável;

11.13.3. Caminho lógico do executável;

11.13.4. Base de assinaturas de certificados digitais válidos e seguros.

11.14. As regras de controle de aplicação devem possuir categorias de aplicações.

11.15. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações.

11.16. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas.

11.17. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos.

11.18. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação.

12. Proteção contra vazamento de informações (DLP) de Endpoints

12.1. Deve ser capaz de realizar a proteção contra vazamento de informações nos seguintes sistemas operacionais:

12.1.1. Microsoft Windows 10 e versões superiores;

12.2. O módulo deve ser integrado como solução do Endpoint e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.

12.2.1. Deve possuir nativamente templates para atender as seguintes regulamentações: PCI/DSS, HIPA, Glba, SB-1386 e US PII.

12.2.2. Deve ser capaz de detectar informações, em documentos nos formatos:

12.2.3. Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html;

12.2.4. Gráficos: visio, postscript, pdf, tiff,

12.2.5. Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;

12.2.6. Códigos: c/c++, java, verilog, autocad.

12.3. Deve ser capaz de detectar informações, com base em:

12.3.1. Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros, através de palavras ou frases exatas, padrão de documentos conhecidos e formato pré-definido de identificação de dados;

12.3.2. Dados não-estruturados, como documentos exportados, reformatados ou sem estrutura de dados definida, através de expressões regulares ou descoberta de dados por aprendizado de padrões e criação de fingerprinting.

12.4. Deve ser capaz de detectar em arquivos compactados.

12.5. Deve permitir a configuração de quantas camadas de compressão serão verificadas.

12.6. Deve permitir a criação de modelos personalizados para identificação de informações.

12.7. Deve permitir a criação de modelos com base em regras e operadores lógicos.

12.8. Deve possuir modelos padrões.

12.9. Deve permitir a importação e exportação de modelos.

12.10. Deve permitir a criação de políticas personalizadas.

12.11. Deve permitir a criação de políticas baseadas em múltiplos modelos.

12.12. Deve permitir mais de uma ação para cada política, como:

12.12.1. Apenas registrar o evento da violação;

12.12.2. Bloquear a transmissão;

12.12.3. Gerar alertar para o usuário;

12.12.4. Gerar alertar na central de gerenciamento;

12.12.5. Capturar informação para uma possível investigação da violação.

12.13. Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede.

12.14. Deve ser capaz de identificar e bloquear informações nos meios de transmissão:

12.14.1. Cliente de *e-mail*;

12.14.2. Protocolos HTTP, HTTPS, FTP;

12.14.3. Mídias removíveis;

12.14.4. Discos óticos CD/DVD;

12.14.5. Gravação CD/DVD;

12.14.6. Aplicações de mensagens instantâneas;

12.14.7. Tecla de print screen;

12.14.8. Aplicações P2P;

12.14.9. Área de transferência do Windows;

12.14.10. Webmail;

12.14.11. Armazenamento em nuvem (cloud);

12.14.12. Impressoras;

12.14.13. Scanners;

12.14.14. Compartilhamentos de arquivos;

12.14.15. Activesync;

12.14.16. Criptografia PGP;

12.14.17. Portas com, lpt, firewire (IEEE 1394);

12.14.18. Modems;

12.14.19. Infravermelho;

12.14.20. Bluetooth.

12.15. Deve permitir a criação de exceções nas restrições dos meios de transmissão.

13. Criptografia de Endpoints

13.1. Deve possuir compatibilidade de instalação nos seguintes sistemas operacionais:

13.1.1. Microsoft Windows 10 e versões superiores.

13.2. O módulo deve ser integrado como solução do Endpoint e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional;

13.3. Deve utilizar, no mínimo, algoritmo AES com chave de 256 bits;

13.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

13.5. Deve verificar a compatibilidade de hardware antes de aplicar a criptografia;

13.6. Deve possuir a capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

13.7. Deve possuir a opção de utilização de TPM para criptografia através do BitLocker;

14. Inventário

14.1. Deve possuir capacidade de atualizar informações sobre hardware presentes nos relatórios após mudanças de hardware nas máquinas gerenciadas;

14.2. Deve possuir capacidade de realizar inventario de software dos endpoints;

14.3. Deve possuir capacidade de suportar pacotes MSI, EXE, BAT, CMD e outros padrões de arquivos executáveis;

14.4. Deve possibilitar a realizar de inventário de todos os dispositivos conectados à rede;

14.5. Deve possibilitar a criação de um inventário centralizado de imagens;

14.6. Deve possuir capacidade de atualizar a lista de pesquisa de forma automática;

14.7. O inventário de hardware deve trazer as seguintes informações:

14.7.1. Fabricante

14.7.2. Mac address

14.7.3. Domínio

14.7.4. Nome do dispositivo

14.7.5. Última vez visto.

14.7.6. Sistema Operacional

14.7.7. Service Pack/Versão do sistema operacional

14.8. O inventário de aplicativos deve trazer as seguintes informações

14.8.1. Nome do aplicativo

14.8.2. Versão

14.8.3. Fabricante

14.8.4. Arquivos executáveis

ANEXO II

CRONOGRAMA DE IMPLANTAÇÃO DOS SERVIÇOS

Prazo Máximo (em dias corridos)	Cronograma de Atividades da Prestação dos Serviços	**Responsável**
D	Emissão da Ordem de Serviço (D)	CONTRATANTE
D + 3	Reunião de planejamento	CONTRATANTE e CONTRATADA
D + 10	Entrega do Plano de Implantação	CONTRATADA
D + 45	Entrega dos *softwares* e equipamentos da solução (E)	CONTRATADA
E + 5	Emissão do **Termo de Recebimento Provisório (TRP1)** da etapa de entrega dos *softwares* e equipamentos da solução.	CONTRATANTE

TRP1 + 15	Instalação e configuração dos *softwares* e equipamentos da solução e entrega das licenças de uso (**I**)	CONTRATADA
I + 5	Emissão o **Termo de Recebimento Provisório (TRP2)** da etapa de instalação e configuração dos *softwares* e equipamentos da solução e entrega das licenças de uso	CONTRATANTE
TRP2 + 10	Emissão o **Termo de Recebimento Definitivo (TRD)** da etapa da entrega, instalação, configuração e licenciamento da solução.	CONTRATANTE
D-TC	Emissão da Ordem de Serviço para o serviço de Transferência de Conhecimento (D-TC)	CONTRATANTE
D-TC + 15	Limite para ínício do serviço de Transferência de Conhecimento	CONTRATADA
D-TC + 45	Limite para o conclusão do serviço de Transferência de Conhecimento	CONTRATADA

ANEXO III

PLANILHA DE COMPOSIÇÃO DE CUSTOS

ITEM	DESCRIÇÃO	QTD	UNIDADE	PREÇO UNITÁRIO	PREÇO TOTAL
1	Proteção para estações de trabalho	580	Dispositivo	R$	R$
2	Proteção para Serviço de *E-mail*	1300	Usuário	R$	R$
3	Proteção para Microsoft 365	550	Usuário	R$	R$
4	Proteção para *Data Center*	60	*Socket*	R$	R$

5	Proteção para *Storage*	2	Servidor	R$	R$
6	Inspeção de Tráfego de Rede (NDR) para 4Gbytes	1	Solução	R$	R$
7	Instalação e Configuração	1	Serviço	R$	R$
8	Suporte Técnico Mensal	36	Meses	R$	R$
9	Repasse de conhecimento para até 5 participantes	1	Turma	R$	R$
TOTAL DA CONTRATAÇÃO:					**R$**

ANEXO IV

TERMO DE CONFIDENCIALIDADE E SIGILO DA CONTRATADA

1 . A empresa [RAZÃO/DENOMINAÇÃO SOCIAL], pessoa jurídica com sede em [ENDEREÇO], inscrita no CNPJ/MF com o n.º [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações sobre o ambiente computacional do Conselho da Justiça Federal – CJF, aceita as regras, condições e obrigações constantes do presente Termo.

2 . O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CJF reveladas à EMPRESA RECEPTORA em função da prestação dos serviços objeto do contrato n.º XX/XXX.

3 . A expressão “informação restrita” abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.

4 . A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do CJF, das informações restritas reveladas.

5 . A EMPRESA RECEPTORA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao CJF, as informações restritas reveladas.

6 . A EMPRESA RECEPTORA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CJF, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

7 . A EMPRESA RECEPTORA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

8. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao CJF qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9 . A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CJF, possibilitará a imediata rescisão de qualquer contrato firmado entre o CJF e a EMPRESA RECEPTORA sem qualquer ônus para o CJF. Nesse caso, a EMPRESA RECEPTORA, estará sujeita, por ação ou omissão, além das multas definidas no Termo de Referência, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CJF, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

10. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CJF.

11 . E, por aceitar todas as condições e as obrigações constantes do presente Termo, a EMPRESA RECEPTORA assina o presente termo através de seus representantes legais.

Brasília, _____ de _____ de 202__.

ASSINATURA DO REPRESENTANTE DA CONTRATADA

_____

CARIMBO E ASSINATURA DO REPRESENTANTE DO CJF

ANEXO V

TERMO DE VISTORIA

Declaro que eu, _____, portador(a) do CPF(MF) nº _____, representante da empresa _____, estabelecida no endereço _____ como seu(sua) representante legal para os fins da presente declaração, tomei conhecimento, com o objetivo de participação no Pregão N._____, de todas as informações necessárias à execução dos serviços licitados e que vistoriei os locais de instalação dos equipamentos e componentes.

Brasília, _____ de _____ de 202___.

_____

ASSINATURA DO RESPONSÁVEL TÉCNICO/ REPRESENTANTE

_____

ASSINATURA DO REPRESENTANTE DO CJF